

WM-03-01/Annex A

PL EUDI Wallet Certification System

Cybersecurity Audit Framework for

PID Providers

VERSION – 1.01

2026.07.21

Document reference	WM-03-01/Annex A Cybersecurity Audit Framework for PID providers
Version	V1.01
Status	FINAL
Date	2026-07-21
Document type	Evaluation Methods and Techniques - General Cybersecurity Audit Framework
Parent framework	WM-03-01
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-910-04	Regulation (EU) No 910/2014 as amended / eIDAS	The person identification data available from the electronic identification scheme under which the European Digital Identity Wallet is provided shall uniquely represent the natural person.	Article 5a(5)(f)	WP-03-01	The assessor reviews how the assessed PID Provider ensures uniqueness of person identification data before issuance or use in the eID scheme: - unique identifiers, matching rules and authoritative datasets used to detect duplicates or collisions; - handling of identity merges, corrections, duplicate candidates and ambiguous matches; - controls preventing PID issuance before uniqueness checks are complete; - records retained to justify the final uniqueness decision.	The assessor tests selected uniqueness decisions for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID records compared with duplicate-check or matching results; - blocked, corrected or escalated duplicate candidates; - source-system evidence showing the person represented by the issued PID; - audit trail linking uniqueness checks to the final issuance decision.
REQ-910-05	Regulation (EU) No 910/2014 as amended / eIDAS	Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider. If the European Digital Identity Wallet is provided by private parties, the provisions of Article 45h (3) shall apply mutatis mutandis, requiring functional separation from other services.	Article 5a (14)	WP-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed PID Provider. The documentation should show: - data flows, stores and interfaces separating wallet personal data from other provider services; - purpose limitation, minimisation and non-combination controls supporting logical separation; - functional separation from other services where the European Digital Identity Wallet is provided by a private party; - governance for exceptions, access to personal data and retention of privacy-related evidence.	The assessor checks selected data-processing and separation cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - architecture diagrams, database or tenant separation evidence and access-control configuration for personal data relating to the provision of the European Digital Identity Wallet; - sampled logs or data-flow evidence showing that wallet personal data is logically separated from other provider data and that cross-service combination is not occurring; - evidence of functional separation from other services where the European Digital Identity Wallet is provided by a private party; - exceptions or support cases to confirm that access to personal data is controlled and recorded.
REQ-1502-03	Commission Implementing Regulation (EU) 2015/1502	Collect the relevant identity data required for identity proofing and verification.	Annex, Section 2.1.1, Level Low, Element 3	WP-03-01	The assessor reviews how the assessed PID Provider determines and collects the identity data needed for proofing, verification and issuance: - the data attributes required for the intended PID or eID means outcome;	The assessor tests sampled data-collection cases for the assessed PID Provider during the on-site Stage 2 assessment: - application records showing which identity attributes were collected and from which source;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- sources of the attributes and checks for completeness, consistency and data quality; - data minimisation rules and separation from data not needed for the issuance decision; - handling of incomplete, conflicting or unsupported identity data.	- validation results for completeness, consistency and source confirmation; - cases rejected or escalated because identity data were missing or inconsistent; - evidence that unnecessary attributes were not collected for the assessed process.
REQ-1502-04	Commission Implementing Regulation (EU) 2015/1502	Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body, and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.	Annex, Section 2.1.2, Level High, Point 1(c)	WP-03-01	The assessor reviews how the assessed PID Provider decides whether previous identity proofing or a prior electronic identification means may be relied upon instead of repeating proofing: - criteria for confirming that the prior electronic identification means was valid at the time of reliance; - separate handling for notified assurance level high means and non-notified means requiring CAB or equivalent-body confirmation; - risk assessment for changes in person identification data since the previous proofing or issuance procedure; - evidence required to demonstrate that the previous procedure remains valid for the current issuance decision; - fallback rules requiring full identity proofing and verification when any reliance condition is not met.	The assessor tests selected reliance decisions for the assessed PID Provider during the on-site Stage 2 assessment: - cases based on a valid notified electronic identification means at assurance level high, where available; - cases based on a non-notified means, including CAB or equivalent-body confirmation of assurance level high; - records showing validity, notification status, assurance level and risk-of-changed-PID-data checks; - decisions where reliance was rejected and the full proofing path was used; - traceability from prior evidence to the final PID or eID means issuance outcome.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-1502-07	Commission Implementing Regulation (EU) 2015/1502	The existence of measures taken to prevent unauthorised suspension, revocation, and/or reactivation.	Annex, Section 2.2.3, Level Low, Element 2	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.
REQ-1502-08	Commission Implementing Regulation (EU) 2015/1502	Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.	Annex, Section 2.2.3, Level Low, Element 3	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.
REQ-1502-09	Commission Implementing Regulation (EU) 2015/1502	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification	Annex, Section 2.2.4, Level Low	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path, including renewal or replacement based on initial identity proofing and verification requirements or on a valid electronic	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications for renewal or replacement; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance renewal 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
		means of the same, or higher, assurance level.			identification means of the same or higher assurance level; - evidence sources, verification checks and manual-review steps supporting assurance level high; - risk assessment for changes in person identification data before renewal or replacement; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing renewal or replacement decision.	replacement occurred only after required proofing steps were completed or on the basis of a valid electronic identification means of the same or higher assurance level; - records showing assessment of risks of changed person identification data; - records showing how exceptions were escalated, corrected or rejected.
REQ-1502-10	Commission Implementing Regulation (EU) 2015/1502	Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.	Annex, Section 2.2.4, Level High	WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - 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; - authoritative-source verification of identity data where renewal or replacement is based on a valid electronic identification means.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement, including renewal or replacement based on a valid electronic identification means; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - authoritative-source verification records for identity data in renewal or replacement cases based on a valid electronic identification means; - cases rejected because the required assurance, authorisation or authoritative-source verification conditions were not met.
REQ-1502-11	Commission Implementing Regulation (EU) 2015/1502	Where identity proofing and verification is performed for assurance level high, the PID Provider shall ensure that	Annex, Section 2.1.2, Level High	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines:	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the requirements applicable to assurance level substantial are fulfilled before applying the additional requirements for assurance level high.			- the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high; - evidence that requirements applicable to assurance level substantial are fulfilled before additional requirements for assurance level high are applied; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	- applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - evidence that assurance level substantial requirements were fulfilled before additional assurance level high requirements were applied; - records showing how exceptions were escalated, corrected or rejected.
REQ-1502-12	Commission Implementing Regulation (EU) 2015/1502	Where photo or biometric identification evidence is used, the PID Provider shall ensure that the evidence is recognised by the Member State, represents the claimed identity, is valid according to an authoritative source, and that the applicant is identified as the claimed identity by comparison of one or more physical characteristics with an authoritative source.	Annex, Section 2.1.2, Level High, Point 1(a)	WP-03-01	The assessor reviews how the assessed PID Provider uses photo, biometric or identity-document evidence to establish the claimed identity: - accepted evidence types and the national recognition or authoritative validity criteria applied to them; - comparison method between the applicant and the authoritative or document-based reference; - liveness, anti-spoofing, manual-review and exception rules where applicable; - rejection criteria for expired, unsupported, inconsistent or insufficient evidence.	The assessor checks selected biometric or document-based proofing cases for the assessed PID Provider during the on-site Stage 2 assessment: - source-validation, document-validation or biometric-comparison results with timestamps; - manual-review notes and final decisions for matched, mismatched and poor-quality evidence; - rejected or escalated cases involving invalid evidence or failed comparison; - audit evidence showing that accepted cases met the required assurance level.
REQ-1502-13	Commission Implementing Regulation (EU) 2015/1502	Where previous identity proofing and verification procedures are relied upon, the PID Provider shall ensure that they provide equivalent assurance level high, that this equivalence is confirmed by a conformity assessment	Annex, Section 2.1.2, Level High, Point 1(b)	WP-03-01	The assessor reviews how the assessed PID Provider relies on previous identity proofing and verification procedures at assurance level high: - criteria for determining that previous proofing provides equivalent assurance level high; - evidence of confirmation by a CAB or equivalent body where equivalence must be demonstrated;	The assessor tests selected cases where the assessed PID Provider relied on previous proofing or rejected such reliance during the on-site Stage 2 assessment: - case records linking the prior proofing result to the current PID issuance decision; - CAB or equivalent-body confirmation evidence where required; - validity checks showing that the prior proofing result was still 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
		body or equivalent body, and that the results of those procedures remain valid.			- checks proving that the previous proofing result remains valid for the current PID issuance decision; - fallback to full identity proofing when equivalence or continued validity cannot be evidenced.	- rejected reliance cases where full proofing was performed instead.
REQ-1502-14	Commission Implementing Regulation (EU) 2015/1502	Where the applicant does not present recognised photo or biometric identification evidence, the PID Provider shall apply the same national procedures as those used to obtain such recognised evidence.	Annex, Section 2.1.2, Level High, Point 2	WP-03-01	The assessor reviews how the assessed PID Provider handles applicants who do not present recognised photo or biometric identification evidence: - national procedures accepted as equivalent to obtaining recognised photo or biometric evidence; - decision criteria for routing an applicant to this alternative path; - evidence required to show that the alternative procedure preserves assurance level high; - rejection or escalation rules when the alternative national procedure cannot be completed.	The assessor tests selected alternative-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment: - cases where recognised photo or biometric evidence was not presented; - records showing which national procedure was applied and why it was applicable; - evidence supporting the final identity decision under that procedure; - cases rejected or escalated because the alternative procedure did not provide sufficient assurance.
REQ-2977-01	Commission Implementing Regulation (EU) 2024/2977	Providers of person identification data shall issue person identification data to wallet units in accordance with the electronic identification schemes under which wallet solutions are provided.	Article 3(1)	WP-03-01	The assessor reviews how the assessed PID Provider controls the PID issuance decision and the conditions that must be met before PID is released to a Wallet Unit: - pre-issuance checks covering proofing result, Wallet Unit eligibility, binding evidence and applicable eID scheme rules; - segregation between successful issuance, rejection, re-issuance and correction paths; - approval, automation and manual-review rules for exceptional issuance cases; - records retained to link the applicant, proofing result, Wallet Unit and issued PID.	The assessor tests selected PID issuance cases for the assessed PID Provider during the on-site Stage 2 assessment: - successful, rejected and re-issued PID cases, where available; - evidence that required proofing, Wallet Unit validation and binding checks were completed before issuance; - issuance logs linking the approved decision with the technical PID creation event; - cases showing that incomplete or failed preconditions prevented PID release.
REQ-2977-02	Commission Implementing Regulation	Providers of person identification data shall ensure that person identification data issued	Article 3(2)	WP-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2977	to wallet units contains the information necessary for authentication and validation of the person identification data.			documentation covers: - mandatory and optional PID data elements for each supported format; - schema, signature, validity-status, authentication information and validation information required by the applicable technical specification; - quality checks preventing incomplete, inconsistent or unsupported PID payloads from being issued; - versioning and change control for PID formats and data mappings.	- issued PID samples or test vectors covering each supported format; - schema validation, signature validation, authentication-information checks and required metadata checks; - cases rejected because required elements, authentication information or validation information were missing; - traceability between the configured format, the issuance request and the issued PID.
REQ-2977-03	Commission Implementing Regulation (EU) 2024/2977	Providers of person identification data shall ensure that person identification data issued to wallet units comply with the technical specifications set out in the Annex.	Article 3(3)	WP-03-01	The assessor reviews how the assessed PID Provider controls PID content, format and validation metadata before issuance: - mandatory and optional PID data elements for each supported format; - schema, signature, validity-status and validation information required by the applicable technical specification; - quality checks preventing incomplete, inconsistent or unsupported PID payloads from being issued; - versioning and change control for PID formats and data mappings.	The assessor examines selected PID payloads or issuance records for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID samples or test vectors covering each supported format; - schema validation, signature validation and required metadata checks; - cases rejected because required elements or validation information were missing; - traceability between the configured format, the issuance request and the issued PID.
REQ-2977-04	Commission Implementing Regulation (EU) 2024/2977	Member States shall ensure that the person identification data issued to a given wallet user is unique for the Member State.	Article 3(4)	WP-03-01	The assessor reviews how the assessed PID Provider ensures uniqueness of person identification data before issuance or use in the eID scheme: - unique identifiers, matching rules and authoritative datasets used to detect duplicates or collisions; - handling of identity merges, corrections, duplicate candidates and ambiguous matches; - controls preventing PID issuance before uniqueness checks are complete; - records retained to justify the final uniqueness decision.	The assessor tests selected uniqueness decisions for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID records compared with duplicate-check or matching results; - blocked, corrected or escalated duplicate candidates; - source-system evidence showing the person represented by the issued PID; - audit trail linking uniqueness checks to the final issuance decision.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2977-05	Commission Implementing Regulation (EU) 2024/2977	Providers of person identification data shall ensure that person identification data that they issue is cryptographically bound to the wallet unit to which it is issued.	Article 3(5)	WP-03-01	The assessor reviews the cryptographic binding design used by the assessed PID Provider for PID or eID means material: - how the intended Wallet Unit is identified and validated before binding; - how the PID public key, proof of possession and proof of association are checked before PID is issued; - how the issued PID is linked to the validated Wallet Unit and to the accepted PID public key; - controls preventing issuance to a substituted Wallet Unit, wrong public key or unverified binding request; - evidence retained for failed, repeated or exceptional binding attempts.	The assessor traces selected cryptographic binding cases for the assessed PID Provider during the on-site Stage 2 assessment: - the approved issuance decision, Wallet Unit identifier, attestation result, PID public key and binding evidence; - proof-of-possession and proof-of-association validation logs; - technical issuance records showing the PID bound to the intended Wallet Unit and public key; - rejected cases involving missing proofs, wrong keys, invalid attestations or replayed binding material.
REQ-2977-06	Commission Implementing Regulation (EU) 2024/2977	Member States shall enrol wallet users in accordance with the requirements relating to enrolment at assurance level high, as set out in Commission Implementing Regulation (EU) 2015/1502. Providers of person identification data shall perform identity verification of the wallet user in accordance with the requirements related to identity proofing and verification before issuing the person identification data to the wallet unit.	Article 3(7)	WP-03-01	The assessor reviews the proofing, onboarding and verification arrangements used by the assessed PID Provider: - the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	The assessor tests selected proofing, onboarding and issuance cases for the assessed PID Provider during the on-site Stage 2 assessment: - normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
REQ-2977-07	Commission Implementing Regulation	When issuing person identification data to wallet units, providers of person identification data	Article 3(8)	WP-03-01	The assessor reviews how the assessed PID Provider authenticates itself to Wallet Units before PID issuance or related exchanges: - certificate profiles or alternative assurance	The assessor checks provider-authentication evidence for the assessed PID Provider during the on-site Stage 2 assessment: - live or retained protocol traces showing use

Requirement 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) 2024/2977	shall identify themselves to wallet units using their wallet-relying party access certificate or by using another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high.			level high authentication mechanisms used for provider identification; - certificate lifecycle controls, trust anchors and revocation checks; - protocol steps that prevent Wallet Units from accepting unauthenticated provider requests; - evidence retained for successful and failed provider-authentication events.	of the wallet-relying party access certificate or approved alternative mechanism; - certificate validity, chain-building and revocation-check results; - logs for rejected exchanges involving invalid, expired or untrusted credentials; - configuration showing that weaker or unapproved authentication paths are not enabled.
REQ-2977-08	Commission Implementing Regulation (EU) 2024/2977	Before issuing person identification data to a wallet unit, providers of person identification data shall authenticate and validate the wallet unit attestation of the wallet unit and verify that the wallet unit belongs to a wallet solution the provider of person identification data accepts, or use another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high.	Article 3(9)	WP-03-01	The assessor reviews technical documentation how the assessed PID Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - requirements to authenticate and validate the Wallet Unit Attestation before PID issuance; - certificate and trust-list requirements used for Wallet Unit Attestation validation; - rules for verifying that the Wallet Unit belongs to a wallet solution accepted by the PID Provider; - approved alternative authentication mechanisms in accordance with an electronic identity scheme notified at assurance level high, where used; - controls preventing PID issuance where Wallet Unit Attestation validation, wallet-solution acceptance or approved alternative authentication fails.	The assessor checks selected Wallet Unit attestation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - PID issuance cases showing Wallet Unit Attestation authentication and validation before issuance; - certificate chain, trust-list and validity-status evidence for the Wallet Unit Attestation; - evidence that the Wallet Unit belongs to a wallet solution accepted by the PID Provider; - evidence for approved alternative authentication mechanisms under a notified assurance level high eID scheme, where used; - rejected cases where attestation validation, wallet-solution acceptance or approved alternative authentication failed.
REQ-2977-09	Commission Implementing Regulation (EU) 2024/2977	Providers of person identification data issued to a wallet unit shall have written and publicly accessible policies relating to validity status management, including, where applicable, the conditions under which	Article 5(1)	WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - authorised triggers, decision roles and evidence required for each lifecycle action; - publicly accessible policy content, including, where applicable, the conditions under which PID can be revoked without delay;	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - written and publicly accessible validity-status-management policies, 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
		such person identification data can be revoked without delay.			- 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.	- conditions for revocation without delay where applicable; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-2977-10	Commission Implementing Regulation (EU) 2024/2977	Where providers of person identification data have revoked person identification data, they shall, through dedicated and secure channels, inform wallet users within 24 hours of the revocation and of the reasons for the revocation, in a manner that is concise, easily accessible and using clear and plain language.	Article 5(3)	WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - triggering events and deadlines for user notification, including the 24-hour deadline after revocation of PID issued to a Wallet Unit where applicable; - dedicated secure channels and message templates used for notification; - required content of the notification, including the revocation and reasons for the revocation, provided in a concise, easily accessible manner and using clear and plain language; - records proving delivery, failure handling and escalation.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - timestamps from PID revocation decision to user notification confirming notification within 24 hours; - message content and channel evidence for notified users, including the reason for revocation and use of a dedicated secure channel; - evidence that the notification was concise, easily accessible and written in clear and plain language; - failed delivery or escalation records; - cases confirming that users were not left without notice after a status change.
REQ-2977-11	Commission Implementing Regulation (EU) 2024/2977	Where providers of person identification data revoke person identification data issued to wallet units, they shall do so in each of the following circumstances: (a) upon the explicit request of the wallet user; (b) where the wallet unit attestation has been revoked; (c) in other	Article 5(4)	WP-03-01	The assessor reviews the PID revocation process maintained by the assessed PID Provider. The documentation should define: - procedures requiring revocation of PID issued to Wallet Units upon explicit request of the wallet user; - procedures requiring revocation of PID where the Wallet Unit Attestation has been revoked; - other revocation situations determined in the PID Provider's policies; - decision roles, authorisation evidence and	The assessor checks selected PID revocation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - PID revocations performed upon explicit request of the wallet user; - PID revocations performed because the Wallet Unit Attestation was revoked; - PID revocations performed under other situations determined in the PID Provider's policies; - records linking the revocation trigger,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		situations determined by the providers in their policies.			timing rules for PID revocation where defined; - controls linking wallet user requests, Wallet Unit Attestation revocation events and policy-defined triggers to the corresponding PID revocation decision; - records and system states used to evidence that PID revocation was completed.	authorisation, timestamp and technical PID revocation event; - validity status records or system evidence showing that the PID was actually revoked; - cases where a required revocation trigger was detected and PID revocation was completed, or where any delay or failure was recorded and escalated as an exception.
REQ-2977-12	Commission Implementing Regulation (EU) 2024/2977	Providers of person identification data issued to a wallet unit shall ensure that revocations cannot be reverted.	Article 5(5)	WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - status model distinguishing suspension, temporary blocking, revocation and end-of-life states for PID; - technical controls preventing a revoked PID from returning to valid status; - authorisation and logging for revocation decisions; - handling of erroneous revocation without reinstating the revoked PID contrary to the requirement; - technical and procedural controls preventing reversal of completed revocations.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID records and subsequent status history; - attempts or procedures for reactivation to confirm that revoked PID cannot return to valid state; - register, status service and publication evidence after revocation; - exception cases showing how mistakes are corrected through controlled re-issuance rather than reversal; - technical and procedural controls preventing reversal of completed revocations.
REQ-2977-13	Commission Implementing Regulation (EU) 2024/2977	The revoked person identification data shall remain accessible for as long as required by Union law or national law.	Article 5(6)	WP-03-01	The assessor reviews the PID revocation and retention arrangements maintained by the assessed PID Provider. The documented controls should define: - legal basis determining how long revoked PID must remain accessible under Union law or national law; - retention rules and technical controls ensuring revoked PID remains accessible for the required period; - integrity, availability and access-control measures for retained revoked PID records; - procedures for lawful deletion or archival	The assessor tests selected revoked PID cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID records and the applicable Union-law or national-law retention/accessibility period; - evidence that revoked PID remains accessible after revocation for the required period; - integrity, availability and access-control evidence for retained revoked PID records; - where applicable, evidence that retained revoked PID was archived or deleted only after the legally required period expired.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					only after the required accessibility period expires.	
REQ-2977-14	Commission Implementing Regulation (EU) 2024/2977	Where providers of person identification data revoke person identification data issued to wallet units, they shall make publicly available the validity status of person identification data they issue, in a privacy preserving manner, and indicate the location of that information in the person identification data.	Article 5(7)	WP-03-01	The assessor reviews privacy-preserving validity-status publication controls maintained by the assessed PID Provider: - location and format of PID or Wallet Unit Attestation status information; - privacy controls preventing status checks from becoming tracking or correlation mechanisms; - how the status-location reference is included in the PID or attestation where required; - availability, integrity and update rules for the status service.	The assessor checks selected validity-status publication cases for the assessed PID Provider during the on-site Stage 2 assessment: - issued and revoked PID or attestation samples with status-location references; - status-service responses for valid, suspended, revoked or unknown items; - privacy tests or configuration evidence limiting correlation and enumeration; - logs and monitoring evidence for status-service updates and availability.
REQ-2977-15	Commission Implementing Regulation (EU) 2024/2977	Only providers of person identification data or electronic attestation of attributes can revoke the person identification data or electronic attestations of attributes issued by them.	Article 5(2)	WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - 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; - controls ensuring that only the PID Provider can revoke person identification data issued by that PID Provider; - assurance checks required before reactivation, renewal or replacement is allowed.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - evidence that revocation was initiated and performed only by the PID Provider that issued the PID; - technical status publication or propagation logs; - cases rejected because the required assurance, authorisation or issuer-only revocation conditions were not met.
REQ-798-01	Commission Implementing Regulation (EU) 2026/798	The PID Provider shall ensure that conformity of the remote identity proofing process is assessed against the	Annex, Sections 1 and 2	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines:	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected 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
		applicable clauses of ETSI TS 119 461 V2.1.1 specified in Section 1 of the Annex, subject to the adaptations specified in Section 2 of the Annex.			- conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required; - the ETSI TS 119 461 use case or clause selected for each proofing route, including the applicable Annex adaptations; - conformity-assessment evidence, scope and results for the applicable ETSI TS 119 461 clauses; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	the applicable ETSI TS 119 461 clause and Annex adaptation; - assessment report, checklist or equivalent evidence showing conformity against the applicable ETSI TS 119 461 V2.1.1 clauses and required adaptations; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP or conformity-assessment conditions.
REQ-798-02	Commission Implementing Regulation (EU) 2026/798	Where the remote identity proofing process is aborted or fails, the PID Provider shall ensure that the individual is provided with sufficient explanations and remedies, particularly in the case of unattended remote identity proofing. The information provided should enable the individual to contribute effectively to the prompt resolution of the problem and, where necessary, to exercise the applicable data subject rights.	Annex, Section 2, Point (7)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - failure conditions that stop the PID or eID means issuance process; - user explanations and remedy information provided after failure, especially for unattended remote proofing, including sufficient information enabling the individual to contribute effectively to prompt resolution of the problem and, where necessary, to exercise applicable data subject rights; - controls preventing partial issuance after a failed or incomplete proofing process; - audit records retained for aborted, timed-out, rejected or escalated attempts.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - records showing termination of the issuance process after proofing failure or abandonment; - user notifications or messages explaining the failure and available remedies, including information sufficient for prompt resolution and, where necessary, exercise of applicable data subject rights; - logs confirming that no PID, Wallet Unit activation or eID means was issued after the failed case; - manual-review or escalation evidence for exceptional cases.
REQ-798-03	Commission Implementing Regulation (EU) 2026/798	The PID Provider shall ensure that measures implementing data protection by design and by default are applied during the onboarding	Annex, Section 2, Point (8)	WP-03-01	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - personal and biometric data collected at each step and the purpose for each data item,	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - sampled onboarding or proofing cases showing data actually collected from physical

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		process, particularly as regards the processing of biometric data. Those measures should limit the collection of biometric data and other personal data from physical and digital identity sources to what is strictly necessary for binding the User's person identification data to the Wallet and to the User's device in which the Wallet Unit is installed.			including data from physical and digital identity sources; - default minimisation, separation, retention and deletion rules, limiting biometric and other personal data to what is strictly necessary for binding the User's PID to the Wallet and to the User's device in which the Wallet Unit is installed; - privacy controls embedded before release of the onboarding or Wallet function; - exception handling where additional data are needed for proofing or security; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	and digital identity sources; - configuration or data-flow evidence supporting minimisation and separation; - evidence that biometric and other personal data collection is limited to what is strictly necessary for binding the User's PID to the Wallet and to the User's device; - retention and deletion evidence for personal or biometric data; - exceptions confirming that additional collection was justified and approved; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
REQ-798-04	Commission Implementing Regulation (EU) 2026/798	Where Baseline LoIP is targeted using an existing electronic identification means as evidence, the electronic identification means shall have been notified at least at assurance level substantial or its assurance level shall have been confirmed by an accredited conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body. Where all applicable requirements are fulfilled, the assessment shall result in a certificate of compliance based on a certification audit and a	Annex, Section 2, Point (9)	WP-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including cases where Baseline LoIP uses an existing electronic identification means as evidence; - evidence that the existing electronic identification means was notified at least at assurance level substantial or that its assurance level was confirmed by an accredited CAB or equivalent body; - the ETSI TS 119 461 use case or clause selected for each proofing route; - certificate of compliance based on a certification audit and security evaluation process referring to assurance levels defined for notified eID means or certified European Digital Identity Wallets, where applicable; - evidence required for previously captured reference face images, including certification	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where Baseline LoIP uses an existing electronic identification means as evidence, including notified assurance level substantial or CAB/equivalent-body confirmation evidence; - certificate of compliance evidence based on certification audit and security evaluation process where applicable; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the existing eID means evidence conditions.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		security evaluation process referring to the assurance levels defined for notified electronic identification means or certified European Digital Identity Wallets under Regulation (EU) No 910/2014.			or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP or as Baseline LoIP based on insufficient eID means evidence.	
REQ-798-05	Commission Implementing Regulation (EU) 2026/798	The PID Provider shall ensure that the evidence used in the identity proofing process is valid at the time of identity proofing.	Annex, Section 2, Point (10)	WP-03-01	The assessor reviews how the assessed PID Provider validates identity evidence and identity data against authoritative or accepted sources: - which authoritative sources are accepted for each evidence type; - timing rules proving that evidence validity is checked at the time of proofing, renewal or reliance; - handling of source unavailability, inconsistent results and expired evidence; - records retained to support the final proofing or issuance decision.	The assessor checks selected source-validation cases for the assessed PID Provider during the on-site Stage 2 assessment: - source responses or validation tokens showing evidence status at the relevant time; - application records where source checks were successful, failed or manually reviewed; - timestamps linking the source check to the proofing or issuance decision; - evidence that expired, unverified or inconsistent evidence was not accepted without justified escalation.
REQ-798-06	Commission Implementing Regulation (EU) 2026/798	Where a physical identity document is used, the effectiveness of the measures required by ETSI TS 119 461 for validating the physical identity document shall be confirmed by an accredited conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.	Annex, Section 2, Point (11)	WP-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required; - the ETSI TS 119 461 use case or clause selected for each proofing route, including routes using a physical identity document; - evidence that the effectiveness of ETSI TS 119 461 measures for validating the physical identity document is confirmed by an accredited CAB or equivalent body where a physical identity document is used; - evidence required for previously captured	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases using a physical identity document, including confirmation by an accredited CAB or equivalent body of the effectiveness of ETSI TS 119 461 measures for validating that document; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP or a physical-document route without the required effectiveness confirmation.	- rejected cases where the route did not meet the required LoIP conditions or lacked the required physical-document validation-effectiveness confirmation.
REQ-798-07	Commission Implementing Regulation (EU) 2026/798	Where a physical identity document is used, the reference face image shall be collected from the document using near field communication, and the process shall perform passive or active authentication of the chip in the physical identity document.	Annex, Section 2, Point (11)	WP-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the documentation covers: - accepted document types and mandatory NFC collection of the reference face image from the physical identity document where such document is used; - passive or active authentication checks performed on the document chip; - handling of failed chip reads, failed authentication, expired documents or unsupported evidence; - retention of technical validation evidence without unnecessary retention of biometric data.	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - NFC read evidence, reference face image collection from the physical identity document, passive or active chip-authentication results and document-status checks; - failed or unsupported chip-reading cases and the resulting proofing decision; - records linking the document result, face reference and final identity decision; - evidence that fallback or manual review did not lower the required assurance level.
REQ-798-08	Commission Implementing Regulation (EU) 2026/798	Where Extended LoIP is targeted, the identity proofing process shall conform to an applicable use case specified in clause 9.5 of ETSI TS 119 461.	Annex, Section 2, Point (12)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required; - the ETSI TS 119 461 use case or clause selected for each proofing route, including the applicable use case specified in clause 9.5 where Extended LoIP is targeted; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable;	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause, including clause 9.5 for Extended LoIP cases; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the applicable clause 9.5 use case.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- controls preventing a lower-assurance route from being accepted as Extended LoIP.	
REQ-798-09	Commission Implementing Regulation (EU) 2026/798	For fully automated identity proofing processes, the PID Provider shall establish and maintain target values for the false accept rate and false reject rate based on a risk analysis and its threat intelligence procedure, using the methodology specified in the ENISA report “Methodology for sectoral cybersecurity assessments” or an equivalent methodology. Those target values shall be equal to or lower than the values established for hybrid use cases, where such values exist.	Annex, Section 2, Point (13)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - risk-analysis and threat-intelligence inputs used to set FAR and FRR targets; - methodology used to compare targets with applicable sectoral or hybrid-use-case values, using the ENISA “Methodology for sectoral cybersecurity assessments” or an equivalent methodology; - evidence that FAR and FRR target values are equal to or lower than the values established for hybrid use cases, where such values exist; - testing and monitoring arrangements for the automated proofing component; - management action required when measured rates exceed the approved targets.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - test reports or production metrics for false accept and false reject rates; - risk-analysis records supporting the chosen targets and the ENISA or equivalent methodology used; - evidence that approved FAR and FRR targets are equal to or lower than hybrid-use-case values where such values exist; - tuning, override or incident records affecting automated proofing performance; - evidence that the automated process remains within the approved risk limits before being relied upon for issuance.
REQ-798-10	Commission Implementing Regulation (EU) 2026/798	Where the applicant is a natural person, including a natural person representing a legal person, whose identity has been proven to Baseline LoIP through authentication using an electronic identification means, and enhancement to Extended LoIP is required, additional identity proofing shall only be applied where the	Annex, Section 2, Point (14)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including cases where Baseline LoIP was achieved through authentication using an electronic identification means by a natural person, including a natural person representing a legal person; - rules ensuring that additional proofing for	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where Baseline LoIP was achieved through authentication using an electronic identification means and enhancement to Extended LoIP was required; - evidence whether the electronic identification means was initially issued in reliance on automated comparison between face images, and that additional proofing was

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		electronic identification means was not initially issued in reliance on automated comparison between face images.			enhancement to Extended LoIP is applied only where the electronic identification means was not initially issued in reliance on automated comparison between face images; - the ETSI TS 119 461 use case or clause selected for each proofing route; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	applied only where that condition was not met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions.
REQ-798-11	Commission Implementing Regulation (EU) 2026/798	Where enhancement from Baseline LoIP to Extended LoIP is performed through full identity proofing using an identity document, the identity proofing process shall fulfil the requirements for Extended LoIP applicable to one of the use cases specified in clauses 9.2.2 or 9.2.3 of ETSI TS 119 461.	Annex, Section 2, Point (15)	WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including enhancement from Baseline LoIP to Extended LoIP through full identity proofing using an identity document; - the ETSI TS 119 461 use case or clause selected for each proofing route, including clauses 9.2.2 or 9.2.3 where this enhancement path is used; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause, including clauses 9.2.2 or 9.2.3 for enhancement from Baseline to Extended through full identity proofing using an identity document; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the applicable 9.2.2/9.2.3 use case.
REQ-798-12	Commission Implementing Regulation (EU) 2026/798	Where enhancement from Baseline LoIP to Extended LoIP uses a previously captured reference face image, the process used to capture the reference face image and bind the	Annex, Section 2, Point (16)	WP-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including enhancement	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where enhancement from Baseline LoIP

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		necessary identity attributes to that image shall: a) fulfil the requirements for Extended LoIP applicable to one of the use cases specified in clauses 9.2.2 or 9.2.3 of ETSI TS 119 461; or b) have been peer reviewed or certified by an accredited conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body as complying with assurance level high under Regulation (EU) No 910/2014.			from Baseline LoIP to Extended LoIP using a previously captured reference face image; - the ETSI TS 119 461 use case or clause selected for each proofing route, including clauses 9.2.2 or 9.2.3 for the process used to capture the reference face image and bind the necessary identity attributes to that image; - evidence required for previously captured reference face images, including peer-review or certification evidence by an accredited CAB or equivalent body demonstrating assurance level high under Regulation (EU) No 910/2014, where the 9.2.2/9.2.3 route is not used; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	to Extended LoIP used a previously captured reference face image; - evidence that the process used to capture the reference face image and bind the necessary identity attributes to it fulfilled ETSI TS 119 461 clauses 9.2.2 or 9.2.3, or was peer reviewed/certified by an accredited CAB or equivalent body as assurance level high; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions.
PDP-01	REQ-1502-01; REQ-1502-02	Before commencing the PID issuance process, the PID Provider shall ensure that the applicant is informed of the terms and conditions related to the use of the PID and of the recommended security precautions.		WP-03-01	The assessor reviews how the assessed PID Provider presents mandatory user information before the user commits to the relevant PID, Wallet Unit or eID means process: - the exact user-facing content, including terms, conditions, obligations, fees, limitations or recommended precautions relevant to the requirement; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it; - version control, approval and language or accessibility handling for the information; - case-level evidence showing which version was presented to the user at the time of onboarding, activation or issuance.	The assessor checks selected user journeys and records for the assessed PID Provider during the on-site Stage 2 assessment: - screens, messages, portal pages or API responses used to present the required information; - sampled user records showing acknowledgement, delivery or acceptance where required; - version history confirming that the correct information applied at the time of the sampled case; - negative or incomplete journeys showing that the process does not continue before the required information is presented.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-02	REQ-1502-03	The PID Provider shall collect the identity data necessary for identity proofing and verification.		WP-03-01	The assessor reviews how the assessed PID Provider determines and collects the identity data needed for proofing, verification and issuance: - the data attributes required for the intended PID or eID means outcome; - sources of the attributes and checks for completeness, consistency and data quality; - data minimisation rules and separation from data not needed for the issuance decision; - handling of incomplete, conflicting or unsupported identity data.	The assessor tests sampled data-collection cases for the assessed PID Provider during the on-site Stage 2 assessment: - application records showing which identity attributes were collected and from which source; - validation results for completeness, consistency and source confirmation; - cases rejected or escalated because identity data were missing or inconsistent; - evidence that unnecessary attributes were not collected for the assessed process.
PDP-03	REQ-910-03; REQ-2977-06; REQ-1502-11-REQ-1502-14	Before issuing PID to a Wallet Unit, the PID Provider shall perform identity proofing and verification of the User in accordance with the requirements applicable to assurance level high.		WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high; - evidence that assurance level substantial requirements are fulfilled before additional assurance level high requirements are applied, where applicable; - rules for applying the applicable assurance level high proofing paths, including photo/biometric evidence, reliance on previous proofing, or national procedures where applicable; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision before PID issuance to the Wallet Unit.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that PID issuance to the Wallet Unit occurred only after required proofing steps were completed; - evidence that assurance level substantial requirements and additional assurance level high requirements were applied where required; - case evidence for applicable high-assurance proofing paths, including photo/biometric evidence, previous proofing reliance or national procedures where applicable; - records showing how exceptions were escalated, corrected or rejected.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-04	REQ-910-06; REQ-798-01	Where the User is onboarded using an electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures, the PID Provider shall ensure that the remote identity proofing process is assessed against the applicable clauses of ETSI TS 119 461 specified in the Annex to CIR (EU) 2026/798, subject to the adaptations specified therein.		WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required; - the ETSI TS 119 461 use case or clause selected for each proofing route, including the applicable clauses specified in the Annex to CIR (EU) 2026/798 and the adaptations specified therein; - conformity-assessment evidence showing that the remote identity proofing process was assessed against those applicable clauses and adaptations; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP or as sufficient additional remote onboarding for the substantial eID means path.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where onboarding used an electronic identification means conforming to assurance level substantial together with additional remote onboarding procedures; - assessment report, checklist or equivalent evidence showing conformity against the applicable ETSI TS 119 461 clauses specified in the Annex to CIR (EU) 2026/798 and the required adaptations; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the Annex/adaptation assessment conditions.
PDP-05	REQ-798-05	The PID Provider shall verify that the evidence used in the identity proofing process is valid at the time of identity proofing.		WP-03-01	The assessor reviews how the assessed PID Provider validates identity evidence and identity data against authoritative or accepted sources: - which authoritative sources are accepted for each evidence type; - timing rules proving that evidence validity is checked at the time of proofing, renewal or reliance; - handling of source unavailability, inconsistent results and expired evidence; - records retained to support the final proofing or issuance decision.	The assessor checks selected source-validation cases for the assessed PID Provider during the on-site Stage 2 assessment: - source responses or validation tokens showing evidence status at the relevant time; - application records where source checks were successful, failed or manually reviewed; - timestamps linking the source check to the proofing or issuance decision; - evidence that expired, unverified or inconsistent evidence was not accepted without justified escalation.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-06	REQ-798-04	Where an existing electronic identification means is used as evidence for Baseline LoIP, the PID Provider shall accept that electronic identification means only where it has been notified at least at assurance level substantial or its assurance level has been confirmed by an accredited conformity assessment body or by an equivalent body in accordance with CIR (EU) 2026/798.		WP-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including use of an existing electronic identification means as evidence for Baseline LoIP; - evidence that the existing electronic identification means was notified at least at assurance level substantial or that its assurance level was confirmed by an accredited conformity assessment body or equivalent body in accordance with CIR (EU) 2026/798; - the ETSI TS 119 461 use case or clause selected for each proofing route; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route or insufficient existing eID means evidence from being accepted as Extended LoIP or Baseline LoIP.	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where an existing electronic identification means was used as evidence for Baseline LoIP; - evidence that the electronic identification means was notified at least at assurance level substantial or that its assurance level was confirmed by an accredited conformity assessment body or equivalent body; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the existing eID means evidence conditions.
PDP-07	REQ-2977-06	The PID Provider shall present to the User the identity verification methods supported for the PID issuance process.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - the accepted proofing paths and the conditions for using each path; - how supported identity verification methods for the PID issuance process are presented to the User before method selection or continuation of the process; - evidence sources, verification checks and manual-review steps supporting assurance level high; - handling of failed, inconsistent, expired or	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - normal, rejected and manually reviewed applications; - screens, messages, portal pages or API responses showing the identity verification methods presented to the User; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
PDP-08	REQ-2977-06	The PID Provider shall execute the identity verification process using the method selected by the User.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - the accepted proofing paths and the conditions for using each path; - how the User selects an identity verification method and how that selected method controls the subsequent verification process; - evidence sources, verification checks and manual-review steps supporting assurance level high; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake and User method selection to the final proofing and issuance decision.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - normal, rejected and manually reviewed applications; - records showing the identity verification method selected by the User and the method actually executed; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed using the selected method or a justified controlled exception; - records showing how exceptions were escalated, corrected or rejected.
PDP-09	REQ-798-02	Where the identity proofing or verification process is aborted or fails, the PID Provider shall terminate the PID issuance process and provide the User with sufficient explanations and available remedies, particularly where unattended remote identity proofing is used.		WP-03-01	The assessor reviews how the assessed PID Provider handles failed or aborted proofing and verification attempts before issuance: - failure conditions that stop the PID or eID means issuance process; - user explanations and remedy information provided after failure, especially for unattended remote proofing; - controls preventing partial issuance after a failed or incomplete proofing process; - audit records retained for aborted, timed-out, rejected or escalated attempts.	The assessor tests selected failed or aborted proofing cases for the assessed PID Provider during the on-site Stage 2 assessment: - records showing termination of the issuance process after proofing failure or abandonment; - user notifications or messages explaining the failure and available remedies; - logs confirming that no PID, Wallet Unit activation or eID means was issued after the failed case; - manual-review or escalation evidence for exceptional cases.
PDP-10	REQ-798-03	The PID Provider shall apply data protection by design and by default during the onboarding		WP-03-01	The assessor reviews data-protection-by-design controls applied by the assessed PID Provider to onboarding, proofing or wallet processing:	The assessor checks selected processing cases and configurations for the assessed PID Provider 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
		process, particularly where biometric data are processed, and shall limit the collection of personal data to what is necessary for identity proofing and PID issuance.			- personal and biometric data collected at each step and the purpose for each data item; - default minimisation, separation, retention and deletion rules; - privacy controls embedded before release of the onboarding or Wallet function; - exception handling where additional data are needed for proofing or security.	- sampled onboarding or proofing cases showing data actually collected; - configuration or data-flow evidence supporting minimisation and separation; - retention and deletion evidence for personal or biometric data; - exceptions confirming that additional collection was justified and approved.
PDP-11	REQ-798-06	Where a physical identity document is used, the PID Provider shall ensure that the effectiveness of the applicable measures used to validate the document has been confirmed by an accredited conformity assessment body or by an equivalent body.		WP-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - accepted evidence types and the national recognition or authoritative validity criteria applied to them; - comparison method between the applicant and the authoritative or document-based reference; - liveness, anti-spoofing, manual-review and exception rules where applicable; - evidence that, where a physical identity document is used, the effectiveness of the applicable document-validation measures has been confirmed by an accredited conformity assessment body or equivalent body; - rejection criteria for expired, unsupported, inconsistent or insufficient evidence.	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - source-validation, document-validation or biometric-comparison results with timestamps; - CAB or equivalent-body confirmation evidence for the effectiveness of applicable physical-document validation measures, where a physical identity document is used; - manual-review notes and final decisions for matched, mismatched and poor-quality evidence; - rejected or escalated cases involving invalid evidence or failed comparison; - audit evidence showing that accepted cases met the required assurance level.
PDP-12	REQ-798-07	Where a physical identity document is used, the reference face image shall be collected from the document using near field communication, and passive or active authentication of the document chip shall be performed.		WP-03-01	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the documentation covers: - accepted document types and mandatory NFC collection of the reference face image from the physical identity document where such document is used; - passive or active authentication checks performed on the document chip;	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - NFC read evidence, reference face image collection from the physical identity document, passive or active chip-authentication results and document-status checks; - failed or unsupported chip-reading cases and the resulting proofing decision; - records linking the document result, face

Requirement 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 of failed chip reads, failed authentication, expired documents or unsupported evidence; - retention of technical validation evidence without unnecessary retention of biometric data.	reference and final identity decision; - evidence that fallback or manual review did not lower the required assurance level.
PDP-13	REQ-798-09	For fully automated identity proofing processes, the PID Provider shall establish and maintain target values for the false accept rate and false reject rate based on risk analysis and threat intelligence. Those values shall be equal to or lower than the values established for hybrid use cases, where such values exist.		WP-03-01	The assessor reviews how the assessed PID Provider sets and maintains accuracy thresholds for fully automated identity proofing: - risk-analysis and threat-intelligence inputs used to set FAR and FRR targets; - methodology used to compare targets with applicable sectoral or hybrid-use-case values; - testing and monitoring arrangements for the automated proofing component; - management action required when measured rates exceed the approved targets.	The assessor examines automated-proofing performance evidence for the assessed PID Provider during the on-site Stage 2 assessment: - test reports or production metrics for false accept and false reject rates; - risk-analysis records supporting the chosen targets; - tuning, override or incident records affecting automated proofing performance; - evidence that the automated process remains within the approved risk limits before being relied upon for issuance.
PDP-14	REQ-798-08	Where enhancement from Baseline LoIP to Extended LoIP is required, the PID Provider shall apply the relevant use case specified in clause 9.5 of ETSI TS 119 461.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including enhancement from Baseline LoIP to Extended LoIP; - the ETSI TS 119 461 use case or clause selected for each proofing route, including the relevant use case specified in clause 9.5 where enhancement to Extended LoIP is required; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause, including clause 9.5 where enhancement from Baseline LoIP to Extended LoIP was required; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the applicable clause 9.5 use case.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-15	REQ-798-10	Where the User's identity has been proven to Baseline LoIP through authentication using an electronic identification means, additional identity proofing intended to achieve Extended LoIP shall only be applied where that electronic identification means was not initially issued in reliance on automated comparison between face images.		WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including cases where Baseline LoIP was achieved through authentication using an electronic identification means; - rules ensuring that additional identity proofing intended to achieve Extended LoIP is applied only where that electronic identification means was not initially issued in reliance on automated comparison between face images; - the ETSI TS 119 461 use case or clause selected for each proofing route; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where Baseline LoIP was achieved through authentication using an electronic identification means and additional proofing was applied to achieve Extended LoIP; - evidence whether that electronic identification means was initially issued in reliance on automated comparison between face images, and that additional proofing was applied only where it was not; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions.
PDP-16	REQ-798-11	Where enhancement from Baseline LoIP to Extended LoIP is performed through full identity proofing using an identity document, the PID Provider shall apply the Extended LoIP requirements applicable to one of the use cases specified in clauses 9.2.2 or 9.2.3 of ETSI TS 119 461.		WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including enhancement from Baseline LoIP to Extended LoIP through full identity proofing using an identity document; - the ETSI TS 119 461 use case or clause selected for each proofing route, including clauses 9.2.2 or 9.2.3 where this enhancement	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - case records showing the route selected and the applicable ETSI TS 119 461 clause, including clauses 9.2.2 or 9.2.3 for enhancement from Baseline to Extended through full identity proofing using an identity document; - evidence that additional proofing was applied only when the preconditions were met; - certification, peer-review or previous-capture evidence for reference face images, where

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					path is used; - evidence required for previously captured reference face images, including certification or peer-review evidence where applicable; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	used; - rejected cases where the route did not meet the required LoIP conditions or the applicable 9.2.2/9.2.3 use case.
PDP-17	REQ-798-12	Where enhancement from Baseline LoIP to Extended LoIP uses a previously captured reference face image, the PID Provider shall ensure that the process used to capture the reference face image and bind the necessary identity attributes to that image fulfils one of the conditions specified in REQ-798-12.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - conditions under which Baseline LoIP is sufficient and when additional Extended LoIP proofing is required, including enhancement from Baseline LoIP to Extended LoIP using a previously captured reference face image; - the ETSI TS 119 461 use case or clause selected for each proofing route, including clauses 9.2.2 or 9.2.3 for the process used to capture the reference face image and bind the necessary identity attributes to that image; - evidence required for previously captured reference face images, including peer-review or certification evidence by an accredited conformity assessment body or equivalent body demonstrating assurance level high under Regulation (EU) No 910/2014, where the 9.2.2/9.2.3 route is not used; - controls preventing a lower-assurance route from being accepted as Extended LoIP.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - case records showing the route selected and the applicable ETSI TS 119 461 clause; - cases where enhancement from Baseline LoIP to Extended LoIP used a previously captured reference face image; - evidence that the process used to capture the reference face image and bind the necessary identity attributes to it fulfilled ETSI TS 119 461 clauses 9.2.2 or 9.2.3, or was peer reviewed/certified by an accredited conformity assessment body or equivalent body as assurance level high; - certification, peer-review or previous-capture evidence for reference face images, where used; - rejected cases where the route did not meet the required LoIP conditions or the REQ-798-12 conditions.
PDP-18	REQ-910-03; REQ-910-06; REQ-2977-06	The PID Provider shall issue PID only after the identity proofing and verification process has been successfully completed and the applicable requirements for assurance level high have been fulfilled.		WP-03-01	The assessor reviews the proofing, onboarding and verification arrangements used by the assessed PID Provider: - the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high; - handling of failed, inconsistent, expired or incomplete evidence;	The assessor tests selected proofing, onboarding and issuance cases for the assessed PID Provider during the on-site Stage 2 assessment: - normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- traceability from application intake to the final proofing and issuance decision.	only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
PDP-19	REQ-2977-07; CEN/TS 18098	When issuing PID to a Wallet Unit, the PID Provider shall identify itself to the Wallet Unit using its wallet-relying party access certificate or another authentication mechanism in accordance with an electronic identification scheme notified at assurance level high.		WP-03-01	The assessor reviews how the assessed PID Provider authenticates itself to Wallet Units before PID issuance or related exchanges: - certificate profiles or alternative assurance level high authentication mechanisms used for provider identification; - certificate lifecycle controls, trust anchors and revocation checks; - protocol steps that prevent Wallet Units from accepting unauthenticated provider requests; - evidence retained for successful and failed provider-authentication events.	The assessor checks provider-authentication evidence for the assessed PID Provider during the on-site Stage 2 assessment: - live or retained protocol traces showing use of the wallet-relying party access certificate or approved alternative mechanism; - certificate validity, chain-building and revocation-check results; - logs for rejected exchanges involving invalid, expired or untrusted credentials; - configuration showing that weaker or unapproved authentication paths are not enabled.
PDP-20	REQ-2977-08; CEN/TS 18098	Before issuing PID, the PID Provider shall authenticate and validate the Wallet Unit Attestation and verify that the Wallet Unit belongs to a wallet solution accepted by the PID Provider.		WP-03-01	The assessor reviews the documented pre-issuance validation process maintained by the assessed PID Provider. The documentation should define: - how the Wallet Unit Attestation is authenticated and validated before PID issuance; - certificate chain, trust-list, validity-status and attestation-integrity checks used for Wallet Unit Attestation validation; - how the PID Provider determines that the Wallet Unit belongs to a wallet solution accepted by the PID Provider; - the register, list, policy or onboarding evidence used to identify accepted wallet solutions; - controls preventing PID issuance where Wallet Unit Attestation validation fails or the Wallet Unit does not belong to an accepted wallet solution; - records retained to evidence the validation	The assessor tests selected PID issuance cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should show: - Wallet Unit Attestation authentication and validation performed before PID issuance; - certificate chain, trust-list, validity-status and attestation-integrity evidence supporting the validation result; - evidence that the Wallet Unit belonged to a wallet solution accepted by the PID Provider at the time of issuance; - logs, workflow records or system timestamps showing that validation and wallet-solution acceptance preceded the technical PID issuance event; - rejected cases where Wallet Unit Attestation validation failed or the Wallet Unit did not belong to an accepted wallet solution; - evidence that PID was not issued where 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
					result and wallet-solution acceptance decision before PID issuance.	required pre-issuance validation or wallet-solution acceptance failed.
PDP-21	REQ-2977-05; CEN/TS 18098	The PID Provider shall verify the binding between the authenticated User and the Wallet Unit, ensuring that the binding method guarantees unity of place and time and is protected against replay and man-in-the-middle attacks.		WP-03-01	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - how the target Wallet Unit and authenticated User are identified before issuance or binding; - how Wallet Unit attestation, public-key material, proof of possession and proof of association are validated; - how the binding method guarantees unity of place and time and is protected against replay and man-in-the-middle attacks; - controls preventing issuance to an unverified, substituted or different Wallet Unit; - evidence retained for failed, repeated or exceptional binding attempts; - rules showing when a new binding or re-issuance is required after Wallet Unit replacement or lifecycle change.	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - the issuance decision, authenticated User, Wallet Unit identifier, attestation evidence and public-key or binding material used; - proof-of-possession and proof-of-association validation results; - evidence that the binding occurred with unity of place and time and that replay or man-in-the-middle attempts are prevented or rejected; - logs showing successful binding and rejection of invalid or incomplete binding requests; - evidence that the resulting PID or eID means cannot be moved to another Wallet Unit without a controlled re-issuance or rebinding process; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
PDP-22	REQ-2977-03; REQ-2977-05; CEN/TS 18098	The PID Provider shall receive the PID issuance request containing: a) the applicable Wallet Unit Validity Attestation and Wallet Unit Trust Attestation; b) the PID public key; c) the Proof of Association; d) the Proof of Possession; and e) the requested PID format.		WP-03-01	The assessor reviews the PID issuance request intake and validation design maintained by the assessed PID Provider. The review should establish whether the interface specification and internal procedure require: - required request content, including applicable Wallet Unit Validity Attestation and Wallet Unit Trust Attestation; - presence and validation of the PID public key, Proof of Association and Proof of Possession; - presence and acceptance of the requested PID format; - certificate and trust-list requirements used	The assessor tests selected PID issuance requests for the assessed PID Provider during the on-site Stage 2 assessment. Using request payloads, validation results and system records, the assessor verifies: - request payloads containing Wallet Unit Validity Attestation, Wallet Unit Trust Attestation, PID public key, Proof of Association, Proof of Possession and requested PID format; - certificate chain, trust-list and validity-status evidence for the received Wallet Unit attestations;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					for validating the received Wallet Unit attestations; - rules rejecting incomplete, malformed, inconsistent or unsupported PID issuance requests.	- validation evidence for PoA, PoP, PID public key and requested PID format; - rejected cases where required request elements were missing, malformed, inconsistent or unsupported.
PDP-23	REQ-2977-05; CEN/TS 18098	The PID Provider shall verify the Proof of Possession of the private key corresponding to the PID public key and the Proof of Association demonstrating that the PID public key is associated with the authenticated User and managed within the Wallet Unit.		WP-03-01	The assessor reviews cryptographic key and proof validation steps used by the assessed PID Provider during Wallet Unit or PID activation: - where keys are generated and how WSCD protection is evidenced; - how public keys, PoA and PoP tokens are retrieved, validated and linked to the correct Wallet Unit or user; - verification rules for structural correctness, freshness and private-key possession; - abort rules preventing activation or credential issuance after failed proof validation.	The assessor tests selected key-generation and proof-validation cases for the assessed PID Provider during the on-site Stage 2 assessment: - key-generation, public-key retrieval and WSCD evidence for sampled Wallet Units; - PoA and PoP validation logs and request payloads; - failed proof or malformed-token cases showing that activation or issuance was stopped; - records linking keys, proofs, Wallet Unit status and the final activation or issuance decision.
PDP-24	REQ-910-03; REQ-2977-08; CEN/TS 18098	The PID Provider shall verify, on the basis of the applicable Wallet Unit attestations and other evidence received, that the use of the PID private key is protected by two independent authentication factors, each resistant to high attack potential.		WP-03-01	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - factor categories used for Wallet Unit, PID private key use or eID means authentication; - evidence, based on applicable Wallet Unit attestations and other received evidence, that use of the PID private key is protected by two independent authentication factors; - resistance to manipulation, duplication, guessing, replay and high attack potential for each factor; - storage, management and verification of factors within the relevant WSCA/WSCD where required; - reset, recovery, fallback and failure handling for each factor type; - how the Wallet Unit identifier, binding	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - configuration and attestation evidence for enabled factors; - evidence that use of the PID private key is protected by two independent authentication factors, each resistant to high attack potential; - successful and failed factor enrolment, verification and recovery cases; - evidence that PIN, password or biometric factors are handled in the required WSCA/WSCD context where applicable; - negative tests showing that weak, duplicated, replayed or unauthorised factors are rejected; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					material, PID public key and issuance decision are linked before release.	technical issuance event and retained audit evidence.
PDP-25	REQ-910-03; REQ-2977-08; CEN/TS 18098	The PID Provider shall verify, on the basis of the applicable Wallet Unit attestations and other evidence received, that the Wallet Unit provides the security and technical capabilities required for the protected storage and use of PID at assurance level high.		WP-03-01	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - evidence, based on applicable Wallet Unit attestations and other received evidence, that the Wallet Unit provides the security and technical capabilities required for protected storage and use of PID at assurance level high; - rules excluding personal data from attestations where the requirement prohibits such data; - how the Wallet Unit identifier, binding material, PID public key and issuance decision are linked before release.	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - issued WUVA or WUTA samples and signature or seal validation evidence; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - evidence that the Wallet Unit provides required security and technical capabilities for protected storage and use of PID at assurance level high; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
PDP-26	REQ-2977-05; REQ-2977-08; CEN/TS 18098	Where the Wallet Unit Attestation, the User-to-Wallet Unit binding, the Proof of Possession, the Proof of Association, the required protection of the PID private key, the security and technical capabilities of the Wallet Unit, or the PID issuance request cannot be successfully verified, the		WP-03-01	The assessor reviews the negative path for failed binding or unverifiable PID issuance requests maintained by the assessed PID Provider. The documented process should make clear: - conditions under which Wallet Unit Attestation, User-to-Wallet Unit binding, Proof of Possession, Proof of Association, PID private-key protection, Wallet Unit security/technical capabilities or PID issuance request verification fails; - certificate and trust-list requirements used	The assessor follows selected failed or exceptional binding attempts for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - cases where Wallet Unit Attestation, User-to-Wallet Unit binding, PoP, PoA, PID private-key protection, Wallet Unit capabilities or PID issuance request verification failed; - certificate chain, trust-list and validity-status evidence for the Wallet Unit Attestation where relevant; - logs or records showing that the request was

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		PID Provider shall reject the request and terminate the binding process without issuing PID.			for validating Wallet Unit attestations before issuance; - rules requiring rejection of the request and termination of the binding process without issuing PID where any required verification cannot be completed successfully; - controls preventing manual override, partial issuance or deferred issuance after failed verification; - records retained for failed, incomplete, malformed or exceptional binding attempts; - the control point where PID generation, signing, persistence and delivery are blocked after a failed verification.	rejected and the binding process was terminated without issuing PID; - evidence that no manual override, partial issuance or later PID issuance occurred without a new successful verification; - exception records for malformed, incomplete or unsupported PID issuance requests; - evidence that no PID was generated, signed, persisted, delivered or made available after the failed verification.
PDP-27	REQ-2977-01; REQ-2977-02; REQ-2977-03; CEN/TS 18098	The PID Provider shall ensure that the PID issued to the Wallet Unit: a) is issued in accordance with the electronic identification scheme under which the wallet solution is provided; b) contains the information necessary for authentication and validation of the PID; c) complies with the applicable technical specifications; and d) is issued in the format requested by the Wallet Unit and supported by the PID Provider.		WP-03-01	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - mandatory and optional PID data elements for each supported format; - rules ensuring that PID is issued in accordance with the electronic identification scheme under which the wallet solution is provided; - schema, signature, validity-status, authentication information and validation information required by the applicable technical specification; - controls ensuring that the issued PID uses the format requested by the Wallet Unit and supported by the PID Provider; - quality checks preventing incomplete, inconsistent or unsupported PID payloads from being issued; - versioning and change control for PID formats and data mappings.	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - issued PID samples or test vectors covering each supported format; - evidence that the issued PID complies with the applicable eID scheme rules; - schema validation, signature validation, authentication-information checks and required metadata checks; - traceability showing the format requested by the Wallet Unit, the format supported by the PID Provider and the format actually issued; - cases rejected because required elements, authentication information, validation information or supported requested format were missing; - traceability between the configured format, the issuance request and the issued PID.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-28	REQ-2977-05; CEN/TS 18098	The PID Provider shall cryptographically bind the PID to the validated Wallet Unit and to the PID public key for which the Proof of Possession and Proof of Association have been successfully verified.		WP-03-01	The assessor reviews the cryptographic binding design used by the assessed PID Provider for PID or eID means material: - how the intended Wallet Unit is identified and validated before binding; - how the PID public key, proof of possession and proof of association are checked before PID is issued; - how the issued PID is linked to the validated Wallet Unit and to the accepted PID public key; - controls preventing issuance to a substituted Wallet Unit, wrong public key or unverified binding request; - evidence retained for failed, repeated or exceptional binding attempts.	The assessor traces selected cryptographic binding cases for the assessed PID Provider during the on-site Stage 2 assessment: - the approved issuance decision, Wallet Unit identifier, attestation result, PID public key and binding evidence; - proof-of-possession and proof-of-association validation logs; - technical issuance records showing the PID bound to the intended Wallet Unit and public key; - rejected cases involving missing proofs, wrong keys, invalid attestations or replayed binding material.
PDP-29	REQ-2977-09	The PID Provider shall establish, maintain and make publicly accessible written policies relating to PID validity status management, including, where applicable, the conditions under which PID shall be revoked without delay.		WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - authorised triggers, decision roles and evidence required for each lifecycle action; - policy content establishing PID validity status management rules, including, where applicable, the conditions under which PID shall be revoked without delay; - controls ensuring that such policies are established, maintained and made publicly accessible; - 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 revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - written and publicly accessible PID validity-status-management policies, including conditions for revocation without delay where applicable; - evidence that the public policy version is maintained and corresponds to the rules applied in sampled cases; - 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
PDP-30	REQ-2977-09; REQ-2977-11; REQ-1502-06; CEN/TS 18098	The PID Provider shall initiate a problem analysis sequence upon ingestion of systemic triggers, including security incidents, cryptographic key leaks, or critical updates received from external official registries.		WP-03-01	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed PID Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor tests selected lifecycle-event and status-decision cases for the assessed PID Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
PDP-31	REQ-2977-11; REQ-1502-06; REQ-1502-09; CEN/TS 18098	The PID Provider shall ingest lifecycle triggers initiated directly by the User, including requests for a PID change or the User's will of discarding the service.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft, PID change requests or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - systemic-trigger and user-trigger cases from intake through analysis and decision, including PID change requests and service discard requests where available; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
PDP-32	REQ-2977-09; REQ-2977-11; CEN/TS 18098	Upon receiving a user-initiated trigger, the PID Provider shall execute a problem analysis sequence to determine		WP-03-01	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed PID Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service	The assessor tests selected lifecycle-event and status-decision cases for the assessed PID Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		status modification parameters.			discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	- records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
PDP-33	REQ-2977-09; REQ-2977-11; REQ-1502-06; REQ-1502-09; CEN/TS 18098	The PID Provider shall evaluate whether an invalidation or a formal change of the PID status is required.		WP-03-01	The assessor reviews lifecycle-event analysis and status-decision rules operated by the assessed PID Provider: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	The assessor tests selected lifecycle-event and status-decision cases for the assessed PID Provider during the on-site Stage 2 assessment: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
PDP-34	CEN/TS 18098	Where the analysis determines that an invalidation or status change is not required, the PID Provider shall terminate the maintenance process flow without status modification.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - systemic and user-initiated triggers that start problem analysis, including incidents, key leaks, registry updates, loss, theft or service discard requests; - criteria for deciding whether suspension, revocation, invalidation, blocking, no status change or another remedy is required; - rules requiring termination of the maintenance process flow without status	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - systemic-trigger and user-trigger cases from intake through analysis and decision; - records showing why the status was changed, left unchanged or temporarily blocked; - cases where analysis determined that invalidation or status change was not required and the maintenance process flow was terminated without status modification;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					modification where the analysis determines that invalidation or status change is not required; - evidence required to support the status-modification decision and the person or system making it; - rules for temporary restrictions, monitoring of blocking time and return to normal status where allowed.	- register and status-service updates after permanent or temporary status changes; - monitoring records showing whether temporary blocking periods were maintained or lifted according to the decision.
PDP-35	REQ-1502-06	The PID Provider shall ensure that PID can be suspended and revoked in a timely and effective manner.		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.
PDP-36	REQ-1502-07	The PID Provider shall implement measures preventing unauthorised suspension, revocation and reactivation of PID.		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
PDP-37	REQ-1502-08	The PID Provider shall reactivate suspended PID only where the same assurance requirements as those established before the suspension continue to be fulfilled.		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.
PDP-38	REQ-2977-15	The PID Provider shall revoke only PID issued by that PID Provider.		WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - 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; - controls ensuring that the PID Provider revokes only PID issued by that PID Provider; - assurance checks required before reactivation, renewal or replacement is allowed.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - evidence that revoked PID was issued by the assessed PID Provider and that PID issued by another provider cannot be revoked by it; - technical status publication or propagation logs; - cases rejected because the required assurance, authorisation or issuer-only revocation conditions were not met.
PDP-39	REQ-2977-11	The PID Provider shall revoke PID issued to a Wallet Unit in each of the following circumstances: a) upon the explicit request of the User; b) where the Wallet Unit		WP-03-01	The assessor reviews the PID revocation and validity status management process maintained by the assessed PID Provider. The documentation should define: - procedures requiring revocation of PID issued to a Wallet Unit upon explicit request of the User;	The assessor checks selected PID revocation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - PID revocations performed upon explicit request of the User; - PID revocations performed because 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
		Attestation has been revoked; or c) in other circumstances defined in the PID Provider's validity status management policy.			- procedures requiring revocation of PID where the Wallet Unit Attestation has been revoked; - other PID revocation circumstances defined in the PID Provider's validity status management policy; - decision roles, authorisation evidence and timing rules for PID revocation where defined; - controls linking User requests, Wallet Unit Attestation revocation events and policy-defined triggers to the corresponding PID revocation decision; - records and system states used to evidence that PID revocation was completed.	Wallet Unit Attestation was revoked; - PID revocations performed under other circumstances defined in the PID Provider's validity status management policy; - records linking the revocation trigger, authorisation, timestamp and technical PID revocation event; - validity status records or system evidence showing that the PID was actually revoked; - cases where a required revocation trigger was detected and PID revocation was completed or, if not completed, escalated as an exception.
PDP-40	REQ-2977-12	The PID Provider shall ensure that revocation of PID cannot be reverted.		WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - status model distinguishing suspension, temporary blocking, revocation and end-of-life states for PID; - technical controls preventing a revoked PID from returning to valid status; - authorisation and logging for revocation decisions; - handling of erroneous revocation without reinstating the revoked PID contrary to the requirement; - technical and procedural controls preventing reversal of completed revocations.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID records and subsequent status history; - attempts or procedures for reactivation to confirm that revoked PID cannot return to valid state; - register, status service and publication evidence after revocation; - exception cases showing how mistakes are corrected through controlled re-issuance rather than reversal; - technical and procedural controls preventing reversal of completed revocations.
PDP-41	REQ-2977-10	Where PID has been revoked, the PID Provider shall inform the User, through dedicated and secure channels, within 24 hours of the revocation and of the reasons for the revocation. The		WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - triggering events and deadlines for user notification, including the 24-hour deadline after PID revocation where applicable; - dedicated secure channels and message	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - timestamps from PID revocation decision to user notification confirming notification within 24 hours; - message content and channel evidence for

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		information shall be concise, easily accessible and provided using clear and plain language.			templates used for notification; - required content of the notification, including reason, status and available remedies where applicable, provided in a concise, easily accessible manner and using clear and plain language; - records proving delivery, failure handling and escalation.	notified users, including the reasons for revocation and use of dedicated secure channels; - evidence that the information was concise, easily accessible and provided using clear and plain language; - failed delivery or escalation records; - cases confirming that users were not left without notice after a status change.
PDP-42	REQ-2977-14	The PID Provider shall make publicly available the validity status of the PID it issues in a privacy-preserving manner and shall indicate the location of that information in the PID.		WP-03-01	The assessor reviews privacy-preserving validity-status publication controls maintained by the assessed PID Provider: - location and format of PID or Wallet Unit Attestation status information; - privacy controls preventing status checks from becoming tracking or correlation mechanisms; - how the status-location reference is included in the PID or attestation where required; - availability, integrity and update rules for the status service.	The assessor checks selected validity-status publication cases for the assessed PID Provider during the on-site Stage 2 assessment: - issued and revoked PID or attestation samples with status-location references; - status-service responses for valid, suspended, revoked or unknown items; - privacy tests or configuration evidence limiting correlation and enumeration; - logs and monitoring evidence for status-service updates and availability.
PDP-43	REQ-2977-13	The PID Provider shall ensure that revoked PID remains accessible for as long as required by Union law or national law.		WP-03-01	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - legal basis determining how long revoked PID must remain accessible under Union law or national law; - retention rules and technical controls ensuring revoked PID remains accessible for the required period; - integrity, availability and access-control measures for retained revoked PID records; - procedures for lawful deletion or archival only after the required accessibility period expires.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID records and the applicable Union-law or national-law retention/accessibility period; - evidence that revoked PID remains accessible after revocation for the required period; - integrity, availability and access-control evidence for retained revoked PID records; - cases where retained revoked PID was archived or deleted only after the legally required period expired.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
PDP-44	REQ-1502-09	Taking into account the risk of changes to the person identification data, the PID Provider shall ensure that renewal or replacement of PID: a) fulfils the same assurance requirements as the initial identity proofing and verification process; or b) is based on a valid electronic identification means of the same or a higher assurance level.		WP-03-01	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path; - risk assessment for changes to the person identification data before renewal or replacement; - evidence sources, verification checks and manual-review steps supporting assurance level high; - rules ensuring that renewal or replacement fulfils the same assurance requirements as the initial identity proofing and verification process, or is based on a valid electronic identification means of the same or a higher assurance level; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - risk assessment for changes to the person identification data in renewal or replacement cases; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - evidence that renewal or replacement fulfilled the same assurance requirements as the initial identity proofing and verification process, or was based on a valid electronic identification means of the same or a higher assurance level; - records showing how exceptions were escalated, corrected or rejected.
PDP-45	REQ-1502-10	Where renewal or replacement of PID is based on a valid electronic identification means, the PID Provider shall verify the identity data against an authoritative source.		WP-03-01	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - authorised triggers, decision roles and evidence required for each lifecycle action; - rules for renewal or replacement of PID based on a valid electronic identification means, including verification of identity data against an authoritative source; - timeliness requirements and technical propagation of status changes; - controls preventing unauthorised suspension, revocation, reactivation or renewal; - assurance checks required before	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - renewal or replacement cases based on a valid electronic identification means, including evidence that identity data were verified against an authoritative source; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					reactivation, renewal or replacement is allowed.	- cases rejected because the required assurance, authorisation or authoritative-source verification conditions were not met.
REQ-1502-09	Commission Implementing Regulation (EU) 2015/1502	Person identification data and authentication data used by the electronic identification means shall be protected against loss, compromise, disclosure, unauthorised use and offline analysis.	Annex, Section 2.2.1 and Section 2.3.1, Level High	WP-03-03	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish whether the documentation covers: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - controls protecting person identification data and authentication data used by the electronic identification means against loss, compromise, disclosure, unauthorised use and offline analysis; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - cryptographic agility process for weakened or deprecated algorithms; - controls against offline analysis, tampering, replay or manipulation by attackers with high attack potential.	The assessor tests selected authentication cases and related security events for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - evidence that person identification data and authentication data used by the electronic identification means are protected against loss, compromise, disclosure, unauthorised use and offline analysis; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-1502-01	Commission Implementing Regulation (EU) 2015/1502	Providers delivering any operational service covered by CIR (EU) 2015/1502 shall be a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services.	Annex, 2.4.1, Level Low, Element 1	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - legal status, ownership or mandate to provide the assessed service, including evidence that the provider is a public authority or a legal entity recognised as such by national law of a Member State; - established organisation and operational capability in all parts relevant for the provision of the assessed services; - financial-capacity evidence, insurance or	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - company, mandate, insurance, guarantee or financial-capacity documents, including evidence of public-authority status or legal-entity recognition under national law of a Member State; - organisation, staffing, process and operational-readiness evidence showing that all service-relevant parts are established and fully operational;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					liability 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.	- 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.
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	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;	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		operations and providing of the 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.	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 responsibility for outsourced commitments and compliance with the scheme policy as if the provider had performed the duties itself; - governance controls ensuring that outsourcing does not transfer or reduce the provider's accountability for scheme-policy compliance; - ongoing monitoring of supplier performance, security issues and changes.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including responsibility clauses for outsourced commitments and scheme-policy compliance; - risk assessments, onboarding approvals and periodic review records; - evidence that the provider monitors and accepts responsibility for outsourced duties as if performed by the provider itself; - supplier incidents, service reports, audit results or vulnerability notifications; - evidence that supplier changes or failures were reflected in risk and continuity processes.

Requirement 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-1502-06	Commission Implementing Regulation (EU) 2015/1502	The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.	Annex, 2.4.2, Level Low, Element 1	WZ-03-01	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should show: - which information must be public, user-facing or provided to relying parties, including a published service definition with all applicable terms, conditions, fees, limitations of usage and a privacy policy; - 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.	The assessor checks selected data-processing and separation cases for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices, including the published service definition, applicable terms, conditions, fees, usage limitations and privacy policy; - 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	Appropriate policies and procedures shall be in place that provide for full	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	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

Requirement 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	and correct responses to requests for information.			identify: - which information must be public, user-facing or provided to relying parties; - policies and procedures for receiving, handling and responding to requests for information; - controls ensuring that responses to information requests are full, correct, approved where required and consistent with the current service definition and policies; - 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.	assessment. The evidence should include: - current public pages, repositories, policy documents or user-facing notices; - sampled requests for information and the responses provided; - evidence that responses were full, correct, timely and consistent with approved public or user-facing information; - change history, approval records and publication timestamps; - 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;	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;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- adherence of the information security management system to proven standards or principles for the management and control of information security risks; - management approval, ownership and review cycle; - allocation of responsibilities and links to operational procedures; - coverage of legal, scheme and cybersecurity obligations relevant to the assessed service.	- evidence that the information security management system adheres to proven standards or principles for managing and controlling information security risks; - interviews with owners of key security and service processes; - evidence that procedures used in operations match the approved policy scope; - examples of updates triggered by service changes, incidents, audit results or risk changes.
REQ-1502-11	Commission Implementing Regulation (EU) 2015/1502	Record and maintain relevant information using an effective record-management system, considering applicable legislation and good practice in relation to data protection and data retention.	Annex, 2.4.4, Level Low, Element 1	WZ-03-01	The assessor reviews the documented arrangements maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should identify: - scope of certification and mapping to Wallet, PID or eID scheme functions; - effective record-management system used to record and maintain relevant information; - responsibilities for maintaining evidence, reporting changes and managing recertification; - applicable legislation and good practice for data protection and data retention reflected in record classification, retention, access and disposal rules; - links between certification obligations, risk register and continuous-compliance activities; - records required for notification to the CAB, supervisory body or scheme owner where applicable.	The assessor checks implementation of the documented arrangements for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - current certificate, certification scope, assessment reports or action plans; - record-management system samples showing relevant information recorded, maintained, classified and protected; - records of changes, recertification decisions or continuous-compliance checks; - retention and data-protection evidence showing consideration of applicable legislation and good practice; - notifications sent to the CAB, supervisory body or scheme owner where required; - evidence that open findings or certification conditions are tracked to closure.
REQ-1502-12	Commission Implementing Regulation (EU) 2015/1502	Retain, as far as it is permitted by national law or other national administrative arrangement and protect records for as long as they	Annex, 2.4.4, Level Low, Element 2	WZ-03-01	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documented arrangements should define:	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:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		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]			- 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.	- 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 out-of-hours support; - dependency on subcontractors and escalation capacity;	The assessor checks staffing-capacity evidence for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - staffing plans, duty rosters, support schedules or service reports; - evidence of backup coverage for critical roles; - open vacancies, overload indicators or subcontractor capacity constraints; - management actions taken when capacity is insufficient.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- monitoring of workload, vacancies or capacity risks.	
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; - 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	The assessor checks selected facility and restricted-area access evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - access lists for facilities or areas holding or processing personal, cryptographic or other sensitive information; - samples showing access granted only to authorised staff or subcontractors; - physical access logs, visitor records, access-review records and access-removal evidence; - exceptions or emergency-access cases and related approvals;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					monitoring of access events; - exceptions, emergency access and evidence retained for physical or facility access decisions.	- 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 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	The assessor checks selected network zones, communication channels and protection controls for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - protocol traces or configuration evidence for channels exchanging personal or sensitive information; - encryption, certificate, key, trust-anchor and integrity-protection evidence; - negative tests showing that eavesdropping, manipulation, replay or downgrade attempts are prevented or rejected;

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

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

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

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

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

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

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

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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		of the status through regular reporting.			- 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.	- review schedules, criteria, results and evidence supporting compliance conclusions; - regular reports submitted to management bodies on compliance status; - records of management decisions, corrective actions and follow-up for identified non-compliance; - evidence that reporting frequency and content match the provider's established governance arrangements.
REQ-2690-14	Commission Implementing Regulation (EU) 2024/2690	The provider shall independently review its approach to managing network and information system security and its implementation, conducted by individuals with appropriate audit competence.	Annex, 2.3.1-2.3.4	WZ-03-01	The assessor reviews information system 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,	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

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

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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2690	causes and documented lessons learned.			and PID Provider for the eID means, as applicable. The review should establish whether the documentation covers: - detection sources, classification criteria and escalation paths; - notification duties toward users, CAB, supervisory bodies, CSIRT or other authorities where applicable; - evidence collection, containment, recovery and post-incident review steps, including root-cause identification and documented lessons learned; - links with vulnerability management, risk assessment, change management and user communication.	the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - events from detection through triage, classification, containment and closure; - notifications sent within required deadlines and the evidence supporting the decision to notify or not notify; - forensic evidence, logs and management decisions retained for the incident; - post-incident actions, root-cause analysis, documented lessons learned and updates to controls, risks or procedures.
REQ-2690-21	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down and maintain a business continuity and disaster recovery plan, based on risk assessment results.	Annex, 4.1.1-4.1.4	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - business continuity and disaster recovery plan maintained for the assessed service; - risk assessment results used as the basis for continuity and disaster recovery planning; - critical processes, dependencies, recovery objectives and disaster recovery scenarios; - roles, communications, escalation, activation criteria and decision-making rules; - review, testing and update rules for the business continuity and disaster recovery plan.	The assessor checks continuity, disaster-recovery, crisis or termination evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The sample should include: - approved business continuity and disaster recovery plan for the assessed service; - evidence linking the plan to risk assessment results; - exercise reports, disaster recovery tests, failover tests or continuity-plan walkthroughs; - records showing roles, communications, escalation and activation decisions; - updates made to the plan after tests, incidents, risk changes or service changes.
REQ-2690-22	Commission Implementing Regulation (EU) 2024/2690	The provider shall maintain backup copies of data and provide sufficient available resources to ensure an appropriate level of redundancy.	Annex, 4.2.1-4.2.6	WZ-03-01	The assessor reviews continuity, disaster-recovery, crisis-management or termination planning maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should define: - critical processes, dependencies and recovery	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
					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 (EU) 2024/2690	The provider shall establish, implement, and apply a supply chain security policy governing relations with direct	Annex, 5.1.1-5.1.7	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supply chain security policy established,	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - supply chain security policy evidence and

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		suppliers and service providers.			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.	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 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;	The assessor checks selected development, acquisition, maintenance or security-testing records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - sampled risks from the register linked to assets, processes and treatment actions, including risks stemming from acquisition of ICT services or ICT products; - procurement or acquisition records showing

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- identification of 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.	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; - change request, approval, testing, implementation and rollback requirements; - segregation between emergency, standard and normal changes; - controls detecting unauthorised configuration drift.	The assessor checks selected configuration and change records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - change tickets from request through approval, testing, deployment and closure; - baseline configuration compared with observed or exported production configuration; - emergency or failed changes and post-implementation reviews;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						- 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; - links between testing results, risk treatment, change management and release decisions.	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; - release or change records showing how test results influenced implementation decisions.
REQ-2690-31	Commission Implementing Regulation	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	The assessor checks selected patch records 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				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.	- 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.
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	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;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					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.	- 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; - handling, escalation and remediation of malware or unauthorised-software detections.	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 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	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					residual exposure; - coordination with patching, change management, incident response and risk management; - communication or disclosure rules for vulnerabilities affecting users or relying parties.	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; - triggers for updating risk assessment after incidents, changes, vulnerabilities or supplier changes.	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; - 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	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					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.	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, 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.	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 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;	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;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					- 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.	- configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-2690-40	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure that employees and direct suppliers and service providers understand and commit to their security responsibilities.	Annex, 10.1.1-10.1.3	WZ-03-01	The assessor reviews supplier, outsourcing and supply-chain governance maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should cover: - supplier inventory and identification of providers supporting Wallet, PID or eID scheme functions; - requirements ensuring that employees, direct suppliers and service providers understand and commit to their security responsibilities; - pre-contract due diligence, risk assessment 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.	The assessor checks selected supplier and outsourced-service records for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - contracts, SLA and security annexes for critical suppliers, including security-responsibility commitments for direct suppliers and service providers; - risk assessments, onboarding approvals and periodic review records; - employee training, acknowledgement or commitment records showing understanding 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	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;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					assignment to sensitive roles; - handling of unsuccessful, delayed or expired checks; - privacy and retention controls for background-check evidence.	- completed verification evidence and dates; - exceptions, delays or compensating approvals; - evidence that role assignment considered the background-verification result.
REQ-2690-42	Commission Implementing Regulation (EU) 2024/2690	The provider shall ensure that security responsibilities that remain valid after termination or change of employment are contractually defined and enforced.	Annex, 10.3.1-10.3.2	WZ-03-01	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should establish: - roles in scope, trusted responsibilities and required competence or screening criteria; - training, awareness and acceptance of employment or confidentiality obligations; - responsibilities after termination or change of employment, including security responsibilities that remain valid after termination or role change and are contractually defined and enforced; - disciplinary process for breaches of security or service procedures, including enforcement of continuing security responsibilities.	The assessor checks selected cryptographic-control and key-management evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - samples of staff or contractors in trusted, operational and support roles; - screening, training, role-description and acknowledgement records; - leaver or role-change cases and evidence of removed responsibilities and access, including contractual clauses defining security responsibilities that remain valid after termination or change of employment; - records showing how policy or procedure 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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
						that the disciplinary process for security-policy violations was communicated and maintained.
REQ-2690-44	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, document, and implement logical and physical access control policies.	Annex, 11.1.1-11.1.3	WZ-03-01	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The documentation should describe: - logical and physical access control policies established, documented and implemented; - roles, privileged functions and segregation-of-duty constraints for the assessed service; - joiner, mover, leaver, approval and periodic-review processes; - authentication requirements for administrative and sensitive access; - physical access requirements for facilities and restricted areas holding or processing sensitive information; - 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: - logical and physical access-control policy evidence and implementation samples; - user and privileged-account samples from request to approval, provisioning and review; - physical access samples for facilities and restricted areas; - terminated or changed personnel records compared with access-removal evidence; - configuration of MFA, privileged access, emergency access and segregation rules; - logs showing use of privileged or sensitive access and related review activity.
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	The provider shall maintain policies for management of privileged	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,	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-

Requirement 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	accounts and system administration accounts.			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.	site Stage 2 assessment. The evidence should include: - policy evidence for management of privileged accounts and system administration accounts; - user and privileged-account samples from request to approval, provisioning and review; - terminated or changed personnel records compared with access-removal evidence; - configuration of MFA, privileged access, emergency access and segregation rules; - logs showing use of privileged or sensitive access and related review activity.
REQ-2690-47	Commission Implementing Regulation (EU) 2024/2690	The provider shall restrict and control the use of system administration systems.	Annex, 11.4.1-11.4.2	WZ-03-01	The assessor reviews controls over system administration systems used by the assessed provider across Wallet, PID and eID scheme responsibilities: - administration workstations, bastions, consoles or management networks in scope; - 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	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;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					identity lifecycle processes; - ownership, periodic review, recertification and removal of obsolete or unused identities; - links between identities, access rights, privileged roles, logging and accountability.	- periodic identity review and recertification records; - evidence that obsolete, unused or unauthorised identities are disabled or removed; - logs or audit trails linking identity lifecycle actions to approvals and accountable owners.
REQ-2690-49	Commission Implementing Regulation (EU) 2024/2690	The provider shall implement secure authentication procedures and technologies.	Annex, 11.6.1-11.6.4	WZ-03-01	The assessor reviews secure-authentication procedures and technologies used by the assessed provider across Wallet, PID and eID scheme responsibilities: - authentication methods required for users, administrators and service components; - MFA, credential lifecycle, logout and session controls; - protection of secrets, tokens and recovery processes; - criteria for stronger authentication on sensitive or privileged operations.	The assessor tests selected authentication controls for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - configuration of MFA, passwordless, certificate or token-based authentication; - successful, failed and locked authentication attempts; - credential reset and recovery cases; - evidence that privileged and sensitive access requires stronger authentication.
REQ-2690-51	Commission Implementing Regulation (EU) 2024/2690	The provider shall lay down classification levels of all assets, including information, for the level of protection required.	Annex, 12.1.1-12.1.3	WZ-03-01	The assessor reviews asset and media-management arrangements for the assessed provider across Wallet, PID and eID scheme responsibilities: - asset inventory scope covering systems, data, keys, media and service components relevant to the assessed function; - ownership, classification, acceptable use and lifecycle rules; - media handling, transfer, storage, sanitisation and destruction controls where relevant; - links between assets, risks, access rights, logging and continuity arrangements.	The assessor checks selected asset and media records for the assessed provider across Wallet, PID and eID scheme responsibilities during the on-site Stage 2 assessment: - inventory entries compared with observed systems, repositories or configuration records; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-52	Commission Implementing Regulation (EU) 2024/2690	The provider shall establish, implement, and apply a policy for the proper handling of assets.	Annex, 12.2.1-12.2.3	WZ-03-01	The assessor reviews asset inventory, classification and handling rules maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - policy for the proper handling of assets,	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					established, 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.	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 relevant, including controls for removable storage media; - 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: - 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; - 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	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					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.	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; - 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; - classification, owner and lifecycle status for sampled assets or media; - transfer, disposal, sanitisation or destruction evidence where applicable, including deposit, return or deletion of assets upon termination of employment; - cases showing that access, monitoring and backup controls are aligned with asset criticality.
REQ-2690-56	Commission Implementing Regulation (EU) 2024/2690	The provider shall prevent loss, damage or compromise of network and information systems due to failure of supporting utilities.	Annex, 13.1.1-13.1.3	WZ-03-01	The assessor reviews technical and 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;	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;

Requirement 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 to continuity, disaster recovery, incident response and risk management.	- 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 incidents, changes, vulnerabilities or supplier changes.	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 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.

Requirement 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-2981-01	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 complemented risk assessment was shared with the certification body for evaluation.	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; - 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.

Requirement 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-2981-03	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; - communication or disclosure rules for vulnerabilities affecting users or relying parties.	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; - 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	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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					employment or confidentiality obligations; - responsibilities after termination or change of employment; - disciplinary process for breaches of security or service procedures.	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; - 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-2981-06	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	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:	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:

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		procedures, considering the procedures set out in existing European and international standards, including EN ISO/IEC 30111:2019.			- 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.	- 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.
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	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,	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,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		solution; (b) possible risks associated with the proximity or likelihood of an attack; (c) whether the vulnerability can be remedied; (d) possible ways to remedy the vulnerability. The report shall be transmitted without undue delay to the certification body. The holder of a certificate of conformity shall establish, maintain, and operate a vulnerability management 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			registration and disclosure, including preparation of a vulnerability impact analysis report for any vulnerability affecting software components of the wallet solution; - report content covering impact on the certified wallet solution, risks associated with proximity or likelihood of an attack, whether the vulnerability can be remedied, and possible ways to remedy it; - remediation, mitigation, retesting and closure rules; - notification to CAB or certification body where vulnerability impact criteria are met, including transmission of the vulnerability impact analysis report to the certification body without undue delay.	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 that affects the software components of the wallet solution, including: (a) the impact on the certified wallet solution; (b) possible risks associated with the proximity or likelihood of an attack; (c) whether the vulnerability can be remedied; (d) possible ways to remedy the vulnerability. The report shall be transmitted without undue delay to the certification body. [Article 5(5), Article 5(6)] REQ-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.				

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		[Article 5(9)] 4.3.3 Public Information (Article 8(5) and Annex V) REQ-2981-12 The provider shall make publicly available, in a clear, comprehensive and easily accessible manner: (a) any limitations on the use of the wallet solution; (b) guidance and recommendations for secure configuration, installation, deployment, operation and maintenance; (c) the period during which security support will be offered, in particular regarding cybersecurity-related 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	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,	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;

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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		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.			- 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.	- available clearly, comprehensively and accessibly; - published limitations on the use of the wallet solution; - published secure configuration, installation, deployment, operation and maintenance guidance; - published security-support period, including cybersecurity-update support; - published contact information and accepted methods for receiving vulnerability information; - published references to online repositories for disclosed vulnerabilities and cybersecurity advisories.
REQ-2981-13	Commission Implementing Regulation (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);	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;

Requirement 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, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities.	- expired or archived records and evidence of secure deletion where retention ended.
REQ-2981-14	Commission Implementing Regulation (EU) 2024/2981	The holder of the certificate of conformity shall make the information referred to in Article 19(1) available to the certification body or the Scheme Owner upon request.	Article 19(3)	WZ-03-01	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed Wallet Provider and PID Provider for the eID means, as applicable. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including the information referred to in Article 19(1) of CIR (EU) 2024/2981; - retention period, including periods after certificate cancellation or expiry where applicable; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including availability of Article 19(1) information to the certification body or the Scheme Owner upon request.	The assessor checks certification and scope evidence for the assessed Wallet Provider and PID Provider for the eID means, as applicable, during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including Article 19(1) information; - storage location, access-control, integrity and retention metadata; - retrieval evidence for CAB or supervisory requests, including evidence that Article 19(1) information is made available to the certification body or the Scheme Owner upon request; - expired or archived records and evidence of secure deletion where retention ended.
REQ-5c-03	Article 5c of eIDAS / Regulation (EU) 910/2014	The person identification data available from the electronic identification scheme under which the European Digital Identity Wallet is provided shall uniquely represent the natural person.	Article 5a(5)(f), applicable to PID Provider via Article 5c	WZ-03-02	The assessor reviews how the assessed PID Provider ensures uniqueness of person identification data before issuance or use in the eID scheme: - unique identifiers, matching rules and authoritative datasets used to detect duplicates or collisions; - handling of identity merges, corrections, duplicate candidates and ambiguous matches; - controls preventing PID issuance before uniqueness checks are complete; - records retained to justify the final uniqueness decision.	The assessor tests selected uniqueness decisions for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID records compared with duplicate-check or matching results; - blocked, corrected or escalated duplicate candidates; - source-system evidence showing the person represented by the issued PID; - audit trail linking uniqueness checks to the final issuance decision.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-5c-04	Article 5c of eIDAS / Regulation (EU) 910/2014	Personal data relating to the provision of personal identification data to the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider.	Article 5a (14)	WZ-03-02	The assessor reviews privacy and separation controls implemented by the assessed PID Provider, PID or eID means data: - data flows, stores and interfaces separating wallet or PID data from other provider services; - purpose limitation, minimisation and non-combination controls; - technical controls preventing tracking, linkability or unauthorised observation of user activity; - governance for exceptions, access to personal data and retention of privacy-related evidence.	The assessor checks implementation of privacy and separation controls for the assessed PID Provider during the on-site Stage 2 assessment: - architecture diagrams, database or tenant separation evidence and access-control configuration; - sampled logs or data-flow evidence showing that cross-service combination or tracking is not occurring; - privacy-relevant configuration for dashboards, transaction logs, analytics and relying-party interactions; - exceptions or support cases to confirm that access to personal data is controlled and recorded.
REQ-1502-E01	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.	Annex, Section 2.1.1, All Assurance Levels, Element 1	WZ-03-02	The assessor reviews how the assessed PID Provider presents mandatory user information before the user commits to the relevant PID, Wallet Unit or eID means process: - the exact user-facing content, including terms, conditions, obligations, fees, limitations or recommended precautions relevant to the requirement; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it; - version control, approval and language or accessibility handling for the information; - case-level evidence showing which version was presented to the user at the time of onboarding, activation or issuance.	The assessor checks selected user journeys and records for the assessed PID Provider during the on-site Stage 2 assessment: - screens, messages, portal pages or API responses used to present the required information; - sampled user records showing acknowledgement, delivery or acceptance where required; - version history confirming that the correct information applied at the time of the sampled case; - negative or incomplete journeys showing that the process does not continue before the required information is presented.
REQ-1502-E02	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure the applicant is aware of recommended security precautions related to the	Annex, Section 2.1.1, All Assurance Levels, Element 2	WZ-03-02	The assessor reviews how the assessed PID Provider presents mandatory user information before the user commits to the relevant PID, Wallet Unit or eID means process: - the exact user-facing content, including	The assessor checks selected user journeys and records for the assessed PID Provider during the on-site Stage 2 assessment: - screens, messages, portal pages or API responses used to present the required

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		electronic identification means.			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.	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-E03	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall collect the relevant identity data required for identity proofing and verification.	Annex, Section 2.1.1, All Assurance Levels, Element 3	WZ-03-02	The assessor reviews how the assessed PID Provider determines and collects the identity data needed for proofing, verification and issuance: - the data attributes required for the intended PID or eID means outcome; - sources of the attributes and checks for completeness, consistency and data quality; - data minimisation rules and separation from data not needed for the issuance decision; - handling of incomplete, conflicting or unsupported identity data.	The assessor tests sampled data-collection cases for the assessed PID Provider during the on-site Stage 2 assessment: - application records showing which identity attributes were collected and from which source; - validation results for completeness, consistency and source confirmation; - cases rejected or escalated because identity data were missing or inconsistent; - evidence that unnecessary attributes were not collected for the assessed process.
REQ-1502-E04	Commission Implementing Regulation (EU) 2015/1502	Where electronic identification means are issued based on a valid notified electronic identification means having the assurance level high, it is not required to repeat the identity proofing and verification processes, considering the risks of a change in the person identification data. Additionally, PID Provider shall ensure that steps are	Annex, Section 2.1.2, Level High, Point 1(c)	WZ-03-02	The assessor reviews how the assessed PID Provider decides whether previous identity proofing or a prior electronic identification means may be relied upon instead of repeating proofing: - criteria for confirming that the prior electronic identification means was valid at the time of reliance; - separate handling for notified assurance level high means and non-notified means requiring CAB or equivalent-body confirmation; - risk assessment for changes in person identification data since the previous proofing or issuance procedure;	The assessor tests selected reliance decisions for the assessed PID Provider during the on-site Stage 2 assessment: - cases based on a valid notified electronic identification means at assurance level high, where available; - cases based on a non-notified means, including CAB or equivalent-body confirmation of assurance level high; - records showing validity, notification status, assurance level and risk-of-changed-PID-data checks; - decisions where reliance was rejected and the full proofing path was used;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.			- evidence required to demonstrate that the previous procedure remains valid for the current issuance decision; - fallback rules requiring full identity proofing and verification when any reliance condition is not met.	- traceability from prior evidence to the final PID or eID means issuance outcome.
REQ-1502-E07	Commission Implementing Regulation (EU) 2015/1502	The evidence can be assumed to be genuine, or to exist according to an authoritative source, and the evidence appears to be valid.	Annex, Section 2.1.2, Level Low, Point 2	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - rules for determining that the evidence can be assumed to be genuine; - authoritative sources used to confirm that the evidence exists; - checks confirming that the evidence appears to be valid at the time of assessment; - handling of expired, unsupported, inconsistent, incomplete or non-verifiable evidence; - traceability from genuineness, source-existence and validity checks to the enrolment or proofing decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - application records showing the evidence assessed for genuineness or authoritative-source existence; - source responses or verification results confirming that the evidence exists according to an authoritative source; - validity checks showing that the evidence appeared valid at the time of assessment; - cases rejected or escalated because evidence was expired, unsupported, inconsistent, incomplete or non-verifiable; - audit trail linking evidence checks to the final enrolment or proofing decision.
REQ-1502-E08	Commission Implementing Regulation (EU) 2015/1502	It is known by an authoritative source that the claimed identity exists, and it may be assumed that the person claiming the identity is one and the same.	Annex, Section 2.1.2, Level Low, Point 3	WZ-03-02	The assessor reviews how the assessed PID Provider confirms existence of the claimed identity and the link to the claimant: - authoritative sources used to confirm that the claimed identity exists; - evidence or inference rules supporting that the claimant is the same person; - handling of ambiguous, duplicate or inconsistent identity-source results; - escalation to stronger proofing when the assumption cannot be justified.	The assessor checks selected authoritative-source cases for the assessed PID Provider during the on-site Stage 2 assessment: - source responses proving existence of the claimed identity; - evidence linking the claimant to the identity; - ambiguous or failed checks and resulting escalation; - final proofing decisions supported by the source evidence.
REQ-1502-E09	Commission Implementing Regulation	Conditional: At least one of requirements REQ-1502-E09-01, REQ-1502-E09-02 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	The assessor tests selected conditional enrolment decisions for the assessed PID Provider 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) 2015/1502				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.	- 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-E09-2	Commission Implementing Regulation (EU) 2015/1502	Alternative: Where an identity document is presented during a registration process in the Member State where the document was issued, the document appears to relate to the person presenting it 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 2	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - accepted evidence types and the national recognition or authoritative validity criteria applied to them, including identity documents presented during a registration process in the Member State where the document was issued; - comparison method between the applicant and the authoritative or document-based reference, including checks that the document appears to relate to the person presenting it; - steps taken to minimise the risk that the person's identity is not the claimed identity; - liveness, anti-spoofing, manual-review and exception rules where applicable; - rejection criteria for expired, unsupported, inconsistent or insufficient evidence.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - source-validation, document-validation or biometric-comparison results with timestamps, including identity-document cases presented in the Member State where the document was issued; - evidence that the document appeared to relate to the person presenting it; - records of steps taken to minimise the risk that the person's identity is not the claimed identity; - manual-review notes and final decisions for matched, mismatched and poor-quality evidence; - rejected or escalated cases involving invalid evidence or failed comparison; - audit evidence showing that accepted cases met the required assurance level.
REQ-1502-E10	Commission Implementing Regulation (EU) 2015/1502	Conditional: At least one of requirements REQ-1502-E10-01, REQ-1502-E10-02,		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;	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;

Requirement 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 required before the provider treats the conditional route as satisfied; - fallback to the stricter proofing route when the conditional route is incomplete or unsupported.	- 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-E10-1	Commission Implementing Regulation (EU) 2015/1502	Alternative: Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State and representing the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source, and the applicant is identified as the claimed identity through comparison of one or more physical characteristics with an authoritative source.	Annex, Section 2.1.2, Level High, Point 1(a)	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - accepted evidence types and the national recognition or authoritative validity criteria applied to them, including photo or biometric identification evidence recognised by the Member State and representing the claimed identity; - verification that the person is in possession of the recognised evidence; - checks determining that the evidence is valid according to an authoritative source; - comparison method between the applicant and the authoritative or document-based reference, including identification of the applicant as the claimed identity through comparison of one or more physical characteristics with an authoritative source; - liveness, anti-spoofing, manual-review and exception rules where applicable; - rejection criteria for expired, unsupported, inconsistent or insufficient evidence.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - source-validation, document-validation or biometric-comparison results with timestamps, including checks that the photo or biometric identification evidence is recognised by the Member State and valid according to an authoritative source; - evidence that the person was verified to be in possession of the recognised evidence; - comparison results showing that the applicant was identified as the claimed identity through comparison of one or more physical characteristics with an authoritative source; - manual-review notes and final decisions for matched, mismatched and poor-quality evidence; - rejected or escalated cases involving invalid evidence or failed comparison; - audit evidence showing that accepted cases met the required assurance level.
REQ-1502-E10-2	Commission Implementing Regulation (EU) 2015/1502	Alternative: Where procedures used previously by a public or private entity in the same Member State for a purpose other than the	Annex, Section 2.1.2, Level High, Point 1(b)	WZ-03-02	In case of rely on other previous identity proofing the assessor reviews the rules used by the assessed PID Provider. The review should confirm: - criteria for determining that the previous procedures provide equivalent assurance to	The assessor tests selected reliance decisions for the assessed PID Provider during the on-site Stage 2 assessment. The sample should demonstrate: - records showing the earlier procedures, their purpose and the entity that performed them;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		issuance of electronic identification means provide equivalent assurance to level high, the entity responsible for registration need not repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body or equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid.			level high; - confirmation of equivalent assurance by a conformity assessment body or equivalent body; - evidence that the previous procedures were used in the same Member State and for another purpose; - steps taken to demonstrate that the results of the earlier procedures remain valid for the current issuance decision; - fallback rules requiring full identity proofing and verification where equivalent assurance or continued validity cannot be demonstrated.	- confirmation by a conformity assessment body or equivalent body that the earlier procedures provide equivalent assurance to level high; - evidence demonstrating that the results of the earlier procedures remain valid; - decisions where reliance was rejected and full identity proofing and verification were performed; - audit trail linking the previous-procedure evidence to the final issuance decision.
REQ-1502-E10-3	Commission Implementing Regulation (EU) 2015/1502	Alternative: Where electronic identification means are issued based on a valid notified electronic identification means having assurance level high, it is not required to repeat the identity proofing and verification processes, considering the risks of a change in the person identification data. Where the electronic identification means serving as the basis has not been notified, assurance level high must be confirmed by a conformity assessment body or equivalent body. Additionally, steps are	Annex, Section 2.1.2, Level High, Point 1(c); 4.4 Electronic Identification Means Management (Section 2.2)	WZ-03-02	The assessor reviews how the assessed PID Provider decides whether previous identity proofing or a prior electronic identification means may be relied upon instead of repeating proofing: - criteria for confirming that the prior electronic identification means was valid at the time of reliance; - separate handling for notified assurance level high means and non-notified means requiring CAB or equivalent-body confirmation; - risk assessment for changes in person identification data since the previous proofing or issuance procedure; - evidence required to demonstrate that the previous procedure remains valid for the current issuance decision; - fallback rules requiring full identity proofing and verification when any reliance condition is not met.	The assessor tests selected reliance decisions for the assessed PID Provider during the on-site Stage 2 assessment: - cases based on a valid notified electronic identification means at assurance level high, where available; - cases based on a non-notified means, including CAB or equivalent-body confirmation of assurance level high; - records showing validity, notification status, assurance level and risk-of-changed-PID-data checks; - decisions where reliance was rejected and the full proofing path was used; - traceability from prior evidence to the final PID or eID means issuance outcome.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.				
REQ-1502-M01	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure that the electronic identification means utilize at least two authentication factors from different authentication factor categories; where the means is used through the wallet, this requirement may be fulfilled by the wallet authentication and control mechanisms.	Annex, Section 2.2.1, Level High, in conjunction with Level Substantial, Element 1	WZ-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the documentation covers: - factor categories used for Wallet Unit, PID key or eID means authentication, including at least two authentication factors from different authentication factor categories; - where the eID means is used through the wallet, evidence that the requirement is fulfilled by wallet authentication and control mechanisms; - 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 PID Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and attestation evidence for enabled factors, including evidence that at least two factors from different authentication factor categories are used; - evidence that wallet authentication and control mechanisms fulfil the requirement where the eID means is used through the wallet; - 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-M02	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure that the electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs; where the means is used through the wallet, this control may be provided by the wallet.	Annex, Section 2.2.1, Level High, in conjunction with Level Substantial, Element 2	WZ-03-02	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - delivery or activation steps linking the user, device, Wallet Unit and activation secret or credential; - checks preventing activation or use by a different person or on an unauthorised device; - design controls showing that the eID means can be assumed to be used only if under the control or possession of the person to whom it belongs, including controls provided by the	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - activation records linking the user, device, Wallet Unit and activation event; - successful and failed activation attempts, including device-change or recovery cases; - logs or protocol traces showing possession or control checks before activation and use where applicable; - evidence that the eID means, 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
					wallet where applicable; - rules for failed activation, lost credentials, device change or support-assisted activation; - evidence retained to prove possession or control at the time of activation and use where applicable.	through wallet controls where applicable, can be assumed to be used only under the control or possession of the person to whom it belongs; - evidence that activation or use was blocked where possession or control could not be confirmed.
REQ-1502-M03	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure that electronic identification means protects against duplication and tampering as well as against attackers with high attack potential; where the means is used through the wallet, these protections may be provided by the wallet security architecture.	Annex, Section 2.2 .1, Level High, Element 1	WZ-03-02	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - 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, including controls protecting the electronic identification means against duplication and tampering; - evidence that these protections are provided by the wallet security architecture where the eID means is used through the wallet.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records; - test or certification evidence for resistance to high attack potential where applicable, including protection against duplication and tampering of the electronic identification means; - evidence that wallet security architecture provides these protections where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
REQ-1502-M04	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall ensure that the electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others; where the means is used through the wallet, this protection may be provided by the wallet user authentication and	Annex, Section 2.2.1, Level High, Element 2	WZ-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the documentation covers: - user authentication and access-control mechanisms protecting the eID means from use by unauthorised persons; - wallet user authentication and access-control mechanisms providing this protection where the eID means is used through the wallet; - controls for enrolment, activation, unlock,	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - configuration and evidence of user authentication and access-control mechanisms protecting the eID means; - wallet user authentication and access-control evidence where the eID means is used through the wallet; - successful and failed access cases showing that only the legitimate holder can use the eID

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		access control mechanisms.			recovery and fallback that prevent use by persons other than the legitimate holder; - negative-case handling for unauthorised access attempts, shared-device scenarios, lost credentials and recovery abuse; - evidence that the protection is reliable for assurance level high.	means; - negative tests for unauthorised use, lost credentials, recovery abuse or attempts by other persons; - evidence that the design provides reliable protection against use by others.
REQ-1502-M05	Commission Implementing Regulation (EU) 2015/1502	The PID Provider shall ensure that the activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.	Annex, Section 2.2.2, Level High	WZ-03-02	The assessor reviews how the assessed PID Provider proves that the eID means or Wallet Unit is activated only under the control of the intended user: - delivery or activation steps linking the user, device, Wallet Unit and activation secret or credential; - checks preventing activation by a different person or on an unauthorised device; - rules for failed activation, lost credentials, device change or support-assisted activation; - evidence retained to prove possession or control at the time of activation.	The assessor tests selected activation cases for the assessed PID Provider during the on-site Stage 2 assessment: - activation records linking the user, device, Wallet Unit and activation event; - successful and failed activation attempts, including device-change or recovery cases; - logs or protocol traces showing possession or control checks before activation; - evidence that activation was blocked where possession or control could not be confirmed.
REQ-1502-M06	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall provide possibility to suspend and/or revoke an electronic identification means in a timely and effective manner.	Annex, Section 2.2.3, All Assurance Levels, Element 1	WZ-03-02	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.
REQ-1502-M07	Commission Implementing Regulation	PID Provider shall implement measures taken to prevent unauthorised suspension,	Annex, Section 2.2.3, All Assurance	WZ-03-02	The assessor reviews lifecycle controls used by the assessed PID Provider for suspension, revocation, reactivation, renewal or replacement:	The assessor tests selected lifecycle-status cases for the assessed PID Provider during the on-site Stage 2 assessment: - suspension, revocation, reactivation, renewal

Requirement 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	revocation and/or reactivation of PID.	Levels, Element 2		- 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.	- or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-1502-M08	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall reactivate the PID only if the same assurance requirements as established before the suspension or revocation continue to be met.	Annex, Section 2.2.3, All Assurance Levels, Element 3	WZ-03-02	The assessor reviews PID reactivation rules maintained by the assessed PID Provider: - conditions allowing suspended PID to be reactivated; - assurance requirements that must remain satisfied before reactivation; - authorisation and evidence required for reactivation; - controls preventing reactivation after revocation or where assurance has degraded.	The assessor tests selected PID reactivation cases for the assessed PID Provider during the on-site Stage 2 assessment: - reactivation records and assurance evidence; - checks performed before restoring valid status; - rejected reactivation cases where assurance conditions were not met; - status-service evidence after reactivation or rejection.
REQ-1502-M09	Commission Implementing Regulation (EU) 2015/1502	PID Provider shall renew or replace the PID only if it meets the same assurance requirements as initial identity proofing or is based on a valid electronic identification means of the high assurance level.	Annex, Section 2.2.4, All Assurance Levels	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path, including renewal or replacement of PID only where the same assurance requirements as initial identity proofing are met or where renewal or replacement is based on a valid electronic identification means of 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	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - evidence that renewal or replacement met the same assurance requirements as initial identity proofing or was based on a valid electronic identification means of assurance level high;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					final proofing and issuance decision, including renewal or replacement decisions.	- records showing how exceptions were escalated, corrected or rejected.
REQ-1502-M10	Commission Implementing Regulation (EU) 2015/1502	Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.	Annex, Section 2.2.4, Level High	WZ-03-02	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - 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, including verification of identity data with an authoritative source where renewal or replacement is based on a valid electronic identification means.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - for renewal or replacement based on a valid electronic identification means, evidence that identity data was verified with an authoritative source; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-1502-O01	Commission Implementing Regulation (EU) 2015/1502	Access to sensitive cryptographic material 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-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. 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 used for issuing electronic identification means and authentication to roles and applications strictly requiring access; - controls ensuring that such sensitive cryptographic material is never persistently	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - key-management records for generation, activation, use, rotation or destruction; - configuration or attestation evidence for protected key storage and cryptographic modules, including evidence that sensitive cryptographic material is never persistently stored in plain text; - access logs and approvals for sensitive key-management actions, including evidence that access is restricted to roles and applications strictly requiring access; - negative or exception cases such as expired certificates, failed rotations or rejected keys.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					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.	
REQ-1502-002	Commission Implementing Regulation (EU) 2015/1502	Sensitive cryptographic material used for issuing electronic identification means and authentication shall be protected from tampering.	Annex, 2.4.6, Level Substantial	WZ-03-02	The assessor reviews the authentication design and related user-protection procedures maintained by the assessed PID Provider. The review should establish whether the documentation covers: - key types, algorithms, trusted components and protected environments used for the assessed function, including protection of sensitive cryptographic material used for issuing electronic identification means and authentication from tampering; - key generation, storage, access, backup, rotation, revocation and destruction rules; - use of WSCD, Wallet Unit Attestation or other cryptographic assurance evidence where relevant; - segregation of duties and logging for sensitive key-management operations.	The assessor tests selected authentication cases and related security events for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - key-management records for generation, activation, use, rotation or destruction; - configuration or attestation evidence for protected key storage and cryptographic modules, including tamper-protection evidence for sensitive cryptographic material; - access logs and approvals for sensitive key-management actions; - negative or exception cases such as expired certificates, failed rotations or rejected keys.
REQ-2977-01	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall issue the PID to Wallet Unit in accordance with the electronic identification schemes under which wallet solutions are provided.	Article 3(1)	WZ-03-02	The assessor reviews PID issuance eligibility rules applied by the assessed PID Provider under the relevant eID scheme: - scheme rules determining which Wallet Units and wallet solutions may receive PID; - public list or trusted source of supported wallet solutions; - checks performed before issuing PID to a Wallet Unit; - evidence linking the issuance decision to the accepted scheme and wallet solution.	The assessor tests selected PID issuance eligibility cases for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID cases linked to the relevant eID scheme; - Wallet Unit and wallet solution validation evidence; - public or trusted list evidence showing support by the Member State; - rejected cases where the Wallet Unit or wallet solution was not supported.
REQ-2977-02	Commission Implementing Regulation	PID Provider shall ensure that the PID issued to Wallet Unit contains the	Article 3(2)	WZ-03-02	The assessor reviews how the assessed PID Provider controls PID content, format and validation metadata before issuance:	The assessor examines selected PID payloads or issuance records for the assessed PID Provider during the on-site Stage 2

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
	(EU) 2024/2977	information necessary for authentication and validation of the PID.			- mandatory and optional PID data elements for each supported format; - schema, signature, validity-status and validation information required by the applicable technical specification; - quality checks preventing incomplete, inconsistent or unsupported PID payloads from being issued; - versioning and change control for PID formats and data mappings.	assessment: - issued PID samples or test vectors covering each supported format; - schema validation, signature validation and required metadata checks; - cases rejected because required elements or validation information were missing; - traceability between the configured format, the issuance request and the issued PID.
REQ-2977-03	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that the PID issued to Wallet Unit complies with the technical specifications set out in the CIR (EU) 2024/2977 Annex TECHNICAL SPECIFICATIONS FOR PERSON IDENTIFICATION DATA REFERRED TO IN ARTICLE 3(3).	Article 3(3)	WZ-03-02	The assessor reviews how the assessed PID Provider validates PID technical-specification compliance before issuance: - applicable CIR 2024/2977 Annex data model, format and validation requirements; - schema, signature, metadata and status-information checks; - versioning of PID formats and mappings; - rejection rules for non-compliant PID payloads.	The assessor checks selected PID samples for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID payloads or test vectors validated against the Annex specification; - schema and signature validation results; - format-version and metadata evidence; - rejected or corrected cases involving non-compliant PID payloads.
REQ-2977-04	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that the PID issued to a given Wallet User is unique for the Member State.	Article 3(4)	WZ-03-02	The assessor reviews the documented arrangements maintained by the assessed PID Provider. The review should identify: - unique identifiers, matching rules and authoritative datasets used to detect duplicates or collisions, including checks that the PID issued to a given Wallet User is unique for the Member State; - handling of identity merges, corrections, duplicate candidates and ambiguous matches; - controls preventing PID issuance before uniqueness checks are complete; - records retained to justify the final uniqueness decision, including the Member State uniqueness scope.	The assessor checks implementation of the documented arrangements for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - issued PID records compared with duplicate-check or matching results, including evidence that the PID issued to a given Wallet User is unique for the Member State; - blocked, corrected or escalated duplicate candidates; - source-system evidence showing the person represented by the issued PID; - audit trail linking uniqueness checks to the final issuance decision.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
REQ-2977-05	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that PID issued to wallet units is cryptographically bound to the wallet unit to which it is issued.	Article 3(5)	WZ-03-02	The assessor reviews the cryptographic binding design used by the assessed PID Provider for PID or eID means material: - how the intended Wallet Unit is identified and validated before binding; - how the PID public key, proof of possession and proof of association are checked before PID is issued; - how the issued PID is linked to the validated Wallet Unit and to the accepted PID public key; - controls preventing issuance to a substituted Wallet Unit, wrong public key or unverified binding request; - evidence retained for failed, repeated or exceptional binding attempts.	The assessor traces selected cryptographic binding cases for the assessed PID Provider during the on-site Stage 2 assessment: - the approved issuance decision, Wallet Unit identifier, attestation result, PID public key and binding evidence; - proof-of-possession and proof-of-association validation logs; - technical issuance records showing the PID bound to the intended Wallet Unit and public key; - rejected cases involving missing proofs, wrong keys, invalid attestations or replayed binding material.
REQ-2977-06	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that person identification data is issued only to wallet units belonging to wallet solutions supported by providers of person identification data under the relevant Member State's electronic identification scheme, as identified in the list of supported wallet solutions made publicly available by that Member State.	Article 3(6)	WZ-03-02	The assessor reviews PID issuance eligibility rules applied by the assessed PID Provider under the relevant eID scheme: - scheme rules determining which Wallet Units and wallet solutions may receive PID; - public list or trusted source of supported wallet solutions; - checks performed before issuing PID to a Wallet Unit; - evidence linking the issuance decision to the accepted scheme and wallet solution.	The assessor tests selected PID issuance eligibility cases for the assessed PID Provider during the on-site Stage 2 assessment: - issued PID cases linked to the relevant eID scheme; - Wallet Unit and wallet solution validation evidence; - public or trusted list evidence showing support by the Member State; - rejected cases where the Wallet Unit or wallet solution was not supported.
REQ-2977-07	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall perform identity verification of the wallet user in accordance with the requirements related to identity proofing and verification before issuing the PID to the Wallet Unit.	Article 3(7)	WZ-03-02	The assessor reviews the proofing, onboarding and verification arrangements used by the assessed PID Provider: - the accepted proofing paths and the conditions for using each path; - evidence sources, verification checks and manual-review steps supporting assurance level high;	The assessor tests selected proofing, onboarding and issuance cases for the assessed PID Provider during the on-site Stage 2 assessment: - normal, rejected and manually reviewed applications; - source checks, operator decisions, timestamps and final assurance-level

Requirement 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 of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	decisions; - evidence that issuance or activation occurred only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
REQ-2977-08	Commission Implementing Regulation (EU) 2024/2977	When issuing PIDs to wallet units, PID Provider shall identify them to Wallet Units using their wallet-relying party access certificate or another authentication mechanism in accordance with an electronic identity scheme notified at assurance level high.	Article 3(8)	WZ-03-02	The assessor reviews how the assessed PID Provider authenticates itself to Wallet Units before PID issuance or related exchanges: - certificate profiles or alternative assurance level high authentication mechanisms used for provider identification; - certificate lifecycle controls, trust anchors and revocation checks; - protocol steps that prevent Wallet Units from accepting unauthenticated provider requests; - evidence retained for successful and failed provider-authentication events.	The assessor checks provider-authentication evidence for the assessed PID Provider during the on-site Stage 2 assessment: - live or retained protocol traces showing use of the wallet-relying party access certificate or approved alternative mechanism; - certificate validity, chain-building and revocation-check results; - logs for rejected exchanges involving invalid, expired or untrusted credentials; - configuration showing that weaker or unapproved authentication paths are not enabled.
REQ-2977-09	Commission Implementing Regulation (EU) 2024/2977	Before issuing PID, PID Provider shall authenticate and validate the wallet unit attestation and verify that the wallet unit belongs to a wallet solution the provider accepts.	Article 3(9)	WZ-03-02	The assessor reviews how the assessed PID Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including authentication and validation of the wallet unit attestation before issuing PID; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - checks verifying that the Wallet Unit belongs to a wallet solution accepted by the PID Provider before PID issuance; - rules excluding personal data from	The assessor checks selected Wallet Unit attestation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including cases where the attestation was authenticated and validated before PID issuance; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - evidence that the Wallet Unit belonged to a wallet solution accepted by the PID Provider before PID was issued; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					attestations where the requirement prohibits such data.	
REQ-2977-10	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall have written and publicly accessible policies relating to validity status management, including the conditions under which PID can be revoked without delay.	Article 5(1)	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - written and publicly accessible policies relating to validity status management; - authorised triggers, decision roles and evidence required for each lifecycle action, including conditions under which PID can be revoked without delay; - 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 revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - written and publicly accessible validity-status-management policies, including conditions for revocation without delay; - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were not met.
REQ-2977-11	Commission Implementing Regulation (EU) 2024/2977	Only PID Provider or electronic attestations of attributes can revoke the PID, or attestations issued by them.	Article 5(2)	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - authorised triggers, decision roles and evidence required for each lifecycle action, including controls ensuring that only the PID Provider or providers of electronic attestations of attributes can revoke the PID or attestations issued by them; - timeliness requirements and technical propagation of status changes; - controls preventing unauthorised suspension, revocation, reactivation or renewal; - assurance checks required before	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes, including evidence that revocation was performed only by the PID Provider or by the provider of the relevant electronic attestation of attributes; - technical status publication or propagation logs; - cases rejected because the required assurance or authorisation conditions were

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					reactivation, renewal or replacement is allowed.	not met, including unauthorised revocation attempts.
REQ-2977-12	Commission Implementing Regulation (EU) 2024/2977	Where PID Provider has revoked the PID, it shall inform Wallet Users within 24 hours of the revocation and of the reasons, in a concise, easily accessible manner using clear and plain language, through dedicated and secure channels.	Article 5(3)	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - triggering events and deadlines for user notification, including the 24-hour deadline where applicable; - dedicated secure channels and message templates used for notification; - required content of the notification, including reason, status and available remedies where applicable, presented in a concise, easily accessible manner using clear and plain language; - records proving delivery, failure handling and escalation.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - timestamps from revocation decision to user notification; - message content and channel evidence for notified users, including the revocation reason and evidence that the message was concise, easily accessible and written in clear and plain language through dedicated secure channels; - failed delivery or escalation records; - cases confirming that users were not left without notice after a status change.
REQ-2977-13	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall revoke PID: (a) upon the explicit request of the wallet user; (b) where the wallet unit attestation has been revoked; (c) in other situations determined by the providers in their policies.	Article 5(4)	WZ-03-02	The assessor reviews policy and revocation procedures. The documentation should identify: - mandatory PID revocation upon explicit request of the Wallet User; - mandatory PID revocation where the wallet unit attestation has been revoked; - other PID revocation situations determined in the PID Provider's policies; - decision roles, evidence required and timelines for each revocation trigger; - links between wallet unit attestation status, PID validity status and user notification; - controls preventing continued PID validity when a mandatory revocation trigger has occurred.	The assessor checks selected Wallet Unit attestation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - Wallet User explicit revocation requests and the resulting PID revocation records; - cases where wallet unit attestation was revoked and the corresponding PID revocation was performed; - cases triggered by other situations determined in the PID Provider's policies; - timestamps, decision evidence and validity-status publication for each sampled revocation; - exceptions or failures showing escalation and correction where mandatory revocation did not occur as expected.

Requirement 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-2977-14	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that revocations cannot be reverted.	Article 5(5)	WZ-03-02	The assessor reviews the policy and technical documentation. The documented controls should define: - validity-status rules making revocation final and irreversible; - technical controls preventing restoration of revoked PID to valid, suspended or active status; - administrative controls preventing operators or systems from reverting revocation decisions; - audit logging, approval and exception handling for attempted changes to revoked status; - fallback rules requiring new issuance or another permitted lifecycle process instead of reverting a revocation; - technical and procedural controls preventing reversal of completed revocations.	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID samples showing final, non-reversible status; - configuration or workflow evidence preventing revoked PID from being restored to valid, suspended or active status; - negative tests or access-control evidence showing that operators and systems cannot revert revocation; - logs of attempted or exceptional changes to revoked status and their rejection or escalation; - evidence that any post-revocation lifecycle action follows a new permitted process rather than reverting revocation; - technical and procedural controls preventing reversal of completed revocations.
REQ-2977-14	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall ensure that revoked PID shall remain accessible for as long as required by Union law or national law.	Article 5(6)	WZ-03-02	The assessor reviews retention and accessibility rules for revoked PID maintained by the assessed PID Provider: - legal or national retention basis for keeping revoked PID accessible; - access, integrity and privacy controls for revoked PID records; - status-service or archive rules after revocation; - secure deletion or archival steps after retention expiry.	The assessor checks selected revoked PID records for the assessed PID Provider during the on-site Stage 2 assessment: - revoked PID samples and retention basis; - status-service or archive evidence showing continued accessibility where required; - access-control and integrity evidence for retained revoked PID; - expiry or deletion cases confirming retention rules were followed.
REQ-2977-15	Commission Implementing Regulation (EU) 2024/2977	Where PID Provider revoke PID issued to Wallet Units, they shall make publicly available the validity status of PID they issue, in a privacy preserving manner, and	Article 5(7)	WZ-03-02	The assessor reviews privacy-preserving validity-status publication controls maintained by the assessed PID Provider: - location and format of PID or Wallet Unit Attestation status information; - privacy controls preventing status checks from becoming tracking or correlation	The assessor checks selected validity-status publication cases for the assessed PID Provider during the on-site Stage 2 assessment: - issued and revoked PID or attestation samples with status-location references; - status-service responses for valid, suspended, revoked or unknown items;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		indicate the location of that information in the PID			mechanisms; - how the status-location reference is included in the PID or attestation where required; - availability, integrity and update rules for the status service.	- privacy tests or configuration evidence limiting correlation and enumeration; - logs and monitoring evidence for status-service updates and availability.
REQ-2977-16	Commission Implementing Regulation (EU) 2024/2977	PID Provider shall enable privacy preserving techniques which ensure unlinkability where the electronic attestations of attributes do not require the identification of the user.		WZ-03-02	The assessor reviews policy and technical documentation. The documented controls should define: - data flows, stores and interfaces separating wallet or PID data from other provider services; - purpose limitation, minimisation and non-combination controls; - technical controls preventing tracking, linkability or unauthorised observation of user activity, including privacy-preserving techniques ensuring unlinkability where electronic attestations of attributes do not require identification of the user; - governance for exceptions, access to personal data and retention of privacy-related evidence.	The assessor tests selected PID issuance samples and design documentation during the on-site Stage 2 assessment. The sample should show: - architecture diagrams, database or tenant separation evidence and access-control configuration; - sampled logs or data-flow evidence showing that cross-service combination or tracking is not occurring; - privacy-relevant configuration for dashboards, transaction logs, analytics and relying-party interactions, including unlinkability techniques for electronic attestations of attributes that do not require user identification; - exceptions or support cases to confirm that access to personal data is controlled and recorded.
REQ-2981-P01	Commission Implementing Regulation (EU) 2024/2981	As part of the electronic identification scheme, PID Provider shall identify threats and risk related to its role in issuing PID and ensure that appropriate risk mitigation measures are included in the scheme's risk assessment and risk management measures.	Article 4(4)(d), Article 4(5)	WZ-03-02	The assessor reviews the risk-management arrangements maintained by the assessed PID Provider. The review should link the requirement to: - threats and risks identified for the PID Provider's role in issuing PID; - risk scenarios covering proofing, Wallet Unit validation, PID issuance, binding, validity status and revocation where relevant; - appropriate risk mitigation measures defined for identified PID issuance risks; - evidence that those mitigation measures are included in the scheme's risk assessment and risk management measures;	The assessor checks selected risk records, decisions and management-review outputs for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - risk-treatment records and mitigation measures for sampled PID issuance risks; - evidence that mitigation measures are reflected in the electronic identification scheme's risk assessment and risk management measures; - links between operational controls and selected risk treatments;

Requirement 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-P02	Commission Implementing Regulation (EU) 2024/2981	PID Provider shall follow policies defined on national level and implement procedures concerning the management of risks associated with PID issuance, including identification, assessment and mitigation of risks.	Article 8(3)(b)	WZ-03-02	The assessor reviews the documented risk management framework for PID issuance. The review should establish whether the documentation covers: - applicable national policies governing PID issuance risk management; - documented procedures for the identification, assessment, treatment and review of PID issuance risks; - risk assessments covering the PID issuance lifecycle; - defined risk treatment measures and residual risk acceptance.	The assessor verifies the implementation of the PID issuance risk management process during the on-site assessment. The evidence should include: - records demonstrating that PID issuance risks are periodically assessed and reviewed; - evidence that identified risk treatment measures have been implemented; - samples demonstrating that operational controls reflect the identified risks;
REQ-2981-P03	Commission Implementing Regulation (EU) 2024/2981	PID Provider shall establish and implement policies defined on national level for the management of changes and vulnerabilities in the PID issuance infrastructure in accordance with Article 5.	Article 8(3)(c)	WZ-03-02	The assessor reviews vulnerability management arrangements maintained by the assessed PID Provider. The review should identify: - national-level policies applicable to management of changes and vulnerabilities in PID issuance infrastructure; - procedures for identifying, assessing, approving, testing and implementing changes affecting PID issuance infrastructure; - procedures for vulnerability identification, assessment, prioritisation, remediation, verification and reporting; - links with risk assessment, incident handling, configuration management and certification-maintenance obligations under Article 5; - planned and event-driven review and update of change and vulnerability management policies and procedures.	The assessor checks selected vulnerability reports, triage decisions and remediation records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - sampled infrastructure changes showing risk assessment, approval, testing, implementation and closure; - vulnerability records showing identification, assessment, prioritisation, remediation and verification; - records of review and update after significant incidents, significant changes or vulnerability findings.
REQ-2981-P04	Commission Implementing Regulation (EU) 2024/2981	PID Provider shall establish and implement human resource management policies established on national level for personnel	Article 8(3)(d)	WZ-03-02	The assessor reviews personnel, competence, training and employment-control arrangements maintained by the assessed PID Provider. The documentation should define: - roles involved in PID issuance operations and required responsibilities, competence,	The assessor checks selected personnel, contractor or training records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - HR policies and the PID Provider's implementing 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
		involved in PID issuance operations.			reliability, experience, training and qualifications; - screening, onboarding, training, awareness and role-assignment rules applicable to PID issuance personnel; - segregation of duties, trusted-role controls and supervision for PID issuance operations; - records demonstrating implementation of the national-level HR policies by the PID Provider; - review and update of HR controls where roles, risks, incidents or national-level policies change.	- samples of personnel involved in PID issuance operations showing role assignment, competence, training, qualifications and reliability evidence; - screening, onboarding, awareness and trusted-role records where applicable; - segregation-of-duties and supervision evidence for PID issuance operations; - exceptions, role changes or incident-related HR actions and their closure.
REQ-2981-P05	Commission Implementing Regulation (EU) 2024/2981	PID Provider shall notify the CAB without undue delay of any breach or compromise of the PID issuance infrastructure that is likely to impact its conformity with the requirements of the national certification scheme.	Article 5(2)	WZ-03-02	The assessor reviews incident handling, breach assessment and notification procedures maintained by the assessed PID Provider. The documented arrangements should define: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies, including any breach or compromise of the PID issuance infrastructure likely to impact conformity with the requirements of the national certification scheme; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data, including impact on conformity with the national certification scheme; - timelines, roles and approval path for notification without undue delay; - evidence retained for the decision to notify or not notify.	The assessor reviews selected incidents, exercises or breach-assessment records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - incident or breach records from detection through classification and notification decision, including breaches or compromises of the PID issuance infrastructure; - notifications sent and timestamps showing timeliness; - evidence supporting impact on conformity, personal data or service integrity, including likely impact on conformity with the requirements of the national certification scheme; - cases where notification was not sent and the documented rationale.
REQ-2981-P06	Commission Implementing Regulation (EU) 2024/2981	PID Provider shall store securely, for at least five years after the cancellation or expiry of the relevant certificate of conformity, records of the information provided to	Article 19(2)	WZ-03-02	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records of the	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including information provided to

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the CAB during the certification process.			information provided to the CAB during the certification process; - retention period, including periods after certificate cancellation or expiry where applicable, and at least five years after cancellation or expiry of the relevant certificate of conformity; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities.	the CAB during the certification process; - 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-2690-P01	Commission Implementing Regulation (EU) 2024/2690	PID Provider shall establish, implement and apply a policy and procedures related to cryptography applicable specifically to the PID issuance infrastructure, including management of PID signing keys.	Annex, 9.1 -9.3	WZ-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed PID Provider. The review should establish: - cryptographic controls applicable to PID issuance infrastructure and PID issuance operations; - management of PID signing keys, including generation, storage, access, activation, use, backup, rotation, revocation and destruction; - approved algorithms, key lengths, cryptographic modules and protected environments used for PID signing; - segregation of duties, logging, auditing and approval rules for PID signing-key operations; - review and update of the cryptography policy and procedures where risks, technology or applicable requirements change.	The assessor checks selected cryptographic-control and key-management evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - PID signing-key lifecycle records covering generation, activation, use, backup, rotation, revocation or destruction; - configuration or attestation evidence for cryptographic modules, algorithms and protected key storage; - audit records for PID signing-key operations;
REQ-2690-P02	Commission Implementing Regulation (EU) 2024/2690	PID Provider shall maintain policies for the management of privileged accounts and system administration accounts for PID issuance systems, including dual control for operations on PID signing key material.	Annex, 11.3.1 - 11.4.2	WZ-03-02	The assessor reviews identity, privileged-access and access-rights management procedures maintained by the assessed PID Provider. The documentation should describe: - management of privileged accounts and system administration accounts used for PID issuance systems; - strong identification, authentication and authorisation for privileged and	The assessor checks selected identity, privileged-access and access-rights records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - samples of privileged and administration accounts showing strong authentication, authorisation, individualisation and restricted privileges;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
					administration accounts; - individualised, restricted and purpose-specific administration accounts; - controls ensuring that administration accounts are used only for authorised administration operations; - dual control for operations on PID signing key material, requiring at least two authorised persons to act together; - documented roles, procedures, approvals and logs for privileged operations and dual-control activities.	- configuration showing that administration accounts are used only for authorised administration operations; - dual-control records for operations on PID signing key material;
REQ-2690-P03	Commission Implementing Regulation (EU) 2024/2690	PID Provider shall establish, implement and apply a policy and procedures for security testing of the PID issuance infrastructure, based on risk assessment.	Annex, 6.5.1-6.5.3	WZ-03-02	The assessor reviews secure acquisition, development, maintenance or testing procedures maintained by the assessed PID Provider. The documentation should show: - risk assessment used to determine the need, scope, frequency and type of security tests; - security-testing coverage of systems, interfaces, components and processes supporting PID issuance; - penetration tests, vulnerability tests, configuration tests and other security tests where applicable; - documentation of test results, critical findings, mitigation actions and retesting; - regular review and update of security-testing policy and procedures based on risk, incidents, changes or findings.	The assessor checks selected development, acquisition, maintenance or security-testing records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - approved security-testing policy and procedures; - risk assessment records defining test scope, frequency and type; - security-test and penetration-test reports for PID issuance infrastructure; - documented findings, mitigation measures, retest evidence and closure approvals; - records showing review and update of testing procedures after risks, incidents, changes or findings.
PP-02	REQ-5c-04; REQ-910-05	Personal data relating to the provision of person identification data shall be kept logically separate from any other data held by PID Provider. The PID issuance service shall be architecturally and operationally separated	Alignmet with international standards - ISO/IEC 27001:2022 A.5.31 (legal requirements); A.5.12 (classification of	WZ-03-02	The assessor reviews privacy, data-separation and data-handling controls maintained by the assessed PID Provider. The documentation should show: - logical separation of personal data relating to provision of person identification data from any other data held by the PID Provider; - architectural and operational separation of the PID issuance service from the PID	The assessor checks evidence that the implemented technical and organisational measures effectively enforce the logical and operational separation of PID processing from other services. The evidence should include: - sampled logs or data-flow evidence showing that cross-service combination or unauthorised access is not occurring;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		from PID Provider's other services, including its Wallet Provider functions. PID Provider shall document the technical and organisational measures implementing this separation and make the documentation available to the CAB.	information). ETSI EN 319 401 §7.1 (Policy); EN 319 411-2 §7.3 (Initial identity validation for qualified certificates). Additional standards and references - GDPR Article 25(1) (data protection by design - technical measures to implement the principle of data minimisation, including logical separation of PID data from other processing activities); ARF v2.8.0 §6 (privacy-by-design requirements for PID Providers). 5.1.3 PID-Specific Risk Assessment		Provider's other services, including Wallet Provider functions; - technical and organisational measures implementing separation, including data stores, interfaces, access controls, tenant boundaries, logging and operational procedures; - controls preventing unauthorised data combination, cross-use, tracking or access between separated functions; - documentation of separation measures and availability of that documentation to the CAB.	
PP-03	REQ-2981-P01; REQ-5c-02	PID Provider shall conduct a PID-specific risk assessment as part of the implementation-specific risk assessment	Alignment with international standards - ISO/IEC 27001:2022	WZ-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - risks arising from reliance on the PESEL	Not 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
		required by EP-14 of WZ-03-01. The PID-specific risk assessment shall address, at a minimum: (a) risks arising from the reliance on the PESEL register and RDO as authoritative sources; (b) risks associated with remote identity proofing processes; (c) risks of PID being issued to or used by an unauthorised person; (d) risks of compromise of PID signing key material; (e) risks arising from the cryptographic binding between PID and wallet units.	A.5.31 (legal requirements); cl. 4.3 (scope of ISMS). ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).		register and RDO as authoritative sources; - risks associated with remote identity proofing processes; - risks of PID being issued to or used by an unauthorised person; - risks of compromise of PID signing key material; - risks arising from cryptographic binding between PID and Wallet Units; - risk treatment decisions, mitigation measures, owners, deadlines and residual-risk acceptance.	
PP-04	REQ-2977-06; REQ-1502-E03	PID Provider shall designate and document the authoritative sources used for identity proofing and verification of person identification data. For natural persons in Poland, the authoritative sources designated in the Trust Framework established by the Ministerstwo Cyfryzacji shall be used. PID Provider shall verify that the authoritative sources provide current, accurate and reliable identity data, and shall have procedures for detecting and responding	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.31 (legal requirements). ETSI EN 319 401 §7.4 -§67.8 (Cryptography); EN 319 411 -2 §6.5.1 (Key pair generation for qualified services); §6.5.2 (Private key protection for	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - which authoritative sources are accepted for each evidence type, including documented designation of authoritative sources used for identity proofing and verification of person identification data; - for natural persons in Poland, use of authoritative sources designated in the Trust Framework established by the Ministerstwo Cyfryzacji; - verification that authoritative sources provide current, accurate and reliable identity data; - timing rules proving that evidence validity is checked at the time of proofing, renewal or	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - source responses or validation tokens showing evidence status at the relevant time, including responses from authoritative sources designated for natural persons in Poland where applicable; - documentation designating authoritative sources used for identity proofing and verification; - application records where source checks were successful, failed or manually reviewed; - timestamps linking the source check to the proofing or issuance decision; - evidence that source currentness, accuracy and reliability are assessed; - evidence that expired, unverified 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
		to failures or unavailability of those sources.	qualified services). Additional standards and references - ETSI TS 119 461 v2.1.1 §7 (identity proofing requirements for trust service subjects at assurance level High, including evidence collection, verification and liveness detection); ARF v2.8.0 §3.4 (PID Provider identity verification requirements).		reliance; - handling of source unavailability, inconsistent results and expired evidence, including procedures for detecting and responding to failures or unavailability of authoritative sources; - records retained to support the final proofing or issuance decision.	inconsistent evidence was not accepted without justified escalation, including failure or unavailability handling records.
PP-05	REQ-2981-P05	PID Provider shall notify the Ministerstwo Cyfryzacji and the CAB without undue delay of any breach or compromise of the PID issuance infrastructure, including any compromise or suspected compromise of PID signing keys, that is likely to impact the conformity of the eID system with the requirements of GP-03.	Alignment with international standards - ISO/IEC 27001:2022 A.5.31 (legal requirements); A.5.36 (compliance). ETSI EN 319 401 §7.4 -§67.8 (Compliance); EN 319 411-2 §6.9.1	WZ-03-02	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - events that trigger notification to the CAB, certification body, supervisory body, users or other relevant bodies, including notification to the Ministerstwo Cyfryzacji and the CAB of any breach or compromise of the PID issuance infrastructure without undue delay; - impact criteria for wallet solution, eID scheme, PID issuance infrastructure or personal data, including likely impact on conformity of the eID system with GP-03;	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - incident or breach records from detection through classification and notification decision, including breaches or compromises of PID issuance infrastructure and PID signing-key compromise or suspected compromise; - notifications sent and timestamps showing timeliness, including notifications to the Ministerstwo Cyfryzacji and the CAB without undue delay; - evidence supporting impact on conformity,

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		PID Provider shall notify the CAB where any private key used to sign the PID is or is suspected to have been compromised	(Organisational requirements for QTSPs); §6.8.15 (Compliance with applicable law). Additional standards and references - GDPR Article 33 (notification of personal data breach to supervisory authority within 72 hours); GDPR Article 34 (communication of breach to data subjects without undue delay); CRA Annex I Part II §5(1) (coordinated vulnerability disclosure obligations).		- compromise or suspected compromise of PID signing keys, including any private key used to sign PID, as a CAB notification trigger; - timelines, roles and approval path for notification without undue delay; - evidence retained for the decision to notify or not notify.	personal data or service integrity, including likely impact on conformity of the eID system with GP-03; - CAB notifications where any private key used to sign PID is or is suspected to have been compromised; - cases where notification was not sent and the documented rationale.
PP-06	REQ-2690-P01; REQ-2690-P02; REQ-1502-001; REQ-1502-002	PID Provider shall establish and implement a key management policy and procedures specific to the PID signing keys used to cryptographically sign person identification data issued to wallet units. The policy shall govern the full lifecycle of PID signing keys, including generation, certification,	Alignment with international standards - ISO/IEC 27001:2022 A.5.1 (IS policies); A.5.2 (IS roles); A.5.15 (access control); cl. 5.1 (leadership). ETSI EN 319 401	WZ-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed PID Provider. The review should establish: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - key management policy and procedures specific to PID signing keys used to cryptographically sign person identification data issued to Wallet Units; - WSCD/WSCA use and evidence of protected	The assessor checks selected cryptographic-control and key-management evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records, including PID signing-key certification, storage, activation and backup records; - dual-control evidence for PID signing-key

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		storage, activation, use, backup, rotation and destruction. The policy shall be subject to the dual control requirements specified in EP-54 and EP-66 of WZ-03- 01. PID Provider shall retain overall responsibility and effective control over the PID signing keys and shall ensure, through documented arrangements and auditable controls, that any organisational entity or third-party provider involved in key management or cryptographic operations applies the same security requirements as those applicable to the PID Provider. NOTE - PID signing keys are private signing keys of the PID Provider within the meaning of CIR (EU) 2024/2981, Article 2(11). Their protection therefore requires the highest level of physical and logical security controls, including HSM-based protection as specified in EP-66 of WZ-03- 01.	§7.1 (Organisational security policy); EN 319 411-1 §6.9.1 (Organisational); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs). Additional standards and references - ARF v2.8.0 §6.2 (cryptographic requirements for PID signing keys); CIR (EU) 2025/849 (updated cryptographic standards for PID format signing); ISO/IEC 18013-5:2021 §9 (mDL issuer authentication mechanisms).		key generation, storage and operation, including full lifecycle controls for PID signing keys covering generation, certification, storage, activation, use, backup, rotation and destruction; - dual control requirements for PID signing-key operations as specified for privileged operations and sensitive cryptographic material; - documented arrangements and auditable controls ensuring that any organisational entity or third-party provider involved in key management or cryptographic operations applies the same security requirements as the PID Provider; - overall responsibility and effective control retained by the PID Provider over PID signing keys.	operations; - documented arrangements and auditable controls for any organisational entity or third-party provider involved in key management or cryptographic operations; - evidence that the PID Provider retains overall responsibility and effective control over PID signing keys; - 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
PP-07	REQ-1502-001; REQ-1502-002; REQ-2690-P02	Key management operations on PID signing keys, including key generation, activation, backup, recovery and destruction, shall be subject to dual control, requiring at least two authorised persons to act together. PID Provider shall maintain records of all such operations.	Alignment with international standards - ISO/IEC 27001:2022 A.5.1 (IS policies); cl. 7.1 (resources); cl. 5.1 (leadership). ETSI EN 319 401 §7.1 (Security policy); EN 319 411-1 §6.9.1 (Organisational).	WZ-03-02	The assessor reviews cryptographic-control and key-management documentation maintained by the assessed PID Provider. The review should establish: - approved algorithms, key lengths and cryptographic profiles for the assessed protocols and components; - WSCD/WSCA use and evidence of protected key generation, storage and operation; - dual control for key management operations on PID signing keys, including key generation, activation, backup, recovery and destruction, requiring at least two authorised persons to act together; - records maintained for all such PID signing-key operations; - 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 PID Provider during the on-site Stage 2 assessment. The evidence should include: - configuration or attestation evidence for algorithms, key lengths, WSCD and WSCA components; - key-generation, use, rotation, revocation or destruction records, including activation, backup and recovery records for PID signing keys; - dual-control evidence showing that at least two authorised persons acted together for sampled PID signing-key operations; - records of all such PID signing-key management operations; - test or certification evidence for resistance to high attack potential where applicable; - migration or exception records for deprecated algorithms or non-standard cryptographic configurations.
PP-08	REQ-2977-09; REQ-2977-15	PID Provider shall establish and operate a publicly available validity status service for person identification data issued to wallet units. The service shall enable relying parties and wallet units to verify the revocation status of issued PID in a privacy-preserving manner. The location of the validity status information shall be indicated in the PID itself.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.8.15 (logging); cl. 8.1 (operational planning). ETSI EN 319 401 §7.4-§67.8 (Cryptography and logging); EN 319 411 -2 §6.3.10	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - authorised triggers, decision roles and evidence required for each lifecycle action; - timeliness requirements and technical propagation of status changes; - publicly available validity status service for person identification data issued to Wallet Units; - privacy-preserving verification of PID revocation status by relying parties and Wallet Units; - controls ensuring that the location of validity status information is indicated in the PID itself; - controls preventing unauthorised	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes; - technical status publication or propagation logs, including evidence of a publicly available validity status service for PID issued to Wallet Units; - issued PID samples showing the location of validity status information; - privacy-preserving status-verification evidence for relying parties and Wallet Units;

Requirement 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 status services for qualified certificates). Additional standards and references - ARF v2.8.0 §6.5 (privacy - preserving validity status mechanisms; unlikability requirements for status tokens); GDPR Article 25(2) (privacy by default for validity status queries - only data necessary for the status check shall be processed).		suspension, revocation, reactivation or renewal.	- cases rejected because the required assurance or authorisation conditions were not met.
PP-09	REQ-2977-09; REQ-2977-12	PID Provider shall establish written and publicly accessible policies relating to PID validity status management, including: (a) the conditions under which PID may be revoked without delay; (b) procedures for processing revocation requests; (c) timeframes for revocation processing; (d) measures to prevent	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.36 A.5.31. ETSI EN 319 401 §7.4 -§67.8 (Cryptography); EN 319 411 -2 §6.5.1 (Key pair generation for	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - written and publicly accessible policies relating to PID validity status management; - authorised triggers, decision roles and evidence required for each lifecycle action, including conditions under which PID may be revoked without delay and procedures for processing revocation requests; - timeliness requirements and technical propagation of status changes, including timeframes for revocation processing;	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - written and publicly accessible PID validity-status-management policies; - suspension, revocation, reactivation, renewal or replacement records relevant to the requirement; - authorisation evidence and timestamps for status changes, including revocation request processing and applicable processing timeframes; - technical status publication or propagation

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		unauthorised revocation; (e) user notification procedures upon revocation.	qualified services); §6.5.2 (Private key protection for qualified services). 5.2.3 Record Retention (PID-Specific)		- controls preventing unauthorised suspension, revocation, reactivation or renewal, including measures to prevent unauthorised revocation; - user notification procedures upon revocation; - assurance checks required before reactivation, renewal or replacement is allowed.	- logs; - evidence of measures preventing unauthorised revocation and user notification procedures upon revocation; - cases rejected because the required assurance or authorisation conditions were not met.
PP-10	REQ-2981-P06	PID Provider shall retain, for at least five years after the cancellation or expiry of the relevant certificate of conformity, records of the information provided to the CAB during the certification process and specimens of hardware components used in PID issuance that were included in the certification scope. PID Provider shall make this information available to the CAB or to UKE upon request.	Alignment with international standards - ISO/IEC 27001:2022 A.5.36 (compliance); cl.	WZ-03-02	The assessor reviews certification, conformity-assessment and scope-maintenance evidence maintained by the assessed PID Provider. The review should confirm: - which records or information must be retained for certification, audit, incident or supervisory purposes, including records of information provided to the CAB during the certification process and specimens of hardware components used in PID issuance that were included in the certification scope; - retention period, including periods after certificate cancellation or expiry where applicable, and at least five years after cancellation or expiry of the relevant certificate of conformity; - integrity, confidentiality, access-control and retrieval controls; - secure deletion, archival and availability to the CAB or competent authorities, including availability to the CAB or to UKE upon request.	The assessor checks certification and scope evidence for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - record samples covering certification, assessment, vulnerability, incident or service evidence, including information provided to the CAB during certification; - evidence of secure retention of specimens of hardware components used in PID issuance and 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, including requests from the CAB or UKE; - expired or archived records and evidence of secure deletion where retention ended.
PP-11	REQ-2981-P04; REQ-2690-41	PID Provider shall ensure that personnel involved in PID issuance operations, including identity proofing, PID signing key management and revocation processing, are subject to enhanced	Alignment with international standards - ISO/IEC 27001:2022 A.6.1 (screening); A.6.3 (IS	WZ-03-02	The assessor reviews personnel-control documentation maintained by the assessed PID Provider. The review should confirm: - roles involved in identity proofing, PID signing-key management, revocation processing and other PID issuance operations; - which PID issuance roles require enhanced background verification and why;	The assessor examines sampled personnel records for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - personnel assigned to identity proofing, PID signing-key management, revocation processing and other PID issuance roles; - completed enhanced background verification

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		background verification and hold appropriate qualifications. PID Provider shall document the roles in the PID issuance process that require enhanced vetting and the criteria applied.	awareness and training). ETSI EN 319 401 §7.4-§67.8 (Personnel security); EN 319 411-		- qualification, competence, experience and training criteria for each role; - criteria applied for enhanced vetting and personnel eligibility decisions; - records and samples available for Stage 2, including screening approvals, exceptions, role changes and periodic reviews.	- for roles requiring it; - qualification, competence, experience or training evidence matching the documented criteria; - role mapping showing which positions require enhanced vetting; - exceptions, role changes, failed vetting or overdue reviews and how they were resolved.
PP-12	REQ-1502-002; REQ-2690-58	The facilities and infrastructure hosting PID signing key material shall be subject to enhanced physical security controls consistent with the classification of PID signing keys as critical assets. PID Provider shall implement physical security perimeters, entry controls, and environmental protection measures at least equivalent to the requirements applicable to secure cryptographic device hosting environments.	Alignment with international standards - ISO/IEC 27001:2022 A.7.1 (physical security perimeters); A.7.2 (physical entry); A.7.4 (physical security monitoring). ETSI EN 319 401 §7.4-§67.8 (Physical security); EN 319 411-1 §6.4.2 (Physical security controls); EN 319 411-	WZ-03-02	The assessor reviews asset inventory, classification and handling rules maintained by the assessed PID Provider. The review should confirm: - classification of PID signing keys as critical assets and resulting physical-security requirements; - physical security perimeters, entry controls and access restrictions for facilities hosting PID signing key material; - environmental protection measures for infrastructure hosting PID signing key material; - physical monitoring, alarm handling, visitor controls and access-log review; - controls at least equivalent to requirements applicable to secure cryptographic device hosting environments; - handling of exceptions, unauthorised access attempts, environmental events and corrective actions.	The assessor checks selected assets and handling records for the assessed PID Provider during the on-site Stage 2 assessment. The sample should include: - inspection or demonstration of physical security perimeters and entry controls for facilities hosting PID signing key material; - access logs, visitor records and approval evidence for secure areas; - environmental protection, monitoring, alarm and maintenance records; - evidence that controls are consistent with PID signing keys being critical assets and at least equivalent to secure cryptographic device hosting environments; - records of unauthorised access attempts, environmental events, exceptions and corrective actions.
PP-13	REQ-1502-001; REQ-2690-P02	Access to PID signing key material shall be restricted to the PID issuance application and personnel with a documented operational requirement. All access to PID signing keys shall be	Alignment with international standards - ISO/IEC 27001:2022 A.8.15 A.5.18 A.8.2. ETSI EN 319 401 §7.1	WZ-03-02	The assessor reviews PID signing-key access-control documentation maintained by the assessed PID Provider. The review should confirm: - which application components and personnel may access PID signing key material; - the documented operational requirement for each authorised application, role or account;	The assessor tests PID signing-key access controls for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should include: - access-control configuration showing that only the PID issuance application and authorised personnel can access PID signing key material;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		logged, and logs shall be retained for the period required by EP-40 of WZ-03-01.	(Policy and risk management); EN 319 411 -1 §6.9.1 (Organisational).		- approval, periodic review and removal rules for PID signing-key access; - requirements for logging every access to PID signing keys, including application, administrator and operator access; - log protection and retention rules aligned with EP-40 of WZ-03-01.	- access approvals, role assignments and periodic review records showing documented operational need; - samples of PID signing-key access logs covering application and personnel access; - evidence that logs are protected and retained for the period required by EP-40 of WZ-03-01; - rejected or unauthorised access attempts and related escalation or corrective actions.
PP-14	REQ-2977-05	PID Provider shall implement technical controls to ensure that PID is cryptographically bound to the wallet unit to which it is issued, in accordance with the technical specifications of CIR (EU) 2024/2977. The binding mechanism shall prevent the transfer of issued PID to a different wallet unit without re-issuance.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.31 (legal requirements). ETSI EN 319 401 §7.4 -§67.8 (Cryptographic controls); EN 319 411 -2 §6.5.1 (Key pair generation for qualified services); §6.5.2 (Private key protection for qualified services).	WZ-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - how the intended Wallet Unit is identified and validated before binding; - how the PID public key, proof of possession and proof of association are checked before PID is issued; - how the issued PID is linked to the validated Wallet Unit and to the accepted PID public key, in accordance with the technical specifications of CIR (EU) 2024/2977; - controls preventing issuance to a substituted Wallet Unit, wrong public key or unverified binding request; - technical controls preventing transfer of issued PID to a different Wallet Unit without re-issuance; - evidence retained for failed, repeated or exceptional binding attempts.	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - the approved issuance decision, Wallet Unit identifier, attestation result, PID public key and binding evidence; - proof-of-possession and proof-of-association validation logs; - technical issuance records showing the PID bound to the intended Wallet Unit and public key, in accordance with CIR (EU) 2024/2977 technical specifications; - negative or design evidence showing that issued PID cannot be transferred to a different Wallet Unit without re-issuance; - rejected cases involving missing proofs, wrong keys, invalid attestations or replayed binding material; - a trace from the approved issuance decision to the Wallet Unit identifier, binding material, technical issuance event and retained audit evidence.
PP-15	REQ-2977-08	PID Provider shall implement technical controls to validate the wallet unit attestation before issuing PID, including verification that	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of	WZ-03-02	The assessor reviews how the assessed PID Provider handles Wallet Unit attestations in the relevant process. The documentation should identify: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA	The assessor checks selected Wallet Unit attestation cases for the assessed PID Provider during the on-site Stage 2 assessment. The sampled evidence should include: - issued WUVA or WUTA samples and signature or seal validation evidence, including

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the wallet unit belongs to a wallet solution accepted by PID Provider and that the wallet unit attestation has not been revoked.	cryptography); A.8.9 (configuration management). ETSI EN 319 401 §7.4 -§67.8 (Cryptographic controls); EN 319 411-2 §6.5.1 (Key pair generation for qualified services).		records, including technical controls to validate the Wallet Unit Attestation before issuing PID; - certificate and trust-list requirements used for attestation signing or sealing; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - checks verifying that the Wallet Unit belongs to a wallet solution accepted by the PID Provider; - validity-status checks confirming that the Wallet Unit Attestation has not been revoked before PID issuance; - rules excluding personal data from attestations where the requirement prohibits such data.	evidence that the attestation was validated before PID issuance; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - evidence that the Wallet Unit belonged to a wallet solution accepted by the PID Provider; - revoked or invalid attestation cases and evidence that status publication or user notification followed the defined process, including evidence that revoked attestations were not accepted for PID issuance.
PP-16	REQ-2977-07	PID Provider shall implement technical controls to authenticate itself to wallet units using its wallet-relying party access certificate, issued under a certificate listed in the applicable trusted list.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.33 (protection of records). ETSI EN 319 401 §7.4 -§67.8 (Key management); EN 319 411 -1 §6.5.2 (Private key protection and cryptographic module engineering controls); EN	WZ-03-02	The assessor reviews relying-party authentication and interaction controls maintained by the assessed PID Provider. The documentation should explain: - certificate profiles or alternative assurance level high authentication mechanisms used for provider identification, including the wallet-relying party access certificate issued under a certificate listed in the applicable trusted list where required; - certificate lifecycle controls, trust anchors and revocation checks; - protocol steps that prevent Wallet Units from accepting unauthenticated provider requests; - evidence retained for successful and failed provider-authentication events.	The assessor tests selected relying-party interaction cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - live or retained protocol traces showing use of the wallet-relying party access certificate or approved alternative mechanism, including evidence that the wallet-relying party access certificate is issued under a certificate listed in the applicable trusted list where required; - certificate validity, chain-building and revocation-check results; - logs for rejected exchanges involving invalid, expired or untrusted credentials; - configuration showing that weaker or unapproved authentication paths are not enabled.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			319 411-2 §6.5.2 (Private key protection for qualified services). 5.6 PID Issuance Process Requirements This subsection specifies organisational requirements for the PID issuance processes. The corresponding process-specific technical and procedural requirements are specified in WP-03-01.			
PP-17	REQ-1502-E01; REQ-1502-E02; REQ-1502-E03	PID Provider shall establish documented procedures for the application and registration phase of PID issuance, ensuring that applicants are: (a) informed of the terms and conditions of the electronic identification means before the identity proofing process is started; (b) informed of recommended security precautions; (c) provided with clear guidance on the identity proofing process,	Alignment with international standards - ISO/IEC 27001:2022 A.5.16 (identity management); A.5.31 (legal requirements); cl. 8.1 (operational planning). ETSI EN 319 401 §7.1 (Organisational requirements); EN 319 411 -1 §7.3 (Initial	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the exact user-facing content, including terms, conditions, obligations, fees, limitations or recommended precautions relevant to the requirement; - clear applicant guidance on the identity proofing process, the information to be collected, data retention, evidence required and any tools the applicant must use; - the point in the journey where the information is shown and whether the user can proceed without seeing or acknowledging it, including presentation of terms and	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - screens, messages, portal pages or API responses used to present the required information; - documented application and registration procedures for PID issuance; - sampled user records showing acknowledgement, delivery or acceptance where required, including terms and conditions before identity proofing starts and recommended security precautions; - guidance evidence covering the proofing process, information to be collected, data retention, required evidence and tools

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		the information to be collected, data retention, the evidence required, and any tools the applicant is required to use. NOTE - Where alternative identity proofing processes are available, PID Provider should allow the applicant to select the process, where the processing of biometric data is involved.	identity validation); §6.3.1 (Certificate application); EN 319 41 1-2 §7.3 (Initial identity validation for qualified certificates).		conditions before identity proofing starts; - 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.	required from the applicant; - 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.
PP-18	REQ-1502-E03; REQ-2977-03; REQ-2977-04; REQ-5c-03	PID Provider shall define the mandatory and optional identity attributes to be collected for each identity proofing context. All mandatory attributes, including at a minimum those stipulated in Table 1 of the Annex to CIR (EU) 2024/2977, shall be collected. The collected attributes shall provide unique identification of the applicant within the Republic of Poland.	Alignment with international standards - ISO/IEC 27001:2022 A.5.16 (identity management); A.5.31 (legal requirements); A.8.24 (cryptography). ETSI EN 319 401 §7.1 (Enrolment and registration); EN 319 411 -2 §6.2 (Qualified certificate registration procedures); EN 319 411-2 §6.5.1 (Key pair generation for qualified	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - the accepted proofing paths and the conditions for using each path; - mandatory and optional identity attributes to be collected for each identity proofing context, including at least the mandatory attributes stipulated in Table 1 of the Annex to CIR (EU) 2024/2977; - evidence sources, verification checks and manual-review steps supporting assurance level high; - checks confirming that the collected attributes provide unique identification of the applicant within the Republic of Poland; - handling of failed, inconsistent, expired or incomplete evidence; - traceability from application intake to the final proofing and issuance decision.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - application records showing mandatory and optional identity attributes collected for the relevant proofing context; - source checks, operator decisions, timestamps and final assurance-level decisions; - evidence that all mandatory attributes, including those stipulated in Table 1 of the Annex to CIR (EU) 2024/2977, were collected; - evidence that collected attributes uniquely identified the applicant within the Republic of Poland; - evidence that issuance or activation occurred only after required proofing steps were completed.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			services); §6.5.2 (Private key protection for qualified services).			
PP-19	REQ-5c-02; REQ-1502-E04; REQ-2977-06	PID Provider shall establish documented procedures for identity proofing and verification that meet the requirements of assurance level High as defined in CIR (EU) 2015/1502, Section 2.1. The identity of the applicant shall be established based on an authentication using an eID means issued under a scheme notified to the Commission for cross-border recognition at assurance level High, or under a scheme confirmed to conform to the same requirements by an accredited conformity assessment body.	Alignment with international standards - ISO/IEC 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).	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - documented procedures for identity proofing and verification meeting assurance level High as defined in CIR (EU) 2015/1502, Section 2.1; - the accepted proofing paths and the conditions for using each path, including authentication using an eID means issued under a scheme notified to the Commission for cross-border recognition at assurance level High or under a scheme confirmed to conform to the same requirements by an accredited conformity assessment body; - 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 assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - normal, rejected and manually reviewed applications; - documented proofing and verification procedures mapped to CIR (EU) 2015/1502, Section 2.1 assurance level High; - source checks, operator decisions, timestamps and final assurance-level decisions, including evidence of authentication using a notified assurance level High eID means or a scheme confirmed by an accredited conformity assessment body; - evidence that issuance or activation occurred only after required proofing steps were completed; - records showing how exceptions were escalated, corrected or rejected.
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 or revoked, and that the person identification data remains accurate and is confirmed by the authoritative sources	Alignment with international standards - ISO/IEC 27001:2022 A.5.16 (identity management); A.8.24 (use of cryptography). ETSI EN 319 401	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 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	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 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

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		designated in the Trust Framework. The process shall confirm that the identity exists and that the person is not known to be deceased.	§7.1 (Identity verification); EN 319 411-2 §7.3 (Initial identity validation for qualified certificates).		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.	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.
PP-21	REQ-2977-01; REQ-2977-02; REQ-2977-03; REQ-2977-05; REQ-2977-07; REQ-2977-08	PID Provider shall establish documented procedures for PID issuance covering: (a) validation of the wallet unit attestation; (b) verification of the revocation status of the wallet unit attestation; (c) issuance of PID in the formats supported by PID Provider, including the mandatory attributes and metadata specified in the Annex to CIR (EU) 2024/2977; (d) cryptographic binding of the PID to the wallet unit; (e) delivery of the PID to the wallet unit through the secure channel established for the issuance.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.16 (identity management); cl. 8.1 (operational planning). ETSI EN 319 401 §7.4-§67.8 (Cryptographic controls); EN 319 411-1 §6.3.2 (CA key life cycle); EN 319 411-2 §6.5.1 (Key pair generation for qualified services); §6.5.2 (Private key protection for	WZ-03-02	The assessor reviews the documented binding model between PID and the Wallet Unit maintained by the assessed PID Provider. The review should show how the process defines: - conditions for issuing, signing, sealing, validating and revoking WUVA or WUTA records, including validation of the wallet unit attestation before PID issuance; - certificate and trust-list requirements used for attestation signing or sealing; - verification of the revocation status of the wallet unit attestation before issuance; - attestation content, including public keys and WSCA/WSCD or device-profile information where required; - issuance of PID in the formats supported by the PID Provider, including mandatory attributes and metadata specified in the Annex to CIR (EU) 2024/2977; - cryptographic binding of the PID to the Wallet Unit.	The assessor traces selected PID-to-Wallet Unit binding cases for the assessed PID Provider during the on-site Stage 2 assessment. The test should connect: - issued WUVA or WUTA samples and signature or seal validation evidence, including validation before PID issuance; - certificate chain, trust-list and validity-status evidence for the signing or sealing certificate, including revocation-status verification of the wallet unit attestation; - attestation content compared with public keys, device profiles and WSCA/WSCD environment details; - issued PID samples showing supported formats, mandatory attributes and metadata specified in the Annex to CIR (EU) 2024/2977; - technical records showing cryptographic binding of the PID to the Wallet Unit; - protocol traces or delivery records showing delivery of PID to the Wallet Unit through the secure issuance channel.

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			qualified services).			
PP-22	REQ-2981-P02	PID Provider should limit the validity period of issued PID to a period proportionate to the risks of change in the person identification data and the ability of PID Provider to detect such changes. A validity period not exceeding five years from the time when the identity proofing procedure was completed is considered proportionate for assurance level High.	Alignment with international standards - ISO/IEC 27001:2022 A.5.31 (legal requirements); cl. 8.1 (operational planning and control). ETSI EN 319 401 §7.1 (Policy requirements); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).	WZ-03-02	The assessor reviews the identity proofing, onboarding or registration procedure maintained by the assessed PID Provider. The review should confirm that the documented process defines: - validity period assigned to issued PID and the rationale for its duration; - risk assessment of changes in person identification data and the PID Provider's ability to detect such changes; - controls ensuring the validity period is proportionate to those risks; - controls ensuring that assurance level High PID validity does not exceed five years from completion of the identity proofing procedure, unless a stricter applicable rule applies; - links between validity period, renewal, replacement, authoritative-source checks and lifecycle-status management.	The assessor traces selected onboarding, registration or identity-proofing cases for the assessed PID Provider during the on-site Stage 2 assessment. The evidence should show: - issued PID samples showing validity period and proofing-completion timestamp; - evidence that the validity period is proportionate to risks of changes in person identification data and detection capability; - records confirming that assurance level High PID validity does not exceed five years from completion of identity proofing; - renewal or replacement cases triggered by validity expiry or changed identity data; - configuration evidence enforcing PID validity periods and preventing issuance with non-compliant validity.
PP-23	REQ-2977-09; REQ-2977-11; REQ-2977-12; REQ-2977-13; REQ-2977-14; REQ-2977-15; REQ-1502-M02; REQ-1502-M03	PID Provider shall establish and operate documented procedures for PID revocation, including: (a) a procedure for the submission and processing of revocation requests; (b) immediate and proactive revocation where PID Provider becomes aware of changes impacting the validity of PID or compromise of the cryptographic binding; (c) measures to prevent	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.8.15 (logging); A.8.8 (vulnerability management); A.5.33 (protection of records). ETSI EN 319 401 §7.4 -§67.8	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - submission and processing of PID revocation requests; - immediate and proactive revocation where the PID Provider becomes aware of changes impacting PID validity or compromise of the cryptographic binding; - measures preventing unauthorised revocation; - user notification within 24 hours of revocation; - maintenance of revoked PID in the validity status service for the legally required period;	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revocation requests and records showing submission, processing, decision and status update; - cases of immediate or proactive revocation caused by changed PID validity or compromised cryptographic binding; - authorisation evidence and rejected unauthorised revocation attempts; - timestamps showing user notification within 24 hours of revocation; - validity-status service evidence showing revoked PID maintained for the legally

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
		unauthorised revocation; (d) user notification within 24 hours of revocation; (e) maintenance of revoked PID in the validity status service for the legally required period.	(Technical controls for key management); EN 319 411-1 §6.5.1 (Key pair generation and installation); §6.3.9 (Certificate revocation and suspension); EN 319 411 -2 §6.5.1 (Key pair generation); §6.3.9 (Certificate revocation for qualified services).		- links between Wallet Unit Attestation status, cryptographic binding status, PID validity status, user notification and retained revocation evidence.	required period; - exceptions, delays or failures and related corrective actions.
PP-24	REQ-2977-13; REQ-1502-M04	PID Provider shall ensure that revocations of PID cannot be reverted. Once PID has been definitively revoked, it shall not be reinstated. Reactivation of a suspended PID shall take place only if the same assurance requirements as established before the suspension continue to be met.	Alignment with international standards - ISO/IEC 27001:2022 A.8.24 (use of cryptography); A.5.33 (protection of records). ETSI EN 319 401 §7.4 -§67.8 (Key management); EN 319 411 -2 §6.5.1 (Key pair generation for qualified services); §6.3.9 (Certificate	WZ-03-02	The assessor reviews the revocation, suspension or validity-status arrangements maintained by the assessed PID Provider. The documented controls should define: - status model distinguishing suspension, temporary blocking, revocation and end-of-life states; - technical controls preventing a revoked PID, Wallet Unit or attestation from returning to valid status; - authorisation and logging for revocation decisions; - handling of erroneous revocation without reinstating the revoked artefact contrary to the requirement; - reactivation rules for suspended PID ensuring that reactivation takes place only if the same assurance requirements as established before the suspension continue to	The assessor tests selected revocation, suspension or validity-status cases for the assessed PID Provider during the on-site Stage 2 assessment. The sample should show: - revoked PID, Wallet Unit or attestation records and subsequent status history; - attempts or procedures for reactivation to confirm that revoked items cannot return to valid state; - register, status service and publication evidence after revocation; - exception cases showing how mistakes are corrected through controlled re-issuance rather than reversal; - suspended PID reactivation records showing that the same assurance requirements as established before suspension continued to be met before reactivation;

Requirement number	Source standard / regulation	Requirement content	Reference to other standards	WZ/WP source document	CAB assessment method - Stage 1	CAB assessment method - Stage 2
			revocation and suspension for qualified services).		be met; - technical and procedural controls preventing reversal of completed revocations.	- technical and procedural controls preventing reversal of completed revocations.