

WZ-03-02

**Organisational and Technical Requirements for
PID Providers including requirements derived
from Article 5c of eIDAS**

VERSION 1.01

04.06.2026

Document reference	WZ-03-02
Version	V1.01 (2026-06)
Status	Final
Date	04.06.2026
Document type	Certification Scheme — Scheme Specification (ISO/IEC 17067)
Parent framework	GP-03 eID Certification Scheme
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	Electronic identification system
Primary audience	PID Provider
Secondary audience	Conformity Assessment Bodies (CABs) accredited according to G-05
Assurance level <identity proofing>	High (CIR (EU) 2015/1502)
Subsidiary Documents	WP-03, WM-03 series

Table of content

1	SCOPE	4
2	LEGAL BASIS.....	5
3	GENERAL PRINCIPLES	8
3.1	Proportionality to Risk	8
3.2	Auditability	8
3.3	National Law	8
3.4	Normative Language.....	8
3.5	Relationship with WZ-03-01 and WP-03 Series.....	9
4	LEGAL REQUIREMENTS	10
4.1	Requirements Derived from Article 5c eIDAS	10
4.2	Requirements Derived from CIR (EU) 2015/1502.....	10
4.3	Enrolment (Section 2.1).....	10
4.4	Electronic Identification Means Management (Section 2.2)	12
4.5	Management and Organisation (Section 2.4)	13
4.6	Requirements Derived from CIR (EU) 2024/2977	13
4.6.1	Issuance of Person Identification Data (Article 3)	13
4.7	Validity Status Management and Revocation (Article 5)	14
4.8	Requirements Derived from CIR (EU) 2024/2981.....	15
4.9	Requirements Derived from CIR (EU) 2024/2690.....	15
5	PROVISIONS.....	17
5.1	General and Scheme-Specific Provisions.....	17
5.1.1	Information Security Management System.....	17
5.1.2	Logical Separation of PID Processing	17
5.1.3	PID-Specific Risk Assessment.....	18
5.1.4	Authoritative Sources.....	18
5.1.5	Certification Body Notification (PID-Specific)	19
5.2	Organisational Controls	19
5.2.1	PID Signing Key Management	20
5.2.2	Validity Status Management.....	21
5.2.3	Record Retention (PID-Specific)	21
5.3	People Controls	22
5.4	Physical Controls	22
5.5	Technological Controls.....	23
5.6	PID Issuance Process Requirements	24
5.6.1	Application and Registration	24
5.6.2	Identity Proofing and Verification.....	25
5.6.3	Issuance and Cryptographic Binding.....	25
5.6.4	Revocation and Validity Status Operations	26
6	ANNEX A (INFORMATIVE) — PROVISION-TO-REQUIREMENT MAPPING	28

1 Scope

- 1 The present document specifies the organisational and technical requirements applicable to PID Provider within the electronic identification system, for the purposes of certification under the eID Certification Scheme (GP-03).
- 2 WZ-03-02 is a subsidiary document of GP-03 in the WZ-series (management system requirements) and a role-specific adoption of WZ-01. WZ-01 (Organisational and Technical Requirements for EUDI Providers) is the base document for all providers in the scheme; WZ-03-02 supplements it with PID Provider-specific requirements. It sets out the organisational, governance, information security, technical and process-specific controls applicable to PID Provider, including those derived from Article 5c of eIDAS and from CIR (EU) 2024/2977 regarding the issuance of person identification data to EUDI Wallets.
- 3 This document is intended to be read in conjunction with WZ-03-01, which specifies the requirements applicable to Wallet Provider providing eID-related services. Where one entity merges roles of Wallet Provider and PID Provider, it shall comply with the requirements of WZ-03-01, WZ-03-02 and WZ-03-03. The CAB shall evaluate Wallet Provider/PID Provider against the respective documents. Where a provision of WZ-03-02 overlaps with or reinforces a provision of WZ-03-01, the more specific provision shall apply.
- 4 The following are outside the scope of this document:
 - I. Process-specific requirements for PID enrolment and lifecycle management — see WP-03-01.
 - II. Requirements for eID means and authentication — see WP-03-03.
 - III. Requirements for the Wallet Provider — see WZ-03-01.
 - IV. Cybersecurity product certification of the wallet solution — see GP-02.
 - V. Functional conformity assessment of the wallet — see GP-01.

2 Legal Basis

5 This document is based on the following legal instruments:

- I.Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 (hereinafter “eIDAS”), in particular Articles 5a and 5c thereof.
- II.Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 (hereinafter “CIR (EU) 2015/1502”), Sections 2.1 (Enrolment), 2.2 (eID system management) and 2.4 (Management and organisation) of the Annex thereto.
- III.Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules as regards person identification data issued to European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2977”), in particular Articles 3 and 5 thereof.
- IV.Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules as regards the certification of European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2981”), Articles 4, 5, 8 and 19 thereof and Annexes I and V thereto.
- V.Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (hereinafter “NIS 2 Directive”), in particular Article 21(2) thereof.
- VI.Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules as regards technical and methodological requirements of cybersecurity risk-management measures (hereinafter “CIR (EU) 2024/2690”), in particular the Annex thereto.
- VII.Polish Act on the mObywatel Application (Dz.U. 2023 poz. 1234, z późn. zm.).
- VIII.Polish Act on Trust Services and Electronic Identification (Dz.U. 2016 poz. 1579, z późn. zm.).
- IX.Polish Cybersecurity Act (Dz.U. 2018 poz. 1560, z późn. zm.).

- X. Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets (hereinafter “CIR (EU) 2024/2979”), published in the Official Journal of the European Union on 4 December 2024, entered into force on 24 December 2024; in particular Articles 3, 4, 5, 6, 7, 9 and 13 thereof.
- XI. Commission Implementing Regulation (EU) 2025/849 of 28 February 2025 amending Implementing Regulations (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 and (EU) 2024/2982 as regards applicable standards and specifications (hereinafter “CIR (EU) 2025/849”). This amending regulation updates references to technical standards and specifications in the implementing regulations to align them with ARF v2.8.0 and the latest ETSI and ISO standards.
- XII. European Digital Identity Cooperation Group (EDICG), Architecture and Reference Framework (ARF) v2.8.0 (current version as of April 2026), maintained under Commission Recommendation (EU) 2021/946 of 3 June 2021 (OJ L 210, 14.6.2021, p. 51) (hereinafter “ARF v2.8.0”). The ARF is an informative technical reference document; it is not legally binding, but specifies the data models, protocols and interoperability requirements referenced in CIR (EU) 2024/2979 and CIR (EU) 2024/2977. The ARF is maintained by the EDICG and updated continuously; the applicable version at the time of certification shall be used.
- XIII. ETSI TS 119 461 v2.1.1 (February 2025) — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (hereinafter “ETSI TS 119 461”). This standard is referenced in the eIDAS implementing acts on identity verification and defines the technical requirements for remote and in-person identity proofing at assurance level High, including the verification of identity evidence and liveness detection requirements.
- XIV. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”), in particular: Article 5 (principles relating to processing of personal data); Article 25 (data protection by

design and by default); Article 32 (security of processing); Article 17 (right to erasure); Article 34 (communication of a personal data breach to the data subject); and Article 83 (general conditions for imposing administrative fines).

XV. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (hereinafter “Cyber Resilience Act” or “CRA”), entered into force on 10 December 2024; in particular Annex I thereto (essential cybersecurity requirements for products with digital elements), as incorporated by reference in Article 5(7) of CIR (EU) 2024/2981 and Article 5(3) of CIR (EU) 2024/2981 (reference to EN ISO/IEC 30111:2019 and CRA Annex I for vulnerability handling).

XVI. ISO/IEC 18013-5:2021 — Personal identification — ISO-compliant driving license — Part 5: Mobile driving license (mDL) application (hereinafter “ISO/IEC 18013-5”). This standard specifies the mdoc credential format and the mDL presentation protocol, which is one of the two mandatory data formats for PID issuance under the Annex to CIR (EU) 2024/2977 as updated by CIR (EU) 2025/849.

XVII. ISO/IEC 29115:2013 — Information technology — Security techniques — Entity authentication assurance framework (hereinafter “ISO/IEC 29115”). This standard defines the four levels of entity authentication assurance (LoA 1–4) and provides the international normative basis for the assurance level High requirements implemented in CIR (EU) 2015/1502, Section 2.3.

XVIII. OpenID Foundation, OpenID for Verifiable Credential Issuance (OID4VCI) — draft specification referenced in ARF v2.8.0 and CIR (EU) 2024/2979 as the standard protocol for issuance of PID and electronic attestations of attributes to EUDI Wallet units; and OpenID for Verifiable Presentations (OID4VP) — draft specification referenced in ARF v2.8.0 and CIR (EU) 2024/2979 as the standard protocol for presentation of PID and attestations to relying parties. The applicable version of these specifications shall be that referenced in the current ARF v2.8.0.

3 General Principles

3.1 Proportionality to Risk

- 6 All provisions in this document shall be understood as requirements at assurance level High in accordance with the Annex to CIR (EU) 2015/1502. PID Provider shall take due account of the risks specific to the person identification data it issues, including the risks listed in Annex I to CIR (EU) 2024/2981, when implementing the provisions of this document.

3.2 Auditability

- 7 This document is intended for use within the eID Certification Scheme (GP-03) as defined in ISO/IEC 17067. PID Provider shall ensure that its implementation of the provisions in this document is documented, traceable and verifiable by an independent conformity assessment body (CAB) accredited against ISO/IEC 17065 pursuant to G-05.
- 8 *NOTE: In the context of this document, a CAB means a certification body.*

3.3 National Law

- 9 Where national law, in particular the Polish Act on Trust Services and Electronic Identification, the Act on the Application and the Polish Cybersecurity Act, imposes requirements that are more stringent than or additional to those set out in this document, PID Provider shall comply with the applicable national law and document the applicable national provisions.

3.4 Normative Language

- 10 The normative terms “shall,” “should” and “may” are used in this document as follows:
- (a) SHALL: indicates a mandatory requirement that the Wallet Provider is required to satisfy;
- (b) SHOULD: indicates a recommendation; where the Wallet Provider deviates from such a recommendation, it shall document and substantiate the reasons for the deviation;
- (c) MAY: indicates a permission or an option left to PID Provider discretion.

3.5 Relationship with WZ-03-01 and WP-03 Series

- 11 The requirements of WZ-03-02 are additional to and do not replace the requirements of WZ-03-01. Where the entity acts as both Wallet Provider and PID Provider, it shall comply with the requirements of both documents, and the CAB shall evaluate the entity against both.
- 12 The process-specific requirements for PID enrolment, identity proofing, issuance, lifecycle management and revocation are specified in WP-03-01. The authentication and eID system requirements applicable at the point of onboarding are specified in WP-03-03. The present document specifies the organisational and technical management requirements that underpin those processes.

4 Legal Requirements

- 13 This section lists, at a granular level, all legal requirements applicable to PID Provider in scope of this document.

4.1 Requirements Derived from Article 5c eIDAS

- 14 The following requirements are derived from Article 5c of Regulation (EU) No 910/2014 as amended, which establishes the conditions for the certification of electronic identification schemes under which European Digital Identity Wallets are provided.

Identifier	Requirement
REQ-5c-01	The electronic identification scheme under which European Digital Identity Wallets are provided shall be certified by a conformity assessment body accredited pursuant to Regulation (EC) No 765/2008. [Article 5c (1)]
REQ-5c-02	The electronic identification scheme shall comply with the requirements set out in Article 8 about assurance level high, including the requirements for enrolment, identity proofing, and electronic identification means management. [Article 5c (3), read with Article 5a (11)]
REQ-5c-03	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]
REQ-5c-04	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)]

4.2 Requirements Derived from CIR (EU) 2015/1502

- 15 The following requirements are derived from the Annex to CIR (EU) 2015/1502, at assurance level High, applicable to PID Provider.

4.3 Enrolment (Section 2.1)

Identifier	Requirement
REQ-1502-E01	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]
REQ-1502-E02	PID Provider shall ensure the applicant is aware of recommended security precautions related to the electronic identification means. [Annex, Section 2.1.1, All Assurance Levels, Element 2]

Identifier	Requirement
REQ-1502-E03	PID Provider shall collect the relevant identity data required for identity proofing and verification. [Annex, Section 2.1.1, All Assurance Levels, Element 3]
REQ-1502-E04	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 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)]
REQ-1502-E05	If electronic identification means are not issued based on notified electronic identification means having the assurance level high requirements REQ-1502-E06 , REQ-1502-E07 , REQ-1502-E08 , REQ-1502-E09 , REQ-1502-E10 apply.
REQ-1502-E06	Conditional: The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identification means is being made and representing the claimed identity. [Annex, Section 2.1.2, Level Low, Point 1]
REQ-1502-E07	Conditional: 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]
REQ-1502-E08	Conditional: 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]
REQ-1502-E09	Conditional: At least one of requirements REQ-1502-E09-01 , REQ-1502-E09-02 apply.
REQ-1502-E09-1	Alternative: The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identification means is being made and representing the claimed identity; the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source; and steps have been taken to minimise the risk that the person's identity is not the claimed identity. [Annex, Section 2.1.2, Level Substantial, Point 1]
REQ-1502-E09-2	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]
REQ-1502-E10	Conditional: At least one of requirements REQ-1502-E10-01 , REQ-1502-E10-02 , REQ-1502-E10-03 apply.
REQ-1502-E10-1	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)]
REQ-1502-E10-2	Alternative: Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic

Identifier	Requirement
	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. [Annex, Section 2.1.2, Level High, Point 1(b)]
REQ-1502-E10-3	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 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)]

4.4 Electronic Identification Means Management (Section 2.2)

Identifier	Requirement
REQ-1502-M01	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]
REQ-1502-M02	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]
REQ-1502-M03	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]
REQ-1502-M04	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 access control mechanisms. [Annex, Section 2.2.1, Level High, Element 2]
REQ-1502-M05	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]
REQ-1502-M06	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]

Identifier	Requirement
REQ-1502-M07	PID Provider shall implement measures taken to prevent unauthorised suspension, revocation and/or reactivation of PID. [Annex, Section 2.2.3, All Assurance Levels, Element 2]
REQ-1502-M08	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]
REQ-1502-M09	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]
REQ-1502-M10	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]

4.5 Management and Organisation (Section 2.4)

- 16 The requirements from Section 2.4 applicable to COI as service provider are specified in WZ-03-01 (EP-01 through EP-69). The following additional requirements from Section 2.4 are specific to the PID Provider role.

Identifier	Requirement
REQ-1502-001	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]
REQ-1502-002	Sensitive cryptographic material used for issuing electronic identification means and authentication shall be protected from tampering. [Annex, 2.4.6, Level Substantial]

4.6 Requirements Derived from CIR (EU) 2024/2977

- 17 The following requirements are derived from CIR (EU) 2024/2977 on person identification data issued to European Digital Identity Wallets.

4.6.1 Issuance of Person Identification Data (Article 3)

Identifier	Requirement
REQ-2977-01	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)]
REQ-2977-02	PID Provider shall ensure that the PID issued to Wallet Unit contains the information necessary for authentication and validation of the PID. [Article 3(2)]

Identifier	Requirement
REQ-2977-03	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)]
REQ-2977-04	PID Provider shall ensure that the PID issued to a given Wallet User is unique for the Member State. [Article 3(4)]
REQ-2977-05	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)]
REQ-2977-06	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)]
REQ-2977-07	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)]
REQ-2977-08	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)]
REQ-2977-09	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)]

4.7 Validity Status Management and Revocation (Article 5)

Identifier	Requirement
REQ-2977-10	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)]
REQ-2977-12	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)]
REQ-2977-13	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)]
REQ-2977-14	PID Provider shall ensure that revocations cannot be reverted. [Article 5(5)]
REQ-2977-14	PID Provider shall ensure that revoked PID shall remain accessible for as long as required by Union law or national law. [Article 5(6)]
REQ-2977-15	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 indicate the location of that information in the PID. [Article 5(7)]

Identifier	Requirement
REQ-2977-16	PID Provider shall enable privacy preserving techniques which ensure unlinkability where the electronic attestations of attributes do not require the identification of the user.

4.8 Requirements Derived from CIR (EU) 2024/2981

Identifier	Requirement
REQ-2981-P01	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)]
REQ-2981-P02	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)]
REQ-2981-P03	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)]
REQ-2981-P04	PID Provider shall establish and implement human resource management policies established on national level for personnel involved in PID issuance operations. [Article 8(3)(d)]
REQ-2981-P05	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)]
REQ-2981-P06	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 the CAB during the certification process. [Article 19(2)]

4.9 Requirements Derived from CIR (EU) 2024/2690

18 The organisational cybersecurity requirements from CIR (EU) 2024/2690 applicable to COI as service provider are specified in WZ-03-01 (EP-10 through EP-69). The following requirements from CIR (EU) 2024/2690 are of relevance to the PID Provider role and are listed here for traceability.

Identifier	Requirement
REQ-2690-P01	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]
REQ-2690-P02	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]

Identifier	Requirement
REQ-2690-P03	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]

5 Provisions

- 19 This chapter establishes the provisions which PID Provider shall comply with for the purposes of certification. Provisions are labelled PP-xx (PID Provider). The structure of Sections 6.1 through 6.5 mirrors WZ-03-01; Section 6.6 contains PID issuance process requirements specific to this document.
- 20 PID Provider, if it is also a Wallet Provider, shall comply with all EP-series provisions of WZ-03-01 in addition to the PP-series provisions of this document. Where a PP-series provision addresses the same subject matter as an EP-series provision, the PP-series provision shall be understood as supplementing the EP-series provision with requirements specific to the PID Provider role.

5.1 General and Scheme-Specific Provisions

5.1.1 Information Security Management System

21 PP-01

Wallet Provider/PID Provider's ISMS established under EP-01 of WZ-03-01 shall explicitly cover the PID issuance infrastructure and all processes related to enrolment, issuance, and lifecycle management of person identification data. The scope of the ISMS shall document the boundary between the Wallet Provider and PID Provider functions and the controls in place to ensure the logical separation required by REQ-5c-04.

[REQ-5c-04; REQ-1502-E03; REQ-2981-P02]

Alignment with international standards — ISO/IEC 27001:2022 A.5.31 (legal, statutory and regulatory requirements); cl. 8.1 (operational planning and control); A.5.16 (identity management). | ETSI EN 319 401 §7.1 (Organisational security); EN 319 411-1 §6.9.1 (Organisational); §5.2 (CPS requirements); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).

Additional standards and references — GDPR Article 25 (data protection by design — ISMS scope must include data minimisation and purpose limitation for PID processing); ARF v2.8.0 §3.4 (PID Provider role and security responsibilities in the EUDI Wallet ecosystem).

5.1.2 Logical Separation of PID Processing

22 PP-02

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 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.

NOTE — Where the entity merges with the roles of Wallet Provider and PID Provider, the same physical infrastructure may be used for both roles, provided that the logical separation required by this provision is demonstrably maintained at the data, process and access control level.

[REQ-5c-04; REQ-910-05]

Alignment with international standards — ISO/IEC 27001:2022 A.5.31 (legal requirements); A.5.12 (classification of 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

23

PP-03

PID Provider shall conduct a PID-specific risk assessment as part of the implementation-specific risk assessment 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.

[REQ-2981-P01; REQ-5c-02]

Alignment with international standards — ISO/IEC 27001:2022 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).

5.1.4 Authoritative Sources

24

PP-04

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 to failures or unavailability of those sources.

NOTE — In the scheme, the PESEL register and the RDO are the authoritative sources designated in the Trust Framework. PID Provider shall ensure that its access to these registers is conducted in accordance with the applicable Polish legal framework governing access to population registers.

[REQ-2977-06; REQ-1502-E03]

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 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).

5.1.5 Certification Body Notification (PID-Specific)

25

PP-05

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. PID Provider shall notify the CAB where any private key used to sign the PID is or is suspected to have been compromised.

[REQ-2981-P05]

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 (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).

5.2 Organisational Controls

26

The organisational control requirements of Sections 6.2.1 through 6.2.11 of WZ-03-01 (EP-10 through EP-41) apply in full to PID Provider role. The

following supplementary provisions address aspects specific to PID issuance operations.

5.2.1 PID Signing Key Management

27

PP-06

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, 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.

[REQ-2690-P01; REQ-2690-P02; REQ-1502-001; REQ-1502-002]

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 §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).

28

PP-07

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.

[REQ-1502-001; REQ-1502-002; REQ-2690-P02]

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).

5.2.2 Validity Status Management

29 PP-08

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.

[REQ-2977-09; REQ-2977-15]

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 (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).

30 PP-09

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 unauthorised revocation; (e) user notification procedures upon revocation.

[REQ-2977-09; REQ-2977-12]

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 qualified services); §6.5.2 (Private key protection for qualified services).

5.2.3 Record Retention (PID-Specific)

31 PP-10

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.

[REQ-2981-P06]

Alignment with international standards — ISO/IEC 27001:2022 A.5.36 (compliance); cl. 9.2 (internal audit). | ETSI EN 319 401 §7.4-§67.8 (Compliance and audit); EN 319 411-2 §6.9.1 (Organisational requirements for QTSPs).

5.3 People Controls

32 The people control requirements of WZ-03-01 (EP-42 through EP-47) apply in full to the PID Provider role.

33 **PP-11**

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 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.

[REQ-2981-P04; REQ-2690-41]

Alignment with international standards — ISO/IEC 27001:2022 A.6.1 (screening); A.6.3 (IS awareness and training). | ETSI EN 319 401 §7.4-§67.8 (Personnel security); EN 319 411-1 §6.3 (TSP personnel); EN 319 411-2 §6.4.4 (Personnel controls for qualified services).

5.4 Physical Controls

34 The physical control requirements of WZ-03-01 (EP-48 through EP-53) apply in full to the PID Provider role.

35 **PP-12**

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.

[REQ-1502-002; REQ-2690-58]

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 319 411-2 §6.4.2 (Physical security controls for qualified services).

5.5 Technological Controls

36 The technological control requirements of WZ-03-01 (EP-54 through EP-69) apply in full to the PID Provider role, subject to the following supplementary provisions.

37 **PP-13**

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 logged, and logs shall be retained for the period required by EP-40 of WZ-03-01.

[REQ-1502-001; REQ-2690-P02]

Alignment with international standards — *ISO/IEC 27001:2022 A.8.15 A.5.18 A.8.2. | ETSI EN 319 401 §7.1 (Policy and risk management); EN 319 411-1 §6.9.1 (Organisational).*

38 **PP-14**

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.

[REQ-2977-05]

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).*

39 **PP-15**

PID Provider shall implement technical controls to validate the wallet unit attestation before issuing PID, including verification that the wallet unit belongs to a wallet solution accepted by PID Provider and that the wallet unit attestation has not been revoked.

[REQ-2977-08]

Alignment with international standards — *ISO/IEC 27001:2022 A.8.24 (use of 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).*

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.

[REQ-2977-07]

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 319 411-2 §6.5.2 (Private key protection for qualified services).

5.6 PID Issuance Process Requirements

41 This subsection specifies organisational requirements for the PID issuance processes. The corresponding process-specific technical and procedural requirements are specified in WP-03-01.

5.6.1 Application and Registration

42 PP-17

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, 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.

[REQ-1502-E01; REQ-1502-E02; REQ-1502-E03]

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 identity validation); §6.3.1 (Certificate application); EN 319 411-2 §7.3 (Initial identity validation for qualified certificates).

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.

[REQ-1502-E03; REQ-2977-03; REQ-2977-04; REQ-5c-03]

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 services); §6.5.2 (Private key protection for qualified services).

5.6.2 Identity Proofing and Verification

44 PP-19

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.

[REQ-5c-02; REQ-1502-E04; REQ-2977-06]

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).

45 PP-20

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 designated in the Trust Framework. The process shall confirm that the identity exists and that the person is not known to be deceased.

[REQ-1502-E04; REQ-2977-06]

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).

5.6.3 Issuance and Cryptographic Binding

46 PP-21

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.

[REQ-2977-01; REQ-2977-02; REQ-2977-03; REQ-2977-05; REQ-2977-07; REQ-2977-08]

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 qualified services).

47

PP-22

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.

[REQ-2981-P02]

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).

5.6.4 Revocation and Validity Status Operations

48

PP-23

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 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.

[REQ-2977-09; REQ-2977-11; REQ-2977-12; REQ-2977-13; REQ-2977-14; REQ-2977-15; REQ-1502-M02; REQ-1502-M03]

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 (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).

49

PP-24

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.

[REQ-2977-13; REQ-1502-M04]

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 revocation and suspension for qualified services).*

6 Annex A (Informative) — Provision-to-Requirement Mapping

Provision	Legal Requirements
PP-01	REQ-5c-04; REQ-1502-E03; REQ-2981-P02
PP-02	REQ-5c-04; REQ-910-05
PP-03	REQ-2981-P01; REQ-5c-02
PP-04	REQ-2977-06; REQ-1502-E03
PP-05	REQ-2981-P05
PP-06	REQ-2690-P01; REQ-2690-P02; REQ-1502-001; REQ-1502-002
PP-07	REQ-1502-001; REQ-1502-002; REQ-2690-P02
PP-08	REQ-2977-09; REQ-2977-15
PP-09	REQ-2977-09; REQ-2977-12
PP-10	REQ-2981-P06
PP-11	REQ-2981-P04; REQ-2690-41
PP-12	REQ-1502-002; REQ-2690-58
PP-13	REQ-1502-001; REQ-2690-P02
PP-14	REQ-2977-05
PP-15	REQ-2977-08
PP-16	REQ-2977-07
PP-17	REQ-1502-E01; REQ-1502-E02; REQ-1502-E03
PP-18	REQ-1502-E03; REQ-2977-03; REQ-2977-04; REQ-5c-03
PP-19	REQ-5c-02; REQ-1502-E04; REQ-2977-06
PP-20	REQ-1502-E04; REQ-2977-06
PP-21	REQ-2977-01; REQ-2977-02; REQ-2977-03; REQ-2977-05; REQ-2977-07; REQ-2977-08
PP-22	REQ-2981-P02
PP-23	REQ-2977-09; REQ-2977-11–15; REQ-1502-M02; REQ-1502-M03
PP-24	REQ-2977-13; REQ-1502-M04