WM-03-03/Annex A

PL EUDI Wallet Certification System

Cybersecurity Audit Framework for EUDI Wallet providers

VERSION – 1.01

2026.07.21

Document reference	WM-03-03/Annex A Cybersecurity Audit Framework for EUDI Wallet providers
Version	V1.01
Status	FINAL
Date	2026-07-21
Document type	Evaluation Methods and Techniques - General Cybersecurity Audit Framework
Parent framework	WM-03-03
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification scheme	GP-03 eID Certification Scheme
Primary audience	Conformity Assessment Bodies (CABs), Audit Team Leaders, auditors and technical experts
Application	Audits performed as part of the evaluation phase under GP-03
Subsidiary Documents	none

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-910-01	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall support common protocols and interfaces for issuance of person identification data.	Article 5a(5)(a)(i)	WP-03-01	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - enabled protocol profiles, versions and endpoints for issuance of person identification data; - trust anchors, certificates and message-validation rules used for PID issuance; - TLS or cipher-suite restrictions and controls for deprecated or weak configurations where relevant to PID issuance interfaces; - negative-test, conformance-test and error-handling evidence required for unsupported requests to PID issuance interfaces.	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - positive and rejected protocol traces, conformance-test results or interoperability evidence for PID issuance protocols and interfaces; - endpoint, certificate, TLS and trust-anchor configuration for PID issuance interfaces; - logs showing malformed, unsupported, unauthorised or downgrade attempts being rejected on PID issuance interfaces; - evidence that the production configuration matches the documented supported profiles for PID issuance.
REQ-910-02	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall securely onboard the user by using an electronic identification means in accordance with Article 5a (24).	Article 5a(5)(a)(iii)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed Wallet Provider. The review should confirm that the documented process defines: - the accepted proofing paths and accepted electronic-identification-means onboarding paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high; - handling of failed, inconsistent, expired or incomplete evidence or unsuccessful electronic-identification-means onboarding attempts; - traceability from application intake to the final proofing and issuance decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - source checks, electronic-identification-means validation evidence, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing and electronic-identification-means onboarding steps were completed; - records showing how exceptions were escalated, corrected or rejected.
REQ-910-03	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall meet the requirements set out in Article 8 with regard to assurance level high, in	Article 5a(5)(d)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed Wallet Provider. The review should confirm that the documented process defines:	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication.			- the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high under Article 8; - electronic identification means management and authentication arrangements relevant to assurance level high; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision and, where applicable, to eID means management or authentication decisions.	- normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - evidence that electronic identification means management and authentication controls for sampled cases support assurance level high under Article 8; - records showing how exceptions were escalated, corrected or rejected.
REQ-1502-05	Commission Implementing Regulation (EU) 2015/1502	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.	Annex, Section 2.2.2, Level High	WP-03-01	The assessor reviews how the assessed Wallet Provider proves that the eID means or Wallet Unit is activated only under the control of the intended user: - delivery or activation steps linking the user, device, Wallet Unit and activation secret or credential; - checks preventing activation by a different person or on an unauthorised device; - rules for failed activation, lost credentials, device change or support-assisted activation; - evidence retained to prove possession or control at the time of activation.	The assessor tests selected activation cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - activation records linking the user, device, Wallet Unit and activation event; - successful and failed activation attempts, including device-change or recovery cases; - logs or protocol traces showing possession or control checks before activation; - evidence that activation was blocked where possession or control could not be confirmed.
REQ-910-01	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall enable the user, in a manner that is user- friendly, transparent, and traceable by the user, to securely request, obtain, store, delete, share and present, under the sole control of the user, person identification data and	Article 5a(4)(a)	WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting data; - controls ensuring that the function is user-friendly, secure, transparent, traceable and under the sole control of the user; - consent and access rules for provider access to wallet logs or logged information;	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstrations or records showing the user initiating the relevant action in a user-friendly, secure, transparent and traceable manner under the sole control of the user; - exported data or logs and evidence of integrity, authenticity and confidentiality protection;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		electronic attestations of attributes.			- technical limits, critical-asset exceptions and safeguards for secure portability or export.	- consent records where the provider accesses logs for wallet-service purposes; - negative cases where export, deletion, sharing or provider access is blocked for security or lack of consent.
REQ-910-02	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall enable the user to download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations.	Article 5a(4)(f)	WP-03-02	The assessor reviews configuration-management arrangements maintained by the assessed Wallet Provider. The documentation should define: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting, downloading or exporting the user's data, electronic attestations of attributes and configurations; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access to wallet logs or logged information; - technical limits, critical-asset exceptions and safeguards for secure portability or export to the extent technically feasible.	The assessor checks selected system configurations and configuration-change records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstrations or records showing the user initiating the relevant action; - exported or downloaded user data, electronic attestations of attributes and configurations and evidence of integrity, authenticity and confidentiality protection; - consent records where the provider accesses logs for wallet-service purposes; - negative cases where export, download, deletion, sharing or provider access is blocked for security, lack of consent or documented technical infeasibility.
REQ-910-03	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall enable the user to exercise the user's rights to data portability.	Article 5a(4)(g)	WP-03-02	The assessor reviews user-control, export and logging functions implemented by the assessed Wallet Provider: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting data; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access to wallet logs or logged information; - technical limits, critical-asset exceptions and safeguards for secure portability or export.	The assessor tests selected user-control, export and log-access scenarios for the assessed Wallet Provider during the on-site Stage 2 assessment: - demonstrations or records showing the user initiating the relevant action; - exported data or logs and evidence of integrity, authenticity and confidentiality protection; - consent records where the provider accesses logs for wallet-service purposes; - negative cases where export, deletion, sharing or provider access is blocked for security or lack of consent.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-910-04	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall support common protocols and interfaces for issuance of person identification data.	Article 5a(5)(a)(i)	WP-03-02	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - enabled protocol profiles, versions and endpoints for issuance of person identification data; - trust anchors, certificates and message-validation rules; - TLS or cipher-suite restrictions and controls for deprecated or weak configurations; - negative-test, conformance-test and error-handling evidence required for unsupported requests.	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - positive and rejected protocol traces, conformance-test results or interoperability evidence for PID issuance; - endpoint, certificate, TLS and trust-anchor configuration; - logs showing malformed, unsupported, unauthorised or downgrade attempts being rejected; - evidence that the production configuration matches the documented supported profiles.
REQ-910-05	Regulation (EU) No 910/2014 as amended / eIDAS	Wallet Provider shall provide Mechanisms that allow verification of the authenticity and validity of European Digital Identity Wallets. 5a(8)(a		WP-03-02	The assessor reviews mechanisms provided by the assessed Wallet Provider for verifying authenticity and validity of Wallets or Wallet Units: - which authenticity and validity checks are exposed to relying parties, PID Providers or other relying components; - trust anchors, attestation status, revocation status and response format used by the mechanism; - privacy and anti-enumeration controls around validity checking; - availability, monitoring and evidence retained for successful and failed verification requests.	The assessor tests selected authenticity and validity verification cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - successful checks for valid Wallet Units and attestations; - rejected checks for revoked, expired, malformed or unsupported Wallet evidence; - protocol traces or API responses showing status, trust-chain and privacy controls; - logs and monitoring evidence for the verification mechanism.
REQ-910-06	Regulation (EU) No 910/2014 as amended / eIDAS	The validity of the European Digital Identity Wallet shall be revocable upon explicit user request, where the Wallet security has been compromised, or upon death of the user /		WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - criteria covering health or safety impact, unauthorised access, operational disruption, data compromise, vulnerable users, certification impact and financial loss where applicable;	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - incident records mapped to each applicable breach criterion; - records for explicit user request, Wallet security compromise, death of the user or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		cessation of activity of the legal person. Art. 5a(9)			- triggers for revocation of Wallet validity, including explicit user request, compromised Wallet security, death of the user or cessation of activity of the legal person; - thresholds, data sources and decision rules for classifying an event as a reportable breach or compromise or as a Wallet-validity revocation trigger; - roles responsible for assessment, notification and remedy decisions; - links to incident response, availability measurement, WUA revocation and user or CAB notification.	cessation of activity of the legal person, where applicable; - evidence supporting the decision that thresholds were or were not met; - notifications to users, CAB, supervisory bodies or other parties where required; - remedy decisions such as suspension, withdrawal, revocation of Wallet validity or service restrictions.
REQ-910-07	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.	Art. 5a(11)	WP-03-02	The assessor reviews how the assessed Wallet Provider demonstrates that the Wallet is provided under an eID scheme at assurance level high: - scheme evidence identifying the assurance level and scope applicable to the Wallet; - mapping between assurance level high requirements and Wallet provisioning, lifecycle and authentication controls; - dependencies on PID Provider, eID scheme governance and certification evidence; - change controls preventing the Wallet from operating outside the approved assurance-level scope.	The assessor checks selected assurance-level evidence for the assessed Wallet Provider during the on-site Stage 2 assessment: - scheme documentation, certification evidence and control mapping for assurance level high; - sampled Wallet Unit activation, authentication or lifecycle cases linked to high-assurance controls; - evidence that changes to scheme, provider or technical scope were assessed before release; - cases where lower-assurance or out-of-scope paths were blocked or segregated.
REQ-910-08	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall ensure security by design.	Art. 5a(11)	WP-03-02	The assessor reviews how the assessed Wallet Provider embeds security-by-design controls into Wallet design and lifecycle decisions: - security requirements captured before architecture, development or release decisions; - threat modelling, misuse cases or design reviews for Wallet components and interfaces; - approval gates requiring security evidence before implementation or deployment;	The assessor checks selected design and release evidence for the assessed Wallet Provider during the on-site Stage 2 assessment: - architecture, threat-model or design-review artefacts for sampled Wallet components; - security requirements linked to development, testing and release records; - findings from design reviews and how they were remediated or accepted;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- traceability from design risks to implemented controls and testing evidence.	- evidence that significant design changes triggered renewed security review.
REQ-910-09	Regulation (EU) No 910/2014 as amended / eIDAS	Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider. If the European Digital Identity Wallet is	Article 5a(14)	WP-03-02	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - controls ensuring that users have full control of the use of and of the data in their Wallet; - data flows, stores and interfaces separating wallet or PID data from other provider services; - purpose limitation, minimisation and non-combination controls, including controls preventing collection of information about Wallet use that is not necessary for Wallet service provision; - controls preventing combination of PID or other personal data stored in or relating to the Wallet with data from other provider or third-party services, unless the user has expressly requested otherwise; - technical controls preventing tracking, linkability or unauthorised observation of user activity; - logical separation of personal data relating to Wallet provision from other provider-held data and functional separation from other services where the Wallet is provided by private parties.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - architecture diagrams, database or tenant separation evidence and access-control configuration; - user journeys or records demonstrating full user control of Wallet use and Wallet data; - sampled logs or data-flow evidence showing that cross-service combination or tracking is not occurring; - evidence that information about Wallet use is collected only where necessary for Wallet service provision; - privacy-relevant configuration for dashboards, transaction logs, analytics and relying-party interactions; - evidence of logical separation of Wallet-service personal data and, for private-party Wallet Providers, functional separation from other services.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		provided by private parties, the provisions of Article 45h(3) shall apply mutatis mutandis, requiring functional separation from other services.				
REQ-910-10	Regulation (EU) No 910/2014 as amended / eIDAS	Where a Wallet, validation mechanism or underlying eID scheme is breached or compromised in a way affecting reliability, provision and use of affected Wallets shall be suspended, and where justified or not remedied, withdrawn and revoked.	Article 5e	WP-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed Wallet Provider. The documented controls should define: - criteria covering breach or compromise of a Wallet, validation mechanism or underlying eID scheme in a way affecting reliability, health or safety impact, unauthorised access, operational disruption, data compromise, vulnerable users, certification impact and financial loss where applicable; - thresholds, data sources and decision rules for classifying an event as a reportable breach or compromise; - roles responsible for assessment, notification and remedy decisions; - links to incident response, availability measurement, WUA revocation and user or CAB notification; - rules requiring suspension of provision and use of affected Wallets and, where justified or not remedied, withdrawal and revocation.	The assessor tests selected revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - incident records mapped to each applicable breach criterion, including breaches or compromises of the Wallet, validation mechanism or underlying eID scheme affecting reliability; - evidence supporting the decision that thresholds were or were not met; - notifications to users, CAB, supervisory bodies or other parties where required; - remedy decisions such as suspension of provision and use of affected Wallets and, where justified or not remedied, withdrawal and revocation or service restrictions.
REQ-2979-01	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall, for each wallet unit, sign or seal at least one wallet unit attestation compliant with the requirements laid down in Article 6. The certificate used to sign or seal the wallet unit attestation shall be issued under a	Article 3(2)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including that at least one Wallet Unit Attestation compliant with Article 6 is signed or sealed for each Wallet Unit; - certificate and trust-list requirements used	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including evidence that each sampled Wallet Unit contains at least one Article 6-compliant attestation;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		certificate listed in the trusted list.			for attestation signing or sealing, including that the certificate used is issued under a certificate listed in the trusted list; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	- certificate chain, trust-list and validity-status evidence for the signing or sealing certificate, including evidence that it is issued under a certificate listed in the trusted list; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
REQ-2979-02	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure integrity, authenticity and confidentiality of the communication between wallet instances and wallet secure cryptographic applications.	Article 4(2)	WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - key types, algorithms, trusted components and protected environments used for the assessed function; - communication mechanisms between wallet instances and wallet secure cryptographic applications, including controls for integrity, authenticity and confidentiality; - key generation, storage, access, backup, rotation, revocation and destruction rules; - use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - segregation of duties and logging for sensitive key-management and communication-security operations.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - key-management records for generation, activation, use, rotation or destruction; - protocol traces, configuration or attestation evidence showing integrity, authenticity and confidentiality of communication between wallet instances and wallet secure cryptographic applications; - configuration or attestation evidence for protected key storage and cryptographic modules; - access logs and approvals for sensitive key-management actions; - negative or exception cases such as expired certificates, failed rotations, rejected keys or rejected unauthenticated or unprotected communication.
REQ-2979-03	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure that each wallet unit contains wallet unit attestations.	Article 6(1)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records;	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- controls ensuring that each Wallet Unit contains the required Wallet Unit Attestations; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	- evidence that each sampled Wallet Unit contains the required Wallet Unit Attestations; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
REQ-2979-04	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure that the wallet unit attestations contain public keys and that the corresponding private keys are protected by a wallet secure cryptographic device.	Article 6(2)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - Wallet Unit Attestation content confirming that attestations contain public keys; - WSCD/WSCA use and evidence of protected key generation, storage and operation, including protection by a Wallet Secure Cryptographic Device of the private keys corresponding to the public keys contained in Wallet Unit Attestations; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - Wallet Unit Attestation samples showing contained public keys and evidence that the corresponding private keys are protected by a Wallet Secure Cryptographic Device; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-2979-05	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall inform wallet users of their rights and obligations in relation to their wallet unit.	Article 6(3)(a)	WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - the exact user-facing content, including rights and obligations in relation to the Wallet Unit, terms, conditions, fees, limitations or recommended precautions relevant to the	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - screens, messages, portal pages or API responses used to present the required information, including wallet users' rights and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					requirement; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it; - version control, approval and language or accessibility handling for the information; - case-level evidence showing which version was presented to the user at the time of onboarding, activation or issuance.	obligations in relation to their Wallet Unit; - sampled user records showing acknowledgement, delivery or acceptance where required; - version history confirming that the correct information applied at the time of the sampled case; - negative or incomplete journeys showing that the process does not continue before the required information is presented.
REQ-2979-06	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall provide mechanisms, independent of wallet units, for the secure identification and authentication of wallet users.	Article 6(3)(b)	WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - user-identification and authentication mechanisms available independently of the Wallet Unit; - security controls protecting those mechanisms against impersonation, replay, credential misuse and unauthorised access; - conditions under which the independent mechanisms are used, including Wallet Unit loss, replacement, revocation requests or account recovery; - registration, lifecycle, recovery and deactivation rules for wallet-user authentication credentials; - logging and evidence retained for successful, failed and exceptional authentication attempts.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstrations or records showing wallet-user identification and authentication without relying on the Wallet Unit; - successful and failed authentication cases, including recovery or Wallet Unit loss/replacement scenarios where applicable; - configuration evidence for authentication strength, credential lifecycle and access protection; - logs showing rejection of unauthorised, replayed or otherwise invalid authentication attempts; - evidence that operational procedures match the approved independent-authentication design.
REQ-2979-07	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure wallet users have the right to request revocation of their wallet unit attestations, using the authentication mechanisms	Article 6(3)(c)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including the wallet user's right to	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		referred to in Article 6(3)(b).			request revocation of their Wallet Unit Attestations; - authentication mechanisms referred to in Article 6(3)(b) used to authenticate the wallet user when submitting a revocation request; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	- wallet-user requests for revocation of Wallet Unit Attestations and evidence that the requester was authenticated using the mechanisms referred to in Article 6(3)(b); - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - revoked or rejected user-request cases and evidence that the defined revocation process was followed; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details.
REQ-2979-08	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall be the only entities capable of revoking wallet unit attestations for wallet units that they have provided.	Article 7(1)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - controls ensuring that only the Wallet Provider can revoke Wallet Unit Attestations for Wallet Units that it has provided; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - evidence that revocation capability is restricted to the Wallet Provider for Wallet Unit Attestations of Wallet Units it has provided; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - rejected cases where an unauthorised entity or another provider attempted to revoke a Wallet Unit Attestation.
REQ-2979-09	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall establish a publicly available policy specifying the conditions and the timeframe for the	Article 7(2)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		revocation of wallet unit attestations.			records; - a publicly available policy specifying the conditions and timeframe for revocation of Wallet Unit Attestations; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - controls ensuring that revocation decisions and timeframes applied in operations are consistent with the public policy; - rules excluding personal data from attestations where the requirement prohibits such data.	signature or seal validation evidence; - publicly available policy specifying revocation conditions and timeframe for Wallet Unit Attestations; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - revoked or invalid attestation cases and evidence that revocation timing and conditions followed the publicly available policy; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details.
REQ-2979-10	Commission Implementing Regulation (EU) 2024/2979	Where wallet providers have revoked wallet unit attestations, they shall inform affected wallet users within 24 hours of the revocation, including the reason for the revocation and the consequences for the wallet user, in a manner that is concise, easily accessible and using clear and plain language.	Article 7(3)	WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - triggers and deadlines for informing affected wallet users within 24 hours after Wallet Unit Attestation revocation; - required notification content, including the reason for revocation and the consequences for the wallet user; - message templates and delivery channels ensuring that the information is concise, easily accessible and written in clear and plain language; - certificate and trust-list requirements used for attestation signing or sealing; - records proving notification delivery, failure handling and escalation.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - timestamps from Wallet Unit Attestation revocation to notification of affected wallet users, confirming notification within 24 hours; - notification content showing the reason for revocation and the consequences for the wallet user; - evidence that the notification was concise, easily accessible and written in clear and plain language; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2979-11	Commission Implementing Regulation (EU) 2024/2979	Where wallet providers have revoked wallet unit attestations, they shall make publicly available the validity status of the wallet unit attestation in a privacy preserving manner and describe the location of that information in the wallet unit attestation.	Article 7(4)	WP-03-02	The assessor reviews privacy-preserving validity-status publication controls maintained by the assessed Wallet Provider: - location and format of PID or Wallet Unit Attestation status information; - privacy controls preventing status checks from becoming tracking or correlation mechanisms; - how the status-location reference is included in the PID or attestation where required; - availability, integrity and update rules for the status service.	The assessor checks selected validity-status publication cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - issued and revoked PID or attestation samples with status-location references; - status-service responses for valid, suspended, revoked or unknown items; - privacy tests or configuration evidence limiting correlation and enumeration; - logs and monitoring evidence for status-service updates and availability.
REQ-2979-12	Commission Implementing Regulation (EU) 2024/2979	The logs shall be accessible to the wallet provider, where it is necessary for the provision of wallet services, on the basis of explicit prior consent by the wallet user.	Article 9(5)	WP-03-02	The assessor reviews wallet log access and protection controls implemented by the assessed Wallet Provider: - conditions under which the provider may access wallet logs for service provision; - explicit prior-consent mechanism and withdrawal or refusal handling; - integrity, authenticity and confidentiality controls for logged information; - user export and access paths for logs where applicable.	The assessor tests selected wallet-log access and protection cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - consent records linked to provider log access; - samples of logged information and integrity or confidentiality protection evidence; - provider access attempts without consent and related rejection evidence; - user export or access cases and the resulting log package.
REQ-2979-13	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure integrity, authenticity and confidentiality of the logged information.	Article 9(3)	WP-03-02	The assessor reviews wallet log access and protection controls implemented by the assessed Wallet Provider: - conditions under which the provider may access wallet logs for service provision; - explicit prior-consent mechanism and withdrawal or refusal handling; - integrity, authenticity and confidentiality controls for logged information; - user export and access paths for logs where applicable.	The assessor tests selected wallet-log access and protection cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - consent records linked to provider log access; - samples of logged information and integrity or confidentiality protection evidence; - provider access attempts without consent and related rejection evidence; - user export or access cases and the resulting log package.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2979-14	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall enable wallet users to export the logged information.	Article 9(7)	WP-03-02	The assessor reviews wallet log access and protection controls implemented by the assessed Wallet Provider: - conditions under which the provider may access wallet logs for service provision; - explicit prior-consent mechanism and withdrawal or refusal handling; - integrity, authenticity and confidentiality controls for logged information; - user export and access paths for logs where applicable.	The assessor tests selected wallet-log access and protection cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - consent records linked to provider log access; - samples of logged information and integrity or confidentiality protection evidence; - provider access attempts without consent and related rejection evidence; - user export or access cases and the resulting log package.
REQ-2979-15	Commission Implementing Regulation (EU) 2024/2979	Wallet units shall, where technically feasible and excepting cases of critical assets, support secure export and portability of personal data of the wallet user, to allow the wallet user to migrate to a wallet unit of a different wallet solution in a way that ensures level of assurance high.	Article 13	WP-03-02	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting personal data of the wallet user; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access to wallet logs or logged information; - technical limits, critical-asset exceptions and safeguards for secure portability or export to allow migration to a Wallet Unit of a different wallet solution in a way that ensures assurance level high, where technically feasible.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstrations or records showing the user initiating the relevant action; - exported personal data or logs and evidence that secure export or portability supports migration to a Wallet Unit of a different wallet solution while ensuring assurance level high; - consent records where the provider accesses logs for wallet-service purposes; - negative cases where export, deletion, sharing or provider access is blocked for security, lack of consent, technical infeasibility or critical-asset exception.
REQ-2981-01	Commission Implementing Regulation (EU) 2024/2981	Wallet Providers shall complement the scheme risk assessment with implementation-specific risks and treatment measures.	Article 4(4)d	WP-03-02	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider. The review should link the requirement to: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes;	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled implementation-specific risks from the register linked to assets, processes and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- identification of implementation-specific threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - traceability showing how implementation-specific risks and treatment measures complement the scheme risk assessment; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	treatment actions; - evidence that implementation-specific risks and treatment measures complement the scheme risk assessment; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2981-02	Commission Implementing Regulation (EU) 2024/2981	Wallet providers shall establish, maintain and operate vulnerability management policies and procedures, including disclosure and registration of publicly known and remediated vulnerabilities.	Article 5	WP-03-02	The assessor reviews vulnerability-management arrangements maintained by the assessed Wallet Provider: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	The assessor checks selected vulnerability records for the assessed Wallet Provider during the on-site Stage 2 assessment: - intake, triage and impact-analysis evidence; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records.
REQ-2981-03	Commission Implementing Regulation (EU) 2024/2981	Wallet providers shall establish and implement policies and procedures for risk management, change management, vulnerability management and personnel management relevant to operation of the Wallet Solution.	Article 8(3)b	WP-03-02	The assessor reviews vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider. The review should identify: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - change-management rules for assessing, approving, testing, releasing and rolling back Wallet Solution changes;	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - sampled Wallet Solution changes showing assessment, approval, testing, release and rollback evidence where applicable; - sampled vulnerability records showing intake, impact analysis, remediation, registration or disclosure and closure; - personnel-management evidence for

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- vulnerability-management rules for intake, impact analysis, remediation, registration or disclosure and closure; - personnel-management rules for responsibilities, competence, training, access lifecycle and operational role changes relevant to Wallet Solution operation.	operational roles, competence, training, access lifecycle and role changes; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture.
REQ-1502-01	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure the wallet user is aware of the terms and conditions related to the use of the electronic identification means.	Annex, Section 2.1.1, All levels, Element 1	WP-03-02	The assessor reviews how the assessed Wallet Provider presents mandatory user information before the user commits to the relevant PID, Wallet Unit or eID means process: - the exact user-facing content, including terms, conditions, obligations, fees, limitations or recommended precautions relevant to the requirement; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it; - version control, approval and language or accessibility handling for the information; - case-level evidence showing which version was presented to the user at the time of onboarding, activation or issuance.	The assessor checks selected user journeys and records for the assessed Wallet Provider during the on-site Stage 2 assessment: - screens, messages, portal pages or API responses used to present the required information; - sampled user records showing acknowledgement, delivery or acceptance where required; - version history confirming that the correct information applied at the time of the sampled case; - negative or incomplete journeys showing that the process does not continue before the required information is presented.
REQ-1502-02	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure the wallet user is aware of recommended security precautions related to the electronic identification means.	Annex, Section 2.1.1, All levels, Element 2	WP-03-02	The assessor reviews how the assessed Wallet Provider presents mandatory user information before the user commits to the relevant PID, Wallet Unit or eID means process: - the exact user-facing content, including terms, conditions, obligations, fees, limitations or recommended precautions relevant to the requirement; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it;	The assessor checks selected user journeys and records for the assessed Wallet Provider during the on-site Stage 2 assessment: - screens, messages, portal pages or API responses used to present the required information; - sampled user records showing acknowledgement, delivery or acceptance where required; - version history confirming that the correct information applied at the time of the sampled case; - negative or incomplete journeys showing

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- version control, approval and language or accessibility handling for the information; - case-level evidence showing which version was presented to the user at the time of onboarding, activation or issuance.	that the process does not continue before the required information is presented.
REQ-1502-03	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure that the electronic identification means utilises at least two authentication factors from different categories.	Annex, Section 2.2.1, Level Substantial, Element 1	WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including evidence that the electronic identification means utilises at least two authentication factors from different categories; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, showing at least two authentication factors from different categories for the electronic identification means; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
REQ-1502-04	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure that the electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.	Annex, Section 2.2.1, Level Substantial, Element 2	WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - delivery or activation steps linking the user, device, Wallet Unit and activation secret or credential; - design and use controls supporting the assumption that the eID means can be used only if under the control or possession of the person to whom it belongs; - checks preventing activation by a different person or on an unauthorised device; - rules for failed activation, lost credentials, device change or support-assisted activation; - evidence retained to prove possession or	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - activation records linking the user, device, Wallet Unit and activation event; - evidence that the eID means is designed so that it can be assumed to be used only under the control or possession of the person to whom it belongs; - successful and failed activation attempts, including device-change or recovery cases; - logs or protocol traces showing possession or control checks before activation or use where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					control at the time of activation and use where applicable.	- evidence that activation or use was blocked where possession or control could not be confirmed.
REQ-1502-05	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure that the activation process includes mechanisms verifying that e electronic identification means has been delivered only into the possession of the person to whom it belongs.		WP-03-02	The assessor reviews how the assessed Wallet Provider proves that the eID means or Wallet Unit is activated only under the control of the intended user: - delivery or activation steps linking the user, device, Wallet Unit and activation secret or credential; - checks preventing activation by a different person or on an unauthorised device; - rules for failed activation, lost credentials, device change or support-assisted activation; - evidence retained to prove possession or control at the time of activation.	The assessor tests selected activation cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - activation records linking the user, device, Wallet Unit and activation event; - successful and failed activation attempts, including device-change or recovery cases; - logs or protocol traces showing possession or control checks before activation; - evidence that activation was blocked where possession or control could not be confirmed.
REQ-1502-06	Commission Implementing Regulation (EU) 2015/1502	The Wallet Provider shall ensure mechanisms for suspending or revoking an electronic identification means in a timely and effective manner.	Annex, Section 2.2.3, All levels, Element 1	WP-03-02	The assessor reviews lifecycle controls used by the assessed Wallet Provider for suspension, revocation, reactivation, renewal or replacement: - authorised triggers, decision roles and evidence required for each lifecycle action; - timeliness requirements and technical propagation of status changes; - controls preventing unauthorised suspension, revocation, reactivation or renewal; - assurance checks required before reactivation, renewal or replacement is allowed.	The assessor tests selected lifecycle-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-1502-07	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall implement measures thatprevent unauthorised suspension, revocation and/or reactivation.	Annex, Section 2.2.3, All levels, Element 2	WP-03-02	The assessor reviews lifecycle controls used by the assessed Wallet Provider for suspension, revocation, reactivation, renewal or replacement: - authorised triggers, decision roles and evidence required for each lifecycle action; - timeliness requirements and technical propagation of status changes;	The assessor tests selected lifecycle-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- controls preventing unauthorised suspension, revocation, reactivation or renewal; - assurance checks required before reactivation, renewal or replacement is allowed.	- technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-1502-08	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall implement mechanisms for reactivation only if the same assurance requirements as established before the suspension or revocation continue to be met.	Annex, Section 2.2.3, All levels, Element 3	WP-03-02	The assessor reviews lifecycle controls used by the assessed Wallet Provider for suspension, revocation, reactivation, renewal or replacement: - authorised triggers, decision roles and evidence required for each lifecycle action; - timeliness requirements and technical propagation of status changes; - controls preventing unauthorised suspension, revocation, reactivation or renewal; - assurance checks required before reactivation, renewal or replacement is allowed.	The assessor tests selected lifecycle-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-1502-09	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall ensure that where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including offline analysis. 3Wallet Provider shall implement security controls to the authentication mechanisms and verification , so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls securing person identification data stored as part of the authentication mechanism against loss and compromise, including offline analysis; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, guessing, eavesdropping, replay or	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - evidence that person identification data stored as part of the authentication mechanism is protected against loss and compromise, including offline analysis; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential, including guessing, eavesdropping, replay or manipulation of communication, where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		communication by an attacker with hig attack potential can subvert the authentication mechanisms.			manipulation by attackers with high attack potential.	- migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
WPP-00	CEN/TS 18098-4 6.1.1, 6.1.2	The Wallet Provider shall request from the User the evidence required to determine User eligibility for Wallet Unit provisioning. The Wallet Provider shall document the eligibility evidence accepted and the decision criteria applied. Where a User Account is created or used for Wallet Unit provisioning or lifecycle management, the Wallet Provider shall ensure that the authentication mechanism used by the Wallet User to access the User Account is commensurate with assurance level high. The authentication mechanism shall be documented and justified by a risk assessment.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - evidence requested from the User to determine eligibility for Wallet Unit provisioning; - documented eligibility evidence accepted and decision criteria applied; - authentication factors, transaction binding and user-consent or intent confirmation where relevant; - where a User Account is created or used for Wallet Unit provisioning or lifecycle management, evidence that the authentication mechanism is commensurate with assurance level high and documented and justified by a risk assessment; - controls protecting authentication secrets, credentials and Wallet Unit keys; - rules for failed attempts, lockout, recovery and factor replacement.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - records showing eligibility evidence requested from the User, accepted evidence and decision criteria applied; - successful and failed authentication transactions, including relying-party interactions where relevant; - configuration enforcing User Account authentication commensurate with assurance level high where the User Account is used for provisioning or lifecycle management; - risk-assessment evidence justifying the User Account authentication mechanism; - configuration enforcing the required factors, lockout rules and recovery controls; - logs linking the Wallet Unit, user action and authentication outcome.
WPP-01	CEN TS 18098-4: REQ-6.2.1	The Wallet Provider shall make the Wallet Unit software application available to the user to enable the download and initiation of the local installation sequence.		WP-03-02	The assessor reviews how the assessed Wallet Provider makes the Wallet Unit application available for trusted download and initiation: - approved distribution channels and package integrity controls; - versioning and compatibility checks before initiation; - user journey from download to first launch;	The assessor tests selected Wallet application download and initiation cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - download source, application version and signature or checksum evidence; - successful and failed initiation records; - rejection of unsupported, outdated or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- records proving which application version was made available and installed.	tampered packages; - traceability from installation to the subsequent activation sequence.
WPP-01a	Reg. 910/2014 Art. 5a	Wallet Unit activation shall support secure onboarding interfaces required for eID-based onboarding under the electronic identification scheme. Where the identity proofing or authentication part is performed under WP-03-01 or WP-03- 03, the Wallet Provider shall ensure that the Wallet Unit activation process exposes the required technical interfaces and preserves the security properties required for assurance level high.		WP-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed Wallet Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path; - technical interfaces required for eID-based onboarding under the electronic identification scheme and how they are exposed by the Wallet Unit activation process; - evidence sources, verification checks and manual-review steps supporting assurance level high; - interfaces and security controls used where the identity proofing or authentication part is performed under WP-03-01 or WP-03-03; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - technical evidence that the Wallet Unit activation process exposes the secure onboarding interfaces required for eID-based onboarding under the electronic identification scheme; - source checks, operator decisions, timestamps and final assurance-level decisions; - cases where proofing or authentication is performed under WP-03-01 or WP-03-03, showing interface use and preservation of assurance level high security properties; - evidence that issuance or activation occurred only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
WPP-02	CEN TS 18098-4: REQ-6.3.2.2.2.1; REQ-6.3.2.2.2.2	Upon the downloading and launching of the installation sequence by the user, the Wallet Provider shall perform a technical verification of the user's device. This verification shall check whether the device meets the mandatory hardware capabilities, security		WP-03-02	The assessor reviews device and application verification controls applied by the assessed Wallet Provider before Wallet Unit activation continues: - mandatory hardware capabilities, security features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - application genuineness and binding checks	The assessor checks selected device and application verification cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - successful verification records for supported devices and application versions; - failed device-capability, integrity, rooting, jailbreaking or tampering cases; - logs showing immediate termination of activation after failed checks; - user notifications explaining the failure and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		features, and deployment policies necessary for the operation of the Wallet Unit.			proving that the Wallet client runs on the verified device; - termination and user-notification rules when device, integrity or application checks fail.	evidence that no Wallet Unit was activated after rejection.
WPP-02a	CEN TS 18098-4: REQ-6.3.2.2.2 REQ-6.3.2.2.3; REQ-6.3.2.2.4	Where the device fails to meet the technical requirements evaluated under WPP- 02, the Wallet Provider shall immediately terminate the activation process and notify the user of the device's failure to meet the required technical and eligibility criteria.		WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - mandatory hardware capabilities, security features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - application genuineness and binding checks proving that the Wallet client runs on the verified device; - termination and user-notification rules when device, integrity or application checks fail, including immediate termination of activation and notification that the device failed to meet the required technical and eligibility criteria.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - successful verification records for supported devices and application versions; - failed device-capability, integrity, rooting, jailbreaking or tampering cases; - logs showing immediate termination of activation after failed checks; - user notifications explaining that the device failed to meet the required technical and eligibility criteria and evidence that no Wallet Unit was activated after rejection.
WPP-03	CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.2	Where the user's device is successfully verified, the Wallet Provider shall execute a mandatory device integrity check. This check shall confirm that the host operating system and system security structures have not been modified or compromised through mechanisms such as rooting or jailbreaking.		WP-03-02	The assessor reviews device and application verification controls applied by the assessed Wallet Provider before Wallet Unit activation continues: - mandatory hardware capabilities, security features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - application genuineness and binding checks proving that the Wallet client runs on the verified device; - termination and user-notification rules	The assessor checks selected device and application verification cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - successful verification records for supported devices and application versions; - failed device-capability, integrity, rooting, jailbreaking or tampering cases; - logs showing immediate termination of activation after failed checks; - user notifications explaining the failure and evidence that no Wallet Unit was activated after rejection.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					when device, integrity or application checks fail.	
WPP-03a	CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.3	Where the device integrity verification under WPP-03 fails, the Wallet Provider shall immediately terminate the activation process and notify the user of the reason(s) why the device integrity checks failed based on the specification of the Wallet Solution.		WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - mandatory hardware capabilities, security features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - application genuineness and binding checks proving that the Wallet client runs on the verified device; - termination and user-notification rules when device, integrity or application checks fail, including immediate termination and notification of the reason(s) why device integrity checks failed based on the Wallet Solution specification.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - successful verification records for supported devices and application versions; - failed device-capability, integrity, rooting, jailbreaking or tampering cases; - logs showing immediate termination of activation after failed checks; - user notifications explaining the reason(s) why device integrity checks failed based on the Wallet Solution specification and evidence that no Wallet Unit was activated after rejection.
WPP-04	CEN TS 18098-4: REQ-6.3.5.1	Once the device's integrity has been successfully verified, the Wallet Unit shall allow the user to select and configure the authentication factors used to protect the wallet. Supported methods include PINs, passwords, or device-supported biometrics.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including PINs, passwords and device-supported biometrics where supported; - rules allowing the user, after successful device integrity verification, to select and configure the authentication factors used to protect the Wallet; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - successful user selection and configuration of Wallet-protection factors after successful device integrity verification, including PIN, password or device-supported biometric methods where supported; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					where required; - reset, recovery, fallback and failure handling for each factor type.	- negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
WPP-05	CEN TS 18098-4: REQ-6.3.3.1	The Wallet Provider shall execute a cryptographic verification to validate the binding of the client application to the user's. This verification shall confirm that the application executes genuinely on the verified device, is not malicious, and has not been tampered with.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - mandatory hardware capabilities, security features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - cryptographic verification of the binding of the client application to the verified user device, including application genuineness and binding checks proving that the Wallet client runs on the verified device, is not malicious and has not been tampered with; - termination and user-notification rules when device, integrity or application checks fail.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - successful verification records for supported devices and application versions; - cryptographic application-binding evidence showing that the Wallet client executes genuinely on the verified device, is not malicious and has not been tampered with; - failed device-capability, integrity, rooting, jailbreaking, tampering or application-binding cases; - logs showing immediate termination of activation after failed checks; - user notifications explaining the failure and evidence that no Wallet Unit was activated after rejection.
WPP-06	CEN TS 18098-4: REQ-6.3.5.1	Upon successful verification of the application binding, the Wallet Provider shall establish a formal cryptographic relationship linking the User, the user's device, and the Wallet Unit.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - prerequisites requiring successful application-binding verification before the relationship is established; - cryptographic mechanism used to link the User, the user's device and the Wallet Unit; - binding material, identifiers, keys or attestations used to evidence the relationship; - controls preventing establishment of the relationship with a substituted user, device, application or Wallet Unit; - evidence retained for successful, failed or	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - records showing successful application-binding verification before relationship establishment; - cryptographic evidence linking the User, the user's device and the Wallet Unit; - keys, identifiers, attestations or protocol traces used to establish and verify the relationship; - rejected cases involving substituted, unverified or inconsistent user, device, application or Wallet Unit evidence;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					repeated cryptographic relationship establishment attempts.	- traceability from relationship establishment to the subsequent Wallet Unit activation sequence.
WPP-07	CEN TS 18098-4: REQ-6.4.2	Following the establishment of the cryptographic binding, the Wallet Provider shall initialize the core configuration layer of the Wallet Unit. During this configuration phase, the Wallet Provider shall maintain a secure communication channel that guarantees the absolute integrity, authenticity, and confidentiality of all transmitted data.		WP-03-02	The assessor reviews the Wallet Unit activation sequence managed by the assessed Wallet Provider after the preliminary verification steps: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported; - register updates, status changes and prerequisites for later PID binding.	The assessor tests selected Wallet Unit activation-sequence records for the assessed Wallet Provider during the on-site Stage 2 assessment: - state-transition logs for configuration, initialisation, attestation issuance and activation; - secure-channel or protocol evidence for transmitted configuration data; - records showing user-selected PID storage options where applicable; - cases where the process stopped because a prerequisite for operational status was not met.
WPP-07a	CEN TS 18098-4: REQ-6.4.1	Where the wallet solution supports alternative logical or physical storage environments for Person Identification Data (PID), the Wallet Unit shall present the available storage options to the user (Present PID storage options, if applicable).		WP-03-02	The assessor reviews site, facility and environmental-protection arrangements maintained by the assessed Wallet Provider. The documentation should identify: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported, including presentation to the user of available logical or physical PID storage environments where the wallet solution supports alternative storage environments; - register updates, status changes and prerequisites for later PID binding.	The assessor inspects relevant facilities, physical controls or supporting utilities for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - state-transition logs for configuration, initialisation, attestation issuance and activation; - secure-channel or protocol evidence for transmitted configuration data; - records showing available PID storage options presented to the user and the user-selected PID storage method where applicable; - cases where the process stopped because a prerequisite for operational status was not met.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WPP-07b	CEN TS 18098-4: REQ-6.4.1	The Wallet Unit shall process and accept the preferred storage method selected by the user from the options presented under WPP-07a (Select option of the PID storage, if applicable).		WP-03-02	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported, including processing and acceptance of the preferred PID storage method selected by the user from the presented options; - register updates, status changes and prerequisites for later PID binding.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - state-transition logs for configuration, initialisation, attestation issuance and activation; - secure-channel or protocol evidence for transmitted configuration data; - records showing user-selected PID storage options where applicable, including processing, acceptance and application of the preferred storage method selected by the user; - cases where the process stopped because a prerequisite for operational status was not met.
WPP-08	CEN TS 18098-4: Clause 6.5	Upon completion of the configuration layer, the system shall initiate the cryptographic initialization sequence of the Wallet Unit (Initialisation of Wallet Unit).		WP-03-02	The assessor reviews the Wallet Unit activation sequence managed by the assessed Wallet Provider after the preliminary verification steps: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported; - register updates, status changes and prerequisites for later PID binding.	The assessor tests selected Wallet Unit activation-sequence records for the assessed Wallet Provider during the on-site Stage 2 assessment: - state-transition logs for configuration, initialisation, attestation issuance and activation; - secure-channel or protocol evidence for transmitted configuration data; - records showing user-selected PID storage options where applicable; - cases where the process stopped because a prerequisite for operational status was not met.
WPP-08a	CEN TS 18098-4: REQ-6.5.1.1; CEN TS 18098-4: REQ-6.5.2.1	The Wallet Unit shall generate localized cryptographic keys within the secure hardware environment of the device (WSCD), and the Wallet Provider shall securely		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components;	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		retrieve the generated public keys from the Wallet Unit.			- WSCD/WSCA use and evidence of protected key generation, storage and operation, including generation of localized cryptographic keys within the secure hardware environment of the device WSCD and secure retrieval of generated public keys from the Wallet Unit by the Wallet Provider; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	components; - key-generation, use, rotation, revocation or destruction records, including evidence that localized cryptographic keys were generated within the device WSCD and that the Wallet Provider securely retrieved the generated public keys from the Wallet Unit; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
WPP-08b	CEN TS 18098-4: REQ-6.5.1.2; CEN TS 18098-4: REQ-6.5.2.2	The Wallet Provider shall retrieve the corresponding Proof of Association (PoA) and Proof of Possession (PoP) tokens for each generated key pair from the Wallet Unit.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - where keys are generated and how WSCD protection is evidenced; - how public keys, PoA and PoP tokens are retrieved, validated and linked to the correct Wallet Unit or user, including retrieval of the corresponding PoA and PoP tokens for each generated key pair from the Wallet Unit; - verification rules for structural correctness, freshness and private-key possession; - abort rules preventing activation or credential issuance after failed proof validation.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - key-generation, public-key retrieval and WSCD evidence for sampled Wallet Units; - PoA and PoP validation logs and request payloads, including corresponding PoA and PoP tokens for each generated key pair; - failed proof or malformed-token cases showing that activation or issuance was stopped; - records linking keys, proofs, Wallet Unit status and the final activation or issuance decision.
WPP-08c	CEN TS 18098-4: REQ-6.5.1.3; CEN TS 18098-4: REQ-6.5.2.3	The Wallet Provider shall verify the validity and structural correctness of the received cryptographic proofs. If any verification step fails, the activation process shall be aborted, and no credentials shall be issued.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - key types, algorithms, trusted components and protected environments used for the assessed function; - key generation, storage, access, backup, rotation, revocation and destruction rules;	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - key-management records for generation, activation, use, rotation or destruction; - configuration or attestation evidence for protected key storage and cryptographic

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - verification rules for the validity and structural correctness of received cryptographic proofs; - abort rules ensuring that if any proof-verification step fails, the activation process is aborted and no credentials are issued; - segregation of duties and logging for sensitive key-management operations.	modules; - received cryptographic proof samples and validation evidence for validity and structural correctness; - access logs and approvals for sensitive key-management actions; - negative or exception cases such as expired certificates, failed rotations, rejected keys or failed proof-verification steps, showing that activation was aborted and no credentials were issued.
WPP-08d	CEN/TS 18098-4 10.7, 10.8, 10.9, 10.10	Wallet keys and PID keys shall be stored in a WSCD and their cryptographic operations shall be executed in the same WSCD. Cryptographic keys should be stored in a local WSCD where technically feasible. Where cryptographic keys are stored in a remote WSCD, the Wallet Provider shall implement adequate security measures to limit the risk of key compromise. Communication between the WSCD and the WSCA shall be protected for integrity, authenticity and confidentiality.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - WSCD/WSCA use and evidence of protected key generation, storage and operation, including storage of Wallet keys and PID keys in a WSCD and execution of their cryptographic operations in the same WSCD; - use of a local WSCD where technically feasible, and adequate security measures limiting key-compromise risk where a remote WSCD is used; - communication protection between the WSCD and WSCA for integrity, authenticity and confidentiality; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components, including evidence that Wallet keys and PID keys are stored in a WSCD and used for cryptographic operations in the same WSCD; - evidence of local WSCD use where technically feasible, or remote WSCD security measures limiting key-compromise risk; - protocol, configuration or attestation evidence that WSCD–WSCA communication is protected for integrity, authenticity and confidentiality; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WPP-09	CEN TS 18098-4: REQ-6.5.1.4; CEN TS 18098-4: REQ-6.5.1.5	Upon successful validation of all cryptographic proofs, the Wallet Provider shall issue the Wallet Unit Validity Attestation (WUVA) to confirm the structural and operational validity of the Wallet Unit.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including issuance of the Wallet Unit Validity Attestation after successful validation of all cryptographic proofs to confirm the structural and operational validity of the Wallet Unit; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including evidence that WUVA was issued only after successful validation of all cryptographic proofs and confirms structural and operational validity of the Wallet Unit; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
WPP-09a	CEN TS 18098-4: REQ-6.5.2.4; CEN TS 18098-4: REQ-6.5.2.5	Concurrently, the Wallet Provider shall issue one or several Wallet Unit Trust Attestations (WUTA) containing the public keys, Wallet Provider and hardware/software (WSCA/WSCD) environment details, device profiles, and a cryptographic signature, while strictly excluding any personal data relating to the User or the PID Subject.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - issuance of one or several Wallet Unit Trust Attestations containing public keys, Wallet Provider and hardware/software WSCA/WSCD environment details, device profiles and a cryptographic signature; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - controls ensuring that WUTA strictly excludes any personal data relating to the User or the PID Subject; - cryptographic agility process for weakened or deprecated algorithms;	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - WUTA samples showing public keys, Wallet Provider details, WSCA/WSCD environment details, device profiles and cryptographic signature; - key-generation, use, rotation, revocation or destruction records; - evidence that WUTA contains no personal data relating to the User or the PID Subject; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	deprecated algorithms or non-standard cryptographic configurations.
WPP-10	CEN TS 18098-4: Clause 6.6	Following the successful issuance of both mandatory attestations, the Wallet Provider shall execute the finalization phase. The Wallet Provider shall accept all verified Proof of Possession (PoP) tokens for the generated keys and update all internal systemic registers.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - where keys are generated and how WSCD protection is evidenced; - how public keys, PoA and PoP tokens are retrieved, validated and linked to the correct Wallet Unit or user; - verification rules for structural correctness, freshness and private-key possession; - finalization rules following successful issuance of both mandatory attestations, including acceptance of all verified PoP tokens for the generated keys and update of all internal systemic registers; - abort rules preventing activation or credential issuance after failed proof validation.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - key-generation, public-key retrieval and WSCD evidence for sampled Wallet Units; - PoA and PoP validation logs and request payloads; - evidence that, after successful issuance of both mandatory attestations, all verified PoP tokens for generated keys were accepted and all internal systemic registers were updated; - failed proof or malformed-token cases showing that activation or issuance was stopped; - records linking keys, proofs, Wallet Unit status and the final activation or issuance decision.
WPP-10a	CEN TS 18098-4: Clause 6.6	Upon successful register updates and acceptanceof the token, the system shall transition the operational status of the Wallet Unit to "Activated", thereby completing the onboarding sequence and fulfilling the mandatory prerequisite required to execute the subsequent PID binding process (7).		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status, including transition of the Wallet Unit operational status to “Activated” after successful register updates and token acceptance; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported;	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - state-transition logs for configuration, initialisation, attestation issuance and activation, including transition to “Activated” after successful register updates and token acceptance; - secure-channel or protocol evidence for transmitted configuration data; - records showing user-selected PID storage options where applicable; - evidence that the “Activated” status completed onboarding and fulfilled the mandatory prerequisite for the subsequent

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- register updates, status changes and prerequisites for later PID binding, including completion of onboarding before the subsequent PID binding process; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	PID binding process; - cases where the process stopped because a prerequisite for operational status was not met; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
WPP-11	CEN TS 18098-4: Clause 7	The Wallet Unit shall enable the user to trigger the sequence by initiating a request to bind the PID credential to the activated Wallet Unit.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles the Wallet Unit side of the PID binding request: - user trigger for starting PID binding from an activated Wallet Unit; - capture and transmission of the verification method selected from PID Provider options; - collection and forwarding of the expected PID format; - state and error handling before the request is sent to the PID Provider.	The assessor checks selected PID binding request cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - records showing the user-triggered binding request from an activated Wallet Unit; - request data containing selected verification method and expected PID format where applicable; - logs showing successful transmission to the PID Provider; - failed or incomplete requests and evidence that binding did not continue with missing data.
WPP-12	CEN TS 18098-4: REQ-7.3.1	The Wallet Unit shall process and transmit the specific verification method selected by the user from the options presented by the PID Provider.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles the Wallet Unit side of the PID binding request: - user trigger for starting PID binding from an activated Wallet Unit; - capture and transmission of the verification method selected from PID Provider options; - collection and forwarding of the expected PID format; - state and error handling before the request is sent to the PID Provider.	The assessor checks selected PID binding request cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - records showing the user-triggered binding request from an activated Wallet Unit; - request data containing selected verification method and expected PID format where applicable; - logs showing successful transmission to the PID Provider; - failed or incomplete requests and evidence that binding did not continue with missing data.
WPP-13	CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3	Prior to the generation of the PID key, the Wallet Unit shall request the User to set the PID key authentication		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		factors (knowledge-based, possession-based, or inherent).			process defines: - factor categories used for Wallet Unit, PID key or eID means authentication, including knowledge-based, possession-based or inherent PID key authentication factors requested from the User before PID key generation; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	- configuration and attestation evidence for enabled factors; - records showing that the User was requested to set PID key authentication factors before PID key generation, including knowledge-based, possession-based or inherent factors; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
WPP-14	CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3	Following authentication factor configuration, the Wallet Unit shall generate a cryptographic key pair dedicated exclusively to the PID credential.		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines: - prerequisites requiring successful authentication-factor configuration before PID credential key generation; - generation of a cryptographic key pair dedicated exclusively to the PID credential; - WSCA/WSCD or other protected environment evidence for generation and protection of the PID credential key pair; - controls preventing reuse of the PID credential key pair for other credentials, Wallet functions or users; - records retained for successful, failed or exceptional PID credential key-generation events;	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - records showing authentication-factor configuration before PID credential key-pair generation; - key-generation evidence for a cryptographic key pair dedicated exclusively to the PID credential; - configuration or attestation evidence for protected key generation and storage in the relevant WSCA/WSCD context; - evidence that the generated PID credential key pair is not reused for other credentials, Wallet functions or users; - failed or exceptional cases showing that PID binding did not continue where key generation failed;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	- a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
WPP-15	CEN TS 18098-4: REQ-7.7.1; REQ-7.7.2; REQ-7.7.4; REQ-7.7.5	The Wallet Unit shall generate and send a formal credential request payload to the PID Provider, incorporating the Wallet Unit Validity Attestation, the Wallet Unit Trust Attestation, the freshly generated PID public key, the Proof of Association (PoA), and the Proof of Possession (PoP).		WP-03-02	The assessor reviews the documented credential request generation process maintained by the assessed Wallet Provider. The review should confirm that the Wallet Unit-side design defines: - when and how the Wallet Unit generates a formal credential request payload for the PID Provider; - the required payload content: Wallet Unit Validity Attestation, Wallet Unit Trust Attestation, freshly generated PID public key, Proof of Association, Proof of Possession and requested credential/PID format where applicable; - how the PID key pair is generated for the request and how the process prevents reuse of an inappropriate or stale PID public key; - how PoA and PoP are created and linked to the same Wallet Unit, PID public key and credential request; - how the payload is transmitted to the PID Provider and which interface, protocol message or system component is responsible for that transmission; - controls preventing transmission or continuation where the credential request payload is incomplete, malformed, inconsistent or missing required evidence.	The assessor tests selected credential request flows for the assessed Wallet Provider during the on-site Stage 2 assessment. Using request payloads, protocol traces, application logs and system records, the assessor verifies: - that the Wallet Unit generated and sent a formal credential request payload to the PID Provider; - that the sampled payloads contained WUVA, WUTA, freshly generated PID public key, PoA and PoP; - that the PID public key in the request corresponds to the key material controlled by the Wallet Unit for that issuance flow; - that PoA and PoP relate to the same Wallet Unit, PID public key and credential request; - that logs or protocol traces show successful transmission of the payload to the PID Provider; - that incomplete, malformed or inconsistent payloads were not accepted for continuation of the PID binding or issuance flow.
WPP-16	CEN TS 18098-4: REQ-7.7.8	The Wallet Unit shall explicitly indicate to the PID Provider in its request for issuance of PID the expected PID format.		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines: - mandatory and optional PID data elements	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - issued PID samples or test vectors covering each supported format;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					for each supported format; - schema, signature, validity-status and validation information required by the applicable technical specification; - rules ensuring that the Wallet Unit explicitly indicates the expected PID format in its request to the PID Provider; - quality checks preventing incomplete, inconsistent or unsupported PID format requests from being issued; - versioning and change control for PID formats and data mappings; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	- schema validation, signature validation and required metadata checks; - request records showing that the Wallet Unit explicitly indicated the expected PID format to the PID Provider; - cases rejected because required elements, validation information or expected PID format were missing; - traceability between the configured format, the issuance request and the issued PID; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
WPP-17	CEN TS 18098-4: REQ-7.7.9	The Wallet Provider shall collect from the Wallet Unit the expected format specified for the PID credential.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles the Wallet Unit side of the PID binding request: - user trigger for starting PID binding from an activated Wallet Unit; - capture and transmission of the verification method selected from PID Provider options; - collection and forwarding of the expected PID format; - state and error handling before the request is sent to the PID Provider.	The assessor checks selected PID binding request cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - records showing the user-triggered binding request from an activated Wallet Unit; - request data containing selected verification method and expected PID format where applicable; - logs showing successful transmission to the PID Provider; - failed or incomplete requests and evidence that binding did not continue with missing data.
WPP-17a	CEN TS 18098-4: REQ-7.7.9	Upon successful collection of the expected format by the Wallet Provider, the PID shall be successfully bound to the Wallet Unit, and the system shall transition the operational status of the Wallet Unit to "operational".		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines: - state transitions from installation through configuration, cryptographic initialisation, binding and operational status, including transition of the Wallet Unit operational status to “operational” after successful	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - state-transition logs for configuration, initialisation, attestation issuance and activation; - secure-channel or protocol evidence for transmitted configuration data; - records showing user-selected PID storage

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					collection of the expected PID format and successful binding of PID to the Wallet Unit; - secure-channel controls protecting integrity, authenticity and confidentiality during configuration; - handling of PID storage options and user-selected storage method where supported; - register updates, status changes and prerequisites for later PID binding, including evidence that the binding prerequisite was completed before operational status was assigned; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	options where applicable; - records showing successful collection of the expected PID format, successful PID binding to the Wallet Unit and transition of the Wallet Unit status to "operational"; - cases where the process stopped because a prerequisite for operational status was not met; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
WPP-17b	Reg. 910/2014 Art. 5a(5)(f)	PID binding with Wallet Unit shall establish the technical association between the PID and the specific Wallet Unit. The uniqueness of PID and the legal determination of the person represented by PID remain the responsibility of the PID Provider and the electronic identification scheme under WP-03-01.		WP-03-02	The assessor reviews the documented PID-to-Wallet Unit binding model maintained by the assessed Wallet Provider. The review should confirm that the documentation explains: - how the technical association between PID and the specific Wallet Unit is established; - which Wallet Unit identifiers, keys, attestations or other binding material are used for this association; - how the process prevents binding PID to a different or unverified Wallet Unit; - how the Wallet Provider's role in technical binding is separated from the PID Provider's and eID scheme's responsibility for PID uniqueness and legal determination of the person represented by PID.	The assessor checks selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should verify: - that the sampled PID was technically associated with the intended Wallet Unit; - that Wallet Unit identifiers, keys, attestations or other binding material support this association; - that the sampled evidence does not show PID binding to a different or unverified Wallet Unit; - that the Wallet Provider's operational records do not indicate that it assumed responsibility for PID uniqueness or legal determination of the person represented by PID.
WPP-18	CEN/TS 18098-4 10.11, 10.12	The Wallet Provider shall maintain continuous monitoring capabilities to detect security incidents affecting the operational integrity of deployed Wallet		WP-03-02	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - mandatory hardware capabilities, security	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - successful verification records for supported

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		Units. The Wallet Provider shall regularly repeat client application genuineness checks, device capability controls and device integrity controls during the lifespan of the Wallet Unit and shall justify the control interval based on risk, threat intelligence, update cadence and the security model of the Wallet Solution.			features and deployment-policy checks for the user's device; - device-integrity checks for compromised operating systems, rooting, jailbreaking or tampering; - application genuineness and binding checks proving that the Wallet client runs on the verified device; - continuous monitoring capabilities to detect security incidents affecting the operational integrity of deployed Wallet Units; - rules for regularly repeating client application genuineness checks, device capability controls and device integrity controls during the Wallet Unit lifespan; - risk-based justification of the control interval using risk, threat intelligence, update cadence and the Wallet Solution security model.	devices and application versions; - monitoring records showing detection of security incidents affecting operational integrity of deployed Wallet Units; - repeated client application genuineness, device capability and device integrity checks during the Wallet Unit lifespan; - risk-based justification of monitoring and control intervals based on risk, threat intelligence, update cadence and the Wallet Solution security model; - failed device-capability, integrity, rooting, jailbreaking or tampering cases; - logs showing immediate termination of activation or appropriate lifecycle action after failed checks.
WPP-19	CIR 2024/2981 Art. 5, 8, 18	Upon detection of a security incident, the Wallet Provider shall execute an immediate problem analysis to determine the scope and impact of the issue.		WP-03-02	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - detection sources, classification criteria and escalation paths; - immediate problem-analysis steps executed upon detection of a security incident to determine the scope and impact of the issue; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps; - links with vulnerability management, risk assessment, change management and user communication.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment and closure; - evidence that immediate problem analysis was executed after security-incident detection and determined the issue scope and impact; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, lessons learned and updates to controls, risks or procedures.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WPP-20	CIR 2024/2981 Annex I risk treatment	The Wallet Provider shall evaluate whether the analyzed security incident applies strictly to a single Wallet Unit, a group of Wallet Units, a Wallet Solution component, a WSCA/WSCD component, a device family or a broader population of Wallet Users.		WP-03-02	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - criteria for determining whether an analysed security incident applies to a single Wallet Unit, a group of Wallet Units, a Wallet Solution component, a WSCA/WSCD component, a device family or a broader population of Wallet Users; - data sources, telemetry, logs and vulnerability information used to determine the affected population; - decision rules for escalating from single-unit treatment to broader risk treatment; - evidence retained for the incident scope determination and the person or system making the decision.	The assessor examines selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - whether the issue was classified as affecting a single Wallet Unit, a group of Wallet Units, a Wallet Solution component, a WSCA/WSCD component, a device family or a broader population of Wallet Users; - logs, telemetry, vulnerability records or other evidence supporting the affected-scope determination; - management or system decisions showing escalation from single-unit treatment to broader treatment where applicable; - cases where the initial scope was revised after further analysis.
WPP-20a	Reg. 910/2014 Art. 5e; CIR 2024/2979 Art. 7	Where the security incident is determined not to apply to a single unit but represents vulnerability or compromise with broader impact, the Wallet Provider shall trigger a mass Wallet Unit Attestation revocation , Wallet Unit invalidation, forced update, blocking, or other measures proportionate to the risk.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including mass Wallet Unit Attestation revocation where an incident represents vulnerability or compromise with broader impact; - criteria for Wallet Unit invalidation, forced update, blocking or other measures proportionate to the risk where the incident is not limited to a single unit; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required;	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - cases where broader vulnerability or compromise triggered mass Wallet Unit Attestation revocation, Wallet Unit invalidation, forced update, blocking or other risk-proportionate measures; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- rules excluding personal data from attestations where the requirement prohibits such data.	evidence that status publication or user notification followed the defined process.
WPP-21	Reg. 910/2014 Art. 5a(10); CIR 2024/2979 Art. 6(3)(b)	The Wallet Provider shall provide reporting channels to ingest lifecycle events, including scenarios where a smartphone is reported as lost, stolen, or damaged, or the User's will of discarding the service. Such mechanisms shall be accessible independently of the affected Wallet Unit where necessary.		WP-03-02	The assessor reviews security governance and ISMS documentation maintained by the assessed Wallet Provider. The review should confirm: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft, damage or service discard requests; - reporting channels used to ingest lifecycle events, including lost, stolen or damaged smartphone scenarios and the User's will of discarding the service; - mechanisms accessible independently of the affected Wallet Unit where necessary; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor checks implementation of the security-governance arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - systemic-trigger and user-trigger cases from intake through analysis and decision, including reports of lost, stolen or damaged smartphones and service discard requests; - evidence that lifecycle-event reporting channels were accessible independently of the affected Wallet Unit where necessary; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
WPP-22	CIR 2015/1502 Annex 2.2.3	Upon receiving a reported lifecycle event, the Wallet Provider shall perform a problem analysis to evaluate the Wallet Unit status modification requirements. The decision and evidence supporting it shall be recorded.		WP-03-02	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed Wallet Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or	The assessor tests selected lifecycle-event and status-decision cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	temporary blocking periods were maintained or lifted according to the decision.
WPP-23	CIR 2024/2979 Art. 7; Reg. 910/2014 Art. 5a(9)	Where the status change is confirmed as permanent, the Wallet Provider shall transition the specific Wallet Unit or Wallet Unit Attestation to an end-of-life, revoked or invalid status, as applicable, and shall update the relevant registers and status services.		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including transition of the specific Wallet Unit or Wallet Unit Attestation to an end-of-life, revoked or invalid status where the status change is confirmed as permanent; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules for updating the relevant registers and status services after permanent status change; - rules excluding personal data from attestations where the requirement prohibits such data.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - cases where a specific Wallet Unit or Wallet Unit Attestation was transitioned to end-of-life, revoked or invalid status after permanent status change confirmation; - register and status-service updates after the permanent status change.
WPP-23a	CIR 2024/2979 Art. 7(3)	Where Wallet Unit Attestations are revoked, the Wallet Provider shall inform affected Wallet Users within 24 hours of the revocation, including the reason for the revocation and the consequences for the Wallet User, in a concise, easily accessible and clear manner. Where a Wallet Unit is withdrawn,		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - triggers and deadlines for informing affected Wallet Users within 24 hours after Wallet Unit Attestation revocation; - required notification content, including the reason for revocation and the consequences for the Wallet User, provided in a concise,	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - timestamps from Wallet Unit Attestation revocation to notification of affected Wallet Users, confirming notification within 24 hours; - notification content showing the reason for revocation and consequences for the Wallet

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		suspended or otherwise restricted, the Wallet Provider shall provide appropriate user notification consistent with the security context.			easily accessible and clear manner; - appropriate user-notification rules where a Wallet Unit is withdrawn, suspended or otherwise restricted, consistent with the security context; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required.	User, in a concise, easily accessible and clear manner; - notification evidence for Wallet Unit withdrawal, suspension or other restriction where applicable; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
WPP-23b	CIR 2024/2979 Art. 7(4)	Where Wallet Unit Attestations are revoked, the Wallet Provider shall make publicly available the validity status of the Wallet Unit Attestation in a privacy-preserving manner and shall describe the location of that information in the Wallet Unit Attestation.		WP-03-02	The assessor reviews privacy-preserving validity-status publication controls maintained by the assessed Wallet Provider: - location and format of PID or Wallet Unit Attestation status information; - privacy controls preventing status checks from becoming tracking or correlation mechanisms; - how the status-location reference is included in the PID or attestation where required; - availability, integrity and update rules for the status service.	The assessor checks selected validity-status publication cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - issued and revoked PID or attestation samples with status-location references; - status-service responses for valid, suspended, revoked or unknown items; - privacy tests or configuration evidence limiting correlation and enumeration; - logs and monitoring evidence for status-service updates and availability.
WPP-23b	CIR 2024/2979 Art. 7(2), 6(3)(c)	The Wallet Provider shall establish and maintain a publicly available policy specifying the conditions and timeframe for revocation of Wallet Unit Attestations. The policy shall also describe the user request channel, independent user authentication mechanism and consequences of revocation.		WP-03-02	The assessor reviews service policy and revocation procedure. The documentation should identify: - publicly available policy specifying the conditions and timeframe for revocation of Wallet Unit Attestations; - policy content describing the user request channel for Wallet Unit Attestation revocation; - independent user authentication mechanism used for revocation requests; - policy content describing the consequences of revocation for the Wallet User; - controls ensuring that operational revocation decisions, timing and user-request handling are consistent with the public policy.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - publicly available policy specifying revocation conditions and timeframe for Wallet Unit Attestations; - policy sections describing the user request channel, independent user authentication mechanism and consequences of revocation; - sampled revocation cases showing that conditions and timeframe followed the public policy; - user-request cases showing use of the documented request channel and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						independent authentication mechanism; - evidence that policy updates are controlled and reflected in operational procedures.
WPP-24	CIR 2015/1502 Annex 2.2.3	Where the status change is determined under WPP-23 not to be permanent, the Wallet Provider shall evaluate whether a temporary blocking or suspension is required.		WP-03-02	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed Wallet Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor tests selected lifecycle-event and status-decision cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
WPP-24a	CIR 2015/1502 Annex 2.2.3	Where a temporary blocking is validated, the Wallet Provider shall apply a temporary restriction to the Wallet Unit for a designated period of time.		WP-03-02	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed Wallet Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor tests selected lifecycle-event and status-decision cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
WPP-24b	CIR 2015/1502 Annex 2.2.3;	The Wallet Provider shall implement measures to prevent unauthorised		WP-03-02	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	CIR 2024/2979 Art. 6(3)(b)-(c)	suspension, revocation, invalidation, reactivation or unblocking of Wallet Units and Wallet Unit Attestations. Such measures shall include secure user identification and authentication mechanisms independent of the Wallet Unit for user-initiated revocation requests.			should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - measures preventing unauthorised suspension, revocation, invalidation, reactivation or unblocking of Wallet Units and Wallet Unit Attestations; - secure user identification and authentication mechanisms independent of the Wallet Unit for user-initiated revocation requests; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - authorisation evidence for suspension, revocation, invalidation, reactivation or unblocking of Wallet Units and Wallet Unit Attestations; - user-initiated revocation request cases showing secure user identification and authentication independent of the affected Wallet Unit; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - negative cases showing that unauthorised lifecycle actions were rejected; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
WPP-25	CIR 2015/1502 Annex 2.2.3	The Wallet Provider shall continuously monitor the status of a temporarily blocked Wallet units to verify if the designated blocking time has elapsed.		WP-03-02	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed Wallet Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor tests selected lifecycle-event and status-decision cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
WPP-25a	CIR 2015/1502 Annex 2.2.3	Where the monitored block time has not elapsed, the system shall maintain the		WP-03-02	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed Wallet Provider:	The assessor tests selected lifecycle-event and status-decision cases for the assessed Wallet Provider during the on-site Stage 2

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		temporary block on the Wallet Unit.			- systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
WPP-25b	CIR 2015/1502 Annex 2.2.3	Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met. Where the conditions for reactivation are not met or the blocking period expires without remediation, the Wallet Provider shall route the flow to permanent invalidation or revocation as appropriate under WPP-23a.		WP-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed Wallet Provider. The documented controls should define: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed, including reactivation only if the same assurance requirements as established before suspension or revocation continue to be met; - routing to permanent invalidation or revocation where reactivation conditions are not met or the blocking period expires without remediation.	The assessor tests selected revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - reactivation cases showing that the same assurance requirements as established before suspension or revocation continued to be met; - cases where reactivation conditions were not met or the blocking period expired without remediation, showing routing to permanent invalidation or revocation; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WPP-26	CEN/TS 18098-4 10.13 POS; CIR 2024/2981 Art. 8	The Wallet Provider shall implement a periodic key renewal process for the Wallet Unit triggered by the expiration of the defined key lifetime.		WP-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - authorised triggers, decision roles and evidence required for each lifecycle action, including periodic Wallet Unit key renewal triggered by expiration of the defined key lifetime; - timeliness requirements and technical propagation of status changes; - controls preventing unauthorised suspension, revocation, reactivation or renewal; - key-lifetime configuration, renewal scheduling and evidence that Wallet Unit key renewal is executed when the defined lifetime expires; - assurance checks required before reactivation, renewal or replacement is allowed.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement, including Wallet Unit key-renewal records triggered by expiration of the defined key lifetime; - authorisation evidence and timestamps for status changes or key-renewal actions; - configuration evidence for key lifetime, renewal schedule and completed renewal events; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
WPP-27	CIR 2024/2981 Art. 5, 8, 18	The Wallet Provider shall establish, maintain and operate vulnerability management, change management and update management policies and procedures. The Wallet Provider shall notify the certification body without undue delay of breaches, compromises, vulnerabilities or changes likely to affect conformity and shall prepare vulnerability impact analysis reports where required. Update		WP-03-02	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure, including preparation of vulnerability impact analysis reports where required; - remediation, mitigation, retesting and closure rules; - change-management policies and procedures for changes likely to affect conformity;	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - intake, triage and impact-analysis evidence; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - vulnerability impact analysis reports where required; - change records and update records for software components of the Wallet Solution and the underlying eID scheme within scope; - notifications to CAB or certification body

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		mechanisms shall cover every software component of the Wallet Solution and underlying eID scheme within scope.			- update-management policies, procedures and mechanisms covering every software component of the Wallet Solution and the underlying eID scheme within scope; - notification to CAB or certification body without undue delay for breaches, compromises, vulnerabilities or changes likely to affect conformity where vulnerability impact criteria are met.	without undue delay for breaches, compromises, vulnerabilities or changes likely to affect conformity and related change or risk records.
WPP-28	CIR 2024/2979 Art. 9(3), 9(5), 9(7)	The Wallet Provider shall ensure integrity, authenticity and confidentiality of logged information. The logs shall be accessible to the Wallet Provider only where necessary for the provision of Wallet services and on the basis of explicit prior consent by the Wallet User. The Wallet Provider shall enable Wallet Users to export the logged information.		WP-03-02	The assessor reviews wallet log access and protection controls implemented by the assessed Wallet Provider: - conditions under which the provider may access wallet logs for service provision; - explicit prior-consent mechanism and withdrawal or refusal handling; - integrity, authenticity and confidentiality controls for logged information; - user export and access paths for logs where applicable.	The assessor tests selected wallet-log access and protection cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - consent records linked to provider log access; - samples of logged information and integrity or confidentiality protection evidence; - provider access attempts without consent and related rejection evidence; - user export or access cases and the resulting log package.
WPP-29	CIR 2024/2979 Art. 13; Reg. 910/2014 Art. 5a(4)(f)-(g)	Where technically feasible and except for critical assets, Wallet Units shall support secure export and portability of the Wallet User's personal data to allow migration to a Wallet Unit of a different Wallet Solution while preserving assurance level high.		WP-03-02	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting data, including secure export and portability of the Wallet User's personal data; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access to wallet logs or logged information;	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstrations or records showing the user initiating the relevant action; - exported data or logs and evidence of integrity, authenticity and confidentiality protection, including secure export and portability of the Wallet User's personal data for migration to a Wallet Unit of a different Wallet Solution while preserving assurance level high; - consent records where the provider accesses

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- technical limits, critical-asset exceptions and safeguards for secure portability or export, including migration to a Wallet Unit of a different Wallet Solution while preserving assurance level high where technically feasible.	logs for wallet-service purposes; - negative cases where export, deletion, sharing or provider access is blocked for security, critical-asset exception, technical infeasibility or lack of consent.
WPP-30	CIR 2024/2981 Art. 19	Relevant information produced during conformity assessment and information provided by the Wallet Provider as certificate holder shall be securely retained and made available to the certification body or supervisory body upon request. Lifecycle events, status changes, updates, revocations, reactivations and evidence supporting decisions shall be logged and retained according to the certification scheme and applicable law. [CIR 2024/2981 Art. 19] 6.5 Common security and authentication factors		WP-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed Wallet Provider. The documented controls should define: - which records or information must be retained for certification, audit, incident or supervisory purposes, including relevant information produced during conformity assessment and information provided by the Wallet Provider as certificate holder; - lifecycle events, status changes, updates, revocations, reactivations and evidence supporting decisions logged and retained according to the certification scheme and applicable law; - retention period, including periods after certificate cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB , certification body, supervisory body or competent authorities.	The assessor tests selected revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - record samples covering certification, assessment, vulnerability, incident or service evidence, including lifecycle events, status changes, updates, revocations, reactivations and evidence supporting decisions; - storage location, access-control, integrity and retention metadata; - retrieval evidence for CAB , certification body or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended.
WPP-31	CEN/TS 18098-4 9.1	The Wallet Provider shall ensure that verification of fulfilment of all assurance level high requirements by the Wallet Unit and by the Wallet Provider processes is based on suitable certifications or other suitable evidence. Such		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - scope of certification and mapping to Wallet, PID or eID scheme functions; - verification that all assurance level high requirements are fulfilled by the Wallet Unit	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, certification scope, assessment reports or action plans; - suitable certifications or other suitable evidence demonstrating fulfilment of all

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		evidence shall be documented, traceable and made available to the conformity assessment body.			and by the Wallet Provider processes, based on suitable certifications or other suitable evidence; - documentation and traceability of the evidence used to demonstrate fulfilment of assurance level high requirements; - responsibilities for maintaining evidence, reporting changes and managing recertification; - links between certification obligations, risk register and continuous-compliance activities; - records required for notification to the CAB, supervisory body or scheme owner where applicable, including evidence made available to the conformity assessment body.	assurance level high requirements by the Wallet Unit and by the Wallet Provider processes; - traceability records linking assurance level high requirements to documented evidence made available to the conformity assessment body; - records of changes, recertification decisions or continuous-compliance checks; - notifications sent to the CAB, supervisory body or scheme owner where required; - evidence that open findings or certification conditions are tracked to closure.
WPP-32	CEN/TS 18098-4 9.2, 9.3, 9.4	Where TLS is used during Wallet Unit activation, PID binding or Wallet Unit lifecycle management, the Wallet Provider shall use at least TLS version 1.2 and follow the required cypher suites. Only cryptographic algorithms recognised as secure by ENISA Agreed Cryptographic Algorithms should be used.		WP-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components, including TLS version at least 1.2 and required cipher suites where TLS is used during Wallet Unit activation, PID binding or Wallet Unit lifecycle management; - use of cryptographic algorithms recognised as secure by ENISA Agreed Cryptographic Algorithms; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential; - how the Wallet Unit identifier, binding	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components, including TLS version at least 1.2 and required cipher suites where TLS is used during Wallet Unit activation, PID binding or Wallet Unit lifecycle management; - evidence that cryptographic algorithms used are recognised as secure by ENISA Agreed Cryptographic Algorithms; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					material, PID public key and issuance decision are linked before release.	technical issuance event and retained audit evidence.
WPP-33	CEN/TS 18098-4 10.1, 10.2	The Wallet Unit shall include additional security measures to protect collected personal data beyond device manufacturer or operating system security. The additional security measures protecting personal data shall be security certified or otherwise evidenced as suitable for assurance level high in accordance with the certification scheme.		WP-03-02	The assessor reviews additional personal-data security measures implemented by the assessed Wallet Provider beyond the device manufacturer or operating system controls: - which personal data in the Wallet Unit require additional protection; - security measures added by the Wallet Provider and how they are independent of or reinforce device and OS security; - certification or other evidence showing suitability for assurance level high; - coverage of storage, processing, access and backup or recovery scenarios.	The assessor checks selected personal-data protection evidence for the assessed Wallet Provider during the on-site Stage 2 assessment: - configuration or design evidence for additional Wallet Unit protections; - certification, test or assurance evidence supporting suitability for assurance level high; - samples showing protected storage or processing of personal data; - negative or exception cases where device or OS protection alone would not be sufficient.
WPP-34	CEN/TS 18098-4 11.1, 11.2	The Wallet Provider shall ensure that the Wallet Unit is designed so that PID key authentication factors are independent from Wallet Unit authentication factors and from User device authentication factors. A successful authentication to the device or to the Wallet Unit shall not automatically satisfy the authentication requirement for use of the PID key.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - design controls ensuring that PID key authentication factors are independent from Wallet Unit authentication factors and from User device authentication factors; - rules ensuring that successful authentication to the device or to the Wallet Unit does not automatically satisfy the authentication requirement for use of the PID key; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required;	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - evidence that PID key authentication factors are independent from Wallet Unit authentication factors and User device authentication factors; - negative cases showing that successful device or Wallet Unit authentication does not automatically satisfy authentication required for use of the PID key; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- reset, recovery, fallback and failure handling for each factor type.	- negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
WPP-35	CEN/TS 18098-4 11.3, 11.4; CIR 2015/1502 Annex 2.2.1	The Wallet Provider shall ensure that at least one Wallet Unit authentication factor is set and that each Wallet Unit authentication factor is resistant to an attacker with high attack potential. The Wallet Provider shall ensure that use of the PID key requires multi-factor authentication using at least two factors from different categories, and that each PID key authentication factor is resistant to an attacker with high attack potential.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including at least one Wallet Unit authentication factor and at least two PID key authentication factors from different categories for use of the PID key; - resistance to manipulation, duplication, guessing, replay and high attack potential, including resistance of each Wallet Unit authentication factor and each PID key authentication factor to an attacker with high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including at least one Wallet Unit authentication factor and multi-factor authentication for PID key use using at least two factors from different categories; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - test or certification evidence that each Wallet Unit authentication factor and each PID key authentication factor is resistant to an attacker with high attack potential; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
WPP-36	CEN/TS 18098-4 11.5, 11.6, 11.7	Where a PIN or password is used as a Wallet Unit authentication factor, account authentication factor or PID key authentication factor, the Wallet Provider shall implement and document a PIN/password complexity policy. The PIN or password shall consist of at least 6 digits or 6 characters and shall allow a		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - documented PIN/password complexity policy where a PIN or password is used as a Wallet Unit authentication factor, account authentication factor or PID key authentication factor; - PIN or password length rules requiring at	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including documented PIN/password complexity policy where PINs or passwords are used; - configuration evidence that PINs or passwords consist of at least 6 digits or 6 characters; - successful and failed factor enrolment,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		maximum of 3 false authentication attempts before blocking or equivalent protective action. The Wallet Provider shall clearly inform the Wallet User of good practices for choosing and managing the PIN or password.			least 6 digits or 6 characters; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type, including a maximum of 3 false authentication attempts before blocking or equivalent protective action.	verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected, including blocking or equivalent protective action after a maximum of 3 false authentication attempts; - evidence that Wallet Users are clearly informed of good practices for choosing and managing the PIN or password.
WPP-37	CEN/TS 18098-4 11.10, 11.11	Where a possession-based authentication factor is used, the Wallet Provider shall ensure that it is resistant to high attack potential against manipulation and duplication, is tamper-resistant, and provides cryptographic functions for secure execution of the authentication protocol. Where PIN/password or biometrics are used as PID key authentication factors, the Wallet Provider shall ensure that the Wallet Unit stores, manages and verifies those factors in the same WSCA/WSCD that stores, manages and uses the corresponding PID key.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - resistance to manipulation, duplication, guessing, replay and high attack potential, including tamper resistance of possession-based factors and cryptographic functions for secure execution of the authentication protocol; - storage, management and verification of factors within the relevant WSCA/WSCD where required, including storage, management and verification of PIN/password or biometric PID key authentication factors in the same WSCA/WSCD that stores, manages and uses the corresponding PID key; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including tamper resistance of possession-based factors and cryptographic functions for secure execution of the authentication protocol; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable, including the same WSCA/WSCD that stores, manages and uses the corresponding PID key; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected, including manipulation or duplication of possession-based factors.
WPP-38	CEN/TS 18098-4 11.13, 11.14	Where biometrics are used as Wallet Unit authentication factors or		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		PID key authentication factors, the Wallet Provider shall ensure that the Wallet Unit provides biometric performance and security consistent with the relevant ISO/IEC or CEN standards required to reach assurance level high. Where the Wallet Provider uses inherent authentication factors as account authentication factors, the Wallet Provider shall not store the reference biometrics.			Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - biometric performance and security controls consistent with the relevant ISO/IEC or CEN standards required to reach assurance level high where biometrics are used as Wallet Unit or PID key authentication factors; - rules ensuring that the Wallet Provider does not store reference biometrics where inherent authentication factors are used as account authentication factors; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including biometric performance and security evidence consistent with the relevant ISO/IEC or CEN standards required to reach assurance level high; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - evidence that the Wallet Provider does not store reference biometrics where inherent authentication factors are used as account authentication factors; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
WPP-39	CEN/TS 18098-4 11.12 C-RECO	Where PIN/password or biometrics are used as Wallet Unit authentication factors or PID key authentication factors, the Wallet Unit should ensure, or at least clearly advise the User, that these factors are different from those used to unlock or authenticate to the User's device.		WP-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - rules ensuring, or at least clearly advising the User, that PIN/password or biometric Wallet Unit or PID key authentication factors are different from those used to unlock or authenticate to the User’s device; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required;	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - evidence that users are either prevented from using, or clearly advised not to use, the same PIN/password or biometric factors as those used to unlock or authenticate to the User’s device; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- reset, recovery, fallback and failure handling for each factor type.	duplicated, replayed or unauthorised factors are rejected.
REQ-910-01	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall meet the requirements set out in Article 8 with regard to assurance level high, as applied to the characteristics of the electronic identification means and the authentication mechanism.	Article 5a(5)(d)	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - authentication factors, transaction binding and user-consent or intent confirmation where relevant; - controls protecting authentication secrets, credentials and Wallet Unit keys; - rules for failed attempts, lockout, recovery and factor replacement; - evidence that assurance level high requirements are met for both the characteristics of the electronic identification means and the authentication mechanism; - evidence retained for authentication events without collecting more personal data than required.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - successful and failed authentication transactions, including relying-party interactions where relevant; - configuration enforcing the required factors, lockout rules and recovery controls; - evidence that the characteristics of the eID means and the authentication mechanism meet assurance level high under Article 8; - logs linking the Wallet Unit, user action and authentication outcome; - negative cases showing that replay, downgrade or unauthorised authentication attempts are rejected.
REQ-910-02	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall support common protocols and interfaces enabling relying parties to request and validate person identification data and electronic attestations of attributes.	Article 5a(5)(a)(ii)	WP-03-03	The assessor reviews common protocol and interface support implemented by the assessed Wallet Provider and authentication functions for relying-party request and validation flows: - supported protocols and interfaces allowing relying parties to request and validate PID and attestations; - message structure, request validation and response validation rules; - trust anchors, certificates or relying-party registration checks used by the protocol; - interoperability and negative-test evidence for unsupported, malformed or unauthorised requests.	The assessor tests selected relying-party protocol interactions for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - successful request-and-validation exchanges for PID and attestation flows; - protocol traces showing request validation, relying-party checks and response validation; - negative cases for malformed, unsupported, unauthorised or replayed requests; - configuration showing that production endpoints match the documented protocol profiles.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-910-03	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall authenticate and identify relying parties registered in accordance with Article 5b of eIDAS, prior to disclosing person identification data or electronic attestations of attributes.	Article 5a(5)(c)	WP-03-03	The assessor reviews relying-party authentication, policy processing and disclosure controls for the assessed Wallet Provider and authentication functions: - mechanisms used to authenticate relying parties registered under Article 5b; - protocol and interface rules under CIR 2024/2979 for relying-party requests; - processing of embedded disclosure policies and verification of relying-party compliance; - controls blocking disclosure to unregistered or non-compliant relying parties.	The assessor tests selected relying-party requests for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - successful and rejected relying-party authentication attempts; - certificate, registration or trust evidence used in the decision; - embedded disclosure policy checks and the result shown to the user; - logs proving that PID or attributes were not disclosed to unregistered or non-compliant relying parties.
REQ-910-04	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall not provide any information to providers of electronic attestations of attributes about the use of those attestations.	Article 5a(5)(b)	WP-03-03	The assessor reviews controls preventing the assessed Wallet Provider and authentication functions from informing attribute providers about user transactions: - data flows between the Wallet, relying parties and providers of electronic attestations of attributes; - technical barriers preventing callbacks, telemetry or transaction-use disclosure to attestation providers; - exceptions, if any, and their legal and user-authorisation basis; - logging and monitoring used to detect prohibited information flows.	The assessor checks selected attestation-use transactions for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - network, API or log evidence showing that no transaction-use information is sent to attestation providers; - tests with issued attestations used at relying parties; - configuration of analytics, telemetry and backend integrations; - exception cases confirming that any disclosure is explicitly authorised and documented.
REQ-910-05	Regulation (EU) No 910/2014 as amended / eIDAS	European Digital Identity Wallets shall support common protocols for sharing and presentation of person identification data and electronic attestations of attributes, both online and in offline mode, and for wallet-to-wallet interaction.	Article 5a(5)(a)(iv), (v), (vi)	WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation protocols, transports and credential formats, covering sharing and presentation of person identification data and electronic attestations of attributes both online and in offline mode, and wallet-to-wallet interaction, including	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations for sharing and presentation of PID and electronic attestations of attributes; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					OID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc, BLE or NFC where applicable; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	- negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
REQ-1502-01	Commission Implementing Regulation (EU) 2015/1502	The electronic identification means shall use at least two authentication factors from different categories (knowledge, possession, inherence).	Annex, Section 2.2.1, Level High, Element 1	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider for the eID means. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including evidence that the electronic identification means uses at least two authentication factors from different categories: knowledge, possession and inherence; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, showing that the electronic identification means uses at least two authentication factors from different categories: knowledge, possession and inherence; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
REQ-1502-02	Commission Implementing Regulation (EU) 2015/1502	The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.	Annex, Section 2.2.1, Level High, Element 2	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider for the eID means. The review should establish whether the documentation covers: - authentication factors, transaction binding and user-consent or intent confirmation	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means during the on-site Stage 2 assessment. The evidence should include: - successful and failed authentication transactions, including relying-party interactions where relevant;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					where relevant; - controls protecting authentication secrets, credentials and Wallet Unit keys against use by persons other than the legitimate holder; - rules for failed attempts, lockout, recovery and factor replacement; - evidence retained for authentication events without collecting more personal data than required.	- configuration enforcing the required factors, lockout rules and recovery controls; - logs linking the Wallet Unit, user action and authentication outcome; - negative cases showing that replay, downgrade or unauthorised authentication attempts , including attempts by persons other than the legitimate holder, are rejected.
REQ-1502-03	Commission Implementing Regulation (EU) 2015/1502	The electronic identification means is designed in such a way that it can be assumed it is used only under the control of the person to whom it belongs.	Annex, Section 2.2.1, Level Substantial, Element 1	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider for the eID means. The review should establish whether the documentation covers: - authentication factors, transaction binding and user-consent or intent confirmation where relevant; - controls protecting authentication secrets, credentials and Wallet Unit keys; - rules for failed attempts, lockout, recovery and factor replacement; - controls preventing use of the eID means outside the control of the legitimate holder; - evidence retained for authentication events without collecting more personal data than required.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means during the on-site Stage 2 assessment. The evidence should include: - successful and failed authentication transactions, including relying-party interactions where relevant; - configuration enforcing the required factors, lockout rules and recovery controls; - logs linking the Wallet Unit, user action and authentication outcome; - negative cases showing that replay, downgrade or unauthorised authentication attempts are rejected, including attempts to use the eID means outside the control of the person to whom it belongs.
REQ-1502-04	Commission Implementing Regulation (EU) 2015/1502	Dynamic authentication is used.	Annex, Section 2.3.1, Level High, Element 1	WP-03-03	The assessor reviews how the assessed Wallet Provider and authentication functions implements dynamic authentication for the eID means: - use of transaction-specific challenges, nonces or session data; - binding of the authentication response to the relying party and current transaction; - protection against replay, pre-computation and reuse of authentication evidence; - requirements for user action or factor use	The assessor tests selected dynamic authentication events for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - protocol traces showing fresh challenge or nonce values; - successful and replayed authentication attempts; - logs linking the dynamic response to the correct relying party and transaction;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					when a dynamic authentication event is created.	- configuration proving that static reusable authentication evidence is not accepted.
REQ-1502-05	Commission Implementing Regulation (EU) 2015/1502	Authentication is designed to prevent disclosure of authentication data relevant to the electronic identification and to prevent authentication from being replayed or forged in any way.	Annex, Section 2.3.1, Level High, Element 2	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - which authentication data and verification artefacts are sensitive; - storage, transmission and processing controls preventing disclosure; - design controls preventing authentication from being replayed or forged in any way; - separation between authentication secrets and verification data; - logs and exception handling for access to authentication data.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration of storage, transport and access controls; - samples showing authentication data is not exposed in logs, APIs or user interfaces; - negative tests showing that replayed or forged authentication evidence is rejected; - failed or unauthorised access attempts; - recovery, reset or support cases involving authentication data.
REQ-1502-06	Commission Implementing Regulation (EU) 2015/1502	The authentication mechanism, including authentication data, provides resistance against high attack potential.	Annex, Section 2.3.1, Level High, Element 3	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls ensuring that the authentication mechanism, including authentication data, provides resistance against high attack potential; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - test, certification or design evidence that the authentication mechanism, including authentication data, provides resistance against high attack potential; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-1502-07	Commission Implementing Regulation (EU) 2015/1502	The electronic identification means shall be designed and implemented to prevent duplication, tampering and unauthorised modification of the means or its authentication factors, taking into account resistance against high attack potential.	Annex, Section 2.2.1 and Section 2.3.1, Level High	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider for the eID means. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - resistance to manipulation, duplication, guessing, replay and high attack potential, including prevention of duplication, tampering and unauthorised modification of the eID means or its authentication factors; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected, including attempted duplication, tampering or unauthorised modification of the eID means or its authentication factors under high attack potential assumptions.
REQ-1502-08	Commission Implementing Regulation (EU) 2015/1502	The authentication mechanism shall enable reliable verification of the electronic identification means and its validity before person identification data are released in an authentication transaction.	Annex, Section 2.3.1, Level High	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider for the eID means. The review should establish whether the documentation covers: - authentication factors, transaction binding and user-consent or intent confirmation where relevant; - reliable verification of the electronic identification means and its validity before person identification data are released in an authentication transaction; - controls protecting authentication secrets, credentials and Wallet Unit keys; - rules for failed attempts, lockout, recovery and factor replacement; - controls blocking release of person identification data where the eID means or its validity cannot be verified;	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means during the on-site Stage 2 assessment. The evidence should include: - successful and failed authentication transactions, including relying-party interactions where relevant; - records showing reliable verification of the electronic identification means and its validity before person identification data were released; - configuration enforcing the required factors, lockout rules and recovery controls; - logs linking the Wallet Unit, user action and authentication outcome; - negative cases showing that replay, downgrade or unauthorised authentication attempts are rejected and that person

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- evidence retained for authentication events without collecting more personal data than required.	identification data are not released where the eID means or its validity cannot be verified.
REQ-1502-09	Commission Implementing Regulation (EU) 2015/1502	Person identification data and authentication data used by the electronic identification means shall be protected against loss, compromise, disclosure, unauthorised use and offline analysis.	Annex, Section 2.2.1 and Section 2.3.1, Level High	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls protecting person identification data and authentication data used by the electronic identification means against loss, compromise, disclosure, unauthorised use and offline analysis; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - evidence that person identification data and authentication data used by the electronic identification means are protected against loss, compromise, disclosure, unauthorised use and offline analysis; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-2979-01	Commission Implementing Regulation (EU) 2024/2979	Wallet providers shall ensure integrity, authenticity and confidentiality of the communication between wallet instances and wallet secure cryptographic applications.	Article 4(2)	WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - key types, algorithms, trusted components and protected environments used for the assessed function; - communication-security controls ensuring integrity, authenticity and confidentiality between wallet instances and wallet secure cryptographic applications; - key generation, storage, access, backup, rotation, revocation and destruction rules;	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - key-management records for generation, activation, use, rotation or destruction; - protocol traces, configuration or attestation evidence showing integrity, authenticity and confidentiality of communication between wallet instances and wallet secure cryptographic applications; - configuration or attestation evidence for protected key storage and cryptographic modules;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - segregation of duties and logging for sensitive key-management operations.	- access logs and approvals for sensitive key-management actions; - negative or exception cases such as expired certificates, failed rotations or rejected keys.
REQ-2979-02	Commission Implementing Regulation (EU) 2024/2979	The wallet unit shall support the presentation of person identification data and electronic attestations of attributes to relying parties online, using the OID4VP protocol as specified in CIR (EU) 2024/2979 and ARF v2.8.0.	Article 5	WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation protocols, transports and credential formats, including online presentation of person identification data and electronic attestations of attributes using OID4VP as specified in CIR (EU) 2024/2979 and ARF v2.8.0, ISO/IEC 18013-5, SD-JWT VC, mdoc, BLE or NFC where applicable; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations, including online presentation of PID and electronic attestations of attributes using OID4VP as specified in CIR (EU) 2024/2979 and ARF v2.8.0; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
REQ-2979-03	Commission Implementing Regulation (EU) 2024/2979	The wallet unit shall support proximity presentation using the ISO/IEC 18013-5 device retrieval protocol over BLE and NFC transport channels.	Article 5	WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation protocols, transports and credential formats, including OID4VP, ISO/IEC 18013-5 device retrieval protocol for proximity presentation over BLE and NFC transport channels, SD-JWT VC, mdoc, BLE or NFC where applicable;	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations, including proximity presentation using ISO/IEC 18013-5 device retrieval protocol over BLE and NFC transport channels; - protocol traces showing nonce handling,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	relying-party binding, selective disclosure and WSCD-signed proof where applicable; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
REQ-2979-04	Commission Implementing Regulation (EU) 2024/2979	The wallet unit shall support wallet-to-wallet interaction protocols as required by Article 5a(5)(a)(vi) of eIDAS and CIR (EU) 2024/2979.	Article 5	WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation and wallet-to-wallet interaction protocols, transports and credential formats, including OID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc, BLE or NFC where applicable, and wallet-to-wallet interaction protocols required by Article 5a(5)(a)(vi) of eIDAS and CIR (EU) 2024/2979; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations, including wallet-to-wallet interaction protocols required by Article 5a(5)(a)(vi) of eIDAS and CIR (EU) 2024/2979; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
EID-01	REQ-1502-01; REQ-1502-06; REQ-1502-07; REQ-2981-01; REQ-2981-02	The authentication factors, authentication mechanism and security measures of the EUDI Wallet shall be planned, executed and maintained so that they protect the integrity and		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - planning, execution and maintenance of authentication factors, authentication	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		confidentiality of the eID means. The eID means shall be able to resist at least high-level threats and attack potential in accordance with assurance level high. The resistance shall be based on a risk assessment including specific assessments of threats directed at authentication mechanisms and authentication factors based on possession, knowledge and inherence, as well as assessment of security measures in place to protect against these threats. The design shall also protect the eID means and its authentication factors against duplication, tampering and unauthorised modification.			mechanisms and security measures protecting the integrity and confidentiality of the eID means; - factor categories used for Wallet Unit, PID key or eID means authentication, including risk assessment of threats directed at possession, knowledge and inherence factors; - resistance to manipulation, duplication, guessing, replay and high attack potential, including resistance to at least high-level threats and attack potential in accordance with assurance level high; - design controls protecting the eID means and its authentication factors against duplication, tampering and unauthorised modification; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	- risk-assessment evidence covering threats to authentication mechanisms and possession, knowledge and inherence factors; - evidence that security measures protect the integrity and confidentiality of the eID means and resist high-level threats and attack potential; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected, including attempted duplication, tampering or unauthorised modification of the eID means or its authentication factors.
EID-02	REQ-1502-01; REQ-1502-02; REQ-1502-03; REQ-2981-02	The features and security measures of the EUDI Wallet shall prevent the possibility that the compromise of one authentication factor would compromise the reliability of other authentication factors. The security measures protecting the eID means shall separate and protect the authentication factors, in particular when they are		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - controls ensuring that compromise of one authentication factor does not compromise the reliability of other authentication factors; - separation and protection of authentication factors, in particular when used on the same terminal device; - independent management of PID key	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - evidence that compromise of one authentication factor does not compromise the reliability of other authentication factors; - evidence that PID key authentication factors, Wallet Unit authentication factors and User device authentication factors are separated and managed independently, including where

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		used on the same terminal device. In particular, the Wallet Provider shall ensure that PID key authentication factors, wallet unit authentication factors, and user device authentication factors are managed independently of each other.			authentication factors, Wallet Unit authentication factors and User device authentication factors; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required.	used on the same terminal device; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
EID-03	REQ-1502-02; REQ-1502-09; REQ-2981-02	The Wallet Provider shall ensure that secret data related to an eID means is not revealed to its staff under any circumstances. The wallet provider shall not make copies of any secret data related to an eID means. Person identification data and authentication data used by the eID means shall be protected against loss, compromise, disclosure, unauthorised use and offline analysis.		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls ensuring that secret data related to an eID means is not revealed to staff under any circumstances and is not copied; - controls protecting person identification data and authentication data used by the eID means against loss, compromise, disclosure, unauthorised use and offline analysis; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - evidence that secret data related to an eID means is not revealed to staff and is not copied; - evidence that person identification data and authentication data used by the eID means are protected against loss, compromise, disclosure, unauthorised use and offline analysis; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
EID-04	REQ-1502-01; REQ-2981-01	The EUDI Wallet shall use at least two authentication factors from different factor categories (possession, knowledge, inherence) for		WP-03-03	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed Wallet Provider. The review should show how the process defines:	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The test should connect: - configuration and attestation evidence for

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		each authentication operation. The possession factor shall be the wallet unit cryptographically bound to the WSCD. The second factor shall be a knowledge factor (passcode) or an inherence factor (biometric), or both.			- factor categories used for Wallet Unit, PID key or eID means authentication, including at least two authentication factors from different factor categories for each authentication operation; - possession factor implemented as the Wallet Unit cryptographically bound to the WSCD; - second factor implemented as a knowledge factor, such as a passcode, or an inherence factor, such as a biometric, or both; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	enabled factors, showing at least two authentication factors from different categories for each authentication operation; - evidence that the possession factor is the Wallet Unit cryptographically bound to the WSCD; - evidence that the second factor is a knowledge factor, such as a passcode, or an inherence factor, such as a biometric, or both; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
EID-04a	REQ-1502-03; REQ-2981-01	The authentication factors of the EUDI Wallet shall be bound to the wallet unit holder in the eID scheme. The EUDI Wallet shall not be bound to a wallet user before the wallet user has passed initial identity proofing as specified in WP-03-01, or it has otherwise been ensured that the eID means is not functional before the initial identity proofing has been performed.		WP-03-03	The assessor reviews the onboarding, identity-proofing and Wallet binding process maintained by the assessed Wallet Provider. The review should confirm that the documentation defines: - how EUDI Wallet authentication factors are bound to the wallet unit holder in the eID scheme; - which identity-proofing outcome from WP-03-01 is required before the Wallet is bound to the wallet user; - controls preventing the EUDI Wallet from being bound to a wallet user before the wallet user has passed initial identity proofing; - controls ensuring that, where any preparatory binding or enrolment step occurs before proofing is complete, the eID means remains non-functional until initial identity proofing has been performed; - records, status fields or system states used	The assessor traces selected onboarding and Wallet binding cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - that EUDI Wallet authentication factors were bound to the correct wallet unit holder in the eID scheme; - that the wallet user passed initial identity proofing under WP-03-01 before the Wallet was bound to that user or before the eID means became functional; - system records, workflow states or logs showing the sequence between identity-proofing completion, Wallet binding and activation of the eID means; - cases where binding or activation was blocked because initial identity proofing had not been completed; - configuration or operational evidence showing that any pre-proofing enrolment

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					to evidence the sequence from identity proofing to Wallet binding and activation.	state did not allow functional use of the eID means.
EID-05	REQ-1502-04; REQ-1502-05; REQ-1502-08; REQ-2981-01; REQ-2981-02	The authentication mechanism shall use dynamic authentication. The proof of authentication shall: (a) be produced using cryptographic techniques; (b) be unique to each authentication transaction; (c) include a nonce or timestamp provided by the verifying party; (d) be bound to the context of the transaction, including the identity of the relying party; and (e) not be replayable or forgeable outside its intended context. Before person identification data are released in an authentication transaction, the authentication mechanism shall verify the electronic identification means and its validity.		WP-03-03	The assessor reviews the documented authentication transaction and PID release controls maintained by the assessed Wallet Provider. The review should confirm that the authentication mechanism design defines: - generation of the proof of authentication using cryptographic techniques; - uniqueness of the proof for each authentication transaction; - inclusion of a nonce or timestamp provided by the verifying party; - binding of the proof to the transaction context, including the identity of the relying party; - controls preventing replay or forgery of the proof outside its intended transaction context; - verification of the electronic identification means and its validity before person identification data are released in the authentication transaction.	The assessor tests selected authentication transactions for the assessed Wallet Provider during the on-site Stage 2 assessment. Using protocol traces, payloads, logs and validation records, the assessor verifies: - cryptographic proof of authentication generated for each sampled authentication transaction; - nonce or timestamp values provided by the verifying party and included in the proof; - evidence that each proof is unique to the sampled transaction; - evidence that the proof is bound to the transaction context and relying-party identity; - negative or replay-test evidence showing that reused, modified or forged proofs are rejected; - records showing that the electronic identification means and its validity were verified before person identification data were released.
EID-06	REQ-1502-04; REQ-1502-05; REQ-1502-06	The authentication mechanism shall be implemented so that it is highly unlikely that an attacker with high attack potential could subvert it through guessing, eavesdropping, replay attacks or manipulation of communication. The		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls ensuring that the authentication mechanism is highly unlikely to be subverted	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		implementation shall be verified as part of the conformity assessment under GP-02 certification scheme.			by an attacker with high attack potential through guessing, eavesdropping, replay attacks or manipulation of communication; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - evidence that the implementation of the authentication mechanism is verified as part of the conformity assessment under the GP-02 certification scheme; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	- test or certification evidence for resistance to high attack potential, including resistance to guessing, eavesdropping, replay attacks and manipulation of communication; - evidence that the authentication-mechanism implementation was verified under the GP-02 certification scheme; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
EID-06a	WZ/WP provision	The EUDI Wallet shall employ internationally or nationally recommended cryptographic methods and protocols. The communications connection between the wallet unit and the wallet provider's systems shall employ encryption methods compliant with the applicable technical standards referenced in ARF v2.8.0 and CIR (EU) 2024/2979. Where Transport Layer Security (TLS) is used, TLS version		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - enabled protocol profiles, versions and endpoints for issuance, presentation or authentication; - internationally or nationally recommended cryptographic methods and protocols used by the EUDI Wallet; - encryption methods for the communication connection between the Wallet Unit and the Wallet Provider’s systems compliant with the applicable technical standards referenced in ARF v2.8.0 and CIR (EU) 2024/2979; - trust anchors, certificates and message-validation rules; - TLS or cipher-suite restrictions and controls for deprecated or weak configurations, including TLS version 1.2 or higher and only cipher suites providing forward secrecy where TLS is used; - negative-test, conformance-test and error-	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - positive and rejected protocol traces, conformance-test results or interoperability evidence; - endpoint, certificate, TLS and trust-anchor configuration, including TLS version 1.2 or higher and cipher suites providing forward secrecy where TLS is used; - evidence that cryptographic methods, protocols and encryption methods used for the Wallet Unit–Wallet Provider communication connection comply with ARF v2.8.0 and CIR (EU) 2024/2979; - logs showing malformed, unsupported, unauthorised or downgrade attempts being rejected; - evidence that the production configuration matches the documented supported profiles.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					handling evidence required for unsupported requests.	
EID-07	REQ-1502-02; REQ-1502-03; REQ-2981-02	The Wallet Provider shall ensure that the EUDI Wallet cannot be used for authentication without the successful completion of the user authentication step. The Wallet Provider shall ensure that no mechanism exists within the wallet solution that allows an authentication transaction to be completed without presentation of the required authentication factors by the wallet user, including by the Wallet Provider itself. Secret information related to the eID means shall not be accessible to the personnel or subcontractors of the wallet provider.		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - controls ensuring that the EUDI Wallet cannot be used for authentication without successful completion of the user authentication step; - controls ensuring that no mechanism within the wallet solution, including mechanisms available to the Wallet Provider, allows an authentication transaction to be completed without presentation of the required authentication factors by the wallet user; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - controls ensuring that secret information related to the eID means is not accessible to personnel or subcontractors of the Wallet Provider.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors; - successful authentication cases showing completion of the user authentication step before authentication use of the EUDI Wallet; - negative cases showing that an authentication transaction cannot be completed without presentation of the required authentication factors by the wallet user, including via Wallet Provider, support or administrative paths; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - evidence that secret information related to the eID means is not accessible to personnel or subcontractors of the Wallet Provider.
EID-08	REQ-1502-01; REQ-1502-02; REQ-1502-06	Where a knowledge-based authentication factor (PIN/passcode) is used, the Wallet Provider shall implement the following controls: (a) the PIN or password shall consist of at least 6 digits or 6 characters; (b) the wallet		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - PIN/passcode controls where a knowledge-based authentication factor is used, including	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including PIN/passcode length of at least 6 digits or 6 characters where used;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		unit shall allow at maximum 3 consecutive false authentication attempts before imposing a lockout or equivalent delay mechanism; (c) the PIN entry shall be protected against eavesdropping and interception; (d) the wallet unit shall prevent PIN/password submission by tools such as password managers and shall ensure the passcode originates from the wallet user; (e) the PIN or password shall not be stored outside the WSCD or equivalent protected storage in an accessible form.			at least 6 digits or 6 characters; - resistance to manipulation, duplication, guessing, replay and high attack potential, including protection of PIN entry against eavesdropping and interception; - controls preventing PIN/password submission by tools such as password managers and ensuring that the passcode originates from the wallet user; - storage, management and verification of factors within the relevant WSCA/WSCD where required, including controls ensuring that the PIN or password is not stored outside the WSCD or equivalent protected storage in an accessible form; - reset, recovery, fallback and failure handling for each factor type, including a maximum of 3 consecutive false authentication attempts before lockout or equivalent delay mechanism.	- successful and failed factor enrolment, verification and recovery cases; - failed-attempt tests showing lockout or equivalent delay after a maximum of 3 consecutive false authentication attempts; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable, including evidence that PIN/password is not stored outside the WSCD or equivalent protected storage in an accessible form; - tests or design evidence showing PIN entry protection against eavesdropping and interception and rejection of PIN/password submission by password managers or other tools; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
EID-08a	REQ-1502-01; REQ-1502-02; REQ-1502-06	Where an inherent authentication factor (biometrics) is used, the wallet provider shall: (a) ensure the biometric system has been evaluated against ISO/IEC 30107-3 for presentation attack detection, covering high attack potential; (b) store and manage the reference biometric data within the WSCD or the trusted execution environment, and not transmit it to any external system; (c) ensure the wallet user is offered an alternative non-biometric		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication; - controls for inherent authentication factors where biometrics are used, including evaluation against ISO/IEC 30107-3 for presentation attack detection covering high attack potential; - resistance to manipulation, duplication, guessing, replay and high attack potential, including threat types targeting the biometric factor taken into account in the authentication-mechanism design; - storage, management and verification of	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including ISO/IEC 30107-3 presentation attack detection evidence for biometrics covering high attack potential; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable, including reference biometric data stored and managed in the WSCD or trusted execution environment and not transmitted to external systems;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		authentication factor and their explicit and freely given consent to biometric processing is obtained; (d) ensure that different threat types that target the biometric factor are taken into account in the design of the authentication mechanism.			factors within the relevant WSCA/WSCD where required, including storage and management of reference biometric data within the WSCD or trusted execution environment and no transmission to any external system; - rules offering the wallet user an alternative non-biometric authentication factor and obtaining explicit and freely given consent to biometric processing; - reset, recovery, fallback and failure handling for each factor type.	- records showing explicit and freely given consent to biometric processing and availability of an alternative non-biometric authentication factor; - design or threat-analysis evidence covering different threat types targeting the biometric factor; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.
EID-09	REQ-1502-06; REQ-2981-02	The Wallet Provider shall implement mechanisms to detect and respond to repeated failed authentication attempts, including temporary or permanent blocking of the wallet unit. Where the wallet unit is blocked following repeated failed attempts, the user shall be notified and a recovery procedure consistent with the assurance requirements of WP-03-02 shall be available.		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - mechanisms detecting repeated failed authentication attempts; - criteria and thresholds for temporary or permanent blocking of the Wallet Unit after repeated failed attempts; - user-notification rules after Wallet Unit blocking; - recovery procedure available to the user and consistent with the assurance requirements of WP-03-02; - logs, evidence retention and authorisation controls for blocking, unblocking and recovery decisions.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - authentication logs showing detection of repeated failed attempts; - cases where the Wallet Unit was temporarily or permanently blocked after repeated failed attempts; - user notifications sent after blocking; - recovery cases showing consistency with WP-03-02 assurance requirements; - negative cases showing that blocked Wallet Units cannot be used until authorised recovery or unblocking is completed.
EID-10	REQ-1502-04; REQ-1502-05	Where single sign-on (SSO) is provided by the EUDI Wallet, the wallet provider shall implement adequate security measures for the management of session length, session transfer and session termination related		WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - session-length rules and maximum session duration for SSO; - controls for secure session transfer and	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration evidence for SSO session length, timeout and maximum duration; - successful and rejected session-transfer

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		to single sign-on, to ensure that the security level of the authentication is maintained throughout the session and that session-related risks are mitigated.			prevention of unauthorised session transfer; - session-termination rules, including logout, timeout, revocation, device change and risk-triggered termination; - controls maintaining the security level of authentication throughout the SSO session; - risk mitigations for session hijacking, fixation, replay, downgrade or unauthorised continuation.	cases; - session-termination cases covering logout, timeout, revocation, device change or risk-triggered termination; - evidence that the authentication security level is maintained throughout the session; - negative cases showing that hijacked, replayed, downgraded, expired or unauthorised sessions are rejected.
EID-11	REQ-910-01; REQ-1502-05	The EUDI Wallet shall present the user with information during each authentication event that enables the user to confirm that the authentication request received by the wallet corresponds to the user's own initiated transaction. This information shall be presented to the user before the user is asked to authorise the authentication, in wallet units that have the technical ability to do so.		WP-03-03	The assessor reviews user-confirmation information shown by the assessed Wallet Provider and authentication functions during authentication events: - which transaction details are presented to the user before authorisation; - how the displayed information lets the user recognise the initiated transaction; - handling for Wallet Units that lack the technical ability to present all details; - evidence retained for the presented information and user authorisation.	The assessor tests selected authentication events for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - screens or UI evidence showing transaction details before authorisation; - logs linking displayed information, user decision and authentication result; - cases where information was incomplete or the Wallet Unit could not present it; - negative tests confirming that authorisation is not requested before the required information is shown.
EID-12	REQ-910-03; REQ-1502-05	The EUDI Wallet shall present the user with information concerning the relying party for whom the authentication is being carried out, during each authentication event. This information shall include at a minimum the verified identity of the relying party and shall be presented to the user before the user is		WP-03-03	The assessor reviews information shown to the user about relying parties by the assessed Wallet Provider and authentication functions: - relying-party name, identifier, registration status and purpose information shown before disclosure or authentication; - source used to verify relying-party information; - handling of incomplete, inconsistent or unregistered relying-party data; - evidence retained for what was displayed to the user.	The assessor tests selected relying-party interaction screens for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - user interface evidence showing relying-party information before the user decision; - verification records for the relying-party identity and registration status; - rejected or warning cases for invalid relying-party information; - logs linking displayed information with the final user decision.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		asked to authorise the disclosure of any person identification data or attestation.				
EID-13	REQ-910-03; REQ-1502-05	Before disclosing person identification data or any electronic attestation of attributes to a relying party, the EUDI Wallet shall verify that the relying party is registered in accordance with Article 5b of eIDAS, using the relying party's registration certificate or another mechanism defined in CIR (EU) 2024/2979 and ARF v2.8.0. The wallet shall not disclose person identification data to relying parties that are not registered in accordance with Article 5b of eIDAS.		WP-03-03	The assessor reviews relying-party authentication and interaction controls maintained by the assessed Wallet Provider. The documentation should explain: - mechanisms used to authenticate relying parties registered under Article 5b, using the relying party's registration certificate or another mechanism defined in CIR (EU) 2024/2979 and ARF v2.8.0; - protocol and interface rules under CIR 2024/2979 and ARF v2.8.0 for relying-party requests; - processing of embedded disclosure policies and verification of relying-party compliance; - controls blocking disclosure to unregistered or non-compliant relying parties.	The assessor tests selected relying-party interaction cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - successful and rejected relying-party authentication attempts; - certificate, registration or trust evidence used in the decision, including the relying party registration certificate or another mechanism defined in CIR (EU) 2024/2979 and ARF v2.8.0; - embedded disclosure policy checks and the result shown to the user; - logs proving that PID or attributes were not disclosed to relying parties not registered under Article 5b or otherwise non-compliant relying parties.
EID-14	REQ-910-03; REQ-910-04; REQ-1502-05	The EUDI Wallet shall implement selective disclosure, ensuring that only the attributes explicitly requested by the relying party and consented to by the user are disclosed. The wallet shall not disclose additional attributes beyond the scope of the verified and consented request.		WP-03-03	The assessor reviews selective-disclosure controls implemented by the assessed Wallet Provider and authentication functions: - attribute-release rules, user-consent points and relying-party request validation; - mapping between requested attributes and attributes actually disclosed; - controls preventing hidden, excessive or bundled disclosure; - logs retained for user review and audit without creating prohibited tracking.	The assessor tests selected attribute-disclosure transactions for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - requests from relying parties and the attributes disclosed in response; - user interface evidence showing consent and requested attributes; - negative cases where unrequested attributes were not released; - transaction logs showing disclosure outcome and relying-party identity.
EID-15	REQ-910-04	The EUDI Wallet shall not provide any information to providers of electronic attestations of attributes		WP-03-03	The assessor reviews controls preventing the assessed Wallet Provider and authentication functions from informing attribute providers about user transactions:	The assessor checks selected attestation-use transactions for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		about the use of those attestations by the wallet user in transactions with relying parties.			- data flows between the Wallet, relying parties and providers of electronic attestations of attributes; - technical barriers preventing callbacks, telemetry or transaction-use disclosure to attestation providers; - exceptions, if any, and their legal and user-authorisation basis; - logging and monitoring used to detect prohibited information flows.	- network, API or log evidence showing that no transaction-use information is sent to attestation providers; - tests with issued attestations used at relying parties; - configuration of analytics, telemetry and backend integrations; - exception cases confirming that any disclosure is explicitly authorised and documented.
EID-16	REQ-910-01; REQ-2979-01	The Wallet Provider shall ensure that the transaction log of the EUDI Wallet records, for each authentication transaction, at a minimum: (a) the timestamp; (b) the verified identifier of the relying party; (c) the attributes disclosed; and (d) the outcome of the transaction. The transaction log shall be accessible to the user and shall be retained for the period specified in WZ-03-01.		WP-03-03	The assessor reviews relying-party authentication and interaction controls maintained by the assessed Wallet Provider. The documentation should explain: - which records or information must be retained for certification, audit, incident or supervisory purposes; - transaction-log content for each authentication transaction, including timestamp, verified identifier of the relying party, attributes disclosed and transaction outcome; - user access to the EUDI Wallet transaction log; - retention period, including periods after certificate cancellation or expiry where applicable, and the period specified in WZ-03-01 for transaction logs; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities.	The assessor tests selected relying-party interaction cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - record samples covering certification, assessment, vulnerability, incident or service evidence; - transaction-log samples for authentication transactions showing timestamp, verified relying-party identifier, disclosed attributes and transaction outcome; - evidence that the transaction log is accessible to the user; - storage location, access-control, integrity and retention metadata, including retention for the period specified in WZ-03-01; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended.
EID-17	REQ-910-02; REQ-910-05; REQ-2979-02; REQ-1502-05	The EUDI Wallet shall support online presentation of person identification data and electronic attestations of attributes to relying parties using the		WP-03-03	The assessor reviews online presentation protocol support implemented by the assessed Wallet Provider and authentication functions: - OID4VP profile support for presenting PID and electronic attestations of attributes;	The assessor tests selected OID4VP online presentation transactions for the assessed Wallet Provider and authentication functions during the on-site Stage 2 assessment: - successful online presentation cases for PID and attestation disclosure;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		OpenID for Verifiable Presentations (OID4VP) protocol as specified in CIR (EU) 2024/2979 and ARF v2.8.0. The implementation shall support selective disclosure for both SD- JWT VC and ISO/IEC 18013-5 (mdoc) credential formats. The response to the relying party shall include a cryptographic proof of possession signed by the WSCD, binding the response to the nonce and the relying party identifier provided in the request.			- SD-JWT VC and ISO/IEC 18013-5 mdoc selective-disclosure handling; - nonce and relying-party identifier binding in the WSCD-signed proof of possession; - negative-test evidence for replayed nonces, unsupported formats and invalid relying-party requests.	- protocol traces showing nonce handling, relying-party identifier binding and WSCD-signed proof; - selective-disclosure evidence for SD-JWT VC and mdoc formats; - rejected cases involving replay, invalid relying-party data, unsupported formats or failed proof validation.
EID-18	REQ-910-05; REQ-2979-03; REQ-1502-05	The EUDI Wallet shall support proximity presentation of person identification data and electronic attestations of attributes using the ISO/IEC 18013-5 device retrieval protocol over BLE and NFC transport channels, as specified in CIR (EU) 2024/2979 and ARF v2.8.0. The proximity session shall provide session encryption equivalent in security to the online protocol, protecting data in transit against eavesdropping and manipulation.		WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation protocols, transports and credential formats, including OID4VP, ISO/IEC 18013-5 device retrieval protocol for proximity presentation of PID and electronic attestations of attributes over BLE and NFC transport channels as specified in CIR (EU) 2024/2979 and ARF v2.8.0, SD-JWT VC, mdoc, BLE or NFC where applicable; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade, including proximity-session encryption equivalent in security to the online protocol and protecting data in transit against	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations, including proximity presentation of PID and electronic attestations of attributes using ISO/IEC 18013-5 device retrieval over BLE and NFC as specified in CIR (EU) 2024/2979 and ARF v2.8.0; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable; - session-encryption evidence showing protection equivalent in security to the online protocol and protection of data in transit against eavesdropping and manipulation; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					eavesdropping and manipulation; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
EID-19	REQ-910-05; REQ-2979-04	The EUDI Wallet shall support wallet-to-wallet interaction for the purposes of presenting person identification data and electronic attestations of attributes between wallet units, in accordance with Article 5a(5)(a)(vi) of eIDAS and the protocols specified in CIR (EU) 2024/2979 and ARF v2.8.0.		WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation and wallet-to-wallet interaction protocols, transports and credential formats, including OID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc, BLE or NFC where applicable, for presenting person identification data and electronic attestations of attributes between Wallet Units in accordance with Article 5a(5)(a)(vi) of eIDAS and the protocols specified in CIR (EU) 2024/2979 and ARF v2.8.0; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations, including wallet-to-wallet interaction for presenting PID and electronic attestations of attributes between Wallet Units in accordance with Article 5a(5)(a)(vi) of eIDAS and CIR (EU) 2024/2979 and ARF v2.8.0; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
EID-20	REQ-1502-06; REQ-2981-02	The wallet provider shall ensure that all cryptographic algorithms and key lengths used in the authentication protocols comply with the cryptographic requirements applicable at assurance level high under the GP-03 scheme and as		WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components, including compliance of all cryptographic algorithms and key lengths used in authentication	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components, showing compliance with assurance level high under GP-03 and references in ARF v2.8.0 and the applicable GP-02 cybersecurity certification scheme;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		referenced in ARF v2.8.0 and the applicable cybersecurity certification scheme under GP-02. The wallet provider shall maintain a cryptographic agility policy enabling timely migration to new algorithms in the event that existing algorithms are weakened or deprecated.			protocols with assurance level high under the GP-03 scheme and with ARF v2.8.0 and the applicable GP-02 cybersecurity certification scheme; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms, including a policy enabling timely migration to new algorithms when existing algorithms are weakened or deprecated; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	- key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations, including evidence of timely migration under the cryptographic agility policy.
REQ-1502-01	Commission Implementing Regulation (EU) 2015/1502	Providers delivering any operational service covered by CIR (EU) 2015/1502 shall be a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.	Annex, 2.4.1, Level Low, Element 1	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - legal status, ownership or mandate to provide the assessed service, including evidence that the provider is a public authority or a legal entity recognised as such by national law of a Member State; - established organisation and operational capability in all parts relevant for the provision of the assessed services; - financial-capacity evidence, insurance or liability arrangements required by the scheme or law; - responsibility for maintaining the evidence and updating it after significant changes; - links between financial or liability limits and user or relying-party information.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - company, mandate, insurance, guarantee or financial-capacity documents, including evidence of public-authority status or legal-entity recognition under national law of a Member State; - organisation, staffing, process and operational-readiness evidence showing that all service-relevant parts are established and fully operational; - validity dates, coverage limits and correspondence with the assessed certification scope; - updates after organisational or service changes; - records showing how limitations or liabilities are communicated where required.
REQ-1502-02	Commission Implementing Regulation	Providers shall comply with any legal requirements incumbent on them in	Annex, 2.4.1, Level Low, Element 2	WZ-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed Wallet Provider	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed Wallet Provider and PID Provider for

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2015/1502	connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.			and PID Provider for the eID means, as applicable. The review should confirm that the documented process defines: - legal requirements incumbent on the provider in connection with operation and delivery of the assessed service; - types of information that may be sought and the legal basis for seeking them; - legal and scheme requirements for how identity proofing is conducted; - which records or information must be retained for certification, audit, incident or supervisory purposes; - retention period, including periods after certificate cancellation or expiry where applicable, and legal limits on what information may be retained and for how long; - integrity, confidentiality, access-control and retrieval controls.	the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - record samples covering certification, assessment, vulnerability, incident or service evidence; - evidence that information sought from users matches the legal requirements and permitted information types; - identity-proofing procedure samples showing compliance with applicable legal and scheme requirements; - storage location, access-control, integrity and retention metadata, including evidence that retained information and retention periods comply with legal requirements; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended.
REQ-1502-03	Commission Implementing Regulation (EU) 2015/1502	Providers shall be able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.	Annex, 2.4.1, Level Low, Element 3	WZ-03-01	The assessor reviews legal, financial-capacity and liability arrangements maintained by the assessed Wallet Provider and PID Provider responsible for the eID means, as applicable. The documentation should identify: - how the provider demonstrates its ability to assume the risk of liability for damages arising from the assessed services; - how the provider demonstrates sufficient financial resources for continued operations and provision of the services; - insurance, guarantee, reserve, financial statement or equivalent evidence used to support liability and financial-capacity claims; - coverage limits, exclusions, validity periods and correspondence with the assessed certification scope; - responsibility for maintaining financial and	The assessor checks financial-capacity, insurance or liability evidence for the assessed Wallet Provider and PID Provider responsible for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current insurance, guarantee, reserve, financial statement or equivalent evidence demonstrating ability to assume liability for damages; - evidence supporting sufficient financial resources for continued operations and service provision; - validity dates, coverage limits, exclusions and alignment with the assessed certification scope; - records showing that financial-capacity and liability evidence has been reviewed and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					liability evidence and updating it after significant organisational, financial or service changes.	updated after significant organisational, financial or service changes; - management review, approval or other governance evidence confirming that liability and financial-capacity arrangements are actively maintained.
REQ-1502-04	Commission Implementing Regulation (EU) 2015/1502	Providers shall be responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.	Annex, 2.4.1, Level Low, Element 4	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements, including clauses preserving the provider's responsibility for outsourced commitments and compliance with the scheme policy as if the provider had performed the duties itself; - governance controls ensuring that outsourcing does not transfer or reduce the provider's accountability for scheme-policy compliance; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including responsibility clauses for outsourced commitments and scheme-policy compliance; - risk assessments, onboarding approvals and periodic review records; - evidence that the provider monitors and accepts responsibility for outsourced duties as if performed by the provider itself; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.
REQ-1502-06	Commission Implementing Regulation (EU) 2015/1502	The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.	Annex, 2.4.2, Level Low, Element 1	WZ-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should show: - which information must be public, user-facing or provided to relying parties, including a published service definition with all applicable terms, conditions, fees, limitations of usage and a privacy policy;	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices, including the published service definition, applicable terms, conditions, fees, usage limitations and privacy policy;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- ownership, approval and version-control rules for published content; - timeliness of updates after changes affecting users, relying parties or certification status; - evidence retained to show when information was published or changed.	- change history, approval records and publication timestamps; - comparison between published content and the assessed service configuration; - cases showing that outdated or inconsistent information was corrected.
REQ-1502-07	Commission Implementing Regulation (EU) 2015/1502	Appropriate policy and procedures shall be in place to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.	Annex, 2.4.2, Level Low, Element 2	WZ-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should show: - which information must be public, user-facing or provided to relying parties; - ownership, approval and version-control rules for published content; - policies and procedures for informing users in a timely and reliable fashion of changes to the service definition, applicable terms, conditions and privacy policy; - timeliness of updates after changes affecting users, relying parties or certification status; - evidence retained to show when information was published, changed or communicated to users.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices; - change history, approval records and publication timestamps; - user-notification evidence showing timely and reliable communication of changes to the service definition, applicable terms, conditions and privacy policy; - comparison between published content and the assessed service configuration; - cases showing that outdated or inconsistent information was corrected.
REQ-1502-08	Commission Implementing Regulation (EU) 2015/1502	Appropriate policies and procedures shall be in place that provide for full and correct responses to requests for information.	Annex, 2.4.2, Level Low, Element 3	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - which information must be public, user-facing or provided to relying parties; - policies and procedures for receiving, handling and responding to requests for information; - controls ensuring that responses to information requests are full, correct, approved where required and consistent with the current service definition and policies;	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices; - sampled requests for information and the responses provided; - evidence that responses were full, correct, timely and consistent with approved public or user-facing information; - change history, approval records and publication timestamps;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- ownership, approval and version-control rules for published content; - timeliness of updates after changes affecting users, relying parties or certification status; - evidence retained to show when information was published or changed and how information requests were answered.	- comparison between published content and the assessed service configuration; - cases showing that outdated or inconsistent information was corrected.
REQ-1502-09	Commission Implementing Regulation (EU) 2015/1502	There shall be an effective information security management system for the management and control of information security risks.	Annex, 2.4.3, Level Low	WZ-03-01	The assessor reviews the information-security governance documents maintained by the assessed provider across Wallet, PID and eID scheme responsibilities: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor verifies that governance is operating for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - approved policies, review records and management decisions; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-1502-10	Commission Implementing Regulation (EU) 2015/1502	The information security management system shall adhere to proven standards or principles for the management and control of information security risks.	Annex, 2.4.3, Level Substantial; Level High is same as Substantial	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should link the requirement to: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - adherence of the information security management system to proven standards or principles for the management and control of information security risks; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions; - evidence that the information security management system adheres to proven standards or principles for managing and controlling information security risks; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						changes, incidents, audit results or risk changes.
REQ-1502-11	Commission Implementing Regulation (EU) 2015/1502	Record and maintain relevant information using an effective record-management system, considering applicable legislation and good practice in relation to data protection and data retention.	Annex, 2.4.4, Level Low, Element 1	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - scope of certification and mapping to Wallet, PID or eID scheme functions; - effective record-management system used to record and maintain relevant information; - responsibilities for maintaining evidence, reporting changes and managing recertification; - applicable legislation and good practice for data protection and data retention reflected in record classification, retention, access and disposal rules; - links between certification obligations, risk register and continuous-compliance activities; - records required for notification to the CAB, supervisory body or scheme owner where applicable.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current certificate, certification scope, assessment reports or action plans; - record-management system samples showing relevant information recorded, maintained, classified and protected; - records of changes, recertification decisions or continuous-compliance checks; - retention and data-protection evidence showing consideration of applicable legislation and good practice; - notifications sent to the CAB, supervisory body or scheme owner where required; - evidence that open findings or certification conditions are tracked to closure.
REQ-1502-12	Commission Implementing Regulation (EU) 2015/1502	Retain, as far as it is permitted by national law or other national administrative arrangement and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed. [Annex, 2.4.4, Level Low, Element 2]	Annex, 2.4.4, Level Low, Element 2	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - which records or information must be retained for certification, audit, incident or supervisory purposes; - retention period, as far as permitted by national law or other national administrative arrangement, including retention required for auditing and investigation of security breaches, including periods after certificate	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - record samples covering certification, assessment, vulnerability, incident or service evidence, including records retained for auditing and investigation of security breaches; - storage location, access-control, integrity and retention metadata, including evidence that retention is permitted by national law or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including secure destruction after the required retention period ends.	other national administrative arrangement; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion or secure destruction where retention ended.
REQ-1502-13	Commission Implementing Regulation (EU) 2015/1502	The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified, and experienced in the skills needed to execute the roles they fulfil.	Annex, 2.4.5, Level Low, Element 1	WZ-03-01	The assessor reviews competence controls for staff and subcontractors used by the assessed provider across Wallet, PID and eID scheme responsibilities: - roles requiring specific skills, qualifications or experience; - training and qualification criteria for those roles; - onboarding and refresher training evidence requirements; - handling of gaps in competence before work is assigned.	The assessor checks selected personnel records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - staff and subcontractor samples in operational and trusted roles; - training, qualification and experience evidence; - records showing assignment only after competence requirements were met; - remediation for expired training or missing qualification evidence.
REQ-1502-14	Commission Implementing Regulation (EU) 2015/1502	The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.	Annex, 2.4.5, Level Low, Element 2	WZ-03-01	The assessor reviews how the assessed provider across Wallet, PID and eID scheme responsibilities demonstrates sufficient staffing and subcontractor capacity for the service: - resource model for operating and supporting the assessed service; - coverage for critical duties, backup roles and out-of-hours support; - dependency on subcontractors and escalation capacity; - monitoring of workload, vacancies or capacity risks.	The assessor checks staffing-capacity evidence for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - staffing plans, duty rosters, support schedules or service reports; - evidence of backup coverage for critical roles; - open vacancies, overload indicators or subcontractor capacity constraints; - management actions taken when capacity is insufficient.
REQ-1502-15	Commission Implementing Regulation (EU) 2015/1502	Facilities used for providing the service shall be continuously monitored for, and protect against, damage caused by environmental events,	Annex, 2.4.5, Level Low, Element 3	WZ-03-01	The assessor reviews facility monitoring and protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should identify: - facilities used for providing the assessed	The assessor inspects relevant facilities, physical controls and supporting utilities for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		unauthorised access and other factors that may impact the security of the service.			service and the security requirements applicable to each facility; - continuous monitoring controls for environmental events such as fire, flooding, power failure, HVAC failure or other environmental conditions; - physical access controls, surveillance, alarms and visitor or contractor controls protecting against unauthorised access; - controls protecting against other factors that may impact the security of the service; - escalation, response, maintenance and evidence-retention rules for facility monitoring and protection events.	- facility monitoring records for environmental events and other conditions affecting service security; - physical access-control, alarm, surveillance, visitor and contractor access records; - evidence that facilities used for providing the service are protected against environmental damage, unauthorised access and other relevant security-impacting factors; - tests or maintenance records for monitoring and protection systems; - incident or exception records showing response and remediation where facility monitoring detected a relevant event.
REQ-1502-16	Commission Implementing Regulation (EU) 2015/1502	Facilities used for providing the service shall ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised staff or subcontractors.	Annex, 2.4.5, Level Low, Element 4	WZ-03-01	The assessor reviews facility and restricted-area access-control arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should identify: - facilities and areas holding or processing personal, cryptographic or other sensitive information; - authorisation rules limiting access to those areas to authorised staff or subcontractors only; - physical access-control mechanisms, visitor controls, access reviews and removal of access after role, contract or employment changes; - segregation of sensitive areas and logging or monitoring of access events; - exceptions, emergency access and evidence retained for physical or facility access decisions.	The assessor checks selected facility and restricted-area access evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - access lists for facilities or areas holding or processing personal, cryptographic or other sensitive information; - samples showing access granted only to authorised staff or subcontractors; - physical access logs, visitor records, access-review records and access-removal evidence; - exceptions or emergency-access cases and related approvals; - evidence that unauthorised access attempts were detected, rejected or escalated.
REQ-1502-17	Commission Implementing Regulation	The existence of proportionate technical controls to manage the risks posed to the security	Annex, 2.4.6, Level Low, Element 1	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should link	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider and PID Provider for the eID means, as applicable,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2015/1502	of the services, protecting the confidentiality, integrity and availability of the information processed.			the requirement to: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - technical controls proportionate to the identified risks to the security of the services; - controls protecting the confidentiality, integrity and availability of information processed by the assessed services; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence of proportionate technical controls implemented to manage service-security risks; - configuration, monitoring or test evidence showing protection of confidentiality, integrity and availability of processed information; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-1502-18	Commission Implementing Regulation (EU) 2015/1502	Electronic communication channels used to exchange personal or sensitive information shall be protected against eavesdropping, manipulation, and replay.	Annex, 2.4.6, Level Low, Element 2	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - electronic communication channels used to exchange personal or sensitive information; - protocols, encryption, authentication and integrity-protection mechanisms used on those channels; - controls protecting the channels against eavesdropping, manipulation and replay; - configuration baselines and certificate, key or trust-anchor rules supporting secure channel operation; - negative-test and monitoring evidence for downgrade, replay, tampering or unauthorised communication attempts.	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - protocol traces or configuration evidence for channels exchanging personal or sensitive information; - encryption, certificate, key, trust-anchor and integrity-protection evidence; - negative tests showing that eavesdropping, manipulation, replay or downgrade attempts are prevented or rejected; - logs or monitoring records for secure-channel failures or suspicious communication attempts; - evidence that production communication-

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						channel settings match the documented secure configuration.
REQ-1502-20	Commission Implementing Regulation (EU) 2015/1502	Procedures shall exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents, and security breaches.	Annex, 2.4.6, Level Low, Element 4	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - criteria covering health or safety impact, unauthorised access, operational disruption, data compromise, vulnerable users, certification impact and financial loss where applicable; - thresholds, data sources and decision rules for classifying an event as a reportable breach or compromise; - procedures ensuring that security is maintained over time, including review, monitoring and continuous-improvement activities; - ability to respond to changes in risk levels, incidents and security breaches; - roles responsible for assessment, notification and remedy decisions; - links to incident response, availability measurement, WUA revocation and user or CAB notification.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - incident records mapped to each applicable breach criterion; - evidence supporting the decision that thresholds were or were not met; - records showing security-maintenance activities over time, such as reviews, monitoring, control updates or continuous-improvement actions; - examples where changes in risk levels, incidents or security breaches triggered procedure updates or risk-treatment actions; - notifications to users, CAB, supervisory bodies or other parties where required; - remedy decisions such as suspension, withdrawal, revocation or service restrictions.
REQ-1502-21	Commission Implementing Regulation (EU) 2015/1502	All media containing personal, cryptographic, or other sensitive information shall be stored, transported, and disposed of in a safe and secure manner.	Annex, 2.4.6, Level Low, Element 5	WZ-03-01	The assessor reviews asset and media-management arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage,	The assessor checks selected asset and media records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-1502-23	Commission Implementing Regulation (EU) 2015/1502	The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.	Annex, 2.4.7, Level High, Element 1	WZ-03-01	The assessor reviews the independent-audit programme maintained by the assessed provider across Wallet, PID and eID scheme responsibilities: - audit scope covering all service parts relevant to compliance; - independence and competence criteria for auditors; - frequency, planning and reporting of external audits; - tracking of findings, corrective actions and management review.	The assessor checks selected independent-audit evidence for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - audit plans, reports and scope statements; - auditor independence and competence evidence; - findings, corrective-action plans and closure evidence; - management review of audit results and recurring issues.
REQ-2690-01	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish a policy on the security of network and information systems setting out its approach, objectives, commitment to continual improvement, resource commitment, roles, documentation requirements, topic-specific policies, indicators and measures, and formal approval by management bodies.	Annex, 1.1.1	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - policy on the security of network and information systems setting out the provider's approach, objectives, commitment to continual improvement and resource commitment; - management approval, ownership and review cycle, including formal approval by management bodies; - allocation of responsibilities and links to operational procedures; - documentation requirements, topic-specific policies, indicators and measures supporting the policy;	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - approved policies, review records and management decisions, including the formally approved policy on the security of network and information systems; - evidence that the policy includes approach, objectives, continual-improvement commitment, resource commitment, roles, documentation requirements, topic-specific policies, indicators and measures; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	
REQ-2690-02	Commission Implementing Regulation (EU) 2024/2690	The policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur.	Annex, 1.1.2	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle, including review and, where appropriate, update by management bodies at least annually; - triggers for policy review and update after significant incidents or significant changes to operations or risks; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions, including evidence of management-body review at least annually; - records showing policy review and, where appropriate, update after significant incidents or significant changes to operations or risks; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-03	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down responsibilities and authorities for network and information system security and assign them to roles and communicate them to management bodies.	Annex, 1.2.1	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and authorities for network and information system security, assigned to defined roles and communicated to management bodies, and links to operational procedures;	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - approved policies, review records and management decisions; - role descriptions or responsibility matrices showing responsibilities and authorities for network and information system security; - evidence that those responsibilities and authorities were communicated to management bodies; - interviews with owners of key security and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-04	Commission Implementing Regulation (EU) 2024/2690	The provider shall require all personnel and third parties to apply network and information system security in accordance with established policies.	Annex, 1.2.2	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - requirements for all personnel and third parties to apply network and information system security in accordance with established policies; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - approved policies, review records and management decisions; - interviews with owners of key security and service processes; - personnel acknowledgements, training records, third-party contractual clauses or onboarding evidence requiring application of network and information system security policies; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-05	Commission Implementing Regulation (EU) 2024/2690	At least one person shall report directly to the management bodies on matters of network and information system security.	Annex, 1.2.3	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle, including designation of at least one person reporting directly to the management bodies on network and information system security matters;	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - approved policies, review records and management decisions; - organisation charts, role mandates or reporting records showing at least one person reporting directly to management bodies on network and information system security matters;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	- interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-06	Commission Implementing Regulation (EU) 2024/2690	Network and information system security shall be covered by dedicated roles or duties conducted in addition to existing roles.	Annex, 1.2.4	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures, including dedicated network and information system security roles or security duties conducted in addition to existing roles; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - approved policies, review records and management decisions; - role descriptions, responsibility matrices or staff assignments showing dedicated network and information system security roles or additional security duties assigned to existing roles; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-07	Commission Implementing Regulation (EU) 2024/2690	Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable.	Annex, 1.2.5	WZ-03-01	The assessor reviews segregation-of-duties arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should identify: - identification of conflicting duties and conflicting areas of responsibility relevant to network and information system security; - rules segregating conflicting duties where applicable; - role, access-right and approval matrices	The assessor checks selected role assignments, access rights and approval workflows for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - role and responsibility matrices identifying conflicting duties and conflicting areas of responsibility; - samples showing that conflicting duties are segregated where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					preventing incompatible responsibilities from being assigned to the same person or function; - compensating controls where segregation is not feasible; - periodic review of responsibility conflicts and segregation exceptions.	- access-right, approval and workflow evidence preventing incompatible responsibilities from being combined; - approved exceptions and compensating controls where segregation is not feasible; - review records showing that responsibility conflicts are periodically assessed and remediated.
REQ-2690-08	Commission Implementing Regulation (EU) 2024/2690	Roles, responsibilities, and authorities shall be reviewed and, where appropriate, updated at planned intervals and when significant incidents or significant changes occur.	Annex, 1.2.6	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle, including review and, where appropriate, update of roles, responsibilities and authorities at planned intervals and when significant incidents or significant changes occur; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions, including records of planned review and update of roles, responsibilities and authorities; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes, including updates to roles, responsibilities or authorities where appropriate.
REQ-2690-09	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems, including performing and documenting risk assessments and	Annex, 2.1.1	WZ-03-01	The assessor reviews security policy and risk management documentation of assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - framework scope and criteria for identifying and addressing risks to the security of network and information systems; - documented risk assessments covering relevant Wallet, PID or eID scheme assets, systems and processes;	The assessor checks selected network zones, communication channels and protection controls, and risk management register, during the on-site Stage 2 assessment. The evidence should include: - documented risk assessments for network and information system security risks; - risk register entries linked to assets, systems, processes and assessed services; - risk treatment plan records showing implementation status, monitoring, owners,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		establishing, implementing, and monitoring a risk treatment plan.			- risk treatment plan established, implemented and monitored by the provider; - risk owners, treatment actions, deadlines, residual-risk acceptance and monitoring status; - links between the risk-management framework, governance, incident handling, vulnerability management, change management and continuous-compliance activities.	deadlines and residual-risk decisions; - evidence that identified risks are addressed through implemented or planned controls; - management review, escalation or update records for risk treatment monitoring.
REQ-2690-10	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish procedures for identification, analysis, assessment, and treatment of risks (cybersecurity risk management process), including the elements set out in Annex, 2.1.2(a) to (j).	Annex, 2.1.2	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should link the requirement to: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes, including procedures for identification, analysis, assessment and treatment of cybersecurity risks and the elements set out in Annex 2.1.2(a) to (j); - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - evidence that the cybersecurity risk management process covers identification, analysis, assessment and treatment of risks, including the elements set out in Annex 2.1.2(a) to (j); - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-11	Commission Implementing Regulation (EU) 2024/2690	When identifying and prioritising risk treatment options, the provider shall consider the risk assessment results, the cost of implementation, the	Annex, 2.1.3	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID	The assessor checks selected assets and handling records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - sampled risks from the register linked to assets, processes and treatment actions,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		asset classification, and the business impact analysis.			scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance, including consideration of risk assessment results, implementation cost, asset classification and business impact analysis when identifying and prioritising risk treatment options; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	including evidence that risk treatment options were identified and prioritised using risk assessment results, implementation cost, asset classification and business impact analysis; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-12	Commission Implementing Regulation (EU) 2024/2690	The provider shall review and, where appropriate, update risk assessments and risk treatment plans at planned intervals, at least annually, and when significant changes or incidents occur.	Annex, 2.1.4	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment and risk treatment plans at planned intervals, at least annually, and after incidents, changes, vulnerabilities or supplier changes, including significant changes or incidents.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - records showing review and, where appropriate, update of risk assessments and risk treatment plans at planned intervals, at least annually, and when significant changes or incidents occur; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-13	Commission Implementing Regulation	The provider shall regularly review compliance with its policies on network and information system	Annex, 2.2.1-2.2.3	WZ-03-01	The assessor reviews security policy and applicable documentation.. The documentation should define: - regular review of compliance with network	The assessor checks selected network zones and information system security management documents, during the on-site Stage 2 assessment. The evidence should include:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2690	security. Management bodies shall be informed of the status through regular reporting.			and information system security policies; - scope, frequency, criteria and responsibilities for policy-compliance reviews; - evidence sources used to assess compliance with established policies; - regular reporting of compliance status to management bodies; - tracking of non-compliances, corrective actions and management decisions.	- completed reviews of compliance with network and information system security policies; - review schedules, criteria, results and evidence supporting compliance conclusions; - regular reports submitted to management bodies on compliance status; - records of management decisions, corrective actions and follow-up for identified non-compliance; - evidence that reporting frequency and content match the provider's established governance arrangements.
REQ-2690-14	Commission Implementing Regulation (EU) 2024/2690	The provider shall independently review its approach to managing network and information system security and its implementation, conducted by individuals with appropriate audit competence.	Annex, 2.3.1-2.3.4	WZ-03-01	The assessor reviews information system secuirty documentation. The documentation should define: - independent review of the provider's approach to managing network and information system security; - review of implementation of that approach across relevant services, systems and processes; - independence criteria for reviewers; - appropriate audit competence of individuals conducting the review; - review planning, reporting, findings, corrective actions and management follow-up.	The assessor checks selected evidence, during the on-site Stage 2 assessment. The evidence should include: - independent-review plans, reports and scope statements covering network and information system security management and its implementation; - evidence of reviewer independence; - audit-competence evidence for individuals conducting the review; - findings, corrective-action plans and closure evidence; - management review and follow-up of independent-review results.
REQ-2690-15	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish and implement an incident handling policy laying down roles, responsibilities, and procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents.	Annex, 3.1.1-3.1.3	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - roles, responsibilities and procedures laid down in the incident handling policy; - detection sources, classification criteria and escalation paths;	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment and closure; - evidence that assigned roles and responsibilities were applied during incident

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps; - links with vulnerability management, risk assessment, change management and user communication.	handling; - records covering analysis, response, recovery, documentation and reporting of incidents; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, lessons learned and updates to controls, risks or procedures.
REQ-2690-16	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down procedures and use tools to monitor and log activities on its network and information systems.	Annex, 3.2.1-3.2.7	WZ-03-01	The assessor reviews logging, monitoring and evidence-retention arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented controls should identify: - network zones, segmentation rules and exposure of administrative or service interfaces; - firewall, routing, remote-access and filtering rules relevant to the assessed service; - procedures and tools used to monitor and log activities on network and information systems; - approval, review and change control for network rules; - monitoring of denied traffic, unauthorised access attempts and configuration drift; - log sources, coverage, retention, review and escalation rules for relevant system and network activities.	The assessor checks monitoring tools, retained logs and selected security events for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - network diagrams compared with firewall, routing and segmentation configuration; - samples of rule approvals, reviews and changes; - monitoring-tool and logging-tool configuration for network and information systems; - logs for denied, suspicious or unauthorised network activity and other relevant system activities; - evidence of log review, retention, alerting and escalation according to the provider's procedures; - tests or demonstrations showing that restricted interfaces are not reachable outside approved paths.
REQ-2690-17	Commission Implementing Regulation (EU) 2024/2690	The provider shall put in place a simple mechanism for reporting suspicious events.	Annex, 3.3.1-3.3.2	WZ-03-01	The assessor reviews the suspicious-event reporting mechanism operated by the assessed provider across Wallet, PID and eID scheme responsibilities: - channels available to personnel, suppliers or	The assessor tests selected suspicious-event reports for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - submitted reports from different channels;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					users for reporting suspicious events; - minimum information required and routing to incident triage; - protection against loss or suppression of reports; - communication and awareness of the reporting mechanism.	- triage records showing assessment and escalation; - cases rejected as non-incidents and the rationale; - evidence that reporters can use the mechanism without relying on informal communication.
REQ-2690-18	Commission Implementing Regulation (EU) 2024/2690	The provider shall assess suspicious events to determine whether they constitute incidents and determine their nature and severity.	Annex, 3.4.1-3.4.2	WZ-03-01	The assessor reviews incident, breach and unauthorised-access handling arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps; - links with vulnerability management, risk assessment, change management and user communication.	The assessor tests selected incident or breach records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - events from detection through triage, classification, containment and closure; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, lessons learned and updates to controls, risks or procedures.
REQ-2690-19	Commission Implementing Regulation (EU) 2024/2690	The provider shall respond to incidents in accordance with documented procedures, including containment, eradication, and recovery.	Annex, 3.5.1-3.5.5	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, eradication, recovery and post-incident review steps performed in accordance with documented procedures; - links with vulnerability management, risk	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment, eradication, recovery and closure; - evidence that the response followed documented incident-response procedures; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					assessment, change management and user communication.	- post-incident actions, lessons learned and updates to controls, risks or procedures.
REQ-2690-20	Commission Implementing Regulation (EU) 2024/2690	The provider shall conduct post-incident reviews to identify root causes and documented lessons learned.	Annex, 3.6.1-3.6.3	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish whether the documentation covers: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps, including root-cause identification and documented lessons learned; - links with vulnerability management, risk assessment, change management and user communication.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - events from detection through triage, classification, containment and closure; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, root-cause analysis, documented lessons learned and updates to controls, risks or procedures.
REQ-2690-21	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down and maintain a business continuity and disaster recovery plan, based on risk assessment results.	Annex, 4.1.1-4.1.4	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - business continuity and disaster recovery plan maintained for the assessed service; - risk assessment results used as the basis for continuity and disaster recovery planning; - critical processes, dependencies, recovery objectives and disaster recovery scenarios; - roles, communications, escalation, activation criteria and decision-making rules; - review, testing and update rules for the business continuity and disaster recovery plan.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - approved business continuity and disaster recovery plan for the assessed service; - evidence linking the plan to risk assessment results; - exercise reports, disaster recovery tests, failover tests or continuity-plan walkthroughs; - records showing roles, communications, escalation and activation decisions; - updates made to the plan after tests, incidents, risk changes or service changes.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2690-22	Commission Implementing Regulation (EU) 2024/2690	The provider shall maintain backup copies of data and provide sufficient available resources to ensure an appropriate level of redundancy.	Annex, 4.2.1-4.2.6	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - critical processes, dependencies and recovery objectives for the assessed service; - backup scope, backup copies of data, protection, restoration testing and retention rules where applicable; - available resources and redundancy arrangements sufficient to ensure an appropriate level of redundancy; - crisis roles, communications, escalation and decision-making criteria; - links between continuity plans, incident response, supplier dependencies and user impact.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - exercise reports, backup jobs, backup-copy evidence, restoration tests or failover tests relevant to the service; - capacity, resource-availability or redundancy evidence showing an appropriate level of redundancy; - sampled continuity actions after incidents, outages or supplier failures; - evidence that recovery objectives and communications were met or deviations were addressed; - updates made to plans following tests, incidents or service changes.
REQ-2690-23	Commission Implementing Regulation (EU) 2024/2690	The provider shall put in place a process for crisis management, including roles, communication means and maintenance of security in crisis situations.	Annex, 4.3.1-4.3.4	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - critical processes, dependencies and recovery objectives for the assessed service; - backup scope, protection, restoration testing and retention rules where applicable; - crisis-management process, including crisis roles, communications, escalation and decision-making criteria; - controls for maintaining security in crisis situations; - links between continuity plans, incident response, supplier dependencies and user impact.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - exercise reports, backup jobs, restoration tests or failover tests relevant to the service; - crisis-management exercise or activation records showing assigned roles, communication means and decision-making; - sampled continuity actions after incidents, outages or supplier failures; - evidence that recovery objectives and communications were met or deviations were addressed; - evidence that security was maintained during crisis situations;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						- updates made to plans following tests, incidents or service changes.
REQ-2690-24	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a supply chain security policy governing relations with direct suppliers and service providers.	Annex, 5.1.1-5.1.7	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supply chain security policy established, implemented and applied to relations with direct suppliers and service providers; - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - supply chain security policy evidence and records showing its application to direct suppliers and service providers; - contracts, SLA and security annexes for critical suppliers; - risk assessments, onboarding approvals and periodic review records; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.
REQ-2690-25	Commission Implementing Regulation (EU) 2024/2690	The provider shall maintain and keep up to date a registry of direct suppliers and service providers.	Annex, 5.2	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supplier inventory or registry of direct suppliers and service providers, maintained and kept up to date, and identification of providers supporting Wallet, PID or eID scheme functions; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current registry of direct suppliers and service providers, including update evidence; - contracts, SLA and security annexes for critical suppliers; - risk assessments, onboarding approvals and periodic review records; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes and in the supplier registry.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2690-26	Commission Implementing Regulation (EU) 2024/2690	The provider shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products.	Annex, 6.1.1-6.1.3	WZ-03-01	The assessor reviews secure acquisition, development, maintenance or testing procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should show: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - processes to manage risks stemming from the acquisition of ICT services or ICT products; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	The assessor checks selected development, acquisition, maintenance or security-testing records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions, including risks stemming from acquisition of ICT services or ICT products; - procurement or acquisition records showing risk assessment and treatment before acquisition or implementation; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-27	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down rules for the secure development of network and information systems and apply them.	Annex, 6.2.1 - 6.2.4	WZ-03-01	The assessor reviews network-security documentation and security policy. The documentation should define: - rules for secure development of network and information systems; - secure design, coding, configuration, review, testing and approval requirements before release; - security requirements for development environments, repositories, dependencies and build or deployment pipelines; - evidence that secure-development rules are applied to relevant systems and changes; - handling of deviations, vulnerabilities and remediation before production deployment.	The assessor checks selected network configurations, during the on-site Stage 2 assessment. The evidence should include: - secure-development policy, standards or procedures for network and information systems; - samples of development changes showing secure design, coding, review, testing and approval before release; - repository, dependency, build, test or deployment evidence showing application of secure-development rules; - vulnerability findings, remediation records and release decisions; - exceptions or deviations and related risk acceptance or corrective actions.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2690-28	Commission Implementing Regulation (EU) 2024/2690	The provider shall take appropriate measures to establish, document, implement and monitor configurations, including security configurations.	Annex, 6.3.1-6.3.3	WZ-03-01	The assessor reviews configuration and change-management controls used by the assessed provider across Wallet, PID and eID scheme responsibilities: - baseline configurations for systems, applications, network and security components; - change request, approval, testing, implementation and rollback requirements; - segregation between emergency, standard and normal changes; - controls detecting unauthorised configuration drift.	The assessor checks selected configuration and change records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - change tickets from request through approval, testing, deployment and closure; - baseline configuration compared with observed or exported production configuration; - emergency or failed changes and post-implementation reviews; - drift, unauthorised change or rollback evidence and related corrective actions.
REQ-2690-29	Commission Implementing Regulation (EU) 2024/2690	The provider shall apply change management procedures to control changes of network and information systems.	Annex, 6.4.1-6.4.4	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - network zones, segmentation rules and exposure of administrative or service interfaces; - firewall, routing, remote-access and filtering rules relevant to the assessed service; - change management procedures applied to control changes of network and information systems; - approval, review and change control for network rules and other network and information system changes; - monitoring of denied traffic, unauthorised access attempts and configuration drift.	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - network diagrams compared with firewall, routing and segmentation configuration; - samples of rule approvals, reviews and changes and change records for network and information systems; - change tickets showing request, approval, testing, implementation and closure for network and information system changes; - logs for denied, suspicious or unauthorised network activity; - tests or demonstrations showing that restricted interfaces are not reachable outside approved paths.
REQ-2690-30	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy and procedures for security testing.	Annex, 6.5.1-6.5.3	WZ-03-01	The assessor reviews security-testing arrangements used by the assessed provider across Wallet, PID and eID scheme responsibilities: - testing scope, frequency and coverage for	The assessor checks selected security-testing evidence for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - test plans, reports and evidence of tested

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					applications, infrastructure and interfaces; - criteria for independent, penetration, vulnerability or configuration testing; - handling of findings, retesting and closure evidence; - links between testing results, risk treatment, change management and release decisions.	components; - findings mapped to owners, deadlines, fixes and retest results; - exceptions, accepted risks or deferred findings; - release or change records showing how test results influenced implementation decisions.
REQ-2690-31	Commission Implementing Regulation (EU) 2024/2690	The provider shall specify and apply procedures for security patch management.	Annex, 6.6.1-6.6.2	WZ-03-01	The assessor reviews patch-management controls used by the assessed provider across Wallet, PID and eID scheme responsibilities: - asset and vulnerability inputs used to determine patch applicability and priority; - testing, approval, deployment and rollback steps; - timelines for critical, high and routine patches; - exception handling and compensating controls for deferred patches.	The assessor checks selected patch records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - patches applied to critical service components from identification to deployment; - test, approval and rollback evidence; - overdue or deferred patches and risk acceptance or compensating controls; - evidence that patch status is reflected in vulnerability and risk records.
REQ-2690-32	Commission Implementing Regulation (EU) 2024/2690	The provider shall take appropriate measures to protect its network and information systems from cyber threats.	Annex, 6.7.1-6.7.3	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - appropriate measures protecting network and information systems from cyber threats; - risk treatment decisions, owners, deadlines and residual-risk acceptance, including preventive, detective and corrective controls proportionate to identified cyber threats; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence of appropriate measures implemented to protect network and information systems from cyber threats; - security monitoring, hardening, filtering, access-control, malware-protection or equivalent control evidence where applicable; - evidence that incidents, changes or vulnerability findings updated the risk picture;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						- operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-33	Commission Implementing Regulation (EU) 2024/2690	The provider shall segment systems into networks or zones in accordance with risk assessment results.	Annex, 6.8.1-6.8.3	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - risk assessment results used to determine segmentation of systems into networks or zones; - network zones, security zones, trust boundaries and segmentation rules for relevant systems and service components; - controls restricting communication between zones according to risk, asset criticality and service function; - approval, review and change control for segmentation rules; - monitoring of segmentation effectiveness, unauthorised paths and configuration drift.	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - network and zone diagrams compared with production firewall, routing, access-control and segmentation configuration; - evidence that segmentation decisions are based on risk assessment results; - tests or demonstrations showing that systems are separated into approved networks or zones and restricted paths are enforced; - logs or monitoring evidence for blocked unauthorised cross-zone communication; - review, change or drift records for segmentation rules.
REQ-2690-34	Commission Implementing Regulation (EU) 2024/2690	The provider shall protect its network and information systems against malicious and unauthorised software.	Annex, 6.9.1-6.9.2	WZ-03-01	The assessor reviews network-security and communication-protection arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - measures protecting network and information systems against malicious software; - measures preventing or detecting unauthorised software installation, execution or use; - malware protection, application control, endpoint protection, scanning, update and alerting rules where applicable; - coverage of servers, endpoints, administrative systems, repositories and	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - configuration evidence for malware protection, application control, endpoint protection or equivalent controls; - coverage evidence for network and information systems relevant to the assessed service; - logs, alerts or test evidence showing detection, prevention or rejection of malicious or unauthorised software; - update, signature, rule or policy

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					service components relevant to the assessed service; - handling, escalation and remediation of malware or unauthorised-software detections.	maintenance records; - incident or exception records and remediation actions for malware or unauthorised-software events.
REQ-2690-35	Commission Implementing Regulation (EU) 2024/2690	The provider shall obtain information about technical vulnerabilities, evaluate exposure, and take appropriate measures to manage vulnerabilities.	Annex, 6.10.1-6.10.4	WZ-03-01	The assessor reviews vulnerability-management and disclosure arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - sources of vulnerability information, including testing, suppliers, researchers and threat intelligence; - triage, severity scoring, ownership, remediation deadlines and acceptance of residual exposure; - coordination with patching, change management, incident response and risk management; - communication or disclosure rules for vulnerabilities affecting users or relying parties.	The assessor checks selected vulnerability records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - intake, triage and severity decisions for sampled vulnerabilities; - patch, mitigation, configuration or compensating-control evidence; - exceptions or overdue vulnerabilities and management approval of residual exposure; - evidence that relevant vulnerabilities were communicated or escalated when required.
REQ-2690-36	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy and procedures to assess whether its cybersecurity risk-management measures are effectively implemented and maintained.	Annex, 7.1- 7.3	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - policy and procedures to assess whether cybersecurity risk-management measures are effectively implemented and maintained; - assessment criteria, frequency, evidence sources and responsibilities for effectiveness	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - records assessing whether cybersecurity risk-management measures are effectively implemented and maintained; - test, review, monitoring or control-evaluation evidence supporting effectiveness conclusions; - evidence that incidents, changes or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					assessment; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2690-37	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure awareness raising and application of cyber hygiene practices for employees, management bodies, and direct suppliers and service providers.	Annex, 8.1.1-8.1.3	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - awareness raising and application of cyber hygiene practices for employees, management bodies, direct suppliers and service providers; - pre-contract due diligence, risk assessment and security requirements, including cyber hygiene expectations for direct suppliers and service providers; - contractual clauses, SLA, audit rights, incident notification and exit arrangements; - ongoing monitoring of supplier performance, security issues and changes; - training, communication, acknowledgement and monitoring evidence for cyber hygiene practices.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers; - risk assessments, onboarding approvals and periodic review records; - training, awareness, acknowledgement or communication records for cyber hygiene practices covering employees, management bodies, direct suppliers and service providers; - supplier incidents, service reports, audit results or vulnerability notifications; - samples showing application of cyber hygiene practices in daily operations and supplier/service-provider governance; - evidence that supplier changes or failures were reflected in risk and continuity processes.
REQ-2690-38	Commission Implementing Regulation (EU) 2024/2690	The provider shall identify employees whose roles require security- relevant skills and ensure they receive regular training.	Annex, 8.2.1-8.2.5	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - roles in scope, trusted responsibilities and required competence or screening criteria, including identification of employees whose roles require security-relevant skills; - training, awareness and acceptance of employment or confidentiality obligations,	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles; - screening, training, role-description and acknowledgement records, including evidence identifying employees whose roles require

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					including regular training for employees in roles requiring security-relevant skills; - responsibilities after termination or change of employment; - disciplinary process for breaches of security or service procedures.	security-relevant skills and showing regular training for those employees; - leaver or role-change cases and evidence of removed responsibilities and access; - records showing how policy or procedure violations were handled.
REQ-2690-39	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy and procedures related to cryptography, including key management.	Annex, 9.1-9.3	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - policy and procedures related to cryptography, including key management, established, implemented and applied by the provider; - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - cryptography and key-management policy and procedure evidence, including records showing implementation and application; - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-2690-40	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure that employees and direct suppliers and service providers understand and commit to their security responsibilities.	Annex, 10.1.1-10.1.3	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - requirements ensuring that employees, direct suppliers and service providers understand and commit to their security responsibilities; - pre-contract due diligence, risk assessment	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including security-responsibility commitments for direct suppliers and service providers; - risk assessments, onboarding approvals and periodic review records; - employee training, acknowledgement or commitment records showing understanding

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements, including security-responsibility commitments for direct suppliers and service providers; - ongoing monitoring of supplier performance, security issues and changes; - training, acknowledgement or commitment evidence for employees.	of security responsibilities; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.
REQ-2690-41	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure, to the extent feasible, verification of the background of employees.	Annex, 10.2.1-10.2.3	WZ-03-01	The assessor reviews background-verification controls for employees of the assessed provider across Wallet, PID and eID scheme responsibilities: - roles requiring background verification and criteria for proportionality; - checks performed before or during assignment to sensitive roles; - handling of unsuccessful, delayed or expired checks; - privacy and retention controls for background-check evidence.	The assessor checks selected background-verification records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - employee samples in sensitive and trusted roles; - completed verification evidence and dates; - exceptions, delays or compensating approvals; - evidence that role assignment considered the background-verification result.
REQ-2690-42	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure that security responsibilities that remain valid after termination or change of employment are contractually defined and enforced.	Annex, 10.3.1-10.3.2	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - roles in scope, trusted responsibilities and required competence or screening criteria; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment, including security responsibilities that remain valid after termination or role change and are contractually defined and enforced; - disciplinary process for breaches of security	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles; - screening, training, role-description and acknowledgement records; - leaver or role-change cases and evidence of removed responsibilities and access, including contractual clauses defining security responsibilities that remain valid after termination or change of employment; - records showing how policy or procedure

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					or service procedures, including enforcement of continuing security responsibilities.	violations were handled, including enforcement of continuing security responsibilities where applicable.
REQ-2690-43	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, communicate, and maintain a disciplinary process for handling violations of security policies.	Annex, 10.4.1-10.4.2	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - roles in scope, trusted responsibilities and required competence or screening criteria; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment; - disciplinary process established, communicated and maintained for breaches of security policies or service procedures.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles; - screening, training, role-description and acknowledgement records; - leaver or role-change cases and evidence of removed responsibilities and access; - records showing how policy or procedure violations were handled, including evidence that the disciplinary process for security-policy violations was communicated and maintained.
REQ-2690-44	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, document, and implement logical and physical access control policies.	Annex, 11.1.1-11.1.3	WZ-03-01	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should describe: - logical and physical access control policies established, documented and implemented; - roles, privileged functions and segregation-of-duty constraints for the assessed service; - joiner, mover, leaver, approval and periodic-review processes; - authentication requirements for administrative and sensitive access; - physical access requirements for facilities and restricted areas holding or processing sensitive information;	The assessor checks selected identity, privileged-access and access-rights records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - logical and physical access-control policy evidence and implementation samples; - user and privileged-account samples from request to approval, provisioning and review; - physical access samples for facilities and restricted areas; - terminated or changed personnel records compared with access-removal evidence; - configuration of MFA, privileged access, emergency access and segregation rules; - logs showing use of privileged or sensitive access and related review activity.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- logging, emergency access and removal of access after role changes or termination.	
REQ-2690-45	Commission Implementing Regulation (EU) 2024/2690	The provider shall provide, modify, remove, and document access rights in accordance with the access control policy.	Annex, 11.2.1-11.2.3	WZ-03-01	The assessor reviews access-control and identity-management arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - roles, privileged functions and segregation-of-duty constraints for the assessed service; - joiner, mover, leaver, approval and periodic-review processes; - authentication requirements for administrative and sensitive access; - logging, emergency access and removal of access after role changes or termination.	The assessor tests selected access-control samples for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - user and privileged-account samples from request to approval, provisioning and review; - terminated or changed personnel records compared with access-removal evidence; - configuration of MFA, privileged access, emergency access and segregation rules; - logs showing use of privileged or sensitive access and related review activity.
REQ-2690-46	Commission Implementing Regulation (EU) 2024/2690	The provider shall maintain policies for management of privileged accounts and system administration accounts.	Annex, 11.3.1 - 11.3.3	WZ-03-01	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should describe: - policies for management of privileged accounts and system administration accounts maintained by the provider; - roles, privileged functions and segregation-of-duty constraints for the assessed service; - joiner, mover, leaver, approval and periodic-review processes; - authentication requirements for administrative and sensitive access; - logging, emergency access and removal of access after role changes or termination.	The assessor checks selected identity, privileged-access and access-rights records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - policy evidence for management of privileged accounts and system administration accounts; - user and privileged-account samples from request to approval, provisioning and review; - terminated or changed personnel records compared with access-removal evidence; - configuration of MFA, privileged access, emergency access and segregation rules; - logs showing use of privileged or sensitive access and related review activity.
REQ-2690-47	Commission Implementing Regulation (EU) 2024/2690	The provider shall restrict and control the use of system administration systems.	Annex, 11.4.1-11.4.2	WZ-03-01	The assessor reviews controls over system administration systems used by the assessed provider across Wallet, PID and eID scheme responsibilities: - administration workstations, bastions, consoles or management networks in scope;	The assessor checks selected system-administration access paths for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - configuration of bastions, admin

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- allowed administrative paths and restrictions on general-purpose use; - monitoring, hardening and access rules for administration systems; - exception and emergency-administration procedures.	workstations or management networks; - access records for administrators and privileged sessions; - evidence that administrative systems are restricted and monitored; - exceptions or emergency sessions and related approvals.
REQ-2690-48	Commission Implementing Regulation (EU) 2024/2690	The provider shall manage the full life cycle of identities of network and information systems and their users.	Annex, 11.5.1-11.5.4	WZ-03-01	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should describe: - identities of network and information systems and their users in scope; - identity creation, approval, provisioning, modification, suspension, deactivation and deletion rules; - joiner, mover, leaver and system/service identity lifecycle processes; - ownership, periodic review, recertification and removal of obsolete or unused identities; - links between identities, access rights, privileged roles, logging and accountability.	The assessor checks selected identity, privileged-access and access-rights records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of user, service, system and privileged identities from creation to modification or removal; - joiner, mover and leaver cases compared with identity provisioning and deprovisioning evidence; - periodic identity review and recertification records; - evidence that obsolete, unused or unauthorised identities are disabled or removed; - logs or audit trails linking identity lifecycle actions to approvals and accountable owners.
REQ-2690-49	Commission Implementing Regulation (EU) 2024/2690	The provider shall implement secure authentication procedures and technologies.	Annex, 11.6.1-11.6.4	WZ-03-01	The assessor reviews secure-authentication procedures and technologies used by the assessed provider across Wallet, PID and eID scheme responsibilities: - authentication methods required for users, administrators and service components; - MFA, credential lifecycle, lockout and session controls; - protection of secrets, tokens and recovery processes; - criteria for stronger authentication on sensitive or privileged operations.	The assessor tests selected authentication controls for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - configuration of MFA, passwordless, certificate or token-based authentication; - successful, failed and locked authentication attempts; - credential reset and recovery cases; - evidence that privileged and sensitive access requires stronger authentication.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2690-51	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down classification levels of all assets, including information, for the level of protection required.	Annex, 12.1.1-12.1.3	WZ-03-01	The assessor reviews asset and media-management arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected asset and media records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-52	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy for the proper handling of assets.	Annex, 12.2.1-12.2.3	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - policy for the proper handling of assets, established, implemented and applied by the provider; - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected assets and handling records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - asset-handling policy evidence and records showing its implementation and application; - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-53	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy on the management of removable storage media.	Annex, 12.3.1-12.3.3	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - policy on the management of removable	The assessor checks selected assets and handling records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - policy evidence and records showing

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					storage media, established, implemented and applied by the provider; - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant, including controls for removable storage media; - links between assets, risks, access rights, logging and continuity arrangements.	implementation and application of removable storage media management; - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media, including removable storage media where used; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-54	Commission Implementing Regulation (EU) 2024/2690	The provider shall develop and maintain a complete, accurate, up- to-date, and consistent inventory of its assets.	Annex, 12.4.1-12.4.3	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function, including controls ensuring that the asset inventory is complete, accurate, up to date and consistent; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected assets and handling records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - inventory entries compared with observed systems, repositories or configuration records, including evidence that the asset inventory is complete, accurate, up to date and consistent; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-55	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish procedures for deposit, return, or deletion of assets upon termination of employment.	Annex, 12.5	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function;	The assessor checks selected assets and handling records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - inventory entries compared with observed systems, repositories or configuration records;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- ownership, classification, acceptable use and lifecycle rules, including procedures for deposit, return or deletion of assets upon termination of employment; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	- classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable, including deposit, return or deletion of assets upon termination of employment; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-56	Commission Implementing Regulation (EU) 2024/2690	The provider shall prevent loss, damage or compromise of network and information systems due to failure of supporting utilities.	Annex, 13.1.1-13.1.3	WZ-03-01	The assessor reviews technical and opeational documentation, and risk documentation. The review should confirm: - supporting utilities required for network and information systems, including power, cooling, connectivity or other facility services; - measures preventing loss, damage or compromise of network and information systems due to failure of supporting utilities; - monitoring, redundancy, backup supply, maintenance and alerting controls for supporting utilities; - escalation and response procedures for utility failures affecting the assessed service; - links to continuity, disaster recovery, incident response and risk management.	The assessor checks selected records during the on-site Stage 2 assessment. The evidence should include: - utility monitoring, maintenance, redundancy and backup-supply records for systems supporting the assessed service; - tests or evidence showing prevention of loss, damage or compromise caused by utility failure; - incident, outage or exception records for supporting-utility failures and related response actions; - evidence that continuity or disaster recovery measures address supporting-utility failures; - corrective actions for detected weaknesses in supporting-utility protection.
REQ-2690-57	Commission Implementing Regulation (EU) 2024/2690	The provider shall prevent or reduce the consequences of events originating from physical and environmental threats.	Annex, 13.2.1-13.2.3	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts, including physical and environmental threats; - risk treatment decisions, owners, deadlines and residual-risk acceptance, including	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions, including risks from physical and environmental threats; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					measures to prevent or reduce the consequences of events originating from physical and environmental threats; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions, including measures preventing or reducing consequences of physical and environmental threat events.
REQ-2690-58	Commission Implementing Regulation (EU) 2024/2690	The provider shall prevent and monitor unauthorised physical access, damage and interference to its network and information systems.	Annex, 13.3.1-13.3.3	WZ-03-01	The assessor reviews physical and environmental controls protecting the assessed provider across Wallet, PID and eID scheme responsibilities's assessed service components: - facilities, rooms, racks or secure areas supporting Wallet, PID or eID scheme operations; - entry-control rules, visitor handling, monitoring and review of access logs; - environmental protection, supporting utilities and maintenance arrangements; - handling of exceptions, alarms, outages and unauthorised access attempts.	The assessor checks physical and environmental-control evidence for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - access logs, visitor records and approval evidence for sampled secure areas; - inspection or demonstration of access-control, monitoring and environmental controls; - maintenance, utility, alarm or outage records affecting the assessed components; - evidence that exceptions were reviewed and corrective actions were completed.
REQ-2981-01	Commission Implementing Regulation (EU) 2024/2981	The provider shall complement the scheme's risk assessment to identify risks and threats specific to its implementation and propose appropriate treatment measures for all relevant risks and threats. The assessment shall be shared with the certification body for evaluation.	Article 4(4)(d), Article 4(5)	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should link the requirement to: - scope of certification and mapping to Wallet, PID or eID scheme functions; - responsibilities for maintaining evidence, reporting changes and managing recertification; - links between certification obligations, risk register and continuous-compliance activities, including the provider's complement to the scheme risk assessment identifying implementation-specific risks and threats and proposing treatment measures for all relevant risks and threats;	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - current certificate, certification scope, assessment reports or action plans; - the provider's complemented scheme risk assessment showing implementation-specific risks, threats and proposed treatment measures; - records of changes, recertification decisions or continuous-compliance checks; - notifications sent to the CAB, supervisory body or scheme owner where required, including evidence that the complemented

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- records required for notification to the CAB, supervisory body or scheme owner where applicable, including evidence that the complemented risk assessment was shared with the certification body for evaluation.	risk assessment was shared with the certification body for evaluation; - evidence that open findings or certification conditions are tracked to closure.
REQ-2981-02	Commission Implementing Regulation (EU) 2024/2981	The provider shall establish and implement policies and procedures concerning the management of risks associated with the operation of a wallet solution, including the identification and assessment of risks and the mitigation of the identified risks.	Article 8(3)(b)	WZ-03-01	The assessor reviews the risk-management arrangements used by the assessed provider across Wallet, PID and eID scheme responsibilities: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	The assessor checks risk-management implementation for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
REQ-2981-03	Commission Implementing Regulation (EU) 2024/2981	The provider shall establish and implement policies and procedures related to the management of changes and to the management of vulnerabilities in accordance with Article 5.	Article 8(3)(c)	WZ-03-01	The assessor reviews vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - policies and procedures related to the management of changes and the management of vulnerabilities in accordance with Article 5; - sources of vulnerability information, including testing, suppliers, researchers and threat intelligence; - triage, severity scoring, ownership, remediation deadlines and acceptance of residual exposure; - change identification, assessment, approval, testing, implementation and rollback rules for changes affecting the wallet solution; - coordination with patching, change	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - intake, triage and severity decisions for sampled vulnerabilities; - patch, mitigation, configuration or compensating-control evidence; - sampled change records showing assessment, approval, testing, implementation and rollback where applicable; - exceptions or overdue vulnerabilities and management approval of residual exposure; - evidence that change-management and vulnerability-management policies and procedures are implemented in accordance

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					management, incident response and risk management; - communication or disclosure rules for vulnerabilities affecting users or relying parties.	with Article 5; - evidence that relevant vulnerabilities were communicated or escalated when required.
REQ-2981-04	Commission Implementing Regulation (EU) 2024/2981	The provider shall establish and implement human resource management policies and procedures, including requirements on expertise, reliability, experience, security training, and qualifications of personnel involved in the development or operation of the wallet solution.	Article 8(3)(d)	WZ-03-01	The assessor reviews secure acquisition, development, maintenance or testing procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should show: - roles in scope, trusted responsibilities and required competence or screening criteria, including personnel involved in the development or operation of the wallet solution; - requirements on expertise, reliability, experience, security training and qualifications for relevant personnel; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment; - disciplinary process for breaches of security or service procedures.	The assessor checks selected development, acquisition, maintenance or security-testing records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles, including personnel involved in development or operation of the wallet solution; - screening, training, role-description and acknowledgement records, including evidence of expertise, reliability, experience, security training and qualifications required by the human-resource management policies and procedures; - leaver or role-change cases and evidence of removed responsibilities and access; - records showing how policy or procedure violations were handled.
REQ-2981-05	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall notify the relevant supervisory body 1 and, where applicable, other relevant bodies, without undue delay, after becoming aware of any breach of security or loss of integrity that has a significant impact on the wallet solution provided or on the personal data maintained therein.	Article 5(1)	WZ-03-01	The assessor reviews breach and compromise notification rules operated by the assessed provider across Wallet, PID and eID scheme responsibilities: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data; - timelines, roles and approval path for notification without undue delay;	The assessor tests selected breach or compromise notification cases for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - incident or breach records from detection through classification and notification decision; - notifications sent and timestamps showing timeliness; - evidence supporting impact on conformity, personal data or service integrity;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- evidence retained for the decision to notify or not notify.	- cases where notification was not sent and the documented rationale.
REQ-2981-06	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall notify their certification body without undue delay of any breach or compromise of the wallet solution, or of the electronic identification scheme under which it is provided, that is likely to impact its conformity with the requirements of the national certification scheme.	Article 5(2)	WZ-03-01	The assessor reviews breach and compromise notification rules operated by the assessed provider across Wallet, PID and eID scheme responsibilities: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data; - timelines, roles and approval path for notification without undue delay; - evidence retained for the decision to notify or not notify.	The assessor tests selected breach or compromise notification cases for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - incident or breach records from detection through classification and notification decision; - notifications sent and timestamps showing timeliness; - evidence supporting impact on conformity, personal data or service integrity; - cases where notification was not sent and the documented rationale.
REQ-2981-07	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management policy and procedures, considering the procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019.	Article 5(3)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure; - consideration of procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - intake, triage and impact-analysis evidence; - evidence that the vulnerability-management policy and procedures are established, maintained and operated; - evidence that the procedures consider existing European and international standards, including EN ISO/IEC 30111:2019; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2981-08	Commission Implementing Regulation (EU) 2024/2981	The holder of the certificate of conformity shall notify the issuing certification body of the vulnerabilities and changes affecting the wallet solution, based on defined criteria on the impact of these vulnerabilities and changes.	Article 5(4)	WZ-03-01	The assessor reviews criteria used by the assessed provider across Wallet, PID and eID scheme responsibilities to notify the issuing certification body about vulnerabilities and changes affecting the wallet solution: - impact criteria for deciding which vulnerabilities and changes must be notified; - links between vulnerability management, change management and certification-body notification; - responsibilities and deadlines for preparing and sending notification; - records required to support the notification decision and its impact assessment.	The assessor checks selected vulnerability and change notification decisions for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - vulnerability or change records assessed against the notification criteria; - notifications sent to the issuing certification body and related timestamps; - cases where notification was not sent and the documented rationale; - evidence that certification-impact decisions were tracked to closure.
REQ-2981-09	Commission Implementing Regulation (EU) 2024/2981	The holder of the certificate of conformity shall prepare a vulnerability impact analysis report for any vulnerability that affects the software components of the wallet solution, including: (a) the impact on the certified wallet solution; (b) possible risks associated with the proximity or likelihood of an attack; (c) whether the vulnerability can be remedied; (d) possible ways to remedy the vulnerability. The report shall be transmitted without undue delay to the certification body.The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management	Article 5(5), Article 5(6)	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish whether the documentation covers: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure, including preparation of a vulnerability impact analysis report for any vulnerability affecting software components of the wallet solution; - report content covering impact on the certified wallet solution, risks associated with proximity or likelihood of an attack, whether the vulnerability can be remedied, and possible ways to remedy it; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met, including transmission of the vulnerability	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - intake, triage and impact-analysis evidence; - reports for vulnerabilities affecting software components of the wallet solution, covering impact on the certified wallet solution, proximity or likelihood of attack, remediability and possible remedies; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records, including evidence that the vulnerability impact analysis report was transmitted to the certification body without undue delay.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		policy and procedures, considering the procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019. [Article 5(3)] REQ-2981-08 The holder of the certificate of conformity shall notify the issuing certification body of the vulnerabilities and changes affecting the wallet solution, based on defined criteria on the impact of these vulnerabilities and changes. [Article 5(4)] REQ-2981-09 The holder of the certificate of conformity shall prepare a vulnerability impact analysis report for any vulnerability that affects the software components of the wallet solution, including: (a) the impact on the certified wallet solution; (b) possible risks associated with the proximity or likelihood of an attack; (c) whether the vulnerability can be remedied; (d) possible ways to remedy the vulnerability. The report shall be transmitted without undue delay to the certification body. [Article 5(5), Article 5(6)] REQ-			impact analysis report to the certification body without undue delay.	

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		2981-10 The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management policy meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act). [Article 5(7)] REQ-2981-11 The holder of a certificate of conformity shall disclose and register any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981. [Article 5(9)] 4.3.3 Public Information (Article 8(5) and Annex V) REQ-2981-12 The provider shall make publicly available, in a clear, comprehensive and easily accessible manner: (a) any limitations on the use of the wallet solution; (b) guidance and recommendations for secure configuration, installation, deployment, operation and maintenance; (c) the period during which security support will be offered, in particular regarding cybersecurity-related				

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		updates; (d) contact information and accepted methods for receiving vulnerability information; (e) a reference to online repositories listing publicly disclosed vulnerabilities and relevant cybersecurity advisories. [Article 8(5), Annex V]				
REQ-2981-10	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management policy meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act).	Article 5(7)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - intake, triage and impact-analysis evidence; - evidence that the vulnerability management policy is established, maintained and operated in accordance with Annex I to Regulation (EU) 2024/2847; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records.
REQ-2981-11	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall disclose and register any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981.	Article 5(9)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure, including	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - intake, triage and impact-analysis evidence; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities, including registration in one of

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					disclosure and registration of any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	the online repositories referred to in Annex V to CIR (EU) 2024/2981; - notifications to CAB or certification body and related change or risk records.
REQ-2981-12	Commission Implementing Regulation (EU) 2024/2981	The provider shall make publicly available, in a clear, comprehensive and easily accessible manner: (a) any limitations on the use of the wallet solution; (b) guidance and recommendations for secure configuration, installation, deployment, operation and maintenance; (c) the period during which security support will be offered, in particular regarding cybersecurity-related updates; (d) contact information and accepted methods for receiving vulnerability information; (e) a reference to online repositories listing publicly disclosed vulnerabilities and relevant cybersecurity advisories.	Article 8(5), Annex V	WZ-03-01	The assessor reviews public information, user communication and service-condition material maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should check: - public availability of information in a clear, comprehensive and easily accessible manner; - limitations on the use of the wallet solution; - guidance and recommendations for secure configuration, installation, deployment, operation and maintenance; - the period during which security support will be offered, in particular for cybersecurity-related updates; - contact information and accepted methods for receiving vulnerability information; - reference to online repositories listing publicly disclosed vulnerabilities and relevant cybersecurity advisories.	The assessor checks the published material, user-facing information and operational records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should show: - public pages, repositories, advisories or user-facing notices showing information made available clearly, comprehensively and accessibly; - published limitations on the use of the wallet solution; - published secure configuration, installation, deployment, operation and maintenance guidance; - published security-support period, including cybersecurity-update support; - published contact information and accepted methods for receiving vulnerability information; - published references to online repositories for disclosed vulnerabilities and cybersecurity advisories.
REQ-2981-13	Commission Implementing Regulation	The holder of the certificate of conformity shall store the following information securely for the purpose of	Article 19(2)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2981	CIR (EU) 2024/2981, and for at least five years after the cancellation or expiry of the relevant certificate of conformity: (a) records of the information provided to the certification body or any of its sub-contractors during the certification process; (b) specimens of hardware components included in the scope of certification.			for the eID means, as applicable. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records of information provided to the certification body or its subcontractors during the certification process and specimens of hardware components included in the scope of certification; - retention period, including periods after certificate cancellation or expiry where applicable, and at least five years after cancellation or expiry of the relevant certificate of conformity for the information required by CIR (EU) 2024/2981 Article 19(2); - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities.	evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including information provided to the certification body or its subcontractors during certification; - evidence for secure storage of specimens of hardware components included in the certification scope; - storage location, access-control, integrity and retention metadata, including retention for at least five years after cancellation or expiry of the relevant certificate of conformity; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended.
REQ-2981-14	Commission Implementing Regulation (EU) 2024/2981	The holder of the certificate of conformity shall make the information referred to in Article 19(1) available to the certification body or the Scheme Owner upon request.	Article 19(3)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including the information referred to in Article 19(1) of CIR (EU) 2024/2981; - retention period, including periods after certificate cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including Article 19(1) information; - storage location, access-control, integrity and retention metadata; - retrieval evidence for CAB or supervisory requests, including evidence that Article 19(1) information is made available to the certification body or the Scheme Owner upon request; - expired or archived records and evidence of secure deletion where retention ended.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					the CAB or competent authorities, including availability of Article 19(1) information to the certification body or the Scheme Owner upon request.	
REQ-847-01	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall establish, implement and maintain decision- making procedures to evaluate whether revocation of affected wallet unit attestations or other additional remedies are necessary to react adequately to a security breach or compromise.	Article 4(2)	WZ-03-01	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - decision-making procedures to evaluate whether revocation of affected Wallet Unit Attestations or other additional remedies are necessary to react adequately to a security breach or compromise; - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - records linking the remedy decision to the relevant breach or compromise assessment; - rules excluding personal data from attestations where the requirement prohibits such data.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process; - decision records showing whether revocation of affected Wallet Unit Attestations or other additional remedies were evaluated and selected after a security breach or compromise.
REQ-847-02	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that suspension or remedy measures do not prevent affected wallet users from exercising data portability, provided this can be done without impairing the security of critical assets of affected wallet units.	Article 4(4)	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting data; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - demonstrations or records showing the user initiating the relevant action; - exported data or logs and evidence of integrity, authenticity and confidentiality protection; - consent records where the provider accesses logs for wallet-service purposes;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					to wallet logs or logged information; - technical limits, critical-asset exceptions and safeguards for secure portability or export, including controls ensuring that suspension or remedy measures do not prevent affected wallet users from exercising data portability where this can be done without impairing the security of critical assets of affected Wallet Units.	- data-portability cases during suspension or remedy measures for affected wallet users; - negative cases where export, deletion, sharing or provider access is blocked for security or lack of consent, including evidence that any portability restriction was justified by impairment of critical-asset security.
REQ-847-03	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall establish, implement and maintain procedures to provide clear, comprehensive and easily accessible information about suspension of a wallet solution without undue delay and no later than 24 hours after suspension.	Article 5(1)	WZ-03-01	The assessor reviews procedures for communicating Wallet suspension information by the assessed Wallet Provider: - triggers for suspension and required communication deadline; - content required to be clear, comprehensive and easily accessible; - channels used to reach users or relying parties without undue delay; - records proving publication or delivery no later than 24 hours after suspension.	The assessor checks selected suspension-communication cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - timestamp from suspension decision to communication; - message content and channel evidence; - accessibility and clarity of published or delivered information; - escalation records where the 24-hour deadline was at risk.
REQ-847-04	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall establish, implement and maintain contact and communication procedures: – enabling notifications to single points of contact, the Commission, affected wallet users and registered wallet-relying parties. [Article 5(1)] – informing relevant parties without undue delay about the re-establishment of the affected wallet solution including the following: – the date and time of remedy, – the date and time	Article 5(1); Article 7; Article 9(1);	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - procedures enabling notifications to single points of contact, the Commission, affected wallet users and registered wallet-relying parties; - rules for informing relevant parties without undue delay about re-establishment of the affected wallet solution; - required re-establishment information, including date and time of remedy, date and time of re-establishment, measures taken, residual impacts and mitigation measures for users; - procedures for providing clear,	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - notifications to single points of contact, the Commission, affected wallet users and registered wallet-relying parties; - records showing communication without undue delay about re-establishment of the affected wallet solution; - message content showing date and time of remedy, date and time of re-establishment, measures taken, residual impacts and mitigation measures for users; - withdrawal communication records showing clear, comprehensive and easily accessible information provided without undue delay

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		of re-establishment, – measures taken, – residual impacts and mitigation measures for users. [Article 7] – providing clear, comprehensive and easily accessible information about withdrawal of a wallet solution without undue delay and no later than 24 hours after withdrawal.			comprehensive and easily accessible information about withdrawal of a wallet solution without undue delay and no later than 24 hours after withdrawal; - channels, roles, approval paths, escalation and evidence retained for each notification or communication.	and no later than 24 hours after withdrawal; - timestamps, channels, approvals and escalation records supporting the notification and communication evidence.
REQ-847-05	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that re-establishing of the provision, activation and use of the affected wallet solution without undue delay including the following: 1) Issuance wallet units under a new version of the wallet solution, where necessary. 2) issuance of new wallet unit attestations to new or previously issued wallet units, provided that those wallet units meet the security requirements applicable after the breach or compromise has been remedied.	Article 6	WZ-03-01	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - procedures for re-establishing the provision, activation and use of the affected wallet solution without undue delay after the breach or compromise has been remedied; - issuance of Wallet Units under a new version of the wallet solution where necessary; - issuance of new Wallet Unit Attestations to new or previously issued Wallet Units only where those Wallet Units meet the security requirements applicable after the breach or compromise has been remedied; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence; - records showing re-establishment of provision, activation and use of the affected wallet solution without undue delay; - cases where Wallet Units were issued under a new version of the wallet solution where necessary; - evidence that new Wallet Unit Attestations were issued to new or previously issued Wallet Units only after confirming compliance with the security requirements applicable after remedy of the breach or compromise; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
REQ-847-06	Commission Implementing Regulation	Wallet Provider shall establish, implement and maintain procedures to	Article 7	WZ-03-01	The assessor reviews communication plan and policy documents. The documented arrangements should define:	The assessor interviews incident/operations roles and reviews recovery records to confirm that relevant parties were informed without

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2025/847	inform relevant parties without undue delay about the re- establishment of the affected wallet solution including the following: – the date and time of remedy, – the date and time of re-establishment, – measures taken, – residual impacts and mitigation measures for users.			- procedures to inform relevant parties without undue delay about the re-establishment of the affected wallet solution; - required communication content, including the date and time of remedy, the date and time of re-establishment, measures taken, residual impacts and mitigation measures for users; - roles, channels, approval paths and escalation rules for re-establishment communications; - records proving that relevant parties were informed without undue delay; - links between the communication, the breach or compromise assessment and the re-establishment decision.	undue delay after wallet solution re-establishment. recovery ticket or incident record; notification log or communication register; date and time of remedy; date and time of re-establishment; measures taken; residual impacts and user mitigation measures.
REQ-847-07	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall withdraw affected wallet solution if a security breach or compromise having led to the suspension of the provision and the use of a wallet solution is not remedied within three months after the date of suspension of the provision and the use of that wallet solution. .	Article 8(1)	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - conditions requiring withdrawal of the affected wallet solution where a security breach or compromise that led to suspension of provision and use is not remedied within three months after the date of suspension; - conditions triggering revocation of affected Wallet Unit Attestations or restriction of Wallet Unit provisioning; - controls preventing new attestations or new Wallet Units under the affected wallet solution where prohibited; - security criteria for allowing data portability during suspension or withdrawal; - records linking the remedy to the breach, compromise or withdrawal decision.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - records showing the suspension date, remediation status and whether the three-month remediation period expired; - withdrawal cases where the breach or compromise leading to suspension was not remedied within three months; - attestation-revocation records and status-service evidence for affected Wallet Units; - configuration or process controls blocking new attestations or Wallet Units where required; - data-portability cases reviewed against critical-asset security constraints; - user, CAB or supervisory communications associated with the remedy.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-847-08	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that withdrawal of the affected wallet solution and revocation of its validity without undue delay and no later than 72 hours after expiry of the three-month remediation period.	Article 8(1)	WZ-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed Wallet Provider. The documented controls should define: - conditions triggering revocation of affected Wallet Unit Attestations or restriction of Wallet Unit provisioning; - conditions and timing for withdrawal of the affected wallet solution and revocation of its validity without undue delay and no later than 72 hours after expiry of the three-month remediation period; - controls preventing new attestations or new Wallet Units under the affected wallet solution where prohibited; - security criteria for allowing data portability during suspension or withdrawal; - records linking the remedy to the breach, compromise or withdrawal decision.	The assessor tests selected revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - attestation-revocation records and status-service evidence for affected Wallet Units; - withdrawal and validity-revocation records showing action without undue delay and no later than 72 hours after expiry of the three-month remediation period; - configuration or process controls blocking new attestations or Wallet Units where required; - data-portability cases reviewed against critical-asset security constraints; - user, CAB or supervisory communications associated with the remedy.
REQ-847-09	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall maintain evidence and reporting capabilities enabling the Member State to use CIRAS operated by ENISA, or an equivalent agreed system, for information exchange with the Commission and single points of contact.	Article 10	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - evidence and reporting capabilities enabling the Member State to use CIRAS operated by ENISA, or an equivalent agreed system; - information-exchange content, formats, responsible roles and reporting workflows supporting communication with the Commission and single points of contact; - records, logs and evidence packages required for CIRAS or equivalent reporting; - availability, integrity and traceability controls for information provided to the Member State; - testing, exercises or procedural evidence	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - reporting procedures, templates, evidence packages or system outputs supporting Member State use of CIRAS or an equivalent agreed system; - records showing information exchange readiness with the Commission and single points of contact; - logs or demonstrations showing availability, integrity and traceability of reportable information; - exercise, test or incident records showing that the reporting capability can be used when required; - exceptions or gaps in CIRAS/equivalent

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					showing that reporting capabilities can be used when required.	reporting readiness and related corrective actions.
REQ-847-10	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall notify planned maintenance in advance to potentially affected wallet users, wallet-relying parties and relevant competent supervisory bodies where such maintenance may affect availability or operation of wallet-related services.	Annex, Point 2(a)	WZ-03-01	The assessor reviews notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - criteria for identifying planned maintenance that may affect availability or operation of wallet-related services; - advance notification procedures for potentially affected wallet users, wallet-relying parties and relevant competent supervisory bodies; - required notification content, timing, channels, roles and approval paths; - records proving that planned maintenance was notified in advance where required; - links between maintenance planning, service availability, user impact and supervisory communication.	The assessor reviews selected records. The evidence should show: - planned-maintenance records showing potential impact on availability or operation of wallet-related services; - advance notifications sent to potentially affected wallet users, wallet-relying parties and relevant competent supervisory bodies; - message content, channels, approval evidence and timestamps demonstrating advance notice; - cases where planned maintenance was not notified and the documented rationale; - evidence that maintenance communications were aligned with service-impact and continuity arrangements.
EP-01	REQ-1502-09; REQ-1502-10; REQ-1502-14; REQ-2690-09	Wallet Provider shall establish, operate, and maintain an information security management system (ISMS) that governs the implementation, monitoring and continual improvement of the controls set out in Sections 6.2 to 6.5 of this document. The ISMS shall adhere to proven standards or principles for the management and control of information security risks.	Alignment with international standards - ISO/IEC 27001:2022 cl. 4.1 -4.4 (context & scope), cl. 5.1-5.3 (leadership), cl. 6.1 -6.3 (planning), cl. 8.1 (operational planning), cl. 9.1 -	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider. The review should link the requirement to: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions, including controls set out in Sections 6.2 to 6.5 of this document; - evidence that the Wallet Provider establishes, operates and maintains an ISMS governing implementation, monitoring and continual improvement of those controls; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service;	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions; - records showing implementation, monitoring and continual improvement of controls set out in Sections 6.2 to 6.5 of this document; - evidence that the ISMS adheres to proven standards or principles for managing and controlling information security risks; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- adherence of the ISMS to proven standards or principles for the management and control of information security risks.	- examples of updates triggered by service changes, incidents, audit results or risk changes.
EP-02	REQ-1502-01	Wallet Provider shall be a public authority a budgetary economy institution or a legal entity recognised as such by the national law of the Republic of Poland. Wallet Provider shall have an established organisation and be fully operational in all parts relevant for the provision of the wallet-related services within the scope of this document.	Alignment with international standards - ISO/IEC 27001:2022 cl. 5.1 (leadership & commitment), cl. 7.1 (resources). | ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews legal-entity, financial-capacity and liability arrangements maintained by the assessed Wallet Provider. The documentation should include: - legal status, ownership or mandate to provide the assessed service, including evidence that the Wallet Provider is a public authority, a budgetary economy institution or a legal entity recognised as such by the national law of the Republic of Poland; - established organisation and full operational capability in all parts relevant for the provision of wallet-related services within the assessed scope; - financial-capacity evidence, insurance or liability arrangements required by the scheme or law; - responsibility for maintaining the evidence and updating it after significant changes; - links between financial or liability limits and user or relying-party information.	The assessor checks financial-capacity, insurance or liability evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - company, mandate, insurance, guarantee or financial-capacity documents, including evidence of public-authority status, budgetary-economy-institution status or legal-entity recognition under the national law of the Republic of Poland; - organisation, staffing, process and operational-readiness evidence showing that all service-relevant parts are established and fully operational; - validity dates, coverage limits and correspondence with the assessed certification scope; - updates after organisational or service changes; - records showing how limitations or liabilities are communicated where required.
EP-03	REQ-1502-02	Wallet Provider shall comply with all applicable legal, regulatory and contractual requirements in connection with the operation and delivery of the wallet-related services, including but not limited to requirements governing the types of information that may be collected, how identity proofing is conducted, what	Alignment with international standards - ISO/IEC 27001:2022 A.5.31 (legal, statutory, regulatory & contractual requirements); A.5.36 (compliance with policies and	WZ-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed Wallet Provider. The review should confirm that the documented process defines: - applicable legal, regulatory and contractual requirements connected with the operation and delivery of wallet-related services; - types of information that may be collected and the legal basis for collection; - requirements governing how identity proofing is conducted; - which records or information must be	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - record samples covering certification, assessment, vulnerability, incident or service evidence; - evidence that collected information matches applicable legal, regulatory and contractual requirements; - identity-proofing procedure samples showing compliance with applicable legal,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		information may be retained and for how long, and applicable data protection legislation including Regulation (EU) 2016/679.	standards). | ETSI EN 319 401 §7.4 -§7.8 (Compliance); EN 319 411 -1 §6.9.1 (Organisational); §6.8.15 (Compliance with applicable law). Additional standards and references - GDPR Article 5(1)(e) (storage limitation); GDPR Article 17 (right to erasure - termination plan shall include procedures for fulfilling user erasure requests upon service termination); ARF v2.8.0 §6 (wallet lifecycle termination and data portability requirements).		retained for certification, audit, incident or supervisory purposes; - retention period, including periods after certificate cancellation or expiry where applicable, and rules on what information may be retained and for how long; - applicable data protection legislation, including Regulation (EU) 2016/679.	scheme and contractual requirements; - storage location, access-control, integrity and retention metadata, including evidence that retained information and retention periods comply with applicable data protection legislation, including Regulation (EU) 2016/679; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended.
EP-04	REQ-1502-03	Wallet Provider shall be able to demonstrate its ability to assume the risk of liability for damages arising from the provision of the wallet-related services, providing the CAB with a	Alignment with international standards - ISO/IEC 27001:2022 cl. 5.1 (leadership commitment -	WZ-03-01	The assessor reviews legal-entity, financial-capacity and liability arrangements maintained by the assessed Wallet Provider. The documentation should include: - ability to assume the risk of liability for damages arising from the provision of wallet-related services;	The assessor checks financial-capacity, insurance or liability evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - formal statement of budgetary guarantees or proof of insurance coverage appropriate to

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		formal statement of budgetary guarantees or proof of insurance coverage appropriate to its legal form; Wallet Provider shall have sufficient financial resources, within the framework applicable to it as a state- owned budgetary unit (jednostka budżetowa) or a budgetary economy institution (instytucja gospodarki budżetowej), to ensure continued operations and service provision.	resources); cl. 7.1 (resources). | ETSI EN 319 401 §7.1 (Organisational security policy); EN 319 411-1 §6.9.1 (Organisational); §6.8.2 (Financial responsibility).		- formal statement of budgetary guarantees or proof of insurance coverage appropriate to the Wallet Provider's legal form and provided to the CAB; - sufficient financial resources, within the framework applicable to a state-owned budgetary unit or budgetary economy institution, to ensure continued operations and service provision; - coverage limits, exclusions and correspondence with the assessed certification scope; - responsibility for maintaining financial and liability evidence and updating it after significant changes.	the Wallet Provider's legal form; - evidence demonstrating ability to assume liability for damages arising from wallet-related services; - financial-resource evidence showing capacity for continued operations and service provision within the applicable public-sector or budgetary framework; - validity dates, coverage limits, exclusions and alignment with the assessed certification scope; - records showing CAB submission, management review and maintenance of liability and financial-capacity evidence.
EP-05		Where the electronic identification scheme is not constituted by national law, Wallet Provider shall have in place an effective termination plan for its services. The termination plan shall include: I. orderly discontinuation of service or continuation by another provider; II. the way relevant authorities and end users are informed , ensuring the electronic identification s cheme stakeers are notified at least three months before the planned cessation of a service provision; III. details on how records are to be protected, retained and destroyed in	ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity); cl. 8.1 (operational planning and control). | ETSI EN 319 401 §7.11 (Business continuity); EN 319 411-1 §6.4.9 (CA/RA termination).	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider. The documentation should define: - whether the electronic identification scheme is not constituted by national law and therefore requires an effective termination plan for Wallet Provider services; - orderly discontinuation of service or continuation by another provider; - procedures for informing relevant authorities and end users, including notification of electronic identification scheme stakeholders at least three months before the planned cessation of service provision; - which records or information must be retained for certification, audit, incident or supervisory purposes; - retention period, including periods after certificate cancellation or expiry where applicable;	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - approved termination plan where the electronic identification scheme is not constituted by national law; - evidence covering orderly service discontinuation or continuation by another provider; - notification templates, records or exercises showing relevant authorities, end users and electronic identification scheme stakeholders informed at least three months before planned cessation of service provision; - record samples covering certification, assessment, vulnerability, incident or service evidence; - storage location, access-control, integrity and retention metadata;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		compliance with the Trust Framework established under G-03. The termination plan shall cover foreseeable circumstances leading to a discontinuation of the service, including cessation by Wallet Provider and shut down by external authorities.			- integrity, confidentiality, access-control and retrieval controls.	- retrieval evidence for CAB or supervisory requests.
EP-06	REQ-1502-06; REQ-2981-12	Wallet Provider shall publish a service definition for the wallet-related services that includes all applicable terms, conditions, and fees, including any limitations of usage. The service definition shall include a privacy policy. In addition, Wallet Provider shall make publicly available, in a clear, comprehensive, and easily accessible manner, security information about the wallet solution, including at a minimum: I. any limitations on the use of the wallet solution; II. guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the wallet solution; III. the period during which security support will be	Alignment with international standards - ISO/IEC 27001:2022 A.5.36 (compliance with policies); A.5.31 (legal requirements). | ETSI EN 319 401 §7.3 (Classification and handling of information); EN 319 411 -1 §6.1 (Publication and repository responsibilities); §5.2 (CPS requirements); EN 319 411-2 §6.1 (Publication and repository responsibilities for QTSPs).	WZ-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - published service definition for wallet-related services, including all applicable terms, conditions, fees, limitations of usage and privacy policy; - publicly available security information made available in a clear, comprehensive and easily accessible manner; - published limitations on the use of the wallet solution; - guidance and recommendations for secure configuration, installation, deployment, operation and maintenance of the wallet solution; - published period during which security support will be offered to end users, including availability of cybersecurity-related updates; - contact information and accepted methods for receiving vulnerability information from end users and security researchers.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - published service definition, terms, conditions, fees, usage limitations and privacy policy; - public pages, repositories or user-facing notices showing security information made available clearly, comprehensively and accessibly; - published secure configuration, installation, deployment, operation and maintenance guidance; - published security-support period, including cybersecurity-update availability; - published contact information and accepted vulnerability-reporting methods; - published references to vulnerability repositories and cybersecurity advisories.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		offered to end users, as regards the availability of cybersecurity-related updates; IV. contact information and accepted methods for receiving vulnerability information from end users and security researchers; V. a reference to online repositories listing publicly disclosed vulnerabilities related to the wallet solution and to any relevant cybersecurity advisories.				
EP-07	REQ-1502-07	Wallet Provider shall have appropriate policies and procedures in place to ensure that interested parties and the Scheme Owner are informed in a timely and reliable fashion of any changes to the service definition, ensuring the Scheme Owner is notified at least one month before implementing any important change including changes to the terms, conditions, and privacy policy.	Alignment with international standards - ISO/IEC 27001:2022 A.5.36 (compliance with policies, rules, and standards); A.8.32 (change management). | ETSI EN 319 401 §7.3 (Information handling); EN 319 411 -1 §6.1 (Publication and repository responsibilities); §5.2 (CPS requirements).	WZ-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - which information must be public, user-facing or provided to relying parties; - ownership, approval and version-control rules for published content; - timeliness of updates after changes affecting users, relying parties or certification status, including policies and procedures ensuring that interested parties and the Scheme Owner are informed in a timely and reliable fashion of changes to the service definition; - controls ensuring that the Scheme Owner is notified at least one month before implementing any important change, including changes to terms, conditions and privacy policy; - evidence retained to show when information was published, changed or notified.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices; - change history, approval records and publication timestamps; - notification evidence showing timely and reliable communication of service-definition changes to interested parties and the Scheme Owner; - records showing Scheme Owner notification at least one month before important changes to terms, conditions or privacy policy; - comparison between published content and the assessed service configuration; - cases showing that outdated or inconsistent information was corrected.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-08	REQ-1502-08	Wallet Provider shall have appropriate policies and procedures in place to provide full and correct responses to requests for information from interested parties and competent authorities.	Alignment with international standards - ISO/IEC 27001:2022 A.5.36 (compliance with policies, rules, and standards). | ETSI EN 319 401 §7.3 (Classification and handling of information).	WZ-03-01	The assessor reviews public information, user communication and service-condition material maintained by the assessed Wallet Provider. The review should check: - which information must be public, user-facing or provided to relying parties; - policies and procedures for receiving, handling and responding to requests for information from interested parties and competent authorities; - controls ensuring that responses are full, correct, approved where required and consistent with current service information; - ownership, approval and version-control rules for published content; - timeliness of updates after changes affecting users, relying parties or certification status; - evidence retained to show when information was published or changed and how information requests were answered.	The assessor checks the published material, user-facing information and operational records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - current public pages, repositories, policy documents or user-facing notices; - sampled requests for information from interested parties and competent authorities and the responses provided; - evidence that responses were full, correct, timely and consistent with approved public or user-facing information; - change history, approval records and publication timestamps; - comparison between published content and the assessed service configuration; - cases showing that outdated or inconsistent information was corrected.
EP-09	REQ-2981-06	Wallet Provider shall notify the Scheme Owner (Ministry of Digital Affairs) and, through the established notification procedure, the CAB, without undue delay of any breach or compromise of the wallet solution or of the electronic identification scheme under which it is provided, that is likely to impact its conformity with the requirements of GP-03 or its subsidiary documents.	Alignment with international standards - ISO/IEC 27001:2022 A.5.24 (planning & preparation of IS incident management); A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Incident management); EN 319 411 -1 §6.4.8 (Compromise and disaster	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies, including notification to the Scheme Owner, the Ministry of Digital Affairs, and through the established notification procedure to the CAB; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data, including likely impact on conformity with GP-03 or its subsidiary documents; - timelines, roles and approval path for notification without undue delay;	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - incident or breach records from detection through classification and notification decision; - notifications sent and timestamps showing timeliness, including notifications to the Scheme Owner, the Ministry of Digital Affairs, and through the established notification procedure to the CAB; - evidence supporting impact on conformity, personal data or service integrity, including likely impact on conformity with GP-03 or its subsidiary documents; - cases where notification was not sent and the documented rationale.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).		- evidence retained for the decision to notify or not notify.	
EP-10	REQ-1502-17; REQ-2690-01; REQ-2690-02	Wallet Provider shall establish an information security policy for the wallet- related services. The policy shall: I. be appropriate for the purposes of providing the wallet-related services in scope of this document; II. set out information security objectives; III. include a commitment to satisfy the requirements of this document; IV. include a commitment to continual improvement of information security. The policy shall have been adopted by top management, be reviewed and, where appropriate, updated by top management at least annually and when significant incidents or significant changes to operations or risks occur.	Alignment with international standards - ISO/IEC 27001:2022 A.5.1 (policies for information security); A.5.2 (IS roles and responsibilities). | ETSI EN 319 401 §7.1 (Organisational security policy); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions, including an information security policy for wallet-related services appropriate to the assessed scope; - information security objectives, commitment to satisfy the requirements of this document and commitment to continual improvement of information security; - management approval, ownership and review cycle, including adoption by top management and review and, where appropriate, update by top management at least annually and when significant incidents or significant changes to operations or risks occur; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions, including the information security policy for wallet-related services adopted by top management; - evidence that the policy sets information security objectives, commits to satisfying this document's requirements and commits to continual improvement; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes, including annual top-management review and review after significant incidents or significant changes to operations or risks.
EP-11	REQ-2690-03; REQ-2690-04; REQ-2690-	Wallet Provider shall define and assign information security responsibilities and authorities to roles, in	Alignment with international standards - ISO/IEC	WZ-03-01	The assessor reviews segregation-of-duties arrangements maintained by the assessed Wallet Provider. The documentation should identify:	The assessor checks selected role assignments, access rights and approval workflows for the assessed Wallet Provider during the on-site Stage 2 assessment. The

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	05; REQ-2690-06; REQ-2690-07; REQ-2690-08	accordance with its operational needs, including the mandatory trusted roles of: Security Officers, System Administrators, System Operators, and System Auditors, and communicate them to top management. Wallet Provider shall ensure that: I. all personnel and contracted parties apply information security in accordance with the established policies; II. at least one person reports directly to top management on matters of information security; III. information security matters are covered by dedicated roles or, depending on the specific function, by duties carried out in addition to existing roles; IV. conflicting duties and conflicting areas of responsibility shall be segregated, where applicable, with clearly defined methods for managing them. Roles, responsibilities, and authorities shall be reviewed and, where appropriate, updated at planned intervals and when significant changes occur.	27001:2022 A.5.2 (IS roles & responsibilities); A.5.3 (segregation of duties). | ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-1 §6.4.4 (Personnel controls).		- assignment of information-security responsibilities and authorities to roles according to operational needs; - mandatory trusted roles, including Security Officers, System Administrators, System Operators and System Auditors; - communication of roles, responsibilities and authorities to top management; - requirements ensuring that all personnel and contracted parties apply information security in accordance with established policies; - direct reporting to top management by at least one person on information-security matters; - coverage of information-security matters by dedicated roles or duties added to existing roles.	evidence should include: - role descriptions, responsibility matrices and authority assignments for information security; - evidence for Security Officers, System Administrators, System Operators and System Auditors; - records showing communication of responsibilities and authorities to top management; - personnel and contracted-party evidence showing application of established information-security policies; - organisation charts or reporting records showing direct reporting to top management; - segregation-of-duties evidence, conflict analyses, approved exceptions and compensating controls.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-12	REQ-2690-09; REQ-2981-02	Wallet Provider shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of its information systems supporting the wallet-related services. Wallet Provider shall perform and document risk assessments and, based on the results, establish, implement, and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by the risk owner or by top management.	Alignment with international standards - ISO/IEC 27001:2022 A.5.7 (threat intelligence); cl. 6.1.2 (IS risk assessment); cl. 6.1.3 (IS risk treatment); cl. 8.2 -8.3 (operational risk assessment and treatment). | ETSI EN 319 401 §7.1 (Risk management); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider. The review should link the requirement to: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - risk management framework established and maintained to identify and address risks to information systems supporting wallet-related services; - documented risk assessments performed by the Wallet Provider; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance, including a risk treatment plan established, implemented and monitored based on risk assessment results; - acceptance of risk assessment results and residual risks by the risk owner or top management.	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - documented risk assessments covering information systems supporting wallet-related services; - risk treatment plan records showing implementation status, monitoring, owners and deadlines; - management acceptance of residual risks and overdue actions, including acceptance by the risk owner or top management; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.
EP-13	REQ-2690-10; REQ-2690-11; REQ-2690-36	As part of the risk management framework, Wallet Provider shall establish a risk assessment process for the identification, analysis, evaluation, and treatment of information security risks. The process shall, as a minimum: I. follow a recognised risk management methodology; II. establish and maintain risk assessment criteria; III. apply risk acceptance criteria that are consistent	Alignment with international standards - ISO/IEC 27001:2022 cl. 6.1.2 (IS risk assessment); cl. 8.2 (operational risk assessment). | ETSI EN 319 401 §7.1 (Risk management framework); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews policy documents, vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider. The review should identify: - recognised risk management methodology and maintained risk assessment criteria; - risk acceptance criteria consistent with assurance level High under CIR (EU) 2015/1502 and limits for acceptable residual risk; - identification and documentation of risks to information systems using an all-hazards approach; - mandatory use of the risk register in Annex I to CIR (EU) 2024/2981 and G-04, threat intelligence, vulnerability-management	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - risk methodology, risk assessment criteria and risk acceptance criteria for assurance level High; - risk assessment records using Annex I to CIR (EU) 2024/2981, G-04, threat intelligence, vulnerability-management outputs, third-party risks and single points of failure as inputs; - sampled risks showing threat, likelihood, impact, resulting risk level and treatment prioritisation;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		with the risk profile of assurance level High as defined in CIR (EU) 2015/1502, ensuring that residual risks do not exceed the level acceptable for the offered assurance level; IV. in line with an all-hazards approach, identify and document the risks posed to the security of information systems, taking into account the risks and threats listed in the risk register set out in Annex I to CIR (EU) 2024/2981 and in G-04, information collected through threat intelligence and vulnerability management procedures, risks from third parties and risks that could lead to disruptions in availability, integrity, authenticity and confidentiality, and the identification of single points of failure; V. evaluate the risks based on the established risk assessment criteria, including threat, likelihood, impact and the resulting risk level; VI. identify and prioritise appropriate risk treatment options and controls, where the chosen risk treatment is documented in a risk			outputs, third-party risks, risks to availability, integrity, authenticity and confidentiality, and single points of failure; - risk evaluation based on threat, likelihood, impact and resulting risk level; - identification and prioritisation of risk treatment options and controls documented in a risk treatment plan.	- risk treatment plan records with controls, timelines, owners and implementation status; - monitoring evidence for risk treatment implementation; - effectiveness-assessment records for implemented treatment measures.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		treatment plan; VII. set out timelines and identify responsibility for the implementation of the risk treatment plan; VIII. continuously monitor the implementation of the risk treatment plan; IX. assess the effectiveness of the risk treatment measures implemented and formally accept residual risks, ensuring that they remain within the limits set out in point (c).				
EP-14	REQ-2981-01	Wallet Provider shall complement the scheme - level risk assessment maintained by the Ministry of Digital Affairs with an assessment of risks and threats specific to its own implementation of the wallet platform. Wallet Provider shall use the risk register set out in Annex I to CIR (EU) 2024/2981 and based on the template contained in G-04 as mandatory inputs and identify any additional risks and threats arising from the specific architecture, operational environment, and supply chain of the platform. Wallet Provider shall propose appropriate treatment measures for all	Alignment with international standards - ISO/IEC 27001:2022 cl. 6.1.2 (IS risk assessment); cl. 8.2 (operational); A.5.7 (threat intelligence). | ETSI EN 319 401 §7.1 (Risk management); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - scope of certification and mapping to Wallet, PID or eID scheme functions; - responsibilities for maintaining evidence, reporting changes and managing recertification; - links between certification obligations, risk register and continuous-compliance activities, including the Wallet Provider's complement to the scheme-level risk assessment maintained by the Ministry of Digital Affairs; - implementation-specific risks and threats arising from the specific architecture, operational environment and supply chain of the wallet platform; - mandatory use of the risk register set out in Annex I to CIR (EU) 2024/2981 and the template contained in G-04; - appropriate treatment measures for all identified risks and threats.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, certification scope, assessment reports or action plans; - implementation-specific risk assessment complementing the Ministry of Digital Affairs scheme-level risk assessment; - evidence that Annex I to CIR (EU) 2024/2981 and G-04 were used as mandatory inputs; - risks and threats specific to architecture, operational environment and supply chain, with proposed treatment measures; - records of changes, recertification decisions or continuous-compliance checks; - notifications sent to the CAB, supervisory body or scheme owner where required, including evidence that the implementation-specific risk assessment was shared with the CAB for evaluation.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		identified risks and threats and share the implementation - specific risk assessment with the CAB for evaluation.				
EP-15	REQ-2690-12	Wallet Provider shall review and, where appropriate, update the risk assessment results and the risk treatment plans at planned intervals, at least annually, and when significant changes to operations or risks occur.	Alignment with international standards - ISO/IEC 27001:2022 cl. 6.1.2 (risk assessment update); cl. 8.2 (operational review); cl. 9.3 (management review). | ETSI EN 319 401 §7.1 (Review of security policy); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-01	The assessor reviews change-management arrangements maintained by the assessed Wallet Provider. The documentation should explain: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment results and risk treatment plans at planned intervals, at least annually, and after incidents, changes, vulnerabilities or supplier changes, including significant changes to operations or risks.	The assessor checks selected changes to relevant systems or services for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - records showing review and, where appropriate, update of risk assessment results and risk treatment plans at planned intervals, at least annually, and when significant changes to operations or risks occur; - operational controls or projects implementing selected risk-treatment decisions.
EP-16	REQ-1502-04; REQ-2690-24	Wallet Provider shall remain responsible for the fulfilment of any commitments outsourced to another organisation, and for compliance with the Trust Framework established by the Ministry of Digital Affairs under G-03, as if Wallet Provider had performed the duties itself.	Alignment with international standards - ISO/IEC 27001:2022 A.5.19 (IS in supplier relationships); A.5.20 (addressing IS within supplier agreements). | ETSI EN 319 401 §7.14 (Supply	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements, including clauses preserving the Wallet Provider's responsibility for outsourced commitments and compliance with the Trust	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including responsibility clauses for outsourced commitments and Trust Framework G-03 compliance; - risk assessments, onboarding approvals and periodic review records; - evidence that the Wallet Provider monitors and accepts responsibility for outsourced duties as if performed by the Wallet Provider itself;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			chain security); EN 319 411 -1 §6.8.6 (Representations and warranties); §6.9.1 (Organisational).		Framework established by the Ministry of Digital Affairs under G-03 as if the Wallet Provider had performed the duties itself; - governance controls ensuring that outsourcing does not transfer or reduce the Wallet Provider's accountability for Trust Framework compliance; - ongoing monitoring of supplier performance, security issues and changes.	- supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.
EP-17	REQ-1502-04; REQ-2690-24	Where Wallet Provider outsources operational functions to third parties in connection with the wallet-related services, Wallet Provider shall ensure that contractual arrangements with such third parties include, as appropriate: I. information security requirements applicable to the third party, consistent with the requirements of this document including an explicit requirement for the third party to acknowledge and confirm in writing (in documentary form) that they have read and understood Wallet Provider's relevant security policies; II. requirements regarding awareness, competence and training of the third party's personnel; III. requirements regarding screening of the third party's personnel; IV. an obligation on the third	Alignment with international standards - ISO/IEC 27001:2022 A.5.19 (IS in supplier relationships); A.5.20 (addressing IS within supplier agreements). | ETSI EN 319 401 §7.14 (Supply chain security); EN 319 411 -1 §6.8.6 (Representations and warranties); §6.9.1 (Organisational).	WZ-03-01	The assessor reviews supplier management documentation. The documented arrangements should define: - information security requirements applicable to the third party and consistent with this document; - documentary acknowledgement that the third party has read and understood the Wallet Provider's relevant security policies; - requirements for awareness, competence and training of the third party's personnel; - requirements for screening of the third party's personnel; - obligation to notify the Wallet Provider without undue delay of incidents presenting a risk to the security of the Wallet Provider's information systems; - right to audit or receive audit reports.	The assessor reviews contractis, SLAs and supplier interaction records. The evidence should show: - contracts, security annexes and acknowledgements showing third-party acceptance of applicable security requirements and relevant Wallet Provider policies; - evidence of awareness, competence, training and screening requirements for third-party personnel; - incident-notification clauses and sampled incident notifications from third parties where applicable; - audit-right clauses or received audit reports; - vulnerability-handling, subcontracting and termination clauses; - retrieval and disposal evidence for information at contract termination where applicable.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		party to notify Wallet Provider without undue delay of incidents presenting a risk to the security of Wallet Provider 's information systems; V. the right to audit or to receive audit reports; VI. an obligation on the third party to handle vulnerabilities presenting a risk to Wallet Provider; VII. requirements regarding subcontracting by the third party; VIII. obligations at the termination of the contract, including retrieval and disposal of information.				
EP-18	REQ-2690-24	Wallet Provider shall establish, implement, and apply a supply chain security policy governing its relations with its direct suppliers and service providers involved in the provision of the wallet-related services, to mitigate identified risks to the security of information systems. The policy shall include criteria for the selection and contracting of suppliers and service providers, taking into account their information security practices, their ability to meet information security specifications set	Alignment with international standards - ISO/IEC 27001:2022 A.5.21 (managing IS in ICT supply chain); A.5.22 (monitoring and review of supplier services). | ETSI EN 319 401 §7.14 (Supply chain security policy); EN 319 411-1 §6.8.6 (Representations and warranties);	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - policy governing relations with direct suppliers and service providers involved in wallet-related services; - link between the policy and mitigation of identified risks to the security of information systems; - criteria for selection and contracting of suppliers and service providers; - assessment of suppliers' information security practices and ability to meet the Wallet Provider's information security specifications; - assessment of overall quality and resilience of provided products and services; - criteria for diversifying sources of supply and limiting vendor lock-in where applicable.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - approved supply chain security policy governing direct suppliers and service providers involved in wallet-related services; - supplier selection and contracting records showing application of information security, quality, resilience, diversification and vendor lock-in criteria; - risk assessments showing mitigation of supply-chain risks to information systems; - contracts, SLA and security annexes aligned with the supply chain security policy; - monitoring, review or decision records showing that the policy is implemented and applied in practice.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		by Wallet Provider, the overall quality and resilience of provided products and services, and the ability of Wallet Provider to diversify sources of supply and limit vendor lock-in, where applicable.	§6.9.1 (Organisational).			
EP-19	REQ-2690-25	Wallet Provider shall maintain and keep up to date a registry of its direct suppliers and service providers involved in the wallet-related services, including contact points and a list of ICT products, ICT services and ICT processes provided.	Alignment with international standards - ISO/IEC 27001:2022 A.5.9 (inventory of information and other associated assets); A.5.21 (ICT supply chain). | ETSI EN 319 401 §7.3 (Asset management); EN 319 411 -1 §6.9.1 (Organisational); §6.8.6 (Representations and warranties).	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - supplier inventory or registry of direct suppliers and service providers involved in wallet-related services, maintained and kept up to date, including contact points and a list of ICT products, ICT services and ICT processes provided; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current registry of direct suppliers and service providers involved in wallet-related services, including contact points and lists of ICT products, ICT services and ICT processes provided; - contracts, SLA and security annexes for critical suppliers; - risk assessments, onboarding approvals and periodic review records; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes and in the supplier registry.
EP-20	REQ-2690-24	Wallet Provider shall review its supply chain security policy and monitor, evaluate and, where necessary, act upon changes in the information security practices of its suppliers and service		WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes;	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - records showing review of the supply chain

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		providers, at planned intervals, and when significant changes to operations or risks occur and when significant incidents related to the provision of ICT services or having impact on the security of ICT products acquired from suppliers occur.			- identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - review of the supply chain security policy at planned intervals and when significant changes to operations or risks occur; - monitoring, evaluation and, where necessary, action upon changes in the information security practices of suppliers and service providers; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes, including significant incidents related to ICT service provision or impacting the security of ICT products acquired from suppliers.	security policy at planned intervals and after significant changes to operations or risks; - supplier and service-provider monitoring records showing evaluation of changes in information security practices and resulting actions where necessary; - management acceptance of residual risks and overdue actions; - evidence that significant incidents related to ICT services or affecting ICT products acquired from suppliers triggered review, evaluation or corrective action; - operational controls or projects implementing selected risk-treatment decisions.
EP-21	REQ-2690-54	Wallet Provider shall develop and maintain a complete, accurate, up-to-date, and consistent inventory of its assets supporting the wallet-related services, recorded in a traceable manner. The inventory shall include the list of operations and services and their descriptions, and the list of information systems and other associated assets. The inventory shall enable identification of relevant relationships between operations, services, information systems and associated assets supporting the wallet	Alignment with international standards - ISO/IEC 27001:2022 A.5.9 (inventory of information and other associated assets); A.5.10 (acceptable use of assets). | ETSI EN 319 401 §7.3 (Asset management); EN 319 411 -1 §6.4.5 (Audit logging procedures); §6.4.6 (Records archival).	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function, including a complete, accurate, up-to-date, consistent and traceable inventory of assets supporting wallet-related services; - inventory content covering the list of operations and services and their descriptions, and the list of information systems and other associated assets; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights,	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - inventory entries compared with observed systems, repositories or configuration records, including evidence that the inventory is complete, accurate, up to date, consistent and traceable; - records showing operations and services, their descriptions, information systems and associated assets supporting wallet-related services; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		related services. Where information on such assets is maintained in more than one record, repository or document, Wallet Provider shall ensure that such information remains consistent and traceable across those records.			logging and continuity arrangements, including relevant relationships between operations, services, information systems and associated assets; - controls ensuring consistency and traceability where asset information is maintained in more than one record, repository or document.	- cross-checks between multiple records, repositories or documents showing consistency, traceability and relationships between operations, services, information systems and associated assets.
EP-22	REQ-2690-51	Wallet Provider shall define and apply an information classification scheme for all assets, including information, commensurate with the level of protection required. The classification shall be based on confidentiality, integrity, authenticity, and availability requirements, taking into account the sensitivity, criticality, risk and business value of the assets and shall be aligned with the delivery and recovery objectives in the business continuity and disaster recovery plan. The classification assigned to assets and information shall be recorded or referenced in a manner consistent with the asset inventory maintained under EP- 21. Wallet Provider shall review the classification levels at planned intervals and	Alignment with international standards - ISO/IEC 27001:2022 A.5.12 (classification of information); A.5.13 (labelling of information). | ETSI EN 319 401 §7.3 (Classification and handling of information); EN 319 411-1 §6.4.6 (Records archival).	WZ-03-01	The assessor reviews security system documentation. The documentation should define: - classification scheme for all assets, including information, commensurate with the required level of protection; - classification criteria based on confidentiality, integrity, authenticity and availability requirements; - consideration of sensitivity, criticality, risk and business value of assets; - alignment of classifications with delivery and recovery objectives in the business continuity and disaster recovery plan; - recording or referencing of assigned classifications consistently with the asset inventory maintained under EP-21; - planned review and update of classification levels where appropriate.	The assessor checks security system documentationt. The sample should include: - classification scheme and classification criteria for assets and information; - sampled assets and information showing assigned classification levels based on confidentiality, integrity, authenticity, availability, sensitivity, criticality, risk and business value; - evidence that classifications are recorded or referenced consistently with the EP-21 asset inventory; - evidence that classification levels align with business continuity and disaster recovery delivery and recovery objectives; - records of planned reviews and updates of classification levels.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		update them where appropriate.				
EP-23	REQ-2690-52	Wallet Provider shall establish, implement, and apply a policy for the proper handling of assets, covering their entire life cycle including acquisition, use, storage, transportation, and disposal. The policy shall provide rules on safe use, safe storage, safe transport, irretrievable deletion and destruction of assets, and secure transfer in accordance with the type and classification of the asset. The policy shall be communicated to anyone who uses or handles assets. Wallet Provider shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations occur.	Alignment with international standards - ISO/IEC 27001:2022 A.5.10 (acceptable use of assets); A.8.10 (information deletion); A.7.7 (clear desk and clear screen policy). | ETSI EN 319 401 §7.3 (Information handling); EN 319 411-1 §6.4.5 (Audit logging procedures); §6.5.1 (Key pair generation and installation). 5.2.6 Access Control	WZ-03-01	The assessor reviews policy documents. The documented arrangements should define: - policy covering the entire asset life cycle, including acquisition, use, storage, transportation and disposal; - rules for safe use, safe storage, safe transport, irretrievable deletion and destruction of assets; - secure transfer rules according to asset type and classification; - communication of the policy to anyone who uses or handles assets; - review and, where appropriate, update of the policy at planned intervals and when significant incidents or significant changes to operations occur.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved asset-handling policy covering acquisition, use, storage, transportation and disposal; - samples showing safe use, safe storage, safe transport, secure transfer, irretrievable deletion and destruction according to asset type and classification; - evidence that the policy was communicated to persons using or handling assets; - records of planned reviews and updates after significant incidents or significant changes to operations; - exceptions, corrective actions or deviations from asset-handling rules.
EP-24	REQ-1502-16; REQ-2690-44	Wallet Provider shall establish, document, and implement logical and physical access control policies for access to its information systems supporting the wallet-related services, based on business and information	Alignment with international standards - ISO/IEC 27001:2022 A.5.15 (access control); A.5.16 (identity management);	WZ-03-01	The assessor reviews policy and acces management documentation. The documentation should cover: - access control policies for information systems supporting wallet-related services, based on business and information security requirements; - logical and physical access by persons, including personnel, visitors, suppliers and	The assessor checks selected records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - approved logical and physical access control policies for information systems supporting wallet-related services; - samples of personnel, visitor, supplier and service-provider access records;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		security requirements. The policies shall address access by persons (personnel, visitors, external parties such as suppliers and service providers) and access by information systems. Access shall only be granted to users and processes that have been adequately authenticated.	A.5.17 (authentication information). | ETSI EN 319 401 §7.4- §7.8 (Access control); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).		service providers; - access by information systems and processes; - controls ensuring that access is granted only to users and processes that have been adequately authenticated; - approval, review, monitoring and enforcement arrangements for logical and physical access controls.	- samples of information-system or process access records; - evidence that access was granted only after adequate authentication of users or processes; - access approvals, reviews, logs, denied-access cases and corrective actions.
EP-25	REQ-2690-45	Wallet Provider shall provision, modify, revoke and document access rights in accordance with its access control policy. Access rights shall be assigned and revoked based on the principles of need-to-know, least privilege and segregation of duties. Wallet Provider shall maintain a register of access rights granted and apply logging to the management of access rights. Access rights shall be reviewed at planned intervals.	Alignment with international standards - ISO/IEC 27001:2022 A.5.18 (access rights); A.8.2 (privileged access rights). | ETSI EN 319 401 §7.4 -§7.8 (Access management); EN 319 411-1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls).	WZ-03-01	The assessor reviews segregation-of-duties arrangements maintained by the assessed Wallet Provider. The documentation should identify: - provisioning, modification, revocation and documentation of access rights in accordance with the access control policy; - assignment and revocation of access rights based on need-to-know, least privilege and segregation of duties; - register of access rights granted to users, processes and privileged roles; - logging of access-rights management activities; - planned review of access rights and remediation of excessive, obsolete or conflicting access.	The assessor checks selected role assignments, access rights and approval workflows for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - provisioning, modification and revocation records for sampled access rights; - evidence that access rights were assigned and revoked according to need-to-know, least privilege and segregation of duties; - current register of granted access rights compared with users, roles, processes and systems; - logs of access-rights management activities and related approvals; - planned access-rights review records and evidence of remediation for excessive, obsolete or conflicting access.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-26	REQ-1502-20; REQ-2690-15; REQ-847-01	Wallet Provider shall establish and implement an incident management policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing, or responding to, recovering from, documenting and reporting incidents in a timely manner. The policy shall be coherent with the business continuity and disaster recovery plan referred to in EP-35 and shall include: I. a categorisation scheme for incidents that incorporate specific thresholds specified by the wallet provider under CIR (EU) 2025/847; II. effective communication plans, including for escalation and reporting in line with the legal and contractual obligations of Wallet Provider, including obligations under the Polish Cybersecurity Act, CIR (EU) 2024/2981 and CIR (EU) 2025/847; III. assignment of roles for incident detection and response to competent personnel; IV. documented information to be used during incident detection	Alignment with international standards - ISO/IEC 27001:2022 A.5.24 (planning & preparation of IS incident management); A.5.25 (assessment and decision on IS events); A.5.26 (response to IS incidents); A.5.27 (learning from IS incidents). | ETSI EN 319 401 §7.9 (Incident management); EN 319 411 -1 §6.4.8 (Compromise and disaster recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services).	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - roles, responsibilities and procedures for detecting, analysing, containing, responding to, recovering from, documenting and reporting incidents in a timely manner; - coherence with the business continuity and disaster recovery plan referred to in EP-35; - incident categorisation scheme incorporating thresholds specified by the Wallet Provider under CIR (EU) 2025/847; - communication plans, escalation and reporting rules aligned with legal and contractual obligations, including the Polish Cybersecurity Act, CIR (EU) 2024/2981 and CIR (EU) 2025/847; - assignment of incident detection and response roles to competent personnel; - documented information used during incident detection and response, including incident response plans, escalation procedures, contact lists and templates.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved incident management policy and procedures covering detection, analysis, containment, response, recovery, documentation and reporting; - incident categorisation criteria and thresholds specified under CIR (EU) 2025/847; - samples of incident response plans, escalation procedures, contact lists and templates used in operations; - records showing assignment of incident detection and response roles to competent personnel; - communication, escalation and reporting evidence aligned with applicable legal and contractual obligations; - evidence of coordination with vulnerability management, change management and business continuity arrangements.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		and response, such as incident response plans, escalation procedures, contact lists and templates. The policy shall also define how incident handling activities are coordinated with related security procedures, including vulnerability management, change management and business continuity arrangements, to the extent necessary for incident analysis, containment, recovery, documentation and post-incident review. The roles, responsibilities and procedures shall be evaluated and reviewed, and where appropriate updated, at planned intervals and after significant incidents.				
EP-27	REQ-2690-17,REQ-847-4	Wallet Provider shall put in place a mechanism allowing its personnel, suppliers, and customers to report information security events. Wallet Provider shall ensure that all personnel are explicitly informed of the rules and procedures for reporting incidents Wallet Provider shall, where appropriate, communicate the event reporting mechanism to its	Alignment with international standards - ISO/IEC 27001:2022 A.5.25 (assessment & decision on IS events); A.6.8 (reporting of IS events). | ETSI EN 319 401 §7.9 (Reporting of incidents); EN	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - detection sources, classification criteria and escalation paths, including a mechanism allowing personnel, suppliers and customers to report information security events; - rules and procedures for reporting incidents and evidence that all personnel are explicitly informed of them; - communication of the event reporting mechanism to suppliers and customers where	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment and closure, including events reported by personnel, suppliers or customers; - evidence that personnel were explicitly informed of incident-reporting rules and procedures; - records showing communication of the reporting mechanism to suppliers and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		suppliers and customers, and shall regularly train personnel on its use.	319 411-1 §6.4.8 (Compromise and disaster recovery).		appropriate; - regular personnel training on the use of the event reporting mechanism; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps.	customers where appropriate; - personnel training records for the use of the event reporting mechanism; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident.
EP-28	REQ-2690-18	Wallet Provider shall assess information security events to determine whether they constitute incidents and, if so, determine their nature and severity. The assessment shall be based on predefined criteria and shall include a triage for prioritisation. Wallet Provider shall assess the existence of recurring incidents on a regular basis.	Alignment with international standards - ISO/IEC 27001:2022 A.5.25 (assessment & decision on IS events). | ETSI EN 319 401 §7.9 (Incident classification); EN 319 411 -1 §6.4.8 (Compromise and disaster recovery).	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - detection sources, classification criteria and escalation paths, including predefined criteria for assessing whether information security events constitute incidents and determining their nature and severity; - triage rules for incident prioritisation; - regular assessment of recurring incidents; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps; - links with vulnerability management, risk assessment, change management and user communication.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment and closure, including assessment against predefined criteria to determine whether the event constituted an incident and to determine its nature and severity; - evidence of triage for prioritisation; - records showing regular assessment of recurring incidents; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, lessons learned and updates to controls, risks or procedures.
EP-29	REQ-2690-19	Wallet Provider shall respond to incidents in accordance with documented procedures, including containment, eradication, and recovery stages. Wallet Provider shall log incident response	Alignment with international standards - ISO/IEC 27001:2022 A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Handling of	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - events from detection through triage, classification, containment, eradication, recovery and closure; - evidence that incident response followed

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		activities and record evidence.	incidents); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).		authorities where applicable; - evidence collection, containment, recovery and post-incident review steps, including documented procedures for incident response with containment, eradication and recovery stages; - logging of incident response activities and recording of evidence; - links with vulnerability management, risk assessment, change management and user communication.	documented procedures; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident, including logs of incident response activities; - post-incident actions, lessons learned and updates to controls, risks or procedures.
EP-30	REQ-2690-20	Wallet Provider shall, where appropriate, conduct post-incident reviews after recovery from incidents. The reviews shall identify, where possible, the root cause of the incident and result in documented lessons learned. Wallet Provider shall ensure that post-incident reviews contribute to improving its approach to information security, risk treatment, and incident management procedures.	Alignment with international standards - ISO/IEC 27001:2022 A.5.27 (learning from IS incidents). | ETSI EN 319 401 §7.9 (Lessons learned from incidents); EN 319 411 -1 §6.4.8 (Compromise and disaster recovery). Additional standards and references - GDPR Article 33 (notification of personal data breach to supervisory authority within 72 hours); GDPR Article 34	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes, including post-incident reviews after recovery, root-cause identification where possible, documented lessons learned and improvements to information security, risk treatment and incident management procedures.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - post-incident review records after recovery, including root-cause identification where possible and documented lessons learned; - evidence that post-incident reviews contributed to improvements in information security, risk treatment and incident management procedures; - operational controls or projects implementing selected risk-treatment decisions.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			(communication of breach to data subjects); CRA Annex I Part II §5(1) (handling and coordinated disclosure of vulnerabilities). Additional standards and references - GDPR Article 33 (notification of personal data breach to supervisory authority within 72 hours of becoming aware); GDPR Article 34 (communication of the breach to the affected data subjects without undue delay where the breach is likely to result in high risk); CRA (Regulation (EU) 2024/2847) Annex I Part II §5(1) (handling and disclosure of vulnerabilities, including coordinated			

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			disclosure obligations).			
EP-31	REQ-2690-35; REQ-2981-07; REQ-2981-10	Wallet Provider shall establish, maintain, and operate a vulnerability management process. The process shall include, as a minimum: I. procedures for the identification of vulnerabilities in the Wallet Provider information systems, including through monitoring of appropriate channels such as announcements of CSIRTs (e.g., CERT Polska), competent authorities, and information provided by suppliers; II. procedures for the evaluation and prioritisation of identified vulnerabilities based on their severity and potential impact on the wallet solution and related services; III. procedures for associating identified vulnerabilities, where applicable, with the affected information systems, software components or other assets supporting the wallet-related services, and with the corresponding treatment decision, remediation action or mitigation plan; IV.	Alignment with international standards - ISO/IEC 27001:2022 A.8.8 (management of technical vulnerabilities). | ETSI EN 319 401 §7.9 (Vulnerability management); EN 319 411 - 1 §6.4.8 (Compromise and disaster recovery).	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - sources of vulnerability information, including public, supplier, testing and researcher reports, CSIRT announcements, competent-authority information and supplier information; - criteria for impact analysis, severity, registration and disclosure, including evaluation and prioritisation based on severity and potential impact on the wallet solution and related services; - association of identified vulnerabilities with affected information systems, software components or other assets and with the corresponding treatment decision, remediation action or mitigation plan; - remediation, mitigation, retesting and closure rules, including timeframes for critical vulnerabilities and verification that remediation or mitigation was effectively applied; - vulnerability scans on public and private IP addresses at least once per quarter where appropriate, with recorded results; - alignment with change management, patch management, risk management and incident management procedures.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - intake, triage and impact-analysis evidence, including sources such as CSIRTs, competent authorities and suppliers; - evidence of prioritisation by severity and potential impact on the wallet solution and related services; - records linking vulnerabilities to affected information systems, software components or other assets and to treatment decisions, remediation actions or mitigation plans; - remediation, mitigation or risk-acceptance records, including timely handling of critical vulnerabilities within defined timeframes; - verification evidence that remediation or mitigation measures were effectively applied; - quarterly vulnerability scan evidence for public and private IP addresses where appropriate.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		procedures for the timely remediation or mitigation of vulnerabilities, ensuring that critical vulnerabilities are addressed without undue delay within timeframes defined in the vulnerability management policy; V. procedures for the verification that remediation or mitigation measures have been effectively applied; VI. where appropriate, performance of vulnerability scans on public and private IP addresses at least once per quarter with evidence of the results recorded. The vulnerability management process shall be aligned with Wallet Provider 's change management, patch management, risk management and incident management procedures, and shall consider the procedures set out in EN ISO/IEC 30111:2019 and the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act).				
EP-32	REQ-2981-08; REQ-2981-09	Wallet Provider shall prepare a vulnerability impact analysis report for any vulnerability that	Alignment with international standards - ISO/IEC	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		affects the software components of the wallet solution and submit it to the Scheme Owner without undue delay. The report shall include: I. the impact of vulnerability on the certified wallet solution; II. possible risks associated with the proximity or likelihood of an attack; III. whether the vulnerability can be remedied using available means; IV. where the vulnerability can be remedied, possible ways to remedy it. The Wallet Provider, acting together with the Scheme Owner, shall determine, based on defined criteria established in accordance with this document, whether notification to the CAB is required.	27001:2022 A.8.8 (technical vulnerability management); A.5.26 (response to IS incidents). | ETSI EN 319 401 §7.9 (Vulnerability analysis); EN 319 411-1 §6.4.8 (Compromise and disaster recovery). Additional standards and references - CRA (Regulation (EU) 2024/2847) Annex I Part I §2(i) (policy on coordinated vulnerability disclosure as essential cybersecurity requirement); ARF v2.8.0 §6.4 (vulnerability management for wallet solution components). Additional standards and references - CRA (Regulation (EU) 2024/2847) Annex I Part I		whether the documentation covers: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure, including preparation of a vulnerability impact analysis report for any vulnerability affecting software components of the wallet solution; - report content covering impact on the certified wallet solution, risks associated with proximity or likelihood of an attack, whether the vulnerability can be remedied using available means and possible ways to remedy it; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met, including submission of the report to the Scheme Owner without undue delay and joint determination with the Scheme Owner, based on defined criteria, whether CAB notification is required.	include: - intake, triage and impact-analysis evidence; - reports for vulnerabilities affecting software components of the wallet solution, covering impact on the certified wallet solution, proximity or likelihood of attack, remediability and possible remedies; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records, including evidence that reports were submitted to the Scheme Owner without undue delay and that the Wallet Provider and Scheme Owner determined, based on defined criteria, whether CAB notification was required.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			§2(i) (essential cybersecurity requirement to have a policy on coordinated vulnerability disclosure); ARF v2.8.0 §6.4 (vulnerability management requirements specific to wallet solution components, including wallet instance and WSCD firmware).			
EP-33	REQ-2981-11	Wallet Provider shall disclose and register any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in	Alignment with international standards - ISO/IEC 27001:2022 A.8.8 (technical vulnerability management). | ETSI EN 319 401 §7.9 (Vulnerability disclosure); EN 319 411 - 2 §6.4.8 (Compromise and disclosure for qualified services).	WZ-03-01	The assessor reviews vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider. The review should identify: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure, including disclosure and registration of any officially known and remediated vulnerability in the wallet solution in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981; - procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy; - remediation, mitigation, retesting and closure rules;	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - intake, triage and impact-analysis evidence; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities, including disclosure and registration in one of the online repositories referred to in Annex V to CIR (EU) 2024/2981; - evidence that vulnerability disclosure followed the applicable national coordinated vulnerability disclosure policy; - notifications to CAB or certification body and related change or risk records.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- notification to CAB or certification body where vulnerability impact criteria are met.	
EP-34	REQ-1502-05; REQ-2690-21	Wallet Provider shall determine its requirements for the continuity of the wallet- related services in adverse situations. Wallet Provider shall identify the critical services and the information systems supporting those services, assess the potential impact of disruptions, and establish recovery objectives, including recovery time objectives and recovery point objectives, for those critical services ensuring sufficient availability by providing at least partial redundancy for network systems, facilities, communication channels, and personnel with necessary competence.	Alignment with international standards - ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity); cl. 8.1 (operational planning). | ETSI EN 319 401 §7.11 (Business continuity); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); §6.4.9 (CA/RA termination); EN 319 411 -2 §6.4.8 (Compromise and disaster recovery for qualified services).	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider. The documentation should define: - requirements for continuity of wallet-related services in adverse situations; - critical processes, dependencies and recovery objectives for the assessed service, including identified critical services and information systems supporting those services; - assessment of the potential impact of disruptions and establishment of recovery objectives, including recovery time objectives and recovery point objectives; - backup scope, protection, restoration testing and retention rules where applicable; - availability measures providing at least partial redundancy for network systems, facilities, communication channels and personnel with necessary competence; - crisis roles, communications, escalation and decision-making criteria.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - exercise reports, backup jobs, restoration tests or failover tests relevant to the service; - evidence identifying critical wallet-related services and supporting information systems; - business impact or disruption-impact evidence and recovery objectives, including RTO and RPO for critical services; - sampled continuity actions after incidents, outages or supplier failures; - evidence of at least partial redundancy for network systems, facilities, communication channels and personnel with necessary competence; - evidence that recovery objectives and communications were met or deviations were addressed.
EP-35	REQ-1502-05; REQ-2690-21	Wallet Provider shall establish and maintain a business continuity and disaster recovery plans to be applied in the case of incidents. The plan shall be		WZ-03-01	The assessor reviews business continuity plans. The documented arrangements should define: - plans to be applied in the case of incidents and based on risk assessment results and business impact analysis;	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved business continuity and disaster

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		based on the results of risk assessments and a business impact analysis, and shall include, where appropriate: I. purpose, scope and audience; II. roles and responsibilities; III. key contacts and communication channels; IV. conditions for plan activation and deactivation; V. order of recovery for operations; VI. recovery plans for specific operations, including recovery objectives; VII. required resources, including backups and redundancies; VIII. restoring and resuming activities from temporary measures. The plan shall be evaluated, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes.			- purpose, scope and audience of the plans; - roles and responsibilities; - key contacts and communication channels; - conditions for plan activation and deactivation; - order of recovery for operations.	recovery plans applied in incident scenarios; - evidence that the plans are based on risk assessments and business impact analysis; - plan content covering purpose, scope, audience, roles, responsibilities, key contacts, communication channels, activation and deactivation conditions, recovery order and operation-specific recovery objectives; - records showing required resources, backups, redundancies and procedures for restoring and resuming from temporary measures; - exercise, test or incident records showing plan application; - records of evaluation, review and updates at planned intervals and after significant incidents or significant changes.
EP-36	REQ-2690-22	Wallet Provider shall maintain backup copies of data at planned intervals commensurate with the criticality of the data and service recovery objectives, ensuring that critical data and logs are backed up according to a defined backup policy at least once	Alignment with international standards - ISO/IEC 27001:2022 A.8.13 (information backup). | ETSI EN 319 401 §7.10 (Backup	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider. The documentation should define: - critical processes, dependencies and recovery objectives for the assessed service; - backup scope, protection, restoration testing and retention rules where applicable, including backup copies of critical data and logs according to a defined backup policy at	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - exercise reports, backup jobs, restoration tests or failover tests relevant to the service, including daily backup evidence for critical data and logs; - backup-plan evidence covering recovery

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		a day and provide sufficient available resources, including facilities, information systems, and personnel, to ensure an appropriate level of redundancy. Wallet Provider shall establish backup plans that address recovery times, backup completeness and accuracy, storage in safe locations, access controls, restoring procedures, and retention periods. Wallet Provider shall perform regular integrity checks on backup copies and regular testing of recovery.	and recovery); EN 319 411-1 §6.4.8 (Compromise and disaster recovery); EN 319 411-2 §6.4.8 (Compromise and disaster recovery for qualified services). Additional standards and references - GDPR Article 32(1)(d) (regularly testing and evaluating effectiveness of security measures); ARF v2.8.0 §6.4 (audit logging requirements for wallet unit lifecycle events and server-side infrastructure). Additional standards and references - GDPR Article 32(1)(d) (processes for regularly testing, assessing, and		least once a day; - backup plans addressing recovery times, backup completeness and accuracy, storage in safe locations, access controls, restoring procedures and retention periods; - regular integrity checks on backup copies and regular testing of recovery; - sufficient available resources, including facilities, information systems and personnel, to ensure an appropriate level of redundancy; - crisis roles, communications, escalation and decision-making criteria.	times, completeness, accuracy, safe storage locations, access controls, restoring procedures and retention periods; - integrity-check records for backup copies and regular recovery-test results; - sampled continuity actions after incidents, outages or supplier failures; - evidence of sufficient redundant resources, including facilities, information systems and personnel; - evidence that recovery objectives and communications were met or deviations were addressed.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			evaluating the effectiveness of technical and organisational measures for ensuring the security of processing, including logging and monitoring); ARF v2.8.0 §6.4 (audit logging requirements for wallet unit lifecycle events and server -side infrastructure).			
EP-37	REQ-2690-23	Wallet Provider shall put in place a process for crisis management that addresses: I. roles and responsibilities for personnel and, where appropriate, suppliers and service providers, in crisis situations; II. appropriate communication between Wallet Provider and relevant competent authorities, including the Scheme Owner, Supervisory Body and CERT Polska; III. application of appropriate measures to ensure the maintenance of information security in crisis situations. Wallet Provider shall	Alignment with international standards - ISO/IEC 27001:2022 A.5.29 (IS during disruption); A.5.30 (ICT readiness for business continuity). | ETSI EN 319 401 §7.10 (Crisis management); EN 319 411-1 §6.4.8 (Compromise and disaster recovery).	WZ-03-01	The assessor reviews busniess continuity and incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - roles and responsibilities for personnel and, where appropriate, suppliers and service providers in crisis situations; - communication procedures with relevant competent authorities, including the Scheme Owner, Supervisory Body and CERT Polska; - measures to maintain information security in crisis situations; - process for managing and making use of information received from CSIRTs or competent authorities concerning incidents, vulnerabilities, threats or mitigation measures; - evaluation, review and, where appropriate, update of the crisis management plan on a regular basis;	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved crisis management process and plan with assigned roles and responsibilities; - crisis communication records, templates, exercises or incidents involving relevant competent authorities, including the Scheme Owner, Supervisory Body and CERT Polska; - evidence of measures maintaining information security during crisis situations; - records showing use of information from CSIRTs or competent authorities on incidents, vulnerabilities, threats or mitigation measures; - exercise, review and update records for the crisis management plan; - corrective actions arising from crisis exercises, incidents or authority information.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		implement a process for managing and making use of information received from CSIRTs or competent authorities concerning incidents, vulnerabilities, threats, or mitigation measures. The crisis management plan shall be evaluated, reviewed and, where appropriate, updated on a regular basis.			- links between crisis management, incident response, continuity, recovery and risk management.	
EP-38	REQ-1502-23; REQ-2690-13; REQ-2690-14	Wallet Provider shall regularly review its compliance with the requirements imposed on it as Wallet Provider through periodical independent internal audits, scoped to include all parts relevant to the provisioning of the wallet-related services. The independent internal audits shall be conducted by an auditor with appropriate competence who is not in the line of authority of the personnel of the area under review. Top management shall be informed of the result of the compliance review based on audit results by means of regular reporting. The audits shall be performed at planned intervals and when significant changes to operations or risks occur.	Alignment with international standards - ISO/IEC 27001:2022 A.5.35 (independent review of IS); A.5.36 (compliance with policies); cl. 9.2 (internal audit). | ETSI EN 319 401 §7.4-§7.8 (Internal audit); EN 319 411 -1 §6.9.1 (Organisational); EN 319 411 -2 §6.9.1 (Organisational requirements for QTSPs). 5.2.11 Record keeping	WZ-03-01	The assessor reviews compliance and change-management arrangements maintained by the assessed Wallet Provider. The documentation should explain: - periodical independent internal audits reviewing compliance with requirements imposed on the Wallet Provider; - audit scope covering all parts relevant to provisioning of wallet-related services; - auditor competence and independence from the line of authority of the personnel in the area under review; - regular reporting of compliance-review results to top management based on audit results; - audit planning at planned intervals and when significant changes to operations or risks occur; - tracking of audit findings, corrective actions and management decisions.	The assessor checks selected changes to relevant systems or services for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - internal audit plans, scopes and reports covering wallet-related service provisioning; - evidence of auditor competence and independence from the area under review; - records showing audits performed at planned intervals and after significant changes to operations or risks; - reports or management-review records showing top-management awareness of compliance-review results; - audit findings, corrective actions, owners, deadlines and closure evidence.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-39	REQ-1502-11	Wallet Provider shall record and maintain relevant documented information using an effective record-management system, considering applicable legislation and good practice in relation to data protection and data retention, including the Act of 14 July 1983 on national archival records and archives (Dz.U. 2020 poz. 164, z późn. zm.) as applicable.	Alignment with international standards - ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Document and records management); EN 319 411-1 §6.4.6 (Records archival); §5.2 (CPS requirements).	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - scope of certification and mapping to Wallet, PID or eID scheme functions; - responsibilities for maintaining evidence, reporting changes and managing recertification; - effective record-management system for recording and maintaining relevant documented information; - consideration of applicable legislation and good practice in relation to data protection and data retention, including the Act of 14 July 1983 on national archival records and archives, where applicable; - links between certification obligations, risk register and continuous-compliance activities; - records required for notification to the CAB, supervisory body or scheme owner where applicable.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, certification scope, assessment reports or action plans; - record-management system evidence showing recording and maintenance of relevant documented information; - samples showing application of data-protection and data-retention rules, including the Act of 14 July 1983 on national archival records and archives where applicable; - records of changes, recertification decisions or continuous-compliance checks; - notifications sent to the CAB, supervisory body or scheme owner where required; - evidence that open findings or certification conditions are tracked to closure.
EP-40	REQ-1502-12	Wallet Provider shall, as far as permitted by national law, retain and protect records for as long as they are required for the purpose of auditing and investigation of security breaches. After the required retention period, records shall be securely destroyed, and such action shall be documented.	Alignment with international standards - ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Records retention); EN 319 411-1 §6.4.6 (Records archival).	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records required for auditing and investigation of security breaches as far as permitted by national law; - retention period, including periods after certificate cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - record samples covering certification, assessment, vulnerability, incident or service evidence, including records retained for auditing and security-breach investigation as far as permitted by national law; - storage location, access-control, integrity and retention metadata; - retrieval evidence for CAB or supervisory requests; - expired or archived records and evidence of secure deletion where retention ended, including documentation of secure

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					the CAB or competent authorities, including documented secure destruction after the required retention period.	destruction after the required retention period.
EP-41	REQ-2981-13; REQ-2981-14	Wallet Provider shall store securely, for at least five years after the cancellation or expiry of the relevant certificate of conformity: I. records of the information provided to the CAB or any of its sub- contractors during the certification process; II. specimens of hardware components that have been included in the scope of certification for the wallet solution. Wallet Provider shall make this documented information available to the CAB or to the Scheme Owner in its capacity as the supervisory body pursuant to Article 46a (1) of Regulation (EU) No 910/2014, upon request.	Alignment with international standards - ISO/IEC 27001:2022 A.5.33 (protection of records); A.5.34 (privacy and protection of PII). | ETSI EN 319 401 §7.3 (Long -term archiving); EN 319 411 -1 §6.4.6 (Records archival); EN 319 411 -2 §6.4.6 (Records archival for qualified services).	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records of information provided to the CAB or any of its subcontractors during the certification process and specimens of hardware components included in the certification scope for the wallet solution; - retention period, including periods after certificate cancellation or expiry where applicable, and at least five years after cancellation or expiry of the relevant certificate of conformity; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including availability to the CAB or to the Scheme Owner in its capacity as supervisory body upon request.	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including information provided to the CAB or any of its subcontractors during certification; - evidence of secure storage of specimens of hardware components included in the certification scope for the wallet solution; - storage location, access-control, integrity and retention metadata, including retention for at least five years after cancellation or expiry of the relevant certificate of conformity; - retrieval evidence for CAB or supervisory requests, including requests from the CAB or Scheme Owner; - expired or archived records and evidence of secure deletion where retention ended.
EP-42	REQ-2690-41	Wallet Provider shall ensure, to the extent feasible and in accordance with applicable Polish law, verification of the background of its personnel, reviewing and updating the background verification policy at least every two years and where	Alignment with international standards - ISO/IEC 27001:2022 A.6.1 (screening); A.6.2 (terms and conditions of employment). |	WZ-03-01	The assessor reviews HR policy and supplier policy. The documentation should cover: - background verification of personnel, to the extent feasible and in accordance with applicable Polish law; - background verification of direct suppliers and service providers where applicable and necessary for their roles, responsibilities and authorisations; - criteria defining which roles require	The assessor checks selected peronel, supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - samples of personnel roles requiring background verification and screening evidence; - samples for direct suppliers or service providers where screening is applicable to

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		applicable of direct suppliers and service providers, where necessary for their role, responsibilities, and authorisations. Wallet Provider shall establish criteria setting out which roles require background verification, considering applicable laws, regulations, and ethics in proportion to risk and the classification of the information systems to be accessed.	ETSI EN 319 401 §7.4 -§7.8 (Personnel security - verification); EN 319 411-1 §6.4.4 (Personnel controls). Additional standards and references - ARF v2.8.0 §6.3 (availability and resilience for WUA issuance and validity status services); GDPR Article 32(1)(b) (resilience of processing systems and services). Additional standards and references - ARF v2.8.0 §6.3 (availability and resilience requirements for WUA issuance services and validity status services); GDPR Article 32(1)(b) (ability to ensure the ongoing confidentiality,		background verification, considering applicable laws, regulations, ethics, risk and classification of information systems to be accessed; - background-verification policy review and update at least every two years; - records showing screening decisions, exceptions, approvals and role-based applicability.	their role, responsibility or authorisation; - criteria mapping roles to background-verification requirements based on law, ethics, risk and system classification; - records showing review and, where appropriate, update of the background-verification policy at least every two years; - exceptions, approvals and evidence of compliance with applicable Polish law.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			integrity, availability and resilience of processing systems and services as an appropriate technical measure).			
EP-43	REQ-2690-40	Wallet Provider shall ensure that all personnel and direct suppliers and service providers understand and commit to their information security responsibilities, as appropriate for the services offered and their role, and in line with Wallet Provider ’s information security policy.	Alignment with international standards - ISO/IEC 27001:2022 A.6.2 (terms and conditions of employment); A.6.5 (responsibilities after termination or change of employment). | ETSI EN 319 401 §7.4 -§7.8 (Personnel obligations); EN 319 411 -1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls).	WZ-03-01	The assessor reviews public information, user communication and service-condition material maintained by the assessed Wallet Provider. The review should check: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures, including controls ensuring that all personnel, direct suppliers and service providers understand and commit to their information-security responsibilities according to their roles and the services offered; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service, in line with the Wallet Provider’s information security policy.	The assessor checks the published material, user-facing information and operational records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions; - interviews with owners of key security and service processes; - acknowledgement, contractual or onboarding evidence showing that personnel, direct suppliers and service providers understand and commit to their information-security responsibilities; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
EP-44	REQ-2690-42	Wallet Provider shall ensure that information security responsibilities and duties that remain valid after termination or change of employment are	Alignment with international standards - ISO/IEC 27001:2022 A.6.5	WZ-03-01	The assessor reviews personnel, competence, training and employment-control arrangements maintained by the assessed Wallet Provider. The documentation should define: - roles in scope, trusted responsibilities and	The assessor checks selected personnel, contractor or training records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		contractually defined and enforced.	(responsibilities after termination or change of employment). | ETSI EN 319 401 §7.4-§7.8 (post-employment obligations); EN 319 411-1 §6.4.4 (Personnel controls).		required competence or screening criteria; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment, including information-security responsibilities and duties that remain valid after termination or change of employment and are contractually defined and enforced; - disciplinary process for breaches of security or service procedures.	operational and support roles; - screening, training, role-description and acknowledgement records; - leaver or role-change cases and evidence of removed responsibilities and access, including contractual clauses or acknowledgements defining continuing information-security duties and evidence of enforcement; - records showing how policy or procedure violations were handled.
EP-45	REQ-1502-13; REQ-2690-38; REQ-2690-40; REQ-2981-04	Wallet Provider shall have procedures in place to ensure that personnel and subcontractors are sufficiently trained, qualified, and experienced in the competences needed to execute the roles they fulfil in connection with the wallet- related services. Wallet Provider shall ensure that personnel whose roles require security-relevant competence receive regular training on information security, ensuring that personnel in trusted roles receive updates on new threats and current security practices at least every 12 months. Wallet Provider shall establish, implement, and apply a training programme in line with its information security policy, which shall: I. be relevant to	Alignment with international standards - ISO/IEC 27001:2022 A.6.3 (IS awareness, education, and training). | ETSI EN 319 401 §7.4-§7.8 (Personnel competence); EN 319 411-	WZ-03-01	The assessor reviews personell and subcontractors onbarding and maitainance docuemntation. The documentation should define: - procedures ensuring that personnel and subcontractors are sufficiently trained, qualified and experienced for roles connected with wallet-related services; - regular information-security training for personnel whose roles require security-relevant competence; - updates on new threats and current security practices for personnel in trusted roles at least every 12 months; - training programme established, implemented and applied in line with the information security policy; - training content relevant to job function, secure configuration and operation of information systems, known threats and behaviour when information-security events occur; - assessment of training effectiveness.	The assessor checks selected records. The evidence should include: - samples of personnel and subcontractors in wallet-related roles showing required training, qualifications and experience; - training records for personnel with security-relevant competence and annual threat/current-practice updates for trusted roles; - training programme materials covering job-function relevance, secure configuration and operation, known threats and behaviour during information-security events; - training-effectiveness assessment records and follow-up actions; - HR records showing expertise, reliability, experience, security training and qualifications for personnel involved in development or operation of the wallet solution.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the job function of the person; II. include instructions regarding the secure configuration and operation of information systems; III. include briefing on known threats; IV. include training on behaviour when information security events occur. The effectiveness of training shall be assessed. Wallet Provider shall ensure that personnel involved in the development or operation of the wallet solution meet the requirements on expertise, reliability, experience, security training, and qualifications established in its human resource management policies.				
EP-46	REQ-2690-37	Wallet Provider shall ensure awareness raising and application of cyber hygiene practices for its personnel, including members of top management, as well as for direct suppliers and service providers where appropriate. Wallet Provider shall offer an awareness raising programme that is scheduled over time,	Alignment with international standards - ISO/IEC 27001:2022 A.6.3 (IS awareness, education, and training); A.5.4 (management responsibilities). | ETSI EN 319 401 §7.4 -§7.8 (Security	WZ-03-01	The assessor reviews policies and plans regarding cyber hygiene of personel. The documentation should cover: - awareness raising and application of cyber hygiene practices for personnel, including members of top management; - awareness raising and cyber hygiene practices for direct suppliers and service providers where appropriate; - awareness raising programme scheduled over time and established in line with the information security policy; - programme content covering relevant threats, information security risk treatment	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - awareness programme schedule, materials and attendance records for personnel and top management; - evidence that direct suppliers and service providers are covered where appropriate; - training or awareness content covering relevant threats, risk treatment measures, contact points, resources and cyber hygiene practices; - interviews or samples confirming personnel

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		established in line with its information security policy, and covers relevant threats, information security risk treatment measures, contact points and resources for additional information, and cyber hygiene practices.	awareness); EN 319 411-1 §6.4.4 (Personnel controls).		measures, contact points and resources for additional information, and cyber hygiene practices; - records showing programme ownership, review, communication and participation.	awareness and application of cyber hygiene practices; - records of reviews, updates and corrective actions for the awareness programme.
EP-47	REQ-2690-43	Wallet Provider shall establish, communicate, and maintain a disciplinary process for handling violations of information security policies.	Alignment with international standards - ISO/IEC 27001:2022 A.6.4 (disciplinary process). | ETSI EN 319 401 §7.4 -§7.8 (Policy violations); EN 319 411 -1 §6.4.4 (Personnel controls).	WZ-03-01	The assessor reviews personnel, competence, training and employment-control arrangements maintained by the assessed Wallet Provider. The documentation should define: - roles in scope, trusted responsibilities and required competence or screening criteria; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment; - disciplinary process for breaches of security or service procedures, including a disciplinary process established, communicated and maintained for handling violations of information security policies.	The assessor checks selected personnel, contractor or training records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles; - screening, training, role-description and acknowledgement records; - leaver or role-change cases and evidence of removed responsibilities and access; - records showing how policy or procedure violations were handled, including evidence that the disciplinary process for information security policy violations was communicated and maintained.
EP-48	REQ-1502-16; REQ-2690-58	Facilities used for providing the wallet-related services service shall ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised personnel or subcontractors. Wallet Provider shall define and use security perimeters, protect areas by	Alignment with international standards - ISO/IEC 27001:2022 A.7.1 (physical security perimeters); A.7.2 (physical entry); A.7.3 (securing offices, rooms, and facilities); A.7.4	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - facilities, rooms, racks or secure areas supporting Wallet, PID or eID scheme operations, including areas holding or processing personal, cryptographic or other sensitive information; - defined security perimeters and physical security for offices, rooms and facilities; - entry-control rules, visitor handling, monitoring and review of access logs,	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - access logs, visitor records and approval evidence for sampled secure areas, including areas holding or processing personal, cryptographic or other sensitive information; - inspection or demonstration of access-control, monitoring and environmental controls, including security perimeters, entry controls, access points and physical security

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		appropriate entry controls and access points, design and implement physical security for offices, rooms, and facilities, and continuously monitor its premises for unauthorised physical access.	(physical security monitoring). | ETSI EN 319 401 §7.4-§7.8 (Physical security); EN 319 411-		including controls limiting access to authorised personnel or subcontractors only; - environmental protection, supporting utilities and maintenance arrangements; - handling of exceptions, alarms, outages and unauthorised access attempts, including continuous monitoring of premises for unauthorised physical access.	for offices, rooms and facilities; - evidence that access is limited to authorised personnel or subcontractors and that premises are continuously monitored for unauthorised physical access; - maintenance, utility, alarm or outage records affecting the assessed components; - evidence that exceptions were reviewed and corrective actions were completed.
EP-49	REQ-1502-15; REQ-2690-57	Facilities used for providing the wallet-related service shall be continuously monitored for, and protected against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.	Alignment with international standards - ISO/IEC 27001:2022 A.7.5 (protecting against physical and environmental threats). | ETSI EN 319 401 §7.4 -§7.8 (Environmental protection); EN 319 411-1 §6.4.2 (Physical security controls).	WZ-03-01	The assessor reviews policies and monitoring documentation. The documentation should identify: - continuous monitoring of facilities for damage caused by environmental events, unauthorised access and other factors that may impact service security; - environmental protection measures for facilities, rooms, racks and secure areas supporting the wallet-related service; - controls for detecting, alerting, responding to and escalating environmental events and unauthorised access; - maintenance, testing and review of environmental monitoring and protection controls; - records linking environmental or physical events to corrective actions and service-security impact assessment.	The assessor inspects relevant facilities, physical controls or supporting utilities for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - monitoring records, alarms, inspections or sensor evidence for facilities supporting wallet-related services; - evidence of protection against environmental events, unauthorised access and other factors affecting service security; - maintenance and test records for environmental protection and monitoring controls; - samples of environmental or physical events, response actions and corrective actions; - evidence that service-security impact was assessed and addressed.
EP-50	REQ-2690-56	Wallet Provider shall prevent loss, damage or compromise of information systems or interruption to their operations due to the failure and disruption of supporting utilities. Wallet Provider shall, where appropriate: I. protect facilities from power		WZ-03-01	The assessor reviews technical and operational documentation. The documentation should identify: - measures preventing loss, damage, compromise or interruption of operations due to failure or disruption of supporting utilities; - protection of facilities from power failures and other supporting-utility disruptions; - use of redundancy in utility services where appropriate;	The assessor inspects relevant facilities, physical controls or supporting utilities for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - utility monitoring, maintenance and test records for power, connectivity, cooling or other supporting utilities; - evidence of redundancy and emergency-supply contracts where appropriate;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		failures and other disruptions caused by failures in supporting utilities; II. consider the use of redundancy in utility services; III. protect utility services that transport data or supply information systems against interception and damage; IV. monitor utility services and report events outside control thresholds; V. conclude contracts for emergency supply; VI. ensure continuous effectiveness, monitor, maintain and test the supply of the information systems necessary for operation.			- protection of utility services transporting data or supplying information systems against interception and damage; - monitoring of utility services and reporting of events outside control thresholds; - contracts for emergency supply.	- records showing protection of utility services transporting data or supplying information systems against interception and damage; - events outside control thresholds and related reporting, escalation and corrective actions; - evidence that failures or disruptions of supporting utilities did not cause uncontrolled loss, damage, compromise or interruption of information-system operations.
EP-51	REQ-1502-21	All media containing personal, cryptographic, or other sensitive information shall be stored, transported, and disposed of in a safe and secure manner.	Alignment with international standards - ISO/IEC 27001:2022 A.7.10 (storage media); A.7.14 (secure disposal or re-use of equipment). | ETSI EN 319 401 §7.3 (Handling of media); EN 319 411-1 §6.4.2 (Physical security controls); §6.4.6	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider. The review should confirm: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant, including safe and secure storage, transport and disposal of media containing personal, cryptographic or other sensitive information; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected assets and handling records for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media, including media containing personal, cryptographic or other sensitive information; - transfer, disposal, sanitisation or destruction evidence where applicable, including evidence of safe and secure storage, transport and disposal; - cases showing that access, monitoring and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			(Records archival).			backup controls are aligned with asset criticality.
EP-52	REQ-2690-53	Wallet Provider shall establish, implement and apply a policy on the management of removable storage media, providing for the technical prohibition of connection of removable media unless there is an organisational reason, disabling of self-execution, scanning for malicious code, measures for controlling portable storage devices, and use of cryptographic techniques where appropriate.	Alignment with international standards - ISO/IEC 27001:2022 A.7.10 (storage media); A.8.11 (data masking). | ETSI EN 319 401 §7.3 (Removable media); EN 319 411 -1 §6.4.2 (Physical security controls).	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider. The review should confirm: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - policy on the management of removable storage media, established, implemented and applied by the Wallet Provider; - media handling, transfer, storage, sanitisation and destruction controls where relevant, including technical prohibition of removable-media connection unless there is an organisational reason, disabling of self-execution, scanning for malicious code, controls for portable storage devices and cryptographic techniques where appropriate; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected assets and handling records for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media, including removable storage media where used; - evidence that connection of removable media is technically prohibited unless organisationally justified; - configuration or test evidence for disabling self-execution, malicious-code scanning, portable-storage-device controls and cryptographic protection where appropriate; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
EP-53	REQ-2690-55	Wallet Provider shall establish procedures for the deposit, return, or deletion of assets upon termination of employment.	Alignment with international standards - ISO/IEC 27001:2022 A.6.5 (responsibilities after termination); A.7.10 (storage media). | ETSI EN 319 401 §7.4 -§7.8 (Return of	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider. The review should confirm: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules, including procedures for deposit, return or deletion of assets upon termination of employment; - media handling, transfer, storage, sanitisation and destruction controls where	The assessor checks selected assets and handling records for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should include: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable, including deposit, return or deletion of assets upon termination of employment;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			assets); EN 319 411-1 §6.4.4 (Personnel controls).		relevant; - links between assets, risks, access rights, logging and continuity arrangements.	- cases showing that access, monitoring and backup controls are aligned with asset criticality.
EP-54	REQ-2690-46; REQ-2690-47; REQ-1502-17	Wallet Provider shall maintain policies for the management of privileged accounts and system administration accounts supporting the wallet-related services. The policies shall establish strong identification, authentication and authorisation procedures for such accounts, set up specific accounts for system administration operations exclusively, individualise and restrict system administration privileges, and provide that system administration accounts are used only to connect to system administration systems. System administration of components that process or manage critical assets shall be subject to dual control, requiring at least two authorised persons to act together for such operations. Wallet Provider shall document the procedures and roles subject to dual control.	Alignment with international standards - ISO/IEC 27001:2022 A.8.2 (privileged access rights); A.5.17 (authentication information); A.5.3 (segregation of duties). | ETSI EN 319 401 §7.4-§7.8 (Privileged accounts); EN 319 411 -1 §6.4.3 (Procedural controls); §6.5.2 (Private key protection and crypto graphic module engineering controls); EN 319 411 -2 §6.5.2 (Private key protection for qualified services).	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - policies for management of privileged accounts and system administration accounts supporting wallet-related services; - strong identification, authentication and authorisation procedures for such accounts; - specific accounts established exclusively for system administration operations; - individualisation and restriction of system administration privileges; - controls ensuring that system administration accounts are used only to connect to system administration systems; - dual control for system administration of components that process or manage critical assets, requiring at least two authorised persons to act together.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - approved policies for privileged accounts and system administration accounts supporting wallet-related services; - samples showing strong identification, authentication and authorisation for privileged and administration accounts; - evidence that system administration operations use specific, individualised and restricted administration accounts; - configuration or log evidence showing administration accounts are used only to connect to system administration systems; - dual-control records for administration of components processing or managing critical assets; - documented procedures, role assignments and approvals for operations subject to dual control.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-55	REQ-2690-48	Wallet Provider shall manage the full life cycle of identities of information systems and their users, including setting up unique identities, linking user identities to a single person, ensuring oversight of identities, and applying logging to the management of identities. Identities assigned to multiple persons shall only be permitted where necessary for business or operational reasons and shall be subject to explicit approval and documentation. Wallet Provider shall regularly review identities of information systems and their users and deactivate identities that are no longer needed without delay.	Alignment with international standards - ISO/IEC 27001:2022 A.5.16 (identity management); A.8.3 (restriction of access to information). | ETSI EN 319 401 §7.4 -§7.8 (Identity management); EN 319 411 -1 §6.4.3 (Procedural controls); §6.4.4 (Personnel controls). Additional standards and references - ARF v2.8.0 §6.2 (cryptographic requirements for WUA signing, PID signing and relying party authentication); CIR (EU) 2025/849 (updated cryptographic standards); ENISA 'Agreed Cryptographic Mechanisms'	WZ-03-01	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed Wallet Provider. The documentation should describe: - full lifecycle of identities of information systems and their users, including creation, modification, review, deactivation and removal; - unique identities and controls linking each user identity to a single person; - oversight of identities, accountable owners and approval rules; - logging applied to the management of identities; - controls for identities assigned to multiple persons, permitted only where necessary for business or operational reasons and subject to explicit approval and documentation; - regular review of identities of information systems and users.	The assessor checks selected identity, privileged-access and access-rights records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - samples of information-system and user identities from creation through modification, review and deactivation; - evidence that user identities are unique and linked to a single person; - approval and documentation for any identities assigned to multiple persons, including business or operational justification; - logs of identity-management activities and related approvals; - regular identity-review records for information systems and users; - cases showing prompt deactivation of identities that are no longer needed.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			(ECSG Sub - group on Cryptography). Additional standards and references - ARF v2.8.0 §6.2 (cryptographic requirements for wallet unit attestation signing, PID signing and relying party authentication, including algorithms, key lengths and certificate formats); CIR (EU) 2025/849 (updated cryptographic standards references for EUD I Wallet ecosystem); ENISA 'Agreed Cryptographic Mechanisms' (ECSG Sub-group on Cryptography, published by ENISA).			
EP-56	REQ-2690-49	Wallet Provider shall implement secure authentication procedures	Alignment with international standards -	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		and technologies. Wallet Provider shall ensure that the strength of authentication is appropriate to the classification of the asset to be accessed. Wallet Provider shall, to the extent feasible, use state-of-the-art authentication methods and unique authentication information.	ISO/IEC 27001:2022 A.8.5 (secure authentication). | ETSI EN 319 401 §7.4 -§7.8 (Personnel authentication); EN 319 411 -1 §6.4.3 (Procedural controls).		Wallet Provider. The review should establish whether the documentation covers: - authentication methods required for users, administrators, processes and service components accessing information systems supporting wallet-related services; - strength of authentication appropriate to the classification of the asset to be accessed; - use of state-of-the-art authentication methods to the extent feasible; - use and protection of unique authentication information; - MFA, credential lifecycle, lockout, recovery and session controls; - criteria for stronger authentication on sensitive, classified or privileged access.	Stage 2 assessment. The evidence should include: - configuration of authentication technologies used for users, administrators, processes and service components; - samples showing authentication strength aligned with the classification of accessed assets; - evidence of state-of-the-art authentication methods where feasible; - evidence that authentication information is unique and protected; - successful, failed and locked authentication attempts; - credential reset, recovery and session-control cases.
EP-57	REQ-2690-50	Wallet Provider shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the information systems supporting the wallet-related services, where appropriate, in accordance with the classification of the asset to be accessed.	Alignment with international standards - ISO/IEC 27001:2022 A.8.5 (secure authentication). | ETSI EN 319 401 §7.4 -§7.8 (Strong authentication); EN 319 411 -1 §6.4.3 (Procedural controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, and for user access to information systems supporting wallet-related services; - multiple authentication factors or continuous authentication mechanisms used where appropriate, in accordance with the classification of the asset to be accessed; - resistance to manipulation, duplication, guessing, replay and high attack potential; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including multiple authentication factors or continuous authentication mechanisms for access to information systems supporting wallet-related services where appropriate; - evidence that the selected authentication mechanism is appropriate to the classification of the asset to be accessed; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
EP-58	REQ-2690-34	Wallet Provider shall protect its information systems against malicious and unauthorised software by implementing measures that detect or prevent the use of such software. Wallet Provider shall, where appropriate, ensure that its systems are equipped with detection and response software that is updated at least daily.	Alignment with international standards - ISO/IEC 27001:2022 A.8.7 (protection against malware). | ETSI EN 319 401 §7.4 -§7.8 (Software protection); EN 319 411 -1 §6.4.3 (Procedural controls); §6.5.5 (Computer security controls).	WZ-03-01	The assessor reviews malware-protection and unauthorised-software controls maintained by the assessed Wallet Provider. The documentation should set out: - systems and endpoints in scope for malware protection; - configuration of prevention, detection, update and quarantine controls, including measures detecting or preventing malicious and unauthorised software; - detection and response software updated at least daily where appropriate; - exception handling for systems where standard protection cannot be installed; - links with incident response, vulnerability management and monitoring.	The assessor checks anti-malware, software-control and alert evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - coverage reports and configuration for sampled systems; - signature or engine update evidence and exception approvals, including evidence that detection and response software is updated at least daily where appropriate; - evidence that controls detect or prevent malicious and unauthorised software; - detections, quarantines or missed updates and how they were handled; - evidence that malware events were escalated when they affected the assessed service.
EP-59	REQ-2690-16	Wallet Provider shall lay down procedures and use tools to monitor and log activities on its information systems to detect events that could constitute incidents. Monitoring shall, to the extent feasible, be automated and conducted either continuously or at periodic intervals. Wallet Provider shall maintain, document and review logs, ensuring that the time used to record events in the audit log is synchronized with UTC at least once a day, which shall include, where appropriate: I. relevant outbound and	Alignment with international standards - ISO/IEC 27001:2022 A.8.15 (logging); A.8.16 (monitoring activities). | ETSI EN 319 401 §7.4 -§7.8 (System monitoring); EN 319 411 -1 §6.4.5 (Audit logging procedures); EN 319 411-2 §6.4.5 (Audit logging for qualified services).	WZ-03-01	The assessor reviews logging and monitoring policy and procedure. The documented controls should identify: - procedures and tools used to monitor and log activities to detect events that could constitute incidents; - automation and continuous or periodic monitoring where feasible; - log maintenance, documentation and regular review; - daily UTC time synchronisation for audit-log event recording; - log coverage for inbound and outbound network traffic, user creation/modification/deletion, system and application access, authentication events, privileged access, critical configuration and backup-file access or changes, security-tool events, system-resource use, physical access, network equipment access,	The assessor checks monitoring tools, retained logs and selected security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - monitoring procedures, tools and configurations used to detect events that could constitute incidents; - evidence of automated, continuous or periodic monitoring where feasible; - samples of maintained, documented and reviewed logs; - evidence of UTC time synchronisation at least once a day for audit logs; - sampled logs covering network traffic, identity changes, access, authentication, privileged activities, critical configuration and backup files, security tools, resource use, physical access, network equipment, log activation/stopping/pausing and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		inbound network traffic; II. creation, modification or deletion of users; III. access to systems and applications; IV. authentication-related events; V. all privileged access activities; VI. access or changes to critical configuration and backup files; VII. event logs from security tools; VIII. use of system resources; IX. physical access to facilities; X. access to network equipment and devices; XI. activation, stopping and pausing of the various logs; XII. environmental events. Logs shall be regularly reviewed, alarm thresholds shall be laid down where appropriate, and logs shall be maintained, backed up, and protected from unauthorised access or changes for a predefined period.			activation/stopping/pausing of logs and environmental events where appropriate; - alarm thresholds where appropriate.	environmental events where appropriate; - alarm-threshold configuration and alert-handling records.
EP-60	REQ-2690-32	Wallet Provider shall respond appropriately to protect its network infrastructure and communication channels from threats. Wallet Provider shall in particular: I. document the architecture of the network in a comprehensible and	Alignment with international standards - ISO/IEC 27001:2022 A.8.20 (networks security); A.8.21 (security of network services). | ETSI	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - comprehensible and up-to-date network architecture documentation, including internal network domains and communication paths; - controls protecting internal domains from	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - network diagrams, firewall/router rules, segmentation or access-control configuration and evidence that production matches the documented architecture; - sampled remote-access, authorised-device

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		up-to-date manner; II. determine and apply controls to protect internal network domains from unauthorised access; III. configure controls to prevent access and network communication not required for the operation of the wallet-related services; IV. determine and apply controls for remote access to information systems; V. not use systems used for administration of the security policy for other purposes; VI. explicitly forbid or deactivate unneeded connections and services; VII. where appropriate, exclusively allow access by devices authorised by Wallet Provider; VIII. allow connections of service providers only after an authorisation request and for a set period; IX. establish communication between distinct systems only through trusted channels that are isolated and provide assured identification of endpoints and protection of channel data; X. apply best practices for DNS security, Internet routing security and	EN 319 401 §7.4 -§7.8 (Network security); EN 319 411-1 §6.5.7 (Network security controls).		unauthorised access and preventing network communication not required for wallet-related services; - remote-access controls, authorised-device restrictions where applicable, and restrictions on service-provider connections to authorised and time-bound access; - controls ensuring that security-policy administration systems are not used for other purposes and that unneeded connections and services are forbidden or deactivated; - trusted channels between distinct systems, including endpoint identification, isolation and protection of channel data; - DNS security, Internet routing security, routing hygiene, transition plans for latest-generation network-layer protocols and modern e-mail communication standards where applicable.	and service-provider access records, including authorisation and time limitation; - configuration evidence that unneeded connections/services are disabled and that administration systems are restricted to administration purposes; - evidence for trusted channels between distinct systems, including endpoint identification and channel-data protection; - DNS security, routing security/routing hygiene and applicable protocol/e-mail transition-plan evidence; - records of planned reviews and updates after significant incidents or significant operational changes.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		routing hygiene. XI. establish and implement a plan for the transition towards latest generation network layer communication protocols, where applicable; XII. adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communication standards, where applicable; Wallet Provider shall review and, where appropriate, update network security measures at planned intervals and when significant incidents or significant changes to operations occur.				
EP-61	REQ-2690-33	Wallet Provider shall segment its systems into networks or zones in accordance with the results of risk assessments. Wallet Provider shall segment its systems and networks from third parties' systems and networks, and shall in particular: I. grant access to a network or zone based on an assessment of its security requirements; II. keep systems critical to Wallet Provider 's operation in secured zones; III. deploy a demilitarised	Alignment with international standards - ISO/IEC 27001:2022 A.8.22 (segregation of networks). | ETSI EN 319 401 §7.4 -§7.8 (Network architecture); EN 319 411 -1 §6.5.7 (Network security controls).	WZ-03-01	The assessor reviews network documentation and procedures. The documented arrangements should define: - segmentation model dividing systems into networks or zones based on risk assessment and security requirements; - separation of Wallet Provider systems and networks from third-party systems and networks; - placement of systems critical to Wallet Provider operations in secured zones and use of a demilitarised zone for secure communication; - rules restricting access and communication between and within zones to what is necessary for operation; - separation of administration	The assessor reviews selected or sampled network configurations and documentation. The evidence should show: - network-zone diagrams, segmentation design and mapping to risk assessments/security requirements; - sampled firewall, routing, ACL, NAC or equivalent rules restricting traffic between and within zones; - evidence that critical systems are in secured zones and that DMZ communication is used where required; - evidence of separation from third-party networks, separation of administration from operational traffic, and separation of production from development/testing; - test, configuration-review or monitoring

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		zone for secure communication; IV. restrict access and communications between and within zones to those necessary for operation; V. separate the dedicated network for administration from the operational network; VI. separate production systems from development and testing systems. VII. define traffic segregation rules taking to account the functional, logical and physical relationship, including location, between trustworthy systems and services; VIII. separate network administration channels from other network traffic; Wallet Provider shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations occur.			networks/channels from operational networks/traffic and separation of production from development and testing systems; - traffic segregation rules reflecting functional, logical, physical and location relationships between trustworthy systems and services.	evidence confirming that unauthorised inter-zone communication is blocked; - records of planned reviews and updates after significant incidents or significant operational changes.
EP-62	REQ-1502-20; REQ-2690-28	Wallet Provider shall take appropriate measures to establish, document, implement and monitor configurations, including security configurations of hardware, software, services, and networks supporting the wallet-	Alignment with international standards - ISO/IEC 27001:2022 A.8.9 (configuration management). | ETSI EN 319 401	WZ-03-01	The assessor reviews technical documentation, and asset inventory maintained by the assessed Wallet Provider. The documented arrangements should define: - documented configuration baselines, including security configurations, for hardware, software, services and networks; - processes to establish, implement and monitor secure configurations for newly	The assessor reviews selected configurations and records of Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled configuration baselines and approved security settings for hardware, software, services and networks; - configuration-management tool output, compliance scans, drift-detection records or

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		related services. Wallet Provider shall establish and ensure secure configurations and implement processes and tools to enforce them for newly installed systems as well as for systems in operation. Wallet Provider shall review and, where appropriate, update configurations at planned intervals and when significant incidents or significant changes to operations occur.	§7.4 -§7.8 (System configuration); EN 319 411 -1 §6.4.3 (Procedural controls); §6.5.5 (Computer security controls).		installed systems and systems in operation; - tools or controls used to enforce approved configurations and detect unauthorised or non-compliant configuration changes; - configuration ownership, approval, exception and remediation rules; - planned review and update of configurations after significant incidents or significant operational changes.	equivalent enforcement evidence; - samples from newly installed and operational systems showing conformance with approved secure configurations; - records of configuration exceptions, approvals, remediation and residual-risk handling where applicable; - records of planned reviews and updates after significant incidents or significant operational changes.
EP-63	REQ-1502-20; REQ-2690-29; REQ-2981-03	Wallet Provider shall apply change management procedures to control changes to information systems supporting the wallet-related services. The procedures shall apply to releases, modifications and emergency changes of any software and hardware in operation and to changes to configuration. Changes shall be documented and based on risk assessment, evaluated and assessed and, where appropriate, tested in view of their potential impact on the wallet-related service, related security controls and configurations, before implementation. Where	Alignment with international standards - ISO/IEC 27001:2022 A.8.32 (change management). | ETSI EN 319 401 §7.4 -§7.8 (Change management); EN 319 411 -1 §6.4.3 (Procedural controls); EN 319 411-2 §6.4.3 (Procedural controls for qualified services).	WZ-03-01	The assessor reviews change management procedures maintained by the assessed Wallet Provider. The review should confirm: - procedures controlling releases, modifications, emergency changes, software and hardware changes in operation, and configuration changes; - requirements that changes are documented, risk-assessed, evaluated and, where appropriate, tested before implementation for their impact on wallet-related services, security controls and configurations; - emergency-change procedures requiring documentation of the reasons and result; - planned review and update of change-management procedures after significant incidents or significant operational changes; - responsibilities for notifying the Ministry of Digital Affairs of changes to the certified wallet solution, obtaining necessary certification maintenance and demonstrating continued compliance with the Trust	The assessor checks change management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled release, modification, emergency-change, hardware/software and configuration-change records; - risk assessments, impact evaluations, approvals and pre-implementation test evidence for sampled changes; - evidence that changes affecting wallet-related services, security controls or configurations were assessed before deployment; - emergency-change records documenting reasons, result, post-implementation review and follow-up actions; - records of procedure review after significant incidents or significant operational changes; - notifications to the Ministry of Digital Affairs, certification-maintenance evidence and continued Trust Framework compliance

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		emergency procedures are followed, the result and reasons shall be documented. Wallet Provider shall review the change management procedures at planned intervals and when significant incidents or significant changes to operations occur, and shall update them where appropriate. Wallet Provider shall notify the Ministry of Digital Affairs of changes to the certified wallet solution. Wallet Provider shall obtain the necessary certification maintenance and, where applicable, demonstrate continued compliance with the Trust Framework before deploying new versions of the wallet solution within the scheme.			Framework before deployment of new versions.	evidence before deployment of new wallet-solution versions where applicable.
EP-64	REQ-1502-20; REQ-2690-31	Wallet Provider shall specify and apply procedures for security patch management, ensuring that: I. security patches are applied within a reasonable time after they become available; II. security patches are tested before being applied in production systems; III. security patches come from	Alignment with international standards - ISO/IEC 27001:2022 A.8.8 (management of technical vulnerabilities); A.8.19 (installation of software on	WZ-03-01	The assessor reviews security patch-management arrangements maintained by the assessed Wallet Provider. The documentation should define: - rules requiring security patches to be applied within a reasonable time after availability; - testing requirements before applying patches in production systems; - requirements that patches come from trusted sources and are checked for integrity; - rules for additional measures and residual-	The assessor checks selected vulnerabilities, patch decisions and deployment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled security patches from identification through testing, approval, deployment and closure; - evidence that patches were obtained from trusted sources and checked for integrity; - timeliness evidence showing the period between patch availability, testing and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		trusted sources and are checked for integrity; IV. additional measures are implemented and residual risks are accepted where a patch is not available or not applied. Wallet Provider may choose not to apply a security patch where the disadvantages outweigh the information security benefits, provided the reasons are documented and substantiated.	operational systems). | ETSI EN 319 401 §7.4-§7.8 (Updates and patching); EN 319 411-1 §6.4.3 (Procedural controls); §6.5.6 (Life cycle security controls).		risk acceptance where a patch is not available or not applied; - criteria and documentation requirements for justified decisions not to apply a patch where disadvantages outweigh information-security benefits.	production deployment; - records of patches not available or not applied, including compensating measures and residual-risk acceptance; - documented and substantiated decisions where a patch was not applied because disadvantages outweighed information-security benefits.
EP-65	REQ-1502-18; REQ-1502-19; REQ-1502-22; REQ-2690-39	Wallet Provider shall establish, implement, and apply a policy and procedures related to cryptography, ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data processed in connection with the wallet-related services. The policy shall establish, as a minimum: I. type, strength and quality of cryptographic measures required, based on the classification of assets; II. protocols, algorithms, cipher strengths, and cryptographic solutions approved for use; III. approach to key management, covering the	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.8.25 (secure development life cycle). | ETSI EN 319 401 §7.4 - §7.8 (Cryptographic policy); EN 319 411 -1 §6.5.1 (Key pair generation and installation); §6.5.2 (Private key protection and cryptographic module engineering	WZ-03-01	The assessor reviews the practice statement and policy documents defining crypography management by the assessed Wallet Provider. The documented controls should define: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components, including protocols, cipher strengths and cryptographic solutions approved for use; - type, strength and quality of cryptographic measures required based on asset classification to protect confidentiality, authenticity and integrity of data processed in connection with wallet-related services; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - key-management approach covering the full key life cycle, including generation, issuance, distribution, storage, change, revocation, recovery, backup, destruction, logging and auditing; - cryptographic agility process for weakened or deprecated algorithms; - planned review and update of the	The assessor tests selected configurations and revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - evidence that cryptographic measures are selected based on asset classification and protect confidentiality, authenticity and integrity; - key-generation, use, rotation, revocation or destruction records, including issuance, distribution, storage, change, recovery, backup, logging and auditing evidence where applicable; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations; - records of planned review and update of the

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		full key life cycle including generation, issuance, distribution, storage, change, revocation, recovery, backup, destruction, logging and auditing. The policy shall be reviewed and updated at planned intervals, considering the state of the art in cryptography. NOTE - The information classification scheme referred to in EP-22 shall ensure that personal or sensitive information is classified at a level that requires cryptographic protection of electronic communication channels against eavesdropping, manipulation, and replay	controls); EN 319 411 -2 §6.5.1 (Key pair generation for qualified services); §6.5.2 (Private key protection for qualified services).		cryptography policy considering the state of the art in cryptography.	cryptography policy considering the state of the art.
EP-66	REQ-1502-19; REQ-1502-22	Access to sensitive cryptographic material used for issuing electronic identification means and authentication in the scheme shall be restricted to the roles and applications strictly requiring access. Such material shall never be persistently stored in plain text. Sensitive cryptographic material shall be protected from tampering. Key management operations on	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.17 (authentication information - key protection). | ETSI EN 319 401 §7.4-§7.8 (Key protection); EN 319 411 -1 §6.5.1 (Key pair	WZ-03-01	The assessor reviews the cryptographis controls maintained by the assessed Wallet Provider. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - WSCD/WSCA use and evidence of protected key generation, storage and operation, including restriction of access to sensitive cryptographic material to roles and applications strictly requiring access; - controls ensuring sensitive cryptographic material is never persistently stored in plain text and is protected from tampering; - dual control for key management operations	The assessor validates cryptographic controls configuration and related security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records, including access-control evidence for sensitive cryptographic material and records for activation, backup and recovery where applicable; - evidence that sensitive cryptographic material is not persistently stored in plain text and is protected from tampering;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		cryptographic material that constitutes critical assets, including key generation, activation, backup, recovery, and destruction, shall be subject to dual control, requiring at least two authorised persons to act together. Wallet Provider shall maintain records of all such operations.	generation and installation); §6.5.2 (Private key protection and cryptographic module engineering controls); EN 319 411- 2 §6.5.2 (Private key protection for qualified services).		on cryptographic material constituting critical assets, including key generation, activation, backup, recovery and destruction, requiring at least two authorised persons to act together; - records of all such critical cryptographic-material operations; - cryptographic agility process for weakened or deprecated algorithms.	- dual-control evidence for critical cryptographic-material operations requiring at least two authorised persons; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
EP-67	REQ-2690-26	Wallet Provider shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components critical to the security of its information systems, throughout their life cycle. The processes shall include security requirements, update requirements, component information, security function documentation, compliance assurance, and validation methods. Wallet Provider shall review and, where appropriate, update these processes at planned intervals and when significant incidents occur.	Alignment with international standards - ISO/IEC 27001:2022 A.5.21 (managing IS in ICT supply chain); A.8.30 (outsourced development). | ETSI EN 319 401 §7.14 (Security of procurement); EN 319 411 -1 §6.9.1 (Organisational); §6.8.6 (Representations and warranties).	WZ-03-01	The assessor reviews ICT product acquisition procedure, incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - processes to manage risks stemming from the acquisition of ICT services or ICT products for components critical to the security of information systems throughout their life cycle; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - security requirements, update requirements, component information, security-function documentation, compliance assurance and validation methods for acquired ICT services or ICT products; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - sampled risks from the register linked to assets, processes and treatment actions; - sampled acquisitions of ICT services or ICT products for security-critical components, showing lifecycle risk management; - evidence of security requirements, update requirements, component information, security-function documentation, compliance assurance and validation methods; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - records showing planned and significant-incident-triggered review or update of ICT acquisition risk processes.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					changes, including review and update of ICT acquisition risk processes at planned intervals and when significant incidents occur.	
EP-68	REQ-2690-27	Before developing information systems, including software, in connection with the wallet-related services, Wallet Provider shall establish rules for secure development. Where Wallet Provider develops systems in-house or outsources development, the rules shall cover all development phases and shall include security requirements analysis, secure engineering and coding principles, security testing processes, and appropriate handling of test data.	Alignment with international standards - ISO/IEC 27001:2022 A.8.25 (secure development life cycle); A.8.26 (application security requirements); A.8.27 (secure systems architecture and engineering principles); A.8.28 (secure coding). | ETSI EN 319 401 §7.4-§7.8 (Secure development); EN 319 411 -1 § 6.5.6 (Life cycle security controls); EN 319 411 -2 §6.5.6 (Life cycle security controls for qualified services).	WZ-03-01	The assessor reviews procedures for in-house developement and/or outsourced suppliers, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - rules covering both in-house development and outsourced development; - coverage of all development phases; - security requirements analysis before and during development; - secure engineering and secure coding principles; - security testing processes for developed systems and software; - appropriate handling, protection and disposal of test data.	The assessor checks selected in-hosue or supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - secure-development rules and procedures for in-house and outsourced development; - sampled development projects showing security requirements analysis across development phases; - evidence of secure engineering and secure coding practices; - security testing records for developed systems or software; - test-data handling records showing appropriate protection, use and disposal; - contracts, development records or supplier evidence showing secure-development rules applied to outsourced development where applicable.
EP-69	REQ-2690-30	Wallet Provider shall establish, implement, and apply a policy and procedures for security	Alignment with international standards - ISO/IEC	WZ-03-01	The assessor reviews secure testing policies and procedures maintained by the assessed Wallet Provider. The documentation should show:	The assessor checks selected development, acquisition, maintenance or security-testing records for the assessed Wallet Provider during the on-site Stage 2 assessment. The

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		testing of the information systems supporting the wallet-related services. Wallet Provider shall establish, based on risk assessment, the need, scope, frequency, and type of security tests, and shall conduct security tests including penetration tests performed at least once per year, document the results, and apply mitigating measures for critical findings. Wallet Provider shall regularly review and, where appropriate, update the security testing policy and procedures.	27001:2022 A.8.29 (security testing in development and acceptance). | ETSI EN 319 401 §7.4-§7.8 (Security testing); EN 319 411-		- risk-based determination of the need, scope, frequency and type of security tests; - security tests, including penetration tests performed at least once per year; - documentation of security-test and penetration-test results; - mitigating measures for critical findings and tracking of remediation; - regular review and, where appropriate, update of the security-testing policy and procedures; - links between security testing, risk assessment, vulnerability management, change management and acceptance before production use.	evidence should include: - approved security-testing policy and procedures for information systems supporting wallet-related services; - risk assessment records defining test need, scope, frequency and type; - security-test records and penetration-test reports showing testing at least once per year; - documented results, critical findings and mitigating measures; - remediation tracking, retest evidence and closure approvals for critical findings; - records of regular review and update of the security-testing policy and procedures.
PP-01	REQ-5c-04; REQ-1502-E03; REQ-2981-P02	Wallet Provider/PID Provider's ISMS established under EP-01 of WZ-03- 01 shall explicitly cover the PID issuance infrastructure and all processes related to enrolment, issuance, and lifecycle management of person identification data. The scope of the ISMS shall document the boundary between the Wallet Provider and PID Provider functions and the controls in place to ensure the logical separation required by REQ-5c-04.	Alignment with international standards - ISO/IEC 27001:2022 A.5.31 (legal, statutory and regulatory requirements); cl. 8.1 (operational planning and control); A.5.16 (identity management). | ETSI EN 319 401 §7.1 (Organisational security); EN	WZ-03-02	The assessor reviews security governance and ISMS documentation maintained by the assessed Wallet Provider. The review should confirm: - explicit inclusion of the PID issuance infrastructure within the ISMS scope; - coverage of all processes related to enrolment, issuance and lifecycle management of person identification data; - documented boundary between Wallet Provider and PID Provider functions; - controls ensuring logical separation of PID processing from other provider functions and data; - links between ISMS scope, risk assessment, operational controls, legal obligations and certification evidence; - availability of ISMS scope and separation documentation for CAB assessment.	The assessor checks implementation of the ISMS implementatin through the following evidence: - sampled user accounts, roles, and access permissions demonstrating logical separation of Wallet Provider and PID Provider functions; - sampled audit logs confirming that access to PID data is restricted to authorised users and systems; - interviews with responsible personnel confirming the operational application of the ISMS controls.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			319 411 -1 §6.9.1 (Organisational); §5.2 (CPS requiremen ts); EN 319 411 -2 §6.9.1 (Organisational requirements for QTSPs). Additional standards and references - GDPR Article 25 (data protection by design - ISMS scope must include data minimisation and purpose limitation for PID processing); ARF v2.8.0 §3.4 (PID Provider role and security responsibilities in the EUDI Wallet ecosystem).			
REQ-5c-01	Article 5c of eIDAS / Regulation (EU) 910/2014	The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8) of eIDAS, the requirement for logical	Article 5c (1) eIDAS	WZ-03-03	The assessor reviews the certification-scope documentation for the assessed Wallet Provider and the related electronic identification scheme. The review should confirm: - conformity certification by a CAB designated by a Member State; - coverage of Article 5a(4), Article 5a(5), Article 5a(8), Article 5a(14) logical separation	The assessor checks certification evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current conformity certificate, assessment report and certification scope for the EUDI Wallet and related eID scheme; - evidence that the CAB was designated by the relevant Member State;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		separation laid down in Article 5a(14), and, where applicable, the standards referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.			and, where applicable, Article 5a(24) standards; - mapping between certified requirements, Wallet components, eID scheme functions and deployed service scope; - responsibilities for maintaining certification evidence, reporting changes and managing certification conditions or renewals.	- mapping of the certification scope to Article 5a(4), Article 5a(5), Article 5a(8), Article 5a(14) and applicable Article 5a(24) standards; - comparison between certified scope and deployed Wallet/eID scheme components; - records of changes, renewals, conditions, findings or notifications to the CAB.
REQ-5c-02	Article 5c of eIDAS / Regulation (EU) 910/2014	Certification of the conformity of the EUDI Wallet with requirements relevant for cybersecurity shall be conducted in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referred to in the implementing acts adopted under Article 5c (6) of eIDAS.	Article 5c (2) eIDAS	WZ-03-03	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including certification of cybersecurity-relevant requirements under European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referred to in the implementing acts adopted under Article 5c(6) of eIDAS where applicable; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including evidence that cybersecurity-relevant certification was conducted under the applicable European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 and referred to in Article 5c(6) implementing acts where applicable; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.
REQ-5c-03	Article 5c of eIDAS / Regulation (EU) 910/2014	For requirements not relevant for cybersecurity, and for cybersecurity requirements not fully covered by European cybersecurity certification schemes, Member States shall establish national certification schemes	Article 5c (3) eIDAS	WZ-03-03	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including evidence of certification under the applicable national certification scheme for non-cybersecurity requirements and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		following the requirements set out in the implementing acts adopted under Article 5c (6).			national certification schemes established for requirements not relevant for cybersecurity and for cybersecurity requirements not fully covered by European cybersecurity certification schemes; - evidence that the applicable national certification scheme follows the requirements set out in implementing acts adopted under Article 5c(6) where relevant to the assessed certification; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	cybersecurity requirements not fully covered by European cybersecurity certification schemes; - evidence that the national certification scheme basis aligns with Article 5c(6) implementing-act requirements where applicable; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.
REQ-5c-04	Article 5c of eIDAS / Regulation (EU) 910/2014	Providers of European Digital Identity Wallets shall, prior to placing the wallet on the market, certify the conformity of their European Digital Identity Wallets under a certification scheme referred to in Article 5c (2) and (3).	Article 5c (4) eIDAS	WZ-03-03	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including certification under a certification scheme referred to in Article 5c(2) and 5c(3); - evidence that conformity of the European Digital Identity Wallet was certified before the wallet was placed on the market; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including evidence that the certificate was issued under a certification scheme referred to in Article 5c(2) and 5c(3); - evidence that certification was completed before the wallet was placed on the market; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-5c-05	Article 5c of eIDAS / Regulation (EU) 910/2014	Certificates of conformity shall be recognised in all Member States and shall specify the cybersecurity certification scheme used and the relevant assurance level.	Article 5c (5) eIDAS	WZ-03-03	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including the cybersecurity certification scheme used and the relevant assurance level specified in the certificate of conformity; - evidence that the certificate of conformity is recognised in all Member States; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including the cybersecurity certification scheme used and the relevant assurance level; - evidence that the certificate of conformity is recognised in all Member States; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.
REQ-2981-W01	Commission Implementing Regulation (EU) 2024/2981	National certification schemes shall contain cybersecurity requirements based on a risk assessment of each specific supported architecture, aimed at treating the identified cybersecurity risks and threats in the risk register set out in Annex I.	Article 8(1)	WZ-03-03	The assessor reviews the risk-management arrangements maintained by the assessed Wallet Provider. The review should link the requirement to: - cybersecurity requirements included in the national certification scheme; - risk assessment for each specific supported architecture; - identified cybersecurity risks and threats mapped to the risk register set out in Annex I; - risk-treatment measures addressing the identified risks and threats; - traceability between architecture, risk assessment, national certification requirements and assessed controls.	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - risk assessment records for each supported wallet architecture; - mapping of identified cybersecurity risks and threats to the Annex I risk register; - national certification scheme cybersecurity requirements derived from or linked to those risks; - evidence that risk-treatment measures are implemented in the assessed architecture; - traceability from scheme requirements to certification evidence and operational controls.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2981-W02	Commission Implementing Regulation (EU) 2024/2981	National certification schemes shall specify that the certificate of conformity covers the wallet unit, the wallet secure cryptographic application (WSCA), and the wallet secure cryptographic device (WSCD) as applicable to the supported architecture.	Article 3	WZ-03-03	The assessor reviews certificate-scope documentation maintained by the assessed Wallet Provider. The review should confirm: - that the national certification scheme specifies coverage of the Wallet Unit; - whether WSCA coverage is required for the supported architecture; - whether WSCD coverage is required for the supported architecture; - mapping between supported architecture components and certificate scope; - justification for any WSCA or WSCD non-applicability.	The assessor checks certificate-scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate of conformity and assessment scope covering the Wallet Unit; - evidence that WSCA and WSCD are covered where applicable to the supported architecture; - architecture and component lists showing Wallet Unit, WSCA and WSCD scope; - documented justification for any WSCA or WSCD non-applicability; - comparison between deployed components and the certified scope.
REQ-2981-W03	Commission Implementing Regulation (EU) 2024/2981	The Wallet Provider shall apply for certification and always maintain a valid certificate of conformity while the wallet is available to users.	Article 4	WZ-03-03	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including evidence that the Wallet Provider applied for certification and maintains a valid certificate of conformity while the wallet is available to users; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including evidence that the certificate is valid while the wallet is available to users; - records showing the Wallet Provider applied for certification and maintains the certificate without gaps during user availability; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2981-W04	Commission Implementing Regulation (EU) 2024/2981	The holder of a certificate of conformity shall notify the certification body without undue delay of any breach or compromise of the EUDI Wallet likely to impact the conformity of the wallet.	Article 5(2)	WZ-03-03	The assessor reviews breach and compromise notification rules operated by the assessed Wallet Provider: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data; - timelines, roles and approval path for notification without undue delay; - evidence retained for the decision to notify or not notify.	The assessor tests selected breach or compromise notification cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - incident or breach records from detection through classification and notification decision; - notifications sent and timestamps showing timeliness; - evidence supporting impact on conformity, personal data or service integrity; - cases where notification was not sent and the documented rationale.
REQ-2981-W05	Commission Implementing Regulation (EU) 2024/2981	The Wallet Provider shall establish and maintain a vulnerability management policy meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act), as referenced in Article 5(7) of CIR (EU) 2024/2981.		WZ-03-03	The assessor reviews vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider. The review should identify: - sources of vulnerability information, including public, supplier, testing and researcher reports; - criteria for impact analysis, severity, registration and disclosure; - policy requirements meeting Annex I to Regulation (EU) 2024/2847, as referenced in Article 5(7) of CIR (EU) 2024/2981; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved vulnerability management policy meeting Annex I to Regulation (EU) 2024/2847; - intake, triage and impact-analysis evidence; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records.
REQ-2981-W06	Commission Implementing Regulation (EU) 2024/2981	National certification schemes shall require assessment at assurance level ‘high’ as defined in the EU Cybersecurity Act, with evaluation criteria covering functional correctness, resistance to attacks, and technical security.	Articles 6 and 9	WZ-03-03	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider. The review should identify: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture; - validity, assurance level, certification body and scheme used for the certificate, including	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including evidence of assurance level “high” as defined in the EU Cybersecurity Act; - assessment evidence showing evaluation of

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					assessment at assurance level “high” as defined in the EU Cybersecurity Act; - evidence that the national certification scheme evaluation criteria cover functional correctness, resistance to attacks and technical security; - alignment between the documented scope, the deployed service and the components made available to users; - process for maintaining the certificate and updating CAB or scheme evidence after material changes.	functional correctness, resistance to attacks and technical security; - comparison between deployed components and the certified scope; - records of changes, renewals, conditions, findings or notifications to the certification body; - public certification information where publication is required.
REQ-2981-W07	Commission Implementing Regulation (EU) 2024/2981	Public information about the certification, including the scope, the certificate identifier, the certification body, and validity period, shall be published and kept up to date.	Article 8(5) and Annex V	WZ-03-03	The assessor reviews public information, user communication and service-condition material maintained by the assessed Wallet Provider. The review should check: - which information must be public, user-facing or provided to relying parties, including public certification information covering certification scope, certificate identifier, certification body and validity period; - ownership, approval and version-control rules for published content; - timeliness of updates after changes affecting users, relying parties or certification status, including keeping public certification information up to date; - evidence retained to show when information was published or changed.	The assessor checks the published material, user-facing information and operational records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - current public pages, repositories, policy documents or user-facing notices, including certification scope, certificate identifier, certification body and validity period; - change history, approval records and publication timestamps; - comparison between published content and the assessed service configuration, including whether certification information is current and complete; - cases showing that outdated or inconsistent information was corrected.
REQ-2981-W08	Commission Implementing Regulation (EU) 2024/2981	Records relating to the conformity assessment shall be retained for the minimum period specified in Article 19 of CIR (EU) 2024/2981 and made available to the CAB and		WZ-03-03	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including records relating to the conformity assessment;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		competent supervisory authorities upon request.			relating to the conformity assessment; - retention period, including periods after certificate cancellation or expiry where applicable, and at least the minimum period specified in Article 19 of CIR (EU) 2024/2981; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including competent supervisory authorities upon request.	- storage location, access-control, integrity and retention metadata, including retention for at least the minimum period specified in Article 19 of CIR (EU) 2024/2981; - retrieval evidence for CAB or supervisory requests, including requests from competent supervisory authorities; - expired or archived records and evidence of secure deletion where retention ended.
REQ-2690-W01	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall adopt a policy on the security of network and information systems covering the scope of the wallet service.	Annex, Section 1	WZ-03-03	The assessor reviews the information-security governance documents maintained by the assessed Wallet Provider: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	The assessor verifies that governance is operating for the assessed Wallet Provider during the on-site Stage 2 assessment: - approved policies, review records and management decisions; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-2690-W02	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall conduct risk management activities, including identification, analysis, evaluation, and treatment of risks to the network and information systems supporting the wallet service.	Annex, Section 2	WZ-03-03	The assessor reviews the risk-management arrangements used by the assessed Wallet Provider: - risk methodology, scope and criteria covering the relevant Wallet, PID or eID scheme assets and processes; - identification of threats, vulnerabilities, dependencies and legal or scheme impacts; - risk treatment decisions, owners, deadlines and residual-risk acceptance; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	The assessor checks risk-management implementation for the assessed Wallet Provider during the on-site Stage 2 assessment: - sampled risks from the register linked to assets, processes and treatment actions; - management acceptance of residual risks and overdue actions; - evidence that incidents, changes or vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2690-W03	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall implement incident handling procedures covering detection, classification, response, and post-incident analysis for the wallet service.	Annex, Section 3	WZ-03-03	The assessor reviews incident, breach and unauthorised-access handling arrangements for the assessed Wallet Provider: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps; - links with vulnerability management, risk assessment, change management and user communication.	The assessor tests selected incident or breach records for the assessed Wallet Provider during the on-site Stage 2 assessment: - events from detection through triage, classification, containment and closure; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, lessons learned and updates to controls, risks or procedures.
REQ-2690-W04	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall implement business continuity and crisis management measures ensuring availability of the wallet service at the required level.	Annex, Section 4	WZ-03-03	The assessor reviews continuity, backup, recovery and crisis-management arrangements for the assessed Wallet Provider: - critical processes, dependencies and recovery objectives for the assessed service; - backup scope, protection, restoration testing and retention rules where applicable; - crisis roles, communications, escalation and decision-making criteria; - links between continuity plans, incident response, supplier dependencies and user impact.	The assessor checks continuity and recovery evidence for the assessed Wallet Provider during the on-site Stage 2 assessment: - exercise reports, backup jobs, restoration tests or failover tests relevant to the service; - sampled continuity actions after incidents, outages or supplier failures; - evidence that recovery objectives and communications were met or deviations were addressed; - updates made to plans following tests, incidents or service changes.
REQ-2690-W05	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall implement supply chain security measures covering service providers and technology components that form part of the wallet infrastructure.	Annex, Section 5	WZ-03-03	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions, including service providers and technology components that form part of the wallet infrastructure; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights,	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers; - records for technology components forming part of the wallet infrastructure, including ownership, supplier/source, security requirements and review evidence; - risk assessments, onboarding approvals and periodic review records;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					incident notification and exit arrangements; - ongoing monitoring of supplier performance, security issues and changes, including security of relevant technology components.	- supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.
REQ-2690-W06	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall implement security measures in the acquisition, development and maintenance of wallet systems and applications.	Annex, Section 6	WZ-03-03	The assessor reviews secure acquisition, development and maintenance arrangements for the assessed Wallet Provider: - security requirements introduced before procurement, design or development starts; - review, testing and approval gates before release or deployment; - control of libraries, dependencies, environments and supplier-developed components; - evidence required before changes are accepted into production.	The assessor checks selected acquisition or development cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - requirements, design, test and approval evidence for sampled changes or components; - security findings and how they were fixed or accepted; - release records confirming that required gates were completed; - environment, dependency or supplier evidence relevant to the implemented component.
REQ-2690-W07	Commission Implementing Regulation (EU) 2024/2690	Wallet Provider shall implement effectiveness assessment, cyber hygiene, cryptography and key management, human resources, access control, asset management, and physical security measures.	Annex, Sections 7-13	WZ-03-03	The assessor reviews the documented security-measures framework maintained by the assessed Wallet Provider. The review should confirm that the documentation covers: - effectiveness assessment of cybersecurity measures; - cyber hygiene and security awareness measures; - cryptography and key-management controls; - human-resources security measures for personnel supporting the wallet service; - logical and physical access-control measures; - asset-management and physical-security measures for wallet systems, applications, devices, media and information assets.	The assessor checks selected control evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - records of effectiveness assessments of cybersecurity measures; - cyber hygiene, awareness or training evidence; - cryptography and key-management evidence; - HR security records for personnel supporting the wallet service; - logical and physical access-control configuration, approvals and reviews; - asset inventory, ownership, classification and handling evidence.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-1502-W01	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall maintain effective management and organisation controls, including information security policy, risk management, access controls, incident management, and record keeping, consistent with Section 2.4 of the Annex to CIR (EU) 2015/1502, at assurance level High.		WZ-03-03	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented arrangements should define: - scope of the policy or management system against the assessed Wallet, PID or eID scheme functions; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service, including management and organisation controls required by Section 2.4 of the Annex to CIR (EU) 2015/1502 at assurance level High; - risk management, access controls, incident management and record-keeping arrangements supporting the wallet service.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved policies, review records and management decisions; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - selected evidence for risk management, access controls, incident management and record keeping consistent with Section 2.4 of CIR (EU) 2015/1502 at assurance level High; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-1502-W02	Commission Implementing Regulation (EU) 2015/1502	Wallet Provider shall be responsible for the fulfilment of any commitments outsourced to another entity as if it had performed the duties itself.	Annex, Section 2.4.1(4)	WZ-03-03	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - pre-contract due diligence, risk assessment and security requirements; - contractual clauses, SLA, audit rights, incident notification and exit arrangements, including clauses confirming that the Wallet Provider remains responsible for outsourced commitments as if it had performed the duties itself; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including evidence that the Wallet Provider retains responsibility for outsourced commitments as if performed itself; - risk assessments, onboarding approvals and periodic review records; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2979-W01	Commission Implementing Regulation (EU) 2024/2979	Wallet Provider shall issue Wallet Unit Attestations (WUA) in accordance with the technical specifications of CIR (EU) 2024/2979 and maintain their validity and revocability.	Articles 3, 4	WZ-03-03	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, in accordance with the technical specifications of CIR (EU) 2024/2979 and maintaining WUA validity and revocability; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including conformity with CIR (EU) 2024/2979 technical specifications; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process, including evidence that WUA validity and revocability are maintained.
REQ-2979-W02	Commission Implementing Regulation (EU) 2024/2979	Wallet Provider shall implement logging and data portability for users and ensure users can revoke their wallet unit.	Articles 6, 7, 9, 13	WZ-03-03	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed Wallet Provider. The documented controls should define: - user actions supported for requesting, obtaining, storing, deleting, sharing, presenting or exporting data, including user-initiated revocation of the Wallet Unit; - controls ensuring that the function is transparent, traceable and under user control; - consent and access rules for provider access to wallet logs or logged information; - technical limits, critical-asset exceptions and safeguards for secure portability or export.	The assessor tests selected revocation, suspension or validity-status cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sample should show: - demonstrations or records showing the user initiating the relevant action, including revocation of the Wallet Unit; - exported data or logs and evidence of integrity, authenticity and confidentiality protection; - consent records where the provider accesses logs for wallet-service purposes; - negative cases where export, deletion, sharing, Wallet Unit revocation or provider access is blocked for security or lack of consent.
REQ-2979-W03	Commission Implementing Regulation	Wallet Provider shall ensure that wallet users can receive qualified	Article 11(1)- (2)	WZ-03-03	The assessor reviews Wallet integration with qualified certificate and signing or sealing functions for the assessed Wallet Provider:	The assessor tests selected signing, sealing or qualified-certificate scenarios for the assessed Wallet Provider during the on-site Stage 2

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2979	certificates for qualified electronic signatures or seals and that Wallet Solutions securely interface with supported signature or seal creation environments.			- supported qualified certificate, signature or seal creation journeys; - interfaces between the Wallet Solution and signature or seal creation environments; - mandatory formats, CSC API support and security controls for integrated applications where applicable; - evidence that the Wallet does not weaken the certified signing or sealing environment.	assessment: - user journeys for obtaining or using qualified certificates, signatures or seals; - interface traces, configuration and supported format evidence; - security checks around authentication, consent and key-use authorisation; - negative or unsupported cases showing that unapproved signing or sealing paths are blocked.
REQ-2979-W04	Commission Implementing Regulation (EU) 2024/2979	Where signature creation applications are provided or integrated with Wallet Instances, Wallet Provider shall ensure that they support the required signing and sealing functions, mandatory formats and, where applicable, the CSC API.	Article 12 and Annex IV	WZ-03-03	The assessor reviews Wallet integration with qualified certificate and signing or sealing functions for the assessed Wallet Provider: - supported qualified certificate, signature or seal creation journeys; - interfaces between the Wallet Solution and signature or seal creation environments; - mandatory formats, CSC API support and security controls for integrated applications where applicable; - evidence that the Wallet does not weaken the certified signing or sealing environment.	The assessor tests selected signing, sealing or qualified-certificate scenarios for the assessed Wallet Provider during the on-site Stage 2 assessment: - user journeys for obtaining or using qualified certificates, signatures or seals; - interface traces, configuration and supported format evidence; - security checks around authentication, consent and key-use authorisation; - negative or unsupported cases showing that unapproved signing or sealing paths are blocked.
REQ-847-W01	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall establish and implement the criteria for assessing a security breach in the wallet solution that include: a) the breach or compromise has caused or is capable of causing the death of a natural person or considerable damage to a natural person's health; b) a successful suspectedly malicious or unauthorised access to the network and information systems has	Annex, Point 1	WZ-03-03	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider. The documentation should show: - criteria covering health impact, unauthorised access, service unavailability, physical-access compromise, data compromise, vulnerable users, certification cancellation and financial loss; - thresholds and data sources used to assess affected users, duration, operational disruption and personal-data impact, including unavailability for more than 12 consecutive hours, unavailability for more than 16 hours on a calendar-week basis,	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - incident records mapped to each applicable breach criterion and threshold, including 12-hour and 16-hour unavailability thresholds, 1% or 100 000 affected-user thresholds, and EUR 500 000 or 5% turnover financial-loss thresholds; - monitoring, access, vulnerability, data-impact, certification or financial evidence supporting the classification; - evidence for suspected malicious activity, known-vulnerability involvement, personal-

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		occurred, or is capable of occurring, in a way that is capable of causing severe operational disruption, c) a wallet solution, or a part of it: - is completely or projected to be completely unavailable to wallet users or wallet-relying parties for more than 12 consecutive hours; - is unavailable or projected to be unavailable to wallet users or wallet-relying parties, for more than 16 hours calculated on a calendar week basis there is a capability of compromise or there has been a compromise of physical access restricted to trusted personnel of concerned entities, or of the protection of such physical access, to one or more of the locations of network and information systems supporting the wallet solution; d) the privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the wallet solution is compromised, or is capable of being compromised, in one or more of the following ways: – it has an impact on more than 1 % of the wallet users of the			impact on more than 1% of wallet users or more than 100 000 users whichever is smaller, and financial loss exceeding EUR 500 000 or 5% of annual turnover whichever is lower; - criteria covering successful suspectedly malicious activity, known vulnerabilities, personal-data breach risk, impact on electronic communications, high risk to rights and freedoms, vulnerable natural persons and cancelled or projected cancelled certification; - roles responsible for classifying the breach and deciding on notification, suspension, withdrawal or revocation remedies; - links between the classification criteria and incident records, monitoring data, vulnerability records and certification status.	data breach risk, electronic-communications impact, high risk to rights and freedoms, vulnerable-person impact and certification cancellation or projected cancellation where applicable; - decisions where criteria were met, not met or uncertain, including management approval and escalation; - resulting notifications or remedies such as suspension, withdrawal, WUA revocation or user communication.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		affected wallet solution or on more than 100 000 of those wallet users, whichever number is smaller; – it is a result of a successful suspectedly malicious activity; – it is a result or is likely to be a result of one or more known vulnerabilities, including those handled in accordance with Commission Implementing Regulation (EU) 2024/2981 (1); – it is likely to impact personal data in a manner that is likely to result in a risk to the rights and freedoms of the natural persons concerned and, in particular, in case of breach of personal data as defined in Articles 9(1) and 10 of Regulation (EU) 2016/679; – it is likely to impact personal electronic communications; – it is likely to result in a high risk to the rights and freedoms of natural persons; – -it is likely to impact vulnerable natural persons; e) the certification of the wallet solution has been cancelled or is projected to be cancelled; f) (h) the breach or compromise has caused or is capable of causing				

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		direct financial loss for a concerned entity, and that loss exceeds EUR 500 000 or, where applicable, 5 % of the concerned entity's total annual turnover in the preceding financial year, whichever is lower. Z komentarzem [EA1]: Kompletnie zmieniłam, ponieważ punkt 1 Aneksu jest o kryteriach a nie o zdolnościach do monitorowania i wykrywania				
REQ-847-W02	Commission Implementing Regulation (EU) 2025/847	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8) , requirements b) , c) and e) of REQ-847-W01 apply to this service as well..	Annex, Point 1	WZ-03-03	The assessor reviews how breach-assessment criteria are applied to validation mechanisms provided by the assessed Wallet Provider under Article 5a(8). The documentation should define: - the validation mechanisms in scope and their supporting architecture; - application of REQ-847-W01 criterion b) for malicious or unauthorised access capable of causing severe operational disruption; - application of REQ-847-W01 criterion c) for service unavailability, projected unavailability and restricted physical-access compromise; - application of REQ-847-W01 criterion e) for cancellation or projected cancellation of certification; - links between validation-mechanism monitoring, classification, notification and remedy decisions.	The assessor tests selected validation-mechanism incidents or exercises for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - service scope and monitoring evidence for validation mechanisms; - incident or event records mapped to REQ-847-W01 criterion b) for unauthorised or malicious access; - availability, projected-unavailability and physical-access evidence mapped to criterion c); - certification-status evidence mapped to criterion e); - classification decisions, notifications or remedies for validation mechanisms, including rationale where criteria were not met.
REQ-847-W03	Commission Implementing Regulation	As regards point (c) of paragraph 1, the duration of an incident affecting availability shall be	Annex 1 Point 3	WZ-03-03	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider. The documented	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2025/847	measured from the moment the proper provision of the affected service is disrupted until the moment the service is restored and operational again. Where the Wallet Provider is unable to determine the moment when the disruption began, the duration of the incident shall be measured from the moment the incident was detected, or from the moment when the incident was recorded in network or system logs or other data sources, whichever is earlier. Complete unavailability of a service shall be measured from the moment the service is fully unavailable to users, to the moment when regular activities or operations have been restored to the level of service provided prior to the incident. Where the Wallet Provider is unable to determine when the complete unavailability of a service began, the unavailability shall be measured from the moment it was detected by the provider.			arrangements should define: - start and end rules for disruption, complete unavailability and limited availability, including measurement from the moment proper provision of the affected service is disrupted until the service is restored and operational again; - monitoring sources, logs and response-time metrics used when exact disruption times are uncertain, including measurement from detection time or from the moment recorded in network or system logs or other data sources, whichever is earlier; - complete-unavailability rules measuring from full unavailability to users until regular activities or operations have been restored to the pre-incident level of service, and from detection where the start cannot be determined; - thresholds for 12-hour, 16-hour weekly or response-time based assessment where applicable; - link between availability measurement and breach classification, notification and remedy decisions.	show: - monitoring records, logs and incident timelines establishing start, detection and restoration times, including evidence of the earlier of detection time or network/system-log or other data-source recording where the disruption start cannot be determined; - evidence that complete unavailability was measured from full unavailability to users until restoration of regular activities or operations to the pre-incident level of service; - calculations for consecutive and weekly unavailability thresholds; - response-time evidence used to determine limited availability; - classification decisions and notifications triggered by the measured impact.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-847-04	Commission Implementing Regulation (EU) 2025/847	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8), REQ-847-W03 applies to this service as well.	Annex, Point 3	WZ-03-03	The assessor reviews how availability-impact measurement rules are applied to validation mechanisms provided by the assessed Wallet Provider under Article 5a(8). The documentation should define: - validation mechanisms in scope; - start and end rules for disruption and complete unavailability of those validation mechanisms; - fallback rules where the start of disruption cannot be determined, including detection time and network or system logs or other data sources; - monitoring, logging and data sources used to measure availability impact; - links between measured availability impact, classification, notification and remedy decisions.	The assessor tests selected availability-impact cases for validation mechanisms during the on-site Stage 2 assessment. The evidence should include: - monitoring records, logs and incident timelines for validation mechanisms; - evidence establishing disruption start, detection, log-recording time and restoration time; - calculations applying REQ-847-W03 measurement rules to validation-mechanism availability incidents; - classification decisions, notifications or remedies triggered by the measured impact; - rationale where no availability-impact classification was triggered.
REQ-847-W05	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall implement objective criteria for defining limited availability which shall be based on the average response times of services shall be used to assess delays in response time.	Annex, Point 4	WZ-03-03	The assessor reviews objective limited-availability criteria maintained by the assessed Wallet Provider. The documentation should define: - services and functions to which limited-availability assessment applies; - average response-time metrics used to define limited availability; - criteria used to assess delayed response times; - monitoring sources, logs and calculation rules for response-time evidence; - link between limited-availability criteria, breach classification and notification decisions.	The assessor checks selected limited-availability cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - monitoring records and response-time data for affected services; - calculations of average response times and delayed response times; - application of objective criteria used to determine limited availability; - classification decisions and notifications triggered by limited availability; - cases where limited availability was considered but not confirmed and the rationale for that decision.
REQ-847-W-06	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall determine direct financial losses resulting from a breach or compromise referred to in point (h) of	Annex, Point 5	WZ-03-03	The assessor reviews how the assessed Wallet Provider calculates direct financial loss for breach or compromise assessment: - categories of costs included and excluded from incident-related financial-loss	The assessor checks selected breach or incident financial assessments for the assessed Wallet Provider during the on-site Stage 2 assessment: - cost calculations covering replacement,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		paragraph 1. The Wallet Provider shall take into account all financial losses incurred as a result of the incident, such as costs for replacement or relocation of software, hardware or infrastructure, staff costs, including costs associated with replacement or relocation of staff, recruitment of extra staff, remuneration of overtime and recovery of lost or impaired skills, fees due to non-compliance with contractual obligations, costs for redress and compensation to customers, losses due to forgone revenues, costs associated with internal and external communication, and advisory costs, including costs associated with legal counselling, forensic services and remediation services. Costs necessary for the day-to-day operation of the business, such as costs for general maintenance of infrastructure, equipment, hardware and software, improvements and risk assessment initiatives, and insurance premiums shall			calculation; - data sources used for actual costs and estimation rules where actual amounts are unavailable; - thresholds based on fixed amount or percentage of annual turnover, where applicable; - approval, evidence retention and escalation when thresholds are met or uncertain.	relocation, staffing, contractual, compensation, communication and advisory costs where relevant; - evidence supporting exclusions for ordinary business-as-usual costs; - turnover data or threshold calculations used for classification; - management decisions and notifications based on the calculated or estimated loss.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		not be considered as financial losses resulting from an incident. Wallet Provider shall calculate the amounts of financial losses based on available data and, where the actual amounts of financial losses cannot be determined, Wallet provider shall estimate those amounts.				
REQ-847-W-07	Commission Implementing Regulation (EU) 2025/847	Where the Wallet Provider provides the validation mechanisms referred to in Article 5a(8), REQ-847-W06 applies to this service as well.	Annex, Point 5	WZ-03-03	The assessor reviews how direct-financial-loss assessment is applied to validation mechanisms provided by the assessed Wallet Provider under Article 5a(8). The documentation should define: - validation mechanisms in scope; - financial-loss categories included and excluded for breaches or compromises affecting those mechanisms; - data sources used for actual cost calculation and estimation rules where actual amounts cannot be determined; - thresholds based on fixed amount or percentage of annual turnover where applicable; - approval, evidence retention, classification and notification rules for validation-mechanism financial-loss assessments.	The assessor checks selected financial-loss assessments for validation-mechanism breaches or compromises during the on-site Stage 2 assessment. The evidence should include: - cost calculations for events affecting validation mechanisms; - evidence supporting included and excluded cost categories; - available data and estimation evidence where actual financial-loss amounts could not be determined; - turnover data or threshold calculations used for classification; - management decisions, notifications or remedies based on the calculated or estimated financial loss.
REQ-847-W08	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall maintain mechanisms to revoke wallet unit attestations of affected wallet units where this is required as a remedy.	Article 4(2)	WZ-03-03	The assessor reviews WUA revocation mechanisms maintained by the assessed Wallet Provider. The documentation should define: - conditions under which Wallet Unit Attestations of affected Wallet Units are revoked as a remedy; - roles, approvals and system actions used to perform such revocation;	The assessor checks selected remedy cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - affected Wallet Units identified for WUA revocation; - records showing revocation of Wallet Unit Attestations where required as a remedy; - status publication and user-notification

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- links between breach, suspension, withdrawal or remedy decisions and WUA revocation; - status publication, user notification and evidence retained for affected Wallet Units; - handling of failed or delayed revocation actions.	evidence where applicable; - timing from remedy decision to WUA revocation; - exceptions, failed revocations or delayed actions and related corrective measures.
REQ-847-W09	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that, upon withdrawal, wallet unit attestations of affected wallet units are revoked and cannot revert to a valid state.	Article 8(2)(a), Article 8(2)(b)	WZ-03-03	The assessor reviews withdrawal-triggered WUA revocation controls maintained by the assessed Wallet Provider. The documentation should define: - how affected Wallet Units are identified upon withdrawal; - automatic or manual steps used to revoke Wallet Unit Attestations of affected Wallet Units; - controls preventing revoked Wallet Unit Attestations from reverting to a valid state; - status publication, notification and evidence retained after withdrawal; - handling of exceptional or failed withdrawal actions.	The assessor checks selected withdrawal cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - affected Wallet Units identified after withdrawal; - Wallet Unit Attestations revoked for those affected Wallet Units; - status history confirming that revoked attestations did not revert to a valid state; - configuration or process controls preventing reinstatement of revoked WUA; - exception, delay or correction records where withdrawal actions did not complete normally.
REQ-847-W10	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that, upon withdrawal, no new wallet unit attestation can be issued to existing wallet units provided under the affected wallet solution.	Article 8(2)(c)	WZ-03-03	The assessor reviews controls preventing new WUA issuance after withdrawal of an affected wallet solution. The documentation should define: - how affected wallet solutions and existing Wallet Units are identified after withdrawal; - rules blocking issuance of new Wallet Unit Attestations to existing Wallet Units under the affected wallet solution; - systems, roles and approvals enforcing the block; - monitoring and exception handling for attempted post-withdrawal issuance; - evidence retained for blocked or rejected issuance attempts.	The assessor checks selected withdrawal cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - the affected wallet solution and existing Wallet Units in scope; - configuration or workflow controls blocking new WUA issuance to existing Wallet Units under the affected solution; - rejected or blocked issuance attempts after withdrawal; - logs or status records showing that no new WUA was issued where the prohibition applied; - exception records and corrective actions if attempted issuance occurred.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-847-W11	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that, upon withdrawal, no new wallet unit can be provided under the affected wallet solution.	Article 8(2)(d)	WZ-03-03	The assessor reviews remedies applied by the assessed Wallet Provider when a wallet solution is suspended, withdrawn or otherwise affected: - conditions triggering revocation of affected Wallet Unit Attestations or restriction of Wallet Unit provisioning; - controls preventing new attestations or new Wallet Units under the affected wallet solution where prohibited; - security criteria for allowing data portability during suspension or withdrawal; - records linking the remedy to the breach, compromise or withdrawal decision.	The assessor tests selected suspension, withdrawal or remedy cases for the assessed Wallet Provider during the on-site Stage 2 assessment: - attestation-revocation records and status-service evidence for affected Wallet Units; - configuration or process controls blocking new attestations or Wallet Units where required; - data-portability cases reviewed against critical-asset security constraints; - user, CAB or supervisory communications associated with the remedy.
REQ-847-W12	Commission Implementing Regulation (EU) 2025/847	Wallet Provider shall ensure that data portability during suspension or withdrawal is technically supported only where it does not impair the security of critical assets of affected wallet units.	Article 4(4), Article 8(3)	WZ-03-03	The assessor reviews data-portability arrangements for suspension or withdrawal scenarios maintained by the assessed Wallet Provider. The documentation should define: - when data portability remains technically supported during suspension or withdrawal; - critical assets of affected Wallet Units and security conditions protecting them; - criteria for blocking or limiting portability where it would impair critical-asset security; - user communication, support and evidence retained for portability decisions; - links between suspension/withdrawal decisions, critical-asset assessment and portability controls.	The assessor tests selected suspension or withdrawal cases involving data portability during the on-site Stage 2 assessment. The evidence should show: - whether data portability was technically supported, limited or blocked; - critical assets of affected Wallet Units considered in the decision; - security assessment showing that portability did not impair those critical assets where it was allowed; - user-facing records, exported data or support tickets for portability requests; - negative cases where portability was blocked or limited because it would impair critical-asset security.
WZR-01	REQ-5c-04; REQ-2981-W03	Wallet Provider shall ensure that the EUDI Wallet solution is certified by a conformity assessment body accredited under G-05 and designated by the Republic of Poland, prior to making the wallet available	Alignment with international standards - ISO/IEC 17067 (conformity assessment); ETSI EN 319 401	WZ-03-03	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - evidence that the EUDI Wallet solution is certified by a conformity assessment body accredited under G-05 and designated by the	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate of conformity and evidence that the CAB is accredited under G-05 and designated by the Republic of Poland; - release or availability records showing that

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		to users, and shall maintain a valid certificate of conformity for the duration of the wallet's availability. The certificate shall cover the wallet unit, the wallet secure cryptographic application (WSCA) and the wallet secure cryptographic device (WSCD) components as applicable to the wallet architecture.	§7.1 (general obligations).		Republic of Poland; - evidence that certification was completed before the wallet was made available to users; - valid certificate of conformity maintained for the duration of the wallet's availability; - certificate scope covering the Wallet Unit, WSCA and WSCD components as applicable to the wallet architecture; - mapping between certified components, deployed wallet architecture and components made available to users; - process for maintaining certificate validity and notifying or updating CAB evidence after material changes.	certification preceded wallet availability to users; - evidence that the certificate remained valid during the period when the wallet was available; - certificate scope, assessment report and component list covering Wallet Unit, WSCA and WSCD where applicable; - comparison between deployed wallet architecture and certified scope; - records of renewals, changes, conditions, findings or CAB notifications.
WZR-02	REQ-5c-01; REQ-2981-W02, REQ-2981-W03, REQ-2981-W04	Wallet Provider shall define and document the scope of certification, covering all software components installed on user devices and all back- end systems that form part of the wallet unit as defined in CIR (EU) 2024/2981. Wallet Provider shall establish a documented governance framework defining management responsibility, decision-making authority, accountability and approval of wallet policies and practices. Wallet Provider shall maintain a Wallet Provider Practice Statement, or an equivalent documented set of policies and procedures, describing the controls used to provide, operate, maintain	Alignment with international standards - ISO/IEC 17067 §6.4 (scheme scope); CIR (EU) 2024/2981 Article 3, ETSI EN 319 401, Clause 6.1.	WZ-03-03	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider. The review should confirm: - whether the certification scope covers the Wallet Unit, WSCA, WSCD, backend systems or other components required by the architecture, including all software components installed on user devices and all back-end systems that form part of the Wallet Unit as defined in CIR (EU) 2024/2981; - validity, assurance level, certification body and scheme used for the certificate; - alignment between the documented scope, the deployed service and the components made available to users, including consistency with CIR (EU) 2024/2981; - documented governance framework defining management responsibility, decision-making authority, accountability and approval of wallet policies and practices; - Wallet Provider Practice Statement or equivalent documented set of policies and	The assessor checks certification and scope evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current certificate, assessment report, certification scope and component list, including all software components installed on user devices and all back-end systems forming part of the Wallet Unit; - comparison between deployed components and the certified scope, including consistency with CIR (EU) 2024/2981; - governance framework records showing management responsibility, decision-making authority, accountability and approval of wallet policies and practices; - Wallet Provider Practice Statement or equivalent policies and procedures describing controls for Wallet Solutions and Wallet Units; - evidence that the certification scope was agreed with the CAB; - records of changes, renewals, conditions, findings or notifications to the certification body.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		Wallet Solutions and Wallet Units.The scope shall be agreed with the CAB and shall be consistent with CIR (EU) 2024/2981.			procedures describing controls used to provide, operate and maintain Wallet Solutions and Wallet Units; - evidence that the certification scope is agreed with the CAB.	
WZR-03	REQ-5c-01 (Article 5a (3) eIDAS)	In accordance with Article 5a (3) of eIDAS, the source code of the application software components of the EUDI Wallet installed on user devices shall be published under an open-source licence. Where duly justified reasons exist for not disclosing the source code of specific components other than those installed on user devices, Wallet Provider shall document those reasons and notify the Ministry of Digital Affairs.	Alignment with international standards - Article 5a (3) eIDAS.	WZ-03-03	The assessor reviews source-code disclosure arrangements maintained by the assessed Wallet Provider. The documentation should identify: - application software components of the EUDI Wallet installed on user devices; - how the source code of those components is published under an open-source licence; - licence, repository, versioning and release-approval rules for published source code; - components not installed on user devices for which non-disclosure is claimed; - documented justification for any non-disclosure and notification to the Ministry of Digital Affairs.	The assessor checks source-code disclosure evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - public repositories for application software components installed on user devices; - open-source licence evidence for the published source code; - version and release records linking published source code to the wallet version made available to users; - documented reasons for any non-disclosed components outside the user-device scope; - notification evidence to the Ministry of Digital Affairs where non-disclosure is relied upon.
WZR-04	REQ-2981-W07	Wallet Provider shall make publicly available the following information: the certificate of conformity (or a reference thereto), the certification body identifier, the scope of certification, the validity period of the certificate, and the cybersecurity certification scheme applied. This information shall be electronically signed or sealed in the form suitable for automated processing. This information shall be	Alignment with international standards - CIR (EU) 2024/2981 Article 8(5) and Annex V; ISO/IEC 17067 §6.4.	WZ-03-03	The assessor reviews public-certification-information arrangements maintained by the assessed Wallet Provider. The documentation should define: - public availability of the certificate of conformity or a reference to it; - publication of certification body identifier, certification scope, certificate validity period and cybersecurity certification scheme applied; - electronic signature or seal applied to the information in a form suitable for automated processing; - update rules without undue delay after any change affecting the information;	The assessor checks public-certification-information evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - current public page, repository or machine-processable publication containing the certificate of conformity or reference to it; - published certification body identifier, certification scope, certificate validity period and cybersecurity certification scheme applied; - electronic signature or seal validation evidence for the published information; - change records and timestamps showing updates without undue delay; - comparison between public certification

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		updated without undue delay upon any change affecting it.			- ownership, approval and evidence retained for publication changes.	information and current certificate/scope evidence.
WZR-05	REQ-5c-02; REQ-2981-W06	Wallet Provider shall certify those components of the EUDI Wallet that are relevant for cybersecurity in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 and referenced in the implementing acts under Article 5c (6) of eIDAS. Wallet Provider shall identify the applicable scheme(s) and confirm with the CAB the coverage against the cybersecurity requirements of Article 5c (2) of eIDAS.	Alignment with international standards - Regulation (EU) 2019/881 (EU Cybersecurity Act), Articles 49-56.	WZ-03-03	The assessor reviews cybersecurity-certification planning maintained by the assessed Wallet Provider. The documentation should confirm: - which EUDI Wallet components are relevant for cybersecurity; - the European cybersecurity certification scheme applied under Regulation (EU) 2019/881; - references to implementing acts under Article 5c(6) of eIDAS; - how the selected scheme covers Article 5c(2) cybersecurity requirements; - how the Wallet Provider confirms coverage with the CAB and manages gaps or changes.	The assessor checks cybersecurity-certification coverage for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - component list identifying EUDI Wallet components relevant for cybersecurity; - certificate and assessment report under the applicable European cybersecurity certification scheme; - evidence linking the scheme to Regulation (EU) 2019/881 and Article 5c(6) implementing acts; - CAB confirmation of coverage against Article 5c(2) cybersecurity requirements; - records of uncovered items, changes, conditions or follow-up actions.
WZR-06	REQ-5c-03; REQ-2981-W01	For requirements not covered by European cybersecurity certification schemes, Wallet Provider shall comply with the national certification scheme established pursuant to Article 5c (3) of eIDAS and the implementing acts under Article 5c (6), as incorporated in this document and in the GP-03 framework. The CAB shall evaluate compliance with this national scheme as part	Alignment with international standards - CIR (EU) 2024/2981 Article 6; GP -03 §6 (evaluation methodology).	WZ-03-03	The assessor reviews national-certification-scheme arrangements maintained by the assessed Wallet Provider. The documentation should define: - requirements not covered by European cybersecurity certification schemes; - national certification scheme requirements applied under Article 5c(3) of eIDAS and Article 5c(6) implementing acts; - how those requirements are incorporated in GP-03 and the assessed document set; - CAB responsibilities for evaluating compliance with the national scheme; - evidence needed to show compliance and manage changes in coverage.	The assessor checks national-certification-scheme compliance evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - assessment records for requirements not covered by European cybersecurity certification schemes; - evidence of compliance with the national certification scheme established under Article 5c(3); - references to applicable Article 5c(6) implementing acts and GP-03 requirements; - CAB evaluation evidence for national-scheme requirements; - findings, conditions or change records affecting national-scheme coverage.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		of the conformity assessment.				
WZR-07	REQ-2981-W01, REQ-847-W02	Wallet Provider shall establish and maintain a risk register for the EUDI Wallet architecture, covering the cybersecurity risks and threats identified in Annex I to CIR (EU) 2024/2981. The risk register shall be updated following any material change to the wallet architecture, a significant incident, or new threat intelligence, and shall be made available to the CAB.	Alignment with international standards - CIR (EU) 2024/2981 Article 8(1) and Annex I; G-04 Risk Register.	WZ-03-03	The assessor reviews the EUDI Wallet architecture risk register maintained by the assessed Wallet Provider. The review should confirm: - coverage of cybersecurity risks and threats identified in Annex I to CIR (EU) 2024/2981; - mapping between wallet architecture components, assets, threats, vulnerabilities and risk-treatment measures; - update triggers following material architecture changes, significant incidents or new threat intelligence; - risk owners, treatment status, residual-risk acceptance and overdue actions; - arrangements for making the risk register available to the CAB.	The assessor checks selected risk-register records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - current EUDI Wallet architecture risk register covering Annex I CIR (EU) 2024/2981 risks and threats; - sampled risks mapped to wallet architecture components, controls and treatment actions; - updates after material architecture changes, significant incidents or new threat intelligence; - management acceptance of residual risks and tracking of treatment actions; - evidence that the risk register is available to the CAB.
WZR-08	REQ-5c-04; REQ-2981-W03	Wallet Provider shall initiate recertification whenever material changes to the wallet software, cryptographic components, or operational architecture may affect conformity. The threshold for triggering recertification shall be defined in the certification plan agreed with the CAB and consistent with Article 4 of CIR (EU) 2024/2981. Wallet Provider shall maintain continuous compliance between certification cycles.	Alignment with international standards - CIR (EU) 2024/2981 Article 4; ISO/IEC 17067 §6.7 (surveillance).	WZ-03-03	The assessor reviews recertification and continuous-compliance arrangements maintained by the assessed Wallet Provider. The documentation should define: - material-change triggers for wallet software, cryptographic components and operational architecture; - thresholds for triggering recertification in the certification plan agreed with the CAB; - alignment with Article 4 of CIR (EU) 2024/2981; - controls for maintaining continuous compliance between certification cycles; - records used to evidence change assessment, CAB interaction and recertification decisions.	The assessor checks recertification and continuous-compliance evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled changes to wallet software, cryptographic components or operational architecture; - assessment of those changes against certification-plan thresholds agreed with the CAB; - recertification decisions and related CAB communications; - evidence that continuous compliance was monitored between certification cycles; - cases where recertification was triggered, not triggered or deferred with documented rationale.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WZR-09	REQ-5c-02; REQ-2981-W02	Wallet Provider shall ensure that the EUDI Wallet uses a Wallet Secure Cryptographic Device (WSCD) and a Wallet Secure Cryptographic Application (WSCA) meeting the requirements specified in CIR (EU) 2024/2981 and the applicable cybersecurity certification scheme. The WSCD shall provide an environment for cryptographic operations in which private keys cannot be extracted and are bound to the wallet unit.	Alignment with international standards - CIR (EU) 2024/2981 Annex I (cryptographic requirements); ARF (current version). 5.3.2 Wallet Unit Attestation (WUA)	WZ-03-03	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider. The review should establish: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - WSCD/WSCA use and evidence of protected key generation, storage and operation, including evidence that the WSCD and WSCA meet CIR (EU) 2024/2981 and the applicable cybersecurity certification scheme requirements; - WSCD controls ensuring that private keys cannot be extracted and are bound to the Wallet Unit; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components, including conformity with CIR (EU) 2024/2981 and the applicable cybersecurity certification scheme; - key-generation, use, rotation, revocation or destruction records, including evidence that private keys are non-extractable and bound to the Wallet Unit; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
WZR-10	REQ-5c-01; REQ-2981-W02	Wallet Provider shall implement the issuance and management of Wallet Unit Attestations (WUA) in accordance with CIR (EU) 2024/2981 and CIR (EU) 2024/2979. Each wallet unit issued by Wallet Provider shall hold a valid WUA signed by Wallet Provider using a key pair protected in accordance with the cryptographic requirements applicable at assurance level High.	Alignment with international standards - CIR (EU) 2024/2981; CIR (EU) 2024/2979 (wallet protocols and interfaces). 5.3.3 Key Management for Wallet Operations	WZ-03-03	The assessor reviews how the assessed Wallet Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including issuance and management of WUA in accordance with CIR (EU) 2024/2981 and CIR (EU) 2024/2979; - certificate and trust-list requirements used for attestation signing or sealing; - controls ensuring that each Wallet Unit issued by the Wallet Provider holds a valid WUA; - protection of the key pair used by the Wallet Provider to sign WUA in accordance with cryptographic requirements applicable at	The assessor checks selected Wallet Unit attestation cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including conformity with CIR (EU) 2024/2981 and CIR (EU) 2024/2979; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - sampled Wallet Units showing that each issued Wallet Unit holds a valid WUA; - evidence that the WUA signing key pair is protected in accordance with cryptographic requirements applicable at assurance level High;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					assurance level High; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - rules excluding personal data from attestations where the requirement prohibits such data.	- attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.
WZR-11	REQ-5c-02; REQ-2690-W07	Wallet Provider shall implement key management procedures for all cryptographic key material used in wallet operations, including WUA signing keys, cryptographic binding of PID and attestations, and keys used for wallet-to-relying-party authentication. Key management shall comply with the requirements of WZ-03-01 (EP-55 and EP-56) and the applicable cybersecurity certification scheme.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); ETSI EN 319 401 §7.6 (cryptographic modules).	WZ-03-03	The assessor reviews key-management procedures maintained by the assessed Wallet Provider. The documentation should cover: - all cryptographic key material used in wallet operations; - WUA signing keys, keys used for cryptographic binding of PID and attestations, and wallet-to-relying-party authentication keys; - key generation, protection, use, rotation, revocation, backup and destruction controls; - compliance with WZ-03-01 EP-55 and EP-56 and the applicable cybersecurity certification scheme; - evidence retained for key lifecycle events, exceptions and reviews.	The assessor checks selected key-management evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - inventories or configuration records for WUA signing keys, PID/attestation binding keys and wallet-to-relying-party authentication keys; - key-generation, use, rotation, revocation, backup or destruction records; - evidence that key-management procedures comply with WZ-03-01 EP-55 and EP-56 and the applicable cybersecurity certification scheme; - access-control and protection evidence for key material; - migration, exception or incident records involving cryptographic key material.
WZR-12	REQ-5c-01 (Article 5a (14) eIDAS)	In accordance with Article 5a (14) of eIDAS, Wallet Provider shall ensure that personal data relating to the provision of the EUDI Wallet is kept logically separate from any other data held by Wallet Provider. The implementation of this logical separation shall be documented and verifiable by the CAB.	Alignment with international standards - Article 5 a (14) eIDAS; ISO/IEC 27001:2022 A.8.3 (information access restriction); GDPR Article 25 (data protection by design).	WZ-03-03	The assessor reviews logical-separation documentation maintained by the assessed Wallet Provider. The documentation should show: - personal data relating to the provision of the EUDI Wallet; - other data held by the Wallet Provider from which that personal data must be logically separated; - architecture, data stores, interfaces and access controls implementing the separation; - evidence package that makes the logical separation verifiable by the CAB;	The assessor checks logical-separation implementation for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - architecture diagrams, database or tenant-separation evidence and access-control configuration; - samples showing separation of personal data relating to EUDI Wallet provision from other data held by the Wallet Provider; - data-flow or log evidence confirming that separation is applied in operational processes;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- governance for exceptions, changes and access to separated data.	- documentation and evidence available for CAB verification; - exceptions or support cases showing controlled access to separated data.
WZR-13	REQ-5c-01 (Article 5a (14) eIDAS)	Wallet Provider shall not collect information about the use of the EUDI Wallet which is not necessary for the provision of wallet services, and shall not combine person identification data or any other personal data stored or relating to the use of the EUDI Wallet with personal data from other services offered by Wallet Provider or from third-party services, unless the user has expressly requested otherwise.	Alignment with international standards - GDPR Articles 5(1)(b), (c) (purpose limitation, data minimisation); Article 5a (14) eiders.	WZ-03-03	The assessor reviews non-collection and non-combination controls maintained by the assessed Wallet Provider. The documentation should show: - what information about use of the EUDI Wallet is collected; - why each collected wallet-use data element is necessary for provision of wallet services; - controls preventing collection of wallet-use information that is not necessary; - controls preventing combination of PID or other wallet-related personal data with data from other Wallet Provider services or third-party services; - how explicit user requests are captured and evidenced where an exception to non-combination is used.	The assessor checks non-collection and non-combination implementation for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - sampled data flows, logs, analytics settings or database records showing wallet-use information collected in operation; - evidence that collected use data is necessary for the wallet service; - configuration or access-control evidence preventing cross-service or third-party data combination; - cases where combination occurred only on the basis of an explicit user request; - negative or exception cases showing that unauthorised collection or combination was blocked or corrected.
WZR-14	REQ-5c-01 (Article 5a (16) eIDAS)	In accordance with Article 5a(16) of eIDAS, Wallet Provider shall implement a technical framework that does not allow any party, after the issuance of an attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, unless explicitly authorised by the user. Wallet Provider shall implement privacy-preserving techniques enabling unlikability where the attestation of attributes	Alignment with international standards - Article 5a (16) eIDAS; ARF (current version) §6 (privacy requirements).	WZ-03-03	The assessor reviews unobservability and unlinkability controls implemented by the assessed Wallet Provider: - architecture preventing attestation issuers or other parties from tracking later user transactions; - privacy-preserving techniques used where user identification is not required; - controls over telemetry, callbacks, identifiers and relying-party correlation; - conditions for explicit user authorisation where an exception is allowed.	The assessor tests selected attestation-use and transaction scenarios for the assessed Wallet Provider during the on-site Stage 2 assessment: - data-flow and log evidence showing that transaction use cannot be linked or correlated by unauthorised parties; - tests using attestations with relying parties without callback to the issuer; - configuration of identifiers, telemetry and analytics controls; - exception cases with explicit user authorisation and recorded justification.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		does not require identification of the user.				
WZR-15	REQ-5c-01 (Article 5a(4)(d) eIDAS); REQ-2979-W02 (CIR (EU) 2024/2979, Article 9(7))	Wallet Provider shall provide users with access to a log of all transactions carried out through the EUDI Wallet, via a common dashboard enabling the user to: view an up-to-date list of relying parties with which the user has established a connection and all data exchanged; easily request the erasure of personal data from a relying party pursuant to Article 17 of Regulation (EU) 2016/679 (GDPR); and report a relying party to the competent national data protection authority. Wallet Provider shall enable users to export the transaction log information kept by the Wallet Instance. Z komentarzem [MT5]: Nie jestem przekonany że jest to przypisane do providera a nie UNIT. Tak jak czytam literalnie to wymaganie to ono jest bardziej na certyfikację unitu niż funkcję providera walelta Z komentarzem [EA6R5]: Tak, zdecydowanie. Mamy to w zbiorze wymagań funkcjonalnych. Do	Alignment with international standards - Article 5a(4)(d) eIDAS; CIR (EU) 2024/2979 Article 9(7); GDPR Article 17 (right to erasure).	WZ-03-03	The assessor reviews transaction-log and dashboard arrangements maintained by the assessed Wallet Provider. The documentation should define: - user access to a log of all transactions carried out through the EUDI Wallet; - common dashboard functions showing an up-to-date list of relying parties and all data exchanged; - functions enabling users to request erasure from relying parties under Article 17 GDPR; - functions enabling users to report relying parties to the competent national data protection authority; - export of transaction-log information kept by the Wallet Instance; - security, integrity and access-control safeguards for the log and dashboard.	The assessor tests selected transaction-log and dashboard functions for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - user access to the transaction log through the common dashboard; - an up-to-date list of relying parties and all data exchanged in sampled cases; - user ability to request erasure from a relying party under Article 17 GDPR; - user ability to report a relying party to the competent national data protection authority; - export of transaction-log information kept by the Wallet Instance; - security controls protecting log integrity, access and confidentiality.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		usunięcia Alignment with international standards - Article 5a(4)(d) eIDAS; CIR (EU) 2024/2979 Article 9(7); GDPR Article 17 (right to erasure). 5.5 Operational Requirements 5.5.1 Assurance Level High				
WZR-16	Articles 5a(5)(d) and 5a (11) eIDAS; REQ-5c-01; REQ-1502-W01	The EUDI Wallet shall be provided under an electronic identification scheme with assurance level High, meeting all requirements of Article 8 of eIDAS as applied to identity proofing and verification and electronic identification means management and authentication.	Alignment with international standards - CIR (EU) 2015/1502 Annex Section 2; Article 8 eIDAS.	WZ-03-03	The assessor reviews assurance-level arrangements for the assessed Wallet Provider within the applicable electronic identification scheme. The documentation should confirm: - the EUDI Wallet is provided under an eID scheme at assurance level High; - mapping to Article 8 of eIDAS requirements; - coverage of identity proofing and verification, electronic identification means management and authentication; - dependencies on PID Provider, eID scheme governance and certification evidence; - change controls preventing operation outside the approved assurance-level scope.	The assessor checks selected assurance-level evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - scheme documentation, certification evidence and control mapping for assurance level High under Article 8 of eIDAS; - Wallet Unit activation, lifecycle or authentication cases linked to high-assurance controls; - evidence that identity proofing, verification, eID means management and authentication dependencies are implemented through the approved scheme and provider arrangements; - changes to scheme, provider or technical scope assessed before release; - lower-assurance or out-of-scope paths blocked or segregated.
WZR-17	Article 5 a(13) of eIDAS; Article 5a (15) eIDAS; REQ-5c-01 (Articles 5a (13) and 5a (15) eIDAS)	The issuance, use and revocation of the EUDI Wallet shall be free of charge to all natural persons. [Article 5 a(13) of eIDAS] The use of the wallet shall be voluntary; access to public and private services, access to the labour market and freedom to conduct business shall	Alignment with international standards - Articles 5a (13) and 5a (15) eIDAS.	WZ-03-03	The assessor reviews no-cost and voluntary-use controls for the EUDI Wallet operated by the assessed Wallet Provider: - user-facing terms confirming free issuance, use and revocation for natural persons; - processes preventing fees from being charged directly or indirectly for required wallet functions; - rules ensuring that non-use of the wallet does not disadvantage access to services, labour market or business activity;	The assessor checks selected user, billing and service-access evidence for the assessed Wallet Provider during the on-site Stage 2 assessment: - published terms, fee schedules and user journeys for issuance, use and revocation; - billing, invoicing or payment configuration showing no charges for natural persons; - service-access cases demonstrating alternatives for users who do not use the Wallet;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		not in any way be restricted or made disadvantageous to persons that do not use the EUDI Wallet.			- complaint or monitoring evidence for cost or coercion concerns.	- complaints or support cases related to charging or voluntary use and how they were resolved.
WZR-18	Article 5a (21) eIDAS; REQ-5c-01 (Article 5a (21) eIDAS)	The EUDI Wallet shall be made accessible for use by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 on the accessibility requirements for products and services (European Accessibility Act). [Article 5a (21) eIDAS] Wallet Provider shall document compliance with this requirement and present evidence to the CAB during the conformity assessment.	Alignment with international standards - Directive (EU) 2019/882 (European Accessibility Act); Article 5a (21) eIDAS.	WZ-03-03	The assessor reviews accessibility compliance documentation maintained by the assessed Wallet Provider. The review should confirm: - accessibility requirements for persons with disabilities on an equal basis with other users; - alignment with Directive (EU) 2019/882; - user journeys, support channels and service functions covered by accessibility controls; - evidence prepared for presentation to the CAB during conformity assessment; - handling of accessibility defects, complaints, exceptions and corrective actions.	The assessor checks selected accessibility evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - demonstration or screenshots of relevant user journeys and accessibility features; - evidence that persons with disabilities can use the EUDI Wallet on an equal basis with other users; - accessibility test results, audit evidence or conformance documentation aligned with Directive (EU) 2019/882; - support tickets, complaints or defect records related to accessibility; - evidence presented or available to the CAB and related corrective actions.
WZR-19	REQ-5c-01 (Article 5a(5)(g) eIDAS); REQ-2979-W03; REQ-2979-W04	Wallet Provider shall ensure that natural persons have, at least for non-professional purposes, free of charge access to signature creation applications enabling the creation of qualified electronic signatures through the EUDI Wallet. The implementation shall use qualified electronic signature creation devices (QSCDs) compliant with Annex II to eIDAS and shall support the interfaces required by CIR (EU) 2024/2979. Wallet	Alignment with international standards - Article 5a(5)(g) eIDAS; Annex II eIDAS (QSCD requirements); CIR (EU) 2024/2979; ETSI EN 319 411- 2; ETSI TS 119 431-2.	WZ-03-03	The assessor reviews qualified electronic signature and seal arrangements maintained by the assessed Wallet Provider. The documentation should cover: - free-of-charge access for natural persons, at least for non-professional purposes, to signature creation applications enabling qualified electronic signatures through the EUDI Wallet; - use of QSCDs compliant with Annex II to eIDAS; - supported journeys for qualified certificates, qualified electronic signatures and qualified electronic seals; - secure interfaces with local QSCD, external WSCD or remote QSCD qualified provider models, as applicable; - mandatory formats, CSC API support and	The assessor tests selected qualified electronic signature or seal journeys for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - free-of-charge access for natural persons to qualified electronic signature creation for non-professional purposes; - QSCD compliance evidence under Annex II to eIDAS where required; - user journeys for receiving qualified certificates and creating qualified signatures or seals; - interface traces, configuration and supported-format evidence for local QSCD, external WSCD or remote QSCD qualified provider models; - CSC API evidence where applicable;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		Provider shall ensure that wallet users can receive qualified certificates for qualified electronic signatures or seals and that the Wallet Solution securely interfaces with supported signature or seal creation environments, including local QSCD, external WSCD or remote QSCD qualified provider models, as applicable. Where signature creation applications are provided or integrated with Wallet Instances, they shall support the required signing and sealing functions, mandatory formats and, where applicable, the CSC API.			security controls for integrated signature or seal creation applications; - evidence that the Wallet does not weaken the certified signing or sealing environment.	- authentication, consent and key-use authorisation controls in sampled signing or sealing flows.
WZR-20	REQ-5c-01 (Article 5a (10) eIDAS)	Wallet Provider shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of the EUDI Wallet, as required by Article 5a (10) of eIDAS. The technical support channel shall be available continuously and shall have a documented response time consistent with the service level agreed under GP-03.	Alignment with international standards - Article 5a (10) eIDAS; ETSI EN 319 401 §7.2 (subscriber agreements).	WZ-03-03	The assessor reviews technical-support and incident-reporting arrangements maintained by the assessed Wallet Provider. The documentation should define: - user paths for requesting technical support and reporting technical problems or incidents affecting use of the EUDI Wallet; - continuous availability of the technical support channel; - documented response time consistent with the service level agreed under GP-03; - ownership, escalation and closure rules for support requests and incident reports; - records retained for requests, failures, complaints and response-time monitoring.	The assessor tests selected technical-support and incident-reporting cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - demonstration or screenshots of technical support and incident-reporting paths; - sampled support tickets, user requests or incident reports affecting Wallet use; - evidence that the support channel is continuously available; - response-time records compared with the GP-03 service level; - exceptions, delays, complaints or unresolved cases and how they were handled.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WZR-21	REQ-5c-01 (Article 5a (9) eIDAS); REQ-2981-W04; REQ-847-W16; REQ-847-W17; REQ-847- W18; REQ-847-W19; REQ-847-W20; REQ-847-W21	Wallet Provider shall ensure that the validity of the EUDI Wallet can be revoked upon the explicit request of the user, where the security of the wallet has been compromised, or upon the death of the user or the cessation of activity of the legal person, as required by Article 5a(9) of eIDAS. Revocation shall take effect without undue delay, and the user shall be informed without delay. The Wallet Provider shall be the only entity capable of revoking Wallet Unit Attestations for Wallet Units it has provided and shall establish a publicly available revocation policy defining conditions and timeframes. Wallet Provider shall ensure that suspension or withdrawal of a Wallet Solution is reflected in the lifecycle of affected Wallet Units and Wallet Unit Attestations, including prevention of further use, provision or activation where required, revocation of affected attestations, and controlled support for data portability where it does not impair	Alignment with international standards - Article 5a (9) eIDAS; Article 5e eIDAS (security breach); CIR (EU) 2024/2979, Article 7. 5.5.7 Record Keeping	WZ-03-03	The assessor reviews wallet validity and Wallet Unit Attestation revocation arrangements maintained by the assessed Wallet Provider. The documentation should define: - revocation of EUDI Wallet validity upon explicit user request, wallet security compromise, death of the user or cessation of activity of the legal person; - revocation taking effect without undue delay and user notification without delay; - controls ensuring that only the Wallet Provider can revoke WUA for Wallet Units it has provided; - publicly available revocation policy defining conditions and timeframes; - lifecycle impact of suspension or withdrawal of a Wallet Solution on affected Wallet Units and WUA; - controls for prevention of further use, provision or activation, WUA revocation and data portability where critical-asset security permits.	The assessor tests selected wallet revocation, suspension or withdrawal cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - user-requested revocation, compromise-related revocation, death or legal-person cessation cases where available; - timestamps showing revocation without undue delay and user notification without delay; - configuration or process evidence showing that only the Wallet Provider can revoke WUA for Wallet Units it has provided; - public revocation policy and sampled cases mapped to defined conditions and timeframes; - suspension or withdrawal cases showing prevention of further use, provision or activation and revocation of affected attestations; - data-portability decisions assessed against critical-asset security constraints.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the security of critical assets.				
WZR-22	REQ-2981-W08; REQ-1502-W01; REQ-847-W12; REQ-847-W13; REQ-847-W14	Wallet Provider shall maintain records sufficient to demonstrate conformity with the requirements of this document and CIR (EU) 2024/2981 for the retention period specified in Article 19 of CIR (EU) 2024/2981. Records shall include conformity assessment documentation, incident logs, security test results, and change management records, and shall be made available to the CAB and supervisory authorities upon request. Records shall include incident records, logs and other data sources sufficient to support incident detection, timing, assessment and reporting, including determination of the beginning and duration of availability incidents.	Alignment with international standards - CIR (EU) 2024/2981 Article 19; CIR (EU) 2025/847; ISO/IEC 27001:2022 A.5.33 (protection of records) ; ETSI EN 319 401 §7.9.1.	WZ-03-03	The assessor reviews record-keeping arrangements maintained by the assessed Wallet Provider. The documentation should define: - records sufficient to demonstrate conformity with this document and CIR (EU) 2024/2981; - conformity assessment documentation, incident logs, security test results and change-management records; - incident records, logs and data sources supporting incident detection, timing, assessment and reporting; - records enabling determination of the beginning and duration of availability incidents; - retention period specified in Article 19 of CIR (EU) 2024/2981; - availability of records to the CAB and supervisory authorities upon request.	The assessor checks selected record-keeping evidence for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - conformity assessment documentation, security test results and change-management records; - incident records, logs and data sources supporting detection, timing, assessment and reporting; - evidence for determining start and duration of availability incidents; - storage location, access-control, integrity and retention metadata for Article 19 retention; - retrieval evidence for CAB or supervisory authority requests; - expired or archived records and secure deletion evidence where retention ended.
WZR-22A	WZ/WP provision	The Wallet Provider shall inform wallet users of their rights and obligations and provide mechanisms independent of Wallet Units for secure user identification and authentication, including for revocation requests.	Alignment with international standards - CIR (EU) 2024/2979, Article 6(3).	WZ-03-03	The assessor reviews independent user-service arrangements maintained by the assessed Wallet Provider. The documentation should define: - information provided to wallet users about their rights and obligations; - mechanisms for secure user identification and authentication that do not depend on access to the Wallet Unit;	The assessor tests independent user-service cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - user-facing rights-and-obligations information and where it is made available; - demonstration or records of secure user identification and authentication independent of the Wallet Unit;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- use of those independent mechanisms for revocation requests; - security controls preventing unauthorised access to independent user services; - records required to evidence user communication, successful authentication, rejected requests and exceptions.	- revocation-request cases handled through the independent mechanism; - negative cases showing that unauthorised or insufficiently authenticated requests are rejected; - logs, approvals or support records for successful, failed and exceptional independent-user-service cases.
WZR-22B	REQ-847-W03, REQ-847-W04, REQ-847-W05; REQ-847-W06; REQ-847-W15	Wallet Provider shall maintain availability monitoring capable of detecting complete or projected complete unavailability or limited availability of the wallet solution, validation mechanisms or electronic identification scheme or wallet-related services. Wallet Provider shall define objective criteria for assessing limited availability, including, where possible, average response times, delayed response times, unavailable functionalities, transaction failure rates and service degradation indicators. Wallet Provider shall maintain availability monitoring capable of detecting complete, projected complete and limited unavailability of the Wallet Solution, validation mechanisms and electronic identification scheme, using	Alignment with international standards - CIR (EU) 2025/847; ISO/IEC 27001:2022 A.8.16 (monitoring activities); ISO/IEC 27001:2022 A.5.30 (ICT readiness for business continuity); ETSI EN 319 401 §7.9.1 and §7.11.	WZ-03-03	The assessor reviews availability-monitoring arrangements maintained by the assessed Wallet Provider. The documentation should define: - monitoring capable of detecting complete, projected complete and limited unavailability; - coverage of the Wallet Solution, validation mechanisms, electronic identification scheme and wallet-related services; - objective criteria for limited availability, including average response times, delayed response times, unavailable functionalities, transaction failure rates and service degradation indicators where possible; - rules for determining when full unavailability begins and ends; - links between monitoring evidence, thresholds under CIR (EU) 2025/847, classification and notification decisions.	The assessor checks availability-monitoring implementation for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - monitoring configuration and records for the Wallet Solution, validation mechanisms, electronic identification scheme and wallet-related services; - alerts or incident timelines showing complete, projected complete or limited unavailability detection; - calculations using average response times, delayed response times, unavailable functionalities, transaction failure rates or service degradation indicators; - evidence showing determination of when full unavailability began and ended; - classification decisions and notifications triggered by the measured availability impact.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the thresholds and objective criteria defined in CIR (EU) 2025/847. The monitoring shall support determination of when full unavailability begins and ends.				
WZR-23	REQ-847-W01; REQ-847-W02; REQ-847-W07; REQ-847-W08	Wallet Provider shall monitor and detect suspected malicious or unauthorised access to network and information systems supporting the wallet solution, validation mechanisms and the electronic identification scheme. Monitoring shall cover, at least, privileged access, administrative actions, authentication failures, abnormal network activity and unauthorised changes to security-relevant components. Wallet Provider shall monitor and detect suspected, successful or potential unauthorised logical or restricted physical access to network and information systems supporting the Wallet Solution, validation mechanisms or electronic identification scheme, including systems identified as critical components.	Alignment with international standards - CIR (EU) 2025/847; ETSI EN 319 401 §7.6 and §7.9.1.	WZ-03-03	The assessor reviews logging, monitoring and evidence-retention arrangements maintained by the assessed Wallet Provider. The documented controls should identify: - monitoring and detection of suspected malicious or unauthorised access to network and information systems supporting the Wallet Solution, validation mechanisms and electronic identification scheme; - coverage of privileged access, administrative actions, authentication failures, abnormal network activity and unauthorised changes to security-relevant components; - monitoring and detection of suspected, successful or potential unauthorised logical access; - monitoring and detection of restricted physical access compromise for systems and locations supporting the Wallet Solution, validation mechanisms or electronic identification scheme; - coverage of systems identified as critical components; - alert handling, escalation, investigation, evidence retention and links to incident classification and breach assessment.	The assessor checks monitoring tools, retained logs and selected security events for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should include: - monitoring configuration, alert rules and log sources for network and information systems supporting the Wallet Solution, validation mechanisms and electronic identification scheme; - samples covering privileged access, administrative actions, authentication failures, abnormal network activity and unauthorised changes to security-relevant components; - logical-access and restricted-physical-access event records, including suspected, successful or potential unauthorised access; - monitoring coverage for systems identified as critical components; - investigation, escalation, incident-classification and corrective-action records for sampled alerts or events.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WZR-23A	REQ-5c-01 (Article 5a (6) eIDAS)	Wallet Provider shall inform users without delay of any security breach that could have entirely or partially compromised their EUDI Wallet or its contents, if the wallet has been suspended or revoked pursuant to Article 5e of eIDAS. Notification shall describe the nature of the breach, the data potentially affected, and the remedial measures taken or recommended.	Alignment with international standards - Article 5 a (6) eIDAS; GDPR Article 34 (communication of personal data breach to data subject).	WZ-03-03	The assessor reviews user-notification procedures maintained by the assessed Wallet Provider. The documentation should define: - when users must be informed without delay after a security breach that could have entirely or partially compromised the EUDI Wallet or its contents; - the link between such notification and suspension or revocation under Article 5e of eIDAS; - required notification content covering the nature of the breach, data potentially affected and remedial measures taken or recommended; - roles, approval path and channels for sending user notifications; - evidence retained for notification decisions, timestamps and notification content.	The assessor tests selected user-notification cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - breach or compromise records where the EUDI Wallet or its contents could have been affected; - suspension or revocation records under Article 5e of eIDAS where applicable; - user notifications sent without delay and related timestamps; - notification content describing the nature of the breach, data potentially affected and remedial measures taken or recommended; - cases where user notification was not sent and the documented rationale.
WZR-24	REQ-2981-W04; REQ-2690-W03 REQ-847-W09; REQ-847-W10; REQ-847-W11	Wallet Provider shall notify the CAB without undue delay of any breach or compromise of the EUDI Wallet likely to impact the conformity of the wallet with the requirements of Article 5c of eIDAS, as required by Article 5(2) of CIR (EU) 2024/2981. Wallet Pr ovider shall also notify the competent national cybersecurity authority in accordance with the Polish Cybersecurity Act and Article 23 of the NIS 2 Directive. For the purpose of determining whether a	Alignment with international standards - CIR (EU) 2024/2981 Article 5(2); CIR (EU) 2025/847; NIS 2 Directive Article 23; Polish Cybersecurity Act.	WZ-03-03	The assessor reviews breach-notification arrangements maintained by the assessed Wallet Provider. The documentation should define: - notification to the CAB without undue delay for breaches or compromises likely to impact conformity with Article 5c of eIDAS; - notification to the competent national cybersecurity authority under the Polish Cybersecurity Act and Article 23 of the NIS 2 Directive; - notifiability criteria covering privacy, integrity, confidentiality and authenticity of Wallet Solution data; - certification-status and direct-financial-loss criteria under CIR (EU) 2025/847; - roles, timelines, approvals and evidence retained for notify or not-notify decisions.	The assessor tests selected breach-notification cases for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - incident or breach records from detection through classification and notification decision; - CAB notifications for EUDI Wallet breaches or compromises likely to impact Article 5c conformity; - notifications to the competent national cybersecurity authority where required; - evidence supporting privacy, integrity, confidentiality or authenticity impact on Wallet Solution data; - certification-status and direct-financial-loss evidence used for CIR (EU) 2025/847 notifiability assessment;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		breach or compromise is notifiable and may affect the co nformity or reliability of the Wallet Solution, Wallet Provider shall take into account any actual or potential compromise of the privacy, integrity, confidentiality or authenticity of data stored, transmitted or processed in the Wallet Solution, the certi fication status of the Wallet Solution, and direct financial losses, in accordance with CIR (EU) 2025/847.				- cases where notification was not sent and the documented rationale.
WZR-25	REQ-2981-W05; REQ-2690-W07	Wallet Provider shall establish and maintain a vulnerability management policy for the EUDI Wallet meeting the requirements set out in Annex I to Regulation (EU) 2024/2847 (Cyber Resilience Act), as referenced in Article 5(7) of CIR (EU) 2024/2981. The policy shall include procedures for the identification, assessment, coordinated disclosur e and remediation of vulnerabilities in wallet software components.	Alignment with international standards - CIR (EU) 2024/2981 Article 5(7); Regulation (EU) 2024/2847 (Cyber Resilience Act) Annex I; ISO/IEC 29147.	WZ-03-03	The assessor reviews vulnerability management and disclosure arrangements maintained by the assessed Wallet Provider. The review should identify: - sources of vulnerability information, including public, supplier, testing and researcher reports; - policy requirements for the EUDI Wallet meeting Annex I to Regulation (EU) 2024/2847, as referenced in Article 5(7) of CIR (EU) 2024/2981; - criteria for impact analysis, severity, registration and disclosure; - procedures for identification, assessment, coordinated disclosure and remediation of vulnerabilities in wallet software components; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed Wallet Provider during the on-site Stage 2 assessment. The evidence should show: - approved vulnerability management policy for the EUDI Wallet meeting Annex I to Regulation (EU) 2024/2847; - intake, triage and impact-analysis evidence; - records for vulnerabilities in wallet software components covering identification, assessment, coordinated disclosure and remediation; - remediation, mitigation or risk-acceptance records; - registration or disclosure evidence for officially known and remediated vulnerabilities; - notifications to CAB or certification body and related change or risk records.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
WZR-26	REQ-5c-01 (Article 5a(5)(c) eIDAS); REQ-2979-W02 (CIR (EU) 2024/2979, Article 10)	Wallet Provider shall implement authentication mechanisms enabling the EUDI Wallet to authenticate and identify relying parties registered in accordance with Article 5b of eIDAS, in accordance with the protocols and interfaces specified in CIR (EU) 2024/2979. Wallet Provider shall ensure that the wallet does not disclose per son identification data to relying parties not registered in accordance with Article 5b of eIDAS. Wallet Provider shall ensure that the Wallet Unit processes applicable embedded disclosure policies in relation to wallet -relying party requests, verifies whether the wallet-relying party complies with those policies, and presents the result of that verification to the wallet user.	Alignment with international standards - Article 5a(5)(c) eIDAS; Article 5a(5)(e) eIDAS; Article 5b eIDAS; CIR (EU) 2024/2979.	WZ-03-03	The assessor reviews relying-party authentication, policy processing and disclosure controls for the assessed Wallet Provider: - mechanisms used to authenticate relying parties registered under Article 5b; - protocol and interface rules under CIR 2024/2979 for relying-party requests; - processing of embedded disclosure policies and verification of relying-party compliance; - controls blocking disclosure to unregistered or non-compliant relying parties.	The assessor tests selected relying-party requests for the assessed Wallet Provider during the on-site Stage 2 assessment: - successful and rejected relying-party authentication attempts; - certificate, registration or trust evidence used in the decision; - embedded disclosure policy checks and the result shown to the user; - logs proving that PID or attributes were not disclosed to unregistered or non-compliant relying parties.
WZR-27	REQ-5c-01 (Article 5a(5)(a) eIDAS)	Wallet Provider shall ensure that the EUDI Wallet supports all common protocols and interfaces specified in Article 5a(5)(a) of eIDAS and in CIR (EU) 2024/2979, including interfaces for issuance of PID and attestations, for	Alignment with international standards - Article 5a(5)(a) eIDAS; CIR (EU) 2024/2979; ARF (current version).	WZ-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the assessed Wallet Provider. The review should determine whether they address: - supported presentation protocols, transports and credential formats, including OID4VP, ISO/IEC 18013-5, SD-JWT VC, mdoc, BLE or NFC where applicable;	The assessor performs protocol and interface checks for the assessed Wallet Provider during the on-site Stage 2 assessment. Selected evidence should include: - successful exchanges covering the supported protocol, transport and credential format combinations; - cases covering issuance of PID and attestations, relying-party request and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		relying parties to request and validate PID and attestations, for sha ring and presentation of data online and in offline mode, and for wallet-to-wallet interaction as required by Article 5a(5)(a)(vi) of eIDAS.			- all common protocols and interfaces specified in Article 5a(5)(a) of eIDAS and CIR (EU) 2024/2979, including interfaces for issuance of PID and attestations, relying-party request and validation of PID and attestations, online and offline sharing and presentation of data, and wallet-to-wallet interaction; - message-validation rules for nonces, relying-party identifiers, selective disclosure and cryptographic proof binding; - session encryption and protection against replay, eavesdropping, manipulation or downgrade; - conformance, interoperability and negative-test evidence retained for each supported protocol profile.	validation of PID and attestations, online and offline sharing and presentation of data, and wallet-to-wallet interaction; - protocol traces showing nonce handling, relying-party binding, selective disclosure and WSCD-signed proof where applicable; - negative cases for replayed nonces, invalid relying-party identifiers, unsupported formats or failed session encryption; - configuration showing that production endpoints match the documented supported profiles.
WZR-28	REQ-5c-01 (Article 5a(5)(b) eIDAS)	In accordance with Article 5a(5)(b) of eIDAS, Wallet Provider shall ensure that the EUDI Wallet does not provide any information to trust service providers of electronic attestations of attributes about the use of those attestations. The technical implementation of this requirement shall be verified by the CAB as part of the conformity assessment.	Alignment with international standards - Article 5a(5)(b) eIDAS; ARF (current version) §6 (privacy requirements).	WZ-03-03	The assessor reviews the privacy and non-tracking design maintained by the assessed Wallet Provider. The review should determine whether the data-flow and protocol documentation addresses: - technical implementation ensuring that the EUDI Wallet does not provide information to trust service providers of electronic attestations of attributes about the use of those attestations; - data flows, callbacks, telemetry, identifiers, status checks and protocol messages that could reveal attestation use to the attestation provider; - privacy-preserving techniques preventing tracking, linking or correlation of attestation use by trust service providers; - exception handling, if any, including explicit legal or user-authorised basis; - evidence prepared for CAB verification as part of the conformity assessment.	The assessor verifies non-tracking in selected attestation-use flows for the assessed Wallet Provider during the on-site Stage 2 assessment. The technical evidence should include: - data-flow and protocol traces showing that use of attestations does not send information to trust service providers of electronic attestations of attributes; - tests confirming absence of callbacks, telemetry, identifiers or status checks revealing attestation use to the attestation provider; - configuration of privacy-preserving and unlinkability controls for attestation use; - negative or monitoring evidence showing that trust service providers cannot observe attestation use; - CAB-verification evidence included in the conformity assessment file.