

WM-03-02/Annex A

PL EUDI Wallet Certification System

Cybersecurity Audit Framework for

eID providers

VERSION – 1.01

2026.07.21

Document reference	WM-03-02/Annex A Cybersecurity Audit Framework for eID providers
Version	V1.01
Status	FINAL
Date	2026-07-21
Document type	Evaluation Methods and Techniques - General Cybersecurity Audit Framework
Parent framework	WM-03-02
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-910-06	Regulation (EU) No 910/2014 as amended / eIDAS	Users shall be onboarded to the European Digital Identity Wallet by electronic identification means conforming to assurance level high, or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high.	Article 5a (24)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the entity responsible for the assessed eID means. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path, including onboarding by electronic identification means conforming to assurance level high, or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet assurance level high; - evidence sources, verification checks and manual-review steps supporting assurance level high; - 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 entity responsible for the assessed eID means during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications for each applicable onboarding path under Article 5a(24); - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed, including validation of the electronic identification means assurance level and, where applicable, completion of additional remote onboarding procedures; - records showing how exceptions were escalated, corrected or rejected.
REQ-1502-01	Commission Implementing Regulation (EU) 2015/1502	Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.	Annex, Section 2.1.1, Level Low, Element 1	WP-03-01	The assessor reviews how the provider responsible for the assessed eID means 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	The assessor checks selected user journeys and records for the provider responsible for the assessed eID means 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.

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
					was presented to the user at the time of onboarding, activation or issuance.	
REQ-1502-02	Commission Implementing Regulation (EU) 2015/1502	Ensure the applicant is aware of recommended security precautions related to the electronic identification means.	Annex, Section 2.1.1, Level Low, Element 2	WP-03-01	The assessor reviews how the provider responsible for the assessed eID means 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 provider responsible for the assessed eID means 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-1502-06	Commission Implementing Regulation (EU) 2015/1502	It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.	Annex, Section 2.2.3, Level Low, Element 1	WP-03-01	The assessor reviews lifecycle controls used by the assessed PID 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 PID 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.

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-1502-01	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 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.	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, including attempts by persons other than the legitimate holder, are rejected.
REQ-1502-03	Commission Implementing	The electronic identification means is designed in such a	Annex, Section 2.2.1, Level	WP-03-03	The assessor reviews the authentication design and related user-protection procedures	The assessor tests selected authentication cases and related security events for 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
	Regulation (EU) 2015/1502	way that it can be assumed it is used only under the control of the person to whom it belongs.	Substantial, Element 1		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.	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-1502-07	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	The authentication mechanism shall enable reliable verification of the	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	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider for the eID means

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	electronic identification means and its validity before person identification data are released in an authentication transaction.			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; - evidence retained for authentication events without collecting more personal data than required.	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 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;	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;

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.	- migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
EID-20a	REQ-1502-06; REQ-2981-02	The identification scheme and its components shall be tested comprehensively and regularly. Each material change to the authentication mechanism or authentication factors shall be tested before it is transferred to production. Negative test cases shall also be tested to prevent the generation of erroneous authentication events.		WP-03-03	The assessor reviews protocol specifications, interface descriptions and conformance evidence maintained by the entity responsible for the assessed eID means. The review should determine whether they address: - factor categories used for Wallet Unit, PID key or eID means authentication; - comprehensive and regular testing of the identification scheme and its components; - testing of each material change to the authentication mechanism or authentication factors before transfer to production; - 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 performs protocol and interface checks for the entity responsible for the assessed eID means during the on-site Stage 2 assessment. Selected evidence should include: - configuration and attestation evidence for enabled factors; - test plans and results showing comprehensive and regular testing of the identification scheme and its components; - evidence that material changes to authentication mechanisms or authentication factors were tested before transfer to production; - 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 negative test cases preventing generation of erroneous authentication events.
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	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;	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;

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
		parts relevant for the provision of the services.			- 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.	- 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 (EU) 2015/1502	Providers shall comply with any legal requirements incumbent on them in 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.	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 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 assessor traces selected onboarding, registration or identity-proofing 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 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.

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-1502-03	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 liability evidence and updating it after significant organisational, financial or service changes.	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 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	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

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
					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.	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-1502-05	Commission Implementing Regulation (EU) 2015/1502	Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.	Annex, 2.4.1, Level Low, Element 5	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the entity responsible for the assessed eID means. The documentation should define: - whether the electronic identification scheme is not constituted by national law and therefore requires an effective termination plan; - orderly discontinuation of service or continuation by another provider; - procedures for informing relevant authorities and end users; - protection, retention and destruction of records in compliance with the scheme policy; - integrity, confidentiality, access-control and retrieval controls for records during termination; - roles, triggers, timelines and evidence required to activate and execute the termination plan.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the entity responsible for the assessed eID means 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 for informing relevant authorities and end users; - record-protection, retention and destruction procedures aligned with the scheme policy; - storage location, access-control, integrity and retention metadata for records affected by termination; - test, review or exercise evidence showing that the termination plan can be executed effectively.
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	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:	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:

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
		its usage. The service definition shall include a privacy policy.			- 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; - 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.	- current public pages, repositories, policy documents or user-facing notices, including the published service definition, applicable terms, conditions, fees, usage limitations and privacy policy; - 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;	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;

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
					- 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; - 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.	- 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; - 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	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

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 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.	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 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	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	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

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 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]			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 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.	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 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	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;

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
					out-of-hours support; - dependency on subcontractors and escalation capacity; - monitoring of workload, vacancies or capacity risks.	- 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, unauthorised access and other factors that may impact the security of the service.	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 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.	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: - 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;	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;

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
					- 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.	- 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 (EU) 2015/1502	The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.	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 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.	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; - 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	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

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-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.	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-channel settings match the documented secure configuration.
REQ-1502-19	Commission Implementing Regulation (EU) 2015/1502	Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, shall be restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.	Annex, 2.4.6, Level Low, Element 3	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the entity responsible for the assessed eID means. The review should establish whether the documentation covers: - key types, algorithms, trusted components and protected environments used for the assessed function; - key generation, storage, access, backup, rotation, revocation and destruction rules, including restriction of access to sensitive cryptographic material to roles and applications strictly requiring access; - controls ensuring that sensitive cryptographic material is never persistently stored in plain text; - use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - segregation of duties and logging for sensitive key-management operations.	The assessor tests selected authentication cases and related security events for the entity responsible for the assessed eID means 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 modules, including evidence that sensitive cryptographic material is never persistently stored in plain text; - access logs and approvals for sensitive key-management actions, showing access restricted to roles and applications strictly requiring access; - negative or exception cases such as expired certificates, failed rotations, rejected keys or attempted unauthorised access to sensitive cryptographic material.
REQ-1502-20	Commission Implementing Regulation	Procedures shall exist to ensure that security is maintained over time and	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	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed Wallet Provider and PID Provider

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	that there is an ability to respond to changes in risk levels, incidents, and security breaches.			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.	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, 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.

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-1502-22	Commission Implementing Regulation (EU) 2015/1502	Sensitive cryptographic material, if used for issuing electronic identification means and authentication, shall be protected from tampering.	Annex, 2.4.6, Level Substantial; Level High is same as Substantial	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the entity responsible for the assessed eID means. The review should establish whether the documentation covers: - key types, algorithms, trusted components and protected environments used for the assessed function; - key generation, storage, access, backup, rotation, revocation and destruction rules; - controls protecting sensitive cryptographic material used for issuing electronic identification means and authentication from tampering; - use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - segregation of duties and logging for sensitive key-management operations.	The assessor tests selected authentication cases and related security events for the entity responsible for the assessed eID means 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 modules, including evidence that sensitive cryptographic material is protected from tampering; - access logs and approvals for sensitive key-management actions; - negative or exception cases such as expired certificates, failed rotations, rejected keys or attempted tampering with sensitive cryptographic material.
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,	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:	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

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
		commitment to continual improvement, resource commitment, roles, documentation requirements, topic-specific policies, indicators and measures, and formal approval by management bodies.			- 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; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	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.
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;	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.

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-2690-03	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; - 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 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 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	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

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
					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.	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; - allocation of responsibilities and links to operational procedures; - 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; - organisation charts, role mandates or reporting records showing at least one person reporting directly to management bodies on network and information system security matters; - 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;	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

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, 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.	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 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.	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; - 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	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

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
					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.	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 establishing, implementing, and monitoring a risk treatment plan.	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; - 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.	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, 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	The provider shall establish procedures for identification, analysis,	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	The assessor checks selected risk records, decisions and management-review outputs for the assessed Wallet Provider and PID Provider

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	assessment, and treatment of risks (cybersecurity risk management process), including the elements set out in Annex, 2.1.2(a) to (j).			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.	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 asset classification, and the business impact analysis.	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 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.	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, 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.

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-2690-12	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 (EU) 2024/2690	The provider shall regularly review compliance with its policies on network and information system security. Management bodies shall be informed of the status through regular reporting.	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 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.	The assessor checks selected network zones and information system security management documents, during the on-site Stage 2 assessment. The evidence should include: - 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.

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-2690-14	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 security 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; - 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.	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 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.

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-2690-16	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 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.	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; - 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	The provider shall assess suspicious events to	Annex, 3.4.1-3.4.2	WZ-03-01	The assessor reviews incident, breach and unauthorised-access handling arrangements	The assessor tests selected incident or breach records for the assessed provider across

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
	Regulation (EU) 2024/2690	determine whether they constitute incidents and determine their nature and severity.			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.	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 assessment, change management and user communication.	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; - 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:	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:

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
					- 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.	- 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.
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	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

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 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.	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; - updates made to plans following tests, incidents or service changes.
REQ-2690-24	Commission Implementing Regulation	The provider shall establish, implement, and apply a supply chain security policy governing	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	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

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	relations with direct suppliers and service providers.			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.	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.
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	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

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
					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.	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.
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;	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;

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
					- change request, approval, testing, implementation and rollback requirements; - segregation between emergency, standard and normal changes; - controls detecting unauthorised configuration drift.	- 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 applications, infrastructure and interfaces; - criteria for independent, penetration, vulnerability or configuration testing; - handling of findings, retesting and closure evidence;	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 components; - findings mapped to owners, deadlines, fixes and retest results; - exceptions, accepted risks or deferred findings;

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 testing results, risk treatment, change management and release decisions.	- 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; - 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-2690-33	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 service components 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: - 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 maintenance records; - incident or exception records 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
					- handling, escalation and remediation of malware or unauthorised-software detections.	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 assessment;	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 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
					- triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	- 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	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;

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
					responsibilities; - pre-contract due diligence, risk assessment 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.	- employee training, acknowledgement or commitment records showing understanding 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	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

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
					termination or role change and are contractually defined and enforced; - disciplinary process for breaches of security or service procedures, including enforcement of continuing security responsibilities.	contractual clauses defining security responsibilities that remain valid after termination or change of employment; - records showing how policy or procedure 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;	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;

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 requirements for administrative and sensitive access; - physical access requirements for facilities and restricted areas holding or processing sensitive information; - logging, emergency access and removal of access after role changes or termination.	- 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-2690-45	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.

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-2690-47	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; - allowed administrative paths and restrictions on general-purpose use; - monitoring, hardening and access rules for administration systems; - exception and emergency-administration procedures.	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 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	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:	The assessor tests selected authentication controls for the assessed provider across Wallet, PID and eID scheme responsibilities 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
	(EU) 2024/2690				- 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.	- 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.
REQ-2690-50	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms, where appropriate.	Annex, 11.7.1-11.7.2	WZ-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the entity responsible for the assessed eID means. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including multiple authentication factors or continuous authentication mechanisms where appropriate; - 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 entity responsible for the assessed eID means 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 where appropriate; - 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-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	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

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
					relevant; - links between assets, risks, access rights, logging and continuity arrangements.	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 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	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 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;

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
					relevant, including controls for removable storage media; - links between assets, risks, access rights, logging and continuity arrangements.	- 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; - 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;	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; - 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

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 assets, risks, access rights, logging and continuity arrangements.	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 operational 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 measures to prevent or reduce the consequences of events originating from physical and environmental threats; - triggers for updating risk assessment after	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 vulnerability findings updated the risk picture; - operational controls or projects implementing selected risk-treatment decisions, including measures preventing 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
					incidents, changes, vulnerabilities or supplier changes.	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; - records required for notification to the CAB, supervisory body or scheme owner where applicable, including evidence that the	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 risk assessment was shared with the certification body 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
					complemented 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 management, incident response and risk management;	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 with Article 5;

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 or disclosure rules for vulnerabilities affecting users or relying parties.	- 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	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,	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
		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)] 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			including transmission of the vulnerability 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
		certification body. [Article 5(5), Article 5(6)] REQ-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				

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, 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]				
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	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,	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

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
		Annex V to CIR (EU) 2024/2981.			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; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met.	records; - registration or disclosure evidence for officially known and remediated vulnerabilities, including registration in one of 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.

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-2981-13	Commission Implementing Regulation (EU) 2024/2981	The holder of the certificate of conformity shall store the following information securely for the purpose of 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.	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 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.	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 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	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)

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 cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including availability of Article 19(1) information to the certification body or the Scheme Owner upon request.	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.
REQ-5c-01	Article 5c of eIDAS / Regulation (EU) 910/2014	The electronic identification scheme under which European Digital Identity Wallets are provided shall be certified by a conformity assessment body accredited pursuant to Regulation (EC) No 765/2008.	Article 5 c (1)	WZ-03-02	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the entity responsible for the assessed eID means. The review should confirm: - scope of certification and mapping to Wallet, PID or eID scheme functions, including evidence that the electronic identification scheme under which European Digital Identity Wallets are provided is certified by a conformity assessment body accredited pursuant to Regulation (EC) No 765/2008; - 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.	Not applicable
REQ-5c-02	Article 5c of eIDAS / Regulation (EU) 910/2014	The electronic identification scheme shall comply with the requirements set out in Article 8 about assurance level high, including the requirements for enrolment, identity	Article 5c (3), read with Article 5a (11)	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the entity responsible for the assessed eID means. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path;	The assessor traces selected onboarding, registration or identity-proofing cases for the entity responsible for the assessed eID means during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications;

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
		proofing, and electronic identification means management.			- evidence sources, verification checks and manual-review steps supporting assurance level high, including compliance of the electronic identification scheme with Article 8 assurance level high requirements; - enrolment, identity proofing and electronic identification means management controls required for assurance level high; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	- source checks, operator decisions, timestamps and final assurance-level decisions, including evidence of compliance with Article 8 assurance level high; - evidence that issuance or activation occurred only after required proofing steps were completed; - evidence that enrolment, identity proofing and electronic identification means management controls meet assurance level high requirements; - records showing how exceptions were escalated, corrected or rejected.
REQ-1502-E05	Commission Implementing Regulation (EU) 2015/1502	If electronic identification means are not issued based on notified electronic identification means having the assurance level high requirements REQ-1502-E06, REQ-1502-E07, REQ-1502-E08, REQ-1502-E09, REQ-1502-E10 apply.		WZ-03-02	The assessor reviews how the assessed PID Provider handles the conditional enrolment route referenced by this requirement: - which linked enrolment requirements become applicable when the condition is met; - decision logic for selecting the applicable alternative; - evidence required before the provider treats the conditional route as satisfied; - fallback to the stricter proofing route when the conditional route is incomplete or unsupported.	The assessor tests selected conditional enrolment decisions for the assessed PID Provider during the on-site Stage 2 assessment: - cases where the conditional route was accepted and the linked requirements were evidenced; - cases where the condition was not met and an alternative or full proofing route was used; - records showing the decision logic and evidence package; - gaps caused by incomplete or ambiguous source text escalated for clarification before relying on the route.
REQ-1502-E06	Commission Implementing Regulation (EU) 2015/1502	The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identification means is being made and representing the claimed identity.	Annex, Section 2.1.2, Level Low, Point 1	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the entity responsible for the assessed eID means. The review should confirm that the documented process defines: - types of evidence recognised by the Member State in which the application for the electronic identification means is made; - rules for determining that the person can be	The assessor traces selected onboarding, registration or identity-proofing cases for the entity responsible for the assessed eID means during the on-site Stage 2 assessment. The evidence should show: - application records showing the evidence presented or relied upon and the Member State recognition basis; - checks confirming that the applicant can be

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
					assumed to be in possession of such evidence; - checks confirming that the evidence represents the claimed identity; - validity, authenticity, completeness and source-check rules for the recognised evidence; - handling of unsupported, expired, inconsistent, incomplete or non-recognised evidence; - traceability from evidence assessment to the enrolment or proofing decision.	assumed to be in possession of the evidence; - source, validity, authenticity and completeness checks for sampled evidence; - evidence that the recognised evidence represents the claimed identity; - cases rejected or escalated because the evidence was unsupported, expired, inconsistent, incomplete or not recognised; - audit trail linking the evidence assessment to the final enrolment or proofing decision.
REQ-1502-E09-1	Commission Implementing Regulation (EU) 2015/1502	Alternative: The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identification means is being made and representing the claimed identity; the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source; and steps have been taken to minimise the risk that the person's identity is not the claimed identity.	Annex, Section 2.1.2, Level Substantial, Point 1	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the entity responsible for the assessed eID means. The review should confirm that the documented process defines: - verification that the person is in possession of evidence recognised by the Member State in which the application is made; - checks confirming that the evidence represents the claimed identity; - checks determining whether the evidence is genuine or known to exist according to an authoritative source; - steps taken to minimise the risk that the person's identity is not the claimed identity; - handling of unsupported, expired, inconsistent, incomplete or non-recognised evidence; - traceability from possession, recognition, genuineness and risk-minimisation checks to the proofing decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the entity responsible for the assessed eID means during the on-site Stage 2 assessment. The evidence should show: - application records showing verified possession of evidence recognised by the Member State where the application is made; - evidence that the recognised evidence represents the claimed identity; - genuineness checks or authoritative-source responses confirming that the evidence exists; - records of steps taken to minimise the risk that the person's identity is not the claimed identity; - rejected or escalated cases involving unsupported, expired, inconsistent, incomplete or non-recognised evidence; - audit trail linking the evidence assessment to the final proofing decision.
PP-20	REQ-1502-E04; REQ-2977-06	The identity proofing process shall confirm that the eID means used is valid and not expired, suspended	Alignment with international standards - ISO/IEC	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider for the eID means. The review should confirm	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider for the eID means 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
		or revoked, and that the person identification data remains accurate and is confirmed by the authoritative sources designated in the Trust Framework. The process shall confirm that the identity exists and that the person is not known to be deceased.	27001:2022 A.5.16 (identity management); A.8.24 (use of cryptography). ETSI EN 319 401 §7.1 (Identity verification); EN 319 411-2 §7.3 (Initial identity validation for qualified certificates).		that the documented process defines: - which authoritative sources are accepted for each evidence type, including authoritative sources designated in the Trust Framework for confirming person identification data; - timing rules proving that evidence validity is checked at the time of proofing, renewal or reliance, including confirmation that the eID means used is valid and not expired, suspended or revoked; - checks confirming that person identification data remains accurate, that the identity exists and that the person is not known to be deceased; - handling of source unavailability, inconsistent results and expired evidence; - records retained to support the final proofing or issuance decision.	evidence should show: - source responses or validation tokens showing evidence status at the relevant time, including confirmation that the eID means was valid and not expired, suspended or revoked; - application records where source checks were successful, failed or manually reviewed; - timestamps linking the source check to the proofing or issuance decision; - evidence that person identification data was confirmed by authoritative sources designated in the Trust Framework and remained accurate; - evidence that the identity exists and that the person is not known to be deceased; - evidence that expired, unverified or inconsistent evidence was not accepted without justified escalation.