

WP-03-01

PL EUDI Wallet Certification System

Requirements for PID Registration and PID
Lifecycle

VERSION 1.01

2026.06.03

Document reference	WP-03-01
Version	V1.01
Status	FINAL
Date	03.06.2026
Document type	Certification Scheme — Service-related requirements (ISO/IEC 17067)
Parent framework	GP-03 eID Certification Scheme WZ-03 series
Scheme Owner	Republic of Poland / Minister of Digital Affairs
Certification target	Requirements for PID Registration and PID/EUDI Wallet Lifecycle
Primary audience	PID Provider, EUDI Wallet Providers
Secondary audience	Conformity Assessment Bodies (CABs) accredited according to G-05
Assurance level <identity proofing>	High (Article 8 eIDAS; CIR (EU) 2015/1502)
Subsidiary Documents	WM-03-01, WM-03-02, WM-03-03

Table of content

1	Scope	4
2	Legal Basis	5
2.1	Legal acts	5
2.2	Normative references	6
3	Terms and Definitions.....	7
4	General Principles.....	8
4.1	Proportionality to risk.....	8
4.2	Auditability	8
4.3	National law.....	8
4.4	Normative language	8
4.5	Relationship with WZ-03-02, WP-03-02 and WP-03-03	9
5	Legal Requirements	10
5.1	Requirements derived from Regulation (EU) No 910/2014 as amended.	10
5.2	Requirements derived from CIR (EU) 2015/1502	11
5.3	Requirements derived from CIR (EU) 2024/2977	12
5.4	Requirements derived from CIR (EU) 2026/798	14
6	Provisions	17
6.1	PID Issuance	17
6.2	Binding PID with Wallet Unit.....	20
6.3	PID Maintenance.....	23
	Annex A (Informative) Mapping of Provisions to Legal Requirements	27
	Annex B (informative) Description of PID lifecycle	28

1 Scope

- 1 The present document specifies the requirements for the enrolment of wallet users and the issuance and life-cycle management of person identification data (PID), for the purposes of certification under the eID Certification Scheme (GP-03).
- 2 This document applies to PID providers being organisations that issue person identification data to the wallet users under an electronic identification scheme.
- 3 This document covers the following processes which create the PID providing services:
 - enrolment and identity proofing;
 - PID issuance;
 - remote onboarding from the PID issuance perspective;
 - PID binding with Wallet Unit;
 - PID maintenance.
- 4 The organisational information security requirements applicable to PID providers as service providers are specified in WZ-03-02. The present document addresses the process-specific requirements for PID enrolment identity proofing, remote onboarding, PID issuance and life-cycle management, without replacing the requirements applicable to Wallet Unit provisioning or authentication mechanisms.
- 5 This document is part of the WP-03 series and is intended to be used by certification bodies accredited against ISO/IEC 17065, complemented by ETSI EN 319 403-1, pursuant to G-05, for the assessment of the PID provider services conformity within the eID Certification Scheme (GP-03), as defined in EN ISO/IEC 17067.

2 Legal Basis

2.1 Legal acts

6 This document is based on the following legal instruments:

- I. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation), as amended by Regulation (EU) 2024/1183, in particular Article 5a thereof;
- II. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014, in particular Sections 2.1 and 2.2 of the Annex thereto;
- III. Commission Implementing Regulation (EU) 2026/798 of 7 April 2026 laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for the remote onboarding of users to the European Digital Identity Wallets by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures where the combination meets the requirements of assurance level high.
- IV. Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 regarding person identification data issued to European Digital Identity Wallets, in particular Articles 3 and 5 thereof;
- V. Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the certification of European Digital Identity Wallets, in particular Articles 3 and 8 thereof and Annex I thereto;
- VI. 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;
- VII. 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, in particular Articles 3 and 4 thereof, insofar as they impose obligations on PID providers regarding issuance protocols and cryptographic security;
- VIII. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. 2024 r. poz. 1275 z późn. zm.);

- IX. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.).

7 For the interpretation of the requirements derived from CIR (EU) 2015/1502, the Guidance for the application of the levels of assurance which support the eIDAS Regulation, developed by the eIDAS Cooperation Network, has been taken into account. References to this guidance document are informative only.

2.2 Normative references

- I. [18098] CEN/TS 18098:2026 - Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets
- II. EDICG Architecture and Reference Framework (ARF) v2.8.0 (April 2026);
- III. ETSI TS 119 461 v2.1.1 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- IV. ISO/IEC 15408-1:2022 — Common Criteria for Information Technology Security Evaluation — Part 1: Introduction and general model;
- V. Common Evaluation Methodology for Information Technology Security Evaluation (CEM:2022), Revision 1;
- VI. ISO/IEC 19989-3 — Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection;
- VII. [18099] CEN/TS 18099 — Biometric data injection attack detection.

8

3 Terms and Definitions

9 For the purposes of this document, the terms and definitions given in G-02 (Vocabulary) apply.

4 General Principles

4.1 Proportionality to risk

- 10 Under Sections 2.1 and 2.2 of the Annex to CIR (EU) 2015/1502, all provisions in this document apply at assurance level high. Accordingly, the requirements for enrolment, identity proofing, issuance, and life-cycle management are more stringent than those applicable at assurance levels substantial or low. Where remote onboarding is performed using an electronic identification means at assurance level substantial together with additional remote onboarding procedures, the combined process shall meet the requirements of assurance level high in accordance with CIR (EU) 2026/798.
- 11 PID Providers shall take due account of the risks specific to the person identification data they issue, including the risks listed in Annex I to CIR (EU) 2024/2981, when implementing the provisions of this document. The overall PID provider IT solution shall be tested to be resistant against an attacker with high attack potential, where the attack potential is evaluated as specified in CEM:2022.

4.2 Auditability

- 12 This document is intended for use within the eID Certification Scheme (GP-03) as defined in ISO/IEC 17067. Conformity Assessment Bodies (CABs) shall be accredited against ISO/IEC 17065, complemented by ETSI EN 319 403-1, pursuant to G-05. PID providers shall ensure that their implementation of the provisions specified in this document is documented, traceable and verifiable by an independent third party.

4.3 National law

- 13 Where national law imposes requirements that are more stringent than or additional to those set out in this document, the PID Provider shall comply with the applicable national law. Where this document permits flexibility or defers to national arrangements, the PID Provider shall document the applicable national provisions and demonstrate compliance with them.

4.4 Normative language

- 14 The normative terms "shall", "should" and "may" are used in this document in accordance with the conventions described in Section 3. Where a PID provider considers that a recommendation ("should") is not applicable or feasible in its specific context, the PID provider shall document and substantiate the reasons for the deviation.

4.5 Relationship with WZ-03-02, WP-03-02 and WP-03-03

- 15 The PID Provider is a service provider within the scope of WZ-03-02 (Organisational and Technical Requirements for PID Providers). WZ-03-02 specifies the organisational information security requirements that apply to PID providers, including requirements related to information security management, risk management, incident management, personnel, physical security, and technological controls. The present document specifies requirements for PID enrolment, identity proofing, remote onboarding, PID issuance and PID lifecycle management. Requirements for Wallet Unit activation, provisioning and lifecycle are specified in WP-03-02. Requirements for the eID means and authentication mechanisms are specified in WP-03-03. Compliance with this document does not replace the requirements of WZ-03-02, WP-03-02 or WP-03-03 and vice versa.

5 Legal Requirements

16 *NOTE: This section lists, at a granular level, all legal requirements applicable to PID providers in the scope of this document. Each requirement is assigned a unique identifier to ensure traceability. The provisions in Section 6 are mapped to these requirements in the Annex.*

5.1 Requirements derived from Regulation (EU) No 910/2014 as amended.

17 *NOTE: The following requirements are derived from Regulation (EU) No 910/2014 of the European Parliament and of the Council, as amended by Regulation (EU) 2024/1183, in particular Article 5a thereof, insofar as they impose obligations relevant to the enrolment and issuance of person identification data.*

Identifier	Requirement
REQ-910-01	European Digital Identity Wallets shall support common protocols and interfaces for issuance of person identification data. [Article 5a(5)(a)(i)]
REQ-910-02	European Digital Identity Wallets shall securely onboard the user by using an electronic identification means in accordance with Article 5a (24). [Article 5a(5)(a)(iii)]
REQ-910-03	European Digital Identity Wallets shall meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication. [Article 5a(5)(d)]
REQ-910-04	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)]
REQ-910-05	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)]
REQ-910-06	Users shall be onboarded to the European Digital Identity Wallet by electronic identification means conforming to assurance level high, or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high. [Article 5a (24)]

5.2 Requirements derived from CIR (EU) 2015/1502

18

NOTE: The following requirements are derived from Sections 2.1 (Enrolment) and 2.2 (Electronic identification means management) of the Annex to CIR (EU) 2015/1502, at assurance level high. In accordance with the structure of that Annex, the requirements at level high incorporate the requirements at levels low and substantial.

Identifier	Requirement
REQ-1502-01	Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. [Annex, Section 2.1.1, Level Low, Element 1]
REQ-1502-02	Ensure the applicant is aware of recommended security precautions related to the electronic identification means. [Annex, Section 2.1.1, Level Low, Element 2]
REQ-1502-03	Collect the relevant identity data required for identity proofing and verification. [Annex, Section 2.1.1, Level Low, Element 3]
REQ-1502-04	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)]
REQ-1502-05	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-1502-06	It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner. [Annex, Section 2.2.3, Level Low, Element 1]
REQ-1502-07	The existence of measures taken to prevent unauthorised suspension, revocation, and/or reactivation. [Annex, Section 2.2.3, Level Low, Element 2]
REQ-1502-08	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]
REQ-1502-09	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 means of the same, or higher, assurance level. [Annex, Section 2.2.4, Level Low]

Identifier	Requirement
REQ-1502-10	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]
REQ-1502-11	Where identity proofing and verification is performed for assurance level high, the PID Provider shall ensure that the requirements applicable to assurance level substantial are fulfilled before applying the additional requirements for assurance level high. [Annex, Section 2.1.2, Level High]
REQ-1502-12	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)]
REQ-1502-13	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 body or equivalent body, and that the results of those procedures remain valid. [Annex, Section 2.1.2, Level High, Point 1(b)]
REQ-1502-14	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]

5.3 Requirements derived from CIR (EU) 2024/2977

19 *NOTE: The following requirements are derived from Commission Implementing Regulation (EU) 2024/2977, which specifies requirements regarding person identification data issued to European Digital Identity Wallets. Article 3(6) (obligation on Member States to publish a list of supported wallet solutions) and Article 5(8) (privacy preserving techniques for unlink ability) are not listed below: Article 3(6) imposes an obligation on the Member State, not on the PID provider; Article 5(8) is a functional requirement addressed in GP-01.*

Identifier	Requirement
REQ-2977-01	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)]
REQ-2977-02	Providers of person identification data shall ensure that person identification data issued to wallet units contains the information necessary for authentication and validation of the person identification data. [Article 3(2)]

Identifier	Requirement
REQ-2977-03	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)]
REQ-2977-04	Member States shall ensure that the person identification data issued to a given wallet user is unique for the Member State. [Article 3(4)]
REQ-2977-05	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)]
REQ-2977-06	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)]
REQ-2977-07	When issuing person identification data to wallet units, providers of person identification data 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. [Article 3(8)]
REQ-2977-08	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)]
REQ-2977-09	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 such person identification data can be revoked without delay. [Article 5(1)]
REQ-2977-10	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)]
REQ-2977-11	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 situations determined by the providers in their policies. [Article 5(4)]
REQ-2977-12	Providers of person identification data issued to a wallet unit shall ensure that revocations cannot be reverted. [Article 5(5)]
REQ-2977-13	The revoked person identification data shall remain accessible for as long as required by Union law or national law. [Article 5(6)]

Identifier	Requirement
REQ-2977-14	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)]
REQ-2977-15	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)]

5.4 Requirements derived from CIR (EU) 2026/798

20 *NOTE: The following requirements are derived from Commission Implementing Regulation (EU) 2026/798, which specifies reference standards and specifications for the remote onboarding of users to European Digital Identity Wallets by electronic identification means at assurance level substantial together with additional remote onboarding procedures, where the combination meets the requirements of assurance level high.*

Identifier	Requirement
REQ-798-01	The PID Provider shall ensure that conformity of the remote identity proofing process is assessed against the 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. [Annex, Sections 1 and 2]
REQ-798-02	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)]
REQ-798-03	The PID Provider shall ensure that measures implementing data protection by design and by default are applied during the onboarding 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. [Annex, Section 2, Point (8)]
REQ-798-04	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

Identifier	Requirement
	based on a certification audit and a 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. [Annex, Section 2, Point (9)]
REQ-798-05	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)]
REQ-798-06	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)]
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 the process shall perform passive or active authentication of the chip in the physical identity document. [Annex, Section 2, Point (11)]
REQ-798-08	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)]
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 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)]
REQ-798-10	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 electronic identification means was not initially issued in reliance on automated comparison between face images. [Annex, Section 2, Point (14)]
REQ-798-11	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)]
REQ-798-12	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 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

Identifier	Requirement
	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. [Annex, Section 2, Point (16)]

6 Provisions

21 *NOTE 1: Description of the PID lifecycle is provided in Annex B.*

22 *NOTE 2: The provisions in this chapter implement the legal requirements Chapter 5. CEN/TS 18098, Clause 5 is used as a supporting technical reference where indicated.*

6.1 PID Issuance

23 *NOTE: This section defines the core requirements for the initialization and execution of the Person Identification Data (PID) issuance process by the PID Provider.*

PDP-01

24 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.

25 *[REQ-1502-01; REQ-1502-02]*

PDP-02

26 The PID Provider shall collect the identity data necessary for identity proofing and verification.

27 *[REQ-1502-03]*

PDP-03

28 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.

29 *[REQ-910-03; REQ-2977-06; REQ-1502-11-REQ-1502-14]*

PDP-04

30 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.

31 *[REQ-910-06; REQ-798-01]*

PDP-05

32 The PID Provider shall verify that the evidence used in the identity proofing process is valid at the time of identity proofing.

33 *[REQ-798-05]*

PDP-06

34 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.

35 *[REQ-798-04]*

PDP-07

36 The PID Provider shall present to the User the identity verification methods supported for the PID issuance process.

37 *[REQ-2977-06]*

PDP-08

38 The PID Provider shall execute the identity verification process using the method selected by the User.

39 *[REQ-2977-06]*

PDP-09

40 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.

41 *[REQ-798-02]*

PDP-10

42 The PID Provider shall apply data protection by design and by default during the onboarding 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.

43 *[REQ-798-03]*

PDP-11

44 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.

45 *[REQ-798-06]*

PDP-12

46 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.

47 *[REQ-798-07]*

PDP-13

48 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.

49 *[REQ-798-09]*

PDP-14

50 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.

51 *[REQ-798-08]*

PDP-15

52 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.

53 *[REQ-798-10]*

PDP-16

54 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.

55 *[REQ-798-11]*

PDP-17

56 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.

57 *[REQ-798-12]*

PDP-18

58 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.

59 *[REQ-910-03; REQ-910-06; REQ-2977-06]*

6.2 Binding PID with Wallet Unit

60 *NOTE: This section specifies the requirements applicable to the PID Provider for issuing PID to and cryptographically binding PID with an activated Wallet Unit. Identity proofing and verification shall be completed in accordance with Section 6.1 before PID is issued.*

PDP-19

61 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.

62 *[REQ-2977-07; CEN/TS 18098]*

PDP-20

63 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.

64 *[REQ-2977-08; CEN/TS 18098]*

PDP-21

65 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.

66 *[REQ-2977-05; CEN/TS 18098]*

PDP-22

67 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.

68 *[REQ-2977-03; REQ-2977-05; CEN/TS 18098]*

PDP-23

69 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.

70 *[REQ-2977-05; CEN/TS 18098]*

PDP-24

71 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.

72 *[REQ-910-03; REQ-2977-08; CEN/TS 18098]*

PDP-25

73 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.

74 *[REQ-910-03; REQ-2977-08; CEN/TS 18098]*

PDP-26

75 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 PID Provider shall reject the request and terminate the binding process without issuing PID.

76 *[REQ-2977-05; REQ-2977-08; CEN/TS 18098]*

PDP-27

77 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.

78 *[REQ-2977-01; REQ-2977-02; REQ-2977-03; CEN/TS 18098]*

PDP-28

79 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.

80 *[REQ-2977-05; CEN/TS 18098]*

6.3 PID Maintenance

81 *NOTE: This section sets out the requirements for the lifecycle maintenance, security incident management, and status modification of the issued Person Identification Data (PID).*

PDP-29

82 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.

83 *[REQ-2977-09]*

PDP-30

84 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.

85 *[REQ-2977-09; REQ-2977-11; REQ-1502-06; CEN/TS 18098]*

PDP-31

86 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.

87 *[REQ-2977-11; REQ-1502-06; REQ-1502-09; CEN/TS 18098]*

PDP-32

88 Upon receiving a user-initiated trigger, the PID Provider shall execute a problem analysis sequence to determine status modification parameters.

89 *[REQ-2977-09; REQ-2977-11; CEN/TS 18098]*

PDP-33

90 The PID Provider shall evaluate whether an invalidation or a formal change of the PID status is required.

91 *[REQ-2977-09; REQ-2977-11; REQ-1502-06; REQ-1502-09; CEN/TS 18098]*

PDP-34

92 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.

93 *[CEN/TS 18098]*

PDP-35

94 The PID Provider shall ensure that PID can be suspended and revoked in a timely and effective manner.

95 *[REQ-1502-06]*

PDP-36

96 The PID Provider shall implement measures preventing unauthorised suspension, revocation and reactivation of PID.

97 *[REQ-1502-07]*

PDP-37

98 The PID Provider shall reactivate suspended PID only where the same assurance requirements as those established before the suspension continue to be fulfilled.

99 *[REQ-1502-08]*

PDP-38

100 The PID Provider shall revoke only PID issued by that PID Provider.

101 *[REQ-2977-15]*

PDP-39

102 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 Attestation has been revoked; or

c) in other circumstances defined in the PID Provider's validity status management policy.

103 *[REQ-2977-11]*

PDP-40

104 The PID Provider shall ensure that revocation of PID cannot be reverted.

105 *[REQ-2977-12]*

PDP-41

106 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 information shall be concise, easily accessible and provided using clear and plain language.

107 *[REQ-2977-10]*

PDP-42

108 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.

109 *[REQ-2977-14]*

PDP-43

110 The PID Provider shall ensure that revoked PID remains accessible for as long as required by Union law or national law.

111 *[REQ-2977-13]*

PDP-44

112 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.

113 *[REQ-1502-09]*

PDP-45

114 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.

115 *[REQ-1502-10]*

Annex A (Informative) Mapping of Provisions to Legal Requirements

Provision	Legal Requirements
PDP-01	CEN TS 18098-4: REQ-7.3.1
PDP-02	CEN TS 18098-4: REQ-7.3.2; REQ-7.3.3; REQ-7.3.4; REQ-7.3.5
PDP-02a	CEN TS 18098-4: REQ-7.3.2
PDP-03	CEN TS 18098-4: Clause 7.4
PDP-04	CEN TS 18098-4: CREQ 7.5.2
PDP-04a	CEN TS 18098-4: Clause 7.5
PDP-05	CEN TS 18098-4: REQ-7.7.4; REQ-7.7.5
PDP-06	CEN TS 18098-4: REQ-7.7.6
PDP-06a	CEN TS 18098-4: REQ-7.7.6
PDP-07	CEN TS 18098-4: REQ-7.7.7
PDP-08	[REQ-TO_BE_COMPLETED]
PDP-09	[REQ-TO_BE_COMPLETED]
PDP-09	[REQ-TO_BE_COMPLETED]
PDP-10	[REQ-TO_BE_COMPLETED]
PDP-11	[REQ-TO_BE_COMPLETED]
PDP-12	[REQ-TO_BE_COMPLETED]
PDP-12a	[REQ-TO_BE_COMPLETED]
PDP-13	[REQ-TO_BE_COMPLETED]
PDP-14	[REQ-TO_BE_COMPLETED]

Annex B (informative) Description of PID lifecycle

A. Introduction

- 116
- The issuer of the person identification data (PID) provides a central function in the European Digital Identity Wallet (EUDIW) ecosystem. Once the PID has been issued to and installed onto the user's device, it can be used to identify the holder of an EUDIW against external entities, including relying parties. The PID comes in the form of a cryptographically sealed dataset, securely bound to the Wallet Unit.
- 117
- The PID Provider is responsible for the whole PID issuance process, including any parts delegated to third parties such as an Identity Verification Provider (IDVP). Where the PID Provider delegates any part of the process, it shall remain responsible for the fulfilment of all requirements of this document as if it had performed the activities itself.
- 118
- Figure 1 illustrates the PID lifecycle and its relationships to Wallet Unit showing how the application activation step link with the issuance and management of the user's digital identity.
- 119
- NOTE: Numbers used in subsequent figures refer to CEN TS 18098-4 Requirements for PID Providers; this document is currently at early stage of development the figures and accompanying description are subject to change in the future.*

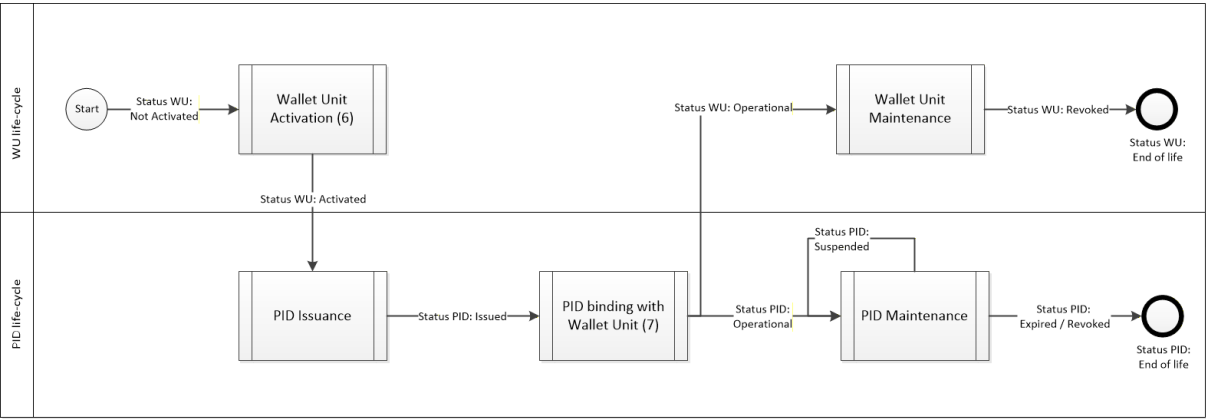


Figure 1 Relationship between PID and Wallet Unit in their lifecycles

- 120
- The processes run in two parallel tracks: Wallet Unit Lifecycle Track and the PID lifecycle track. Relationships of these tracks are defined by binding the PID to the Walet Unit of the PID holder (User).

- 125 The process starts with the User action, upon receiving the message that the Wallet Unit on his/her smartphone is activated.
- 126 The PID Provider presents supported identity verification methods to the User (if more than one available).
- 127 The PID Provider executes the User identity verification process based on the method selected by the User.
- 128 Upon successful completion of the verification process the PID Provider authenticates the Wallet Unit.
- 129 Following Wallet Unit authentication, the PID Provider shall verify the binding between the authenticated user and the Wallet Unit. To complete this step the Wallet Unit shall request the User to set the PID key authentication factors (knowledge-based, possession-based, or inherent).
- 130 In the next step, the Wallet Unit generates a cryptographic key pair dedicated exclusively to the PID credential.
- 131 Further, the Wallet Unit generates and sends a formal credential request payload to the PID Provider, incorporating the Wallet Unit Validity Attestation, the Wallet Unit Trust Attestation, the freshly generated PID public key, the Proof of Association (PoA), and the Proof of Possession (PoP), all of which are collected by the PID Provider.
- 132 After successful verification of the strength of authentication mechanisms presented by the Wallet Unit, the Wallet Unit requests the PID in expected format.
- 133 The PID provider delivers the PID which is successfully bound to the Wallet Unit. By completing this step, the status of Wallet Unit is changed to “operational”.
- D. PID Maintenance**
- 134 Several events that can occur in the PID maintenance phase have impact on the D lifecycle. The process is presented in Figure 3.

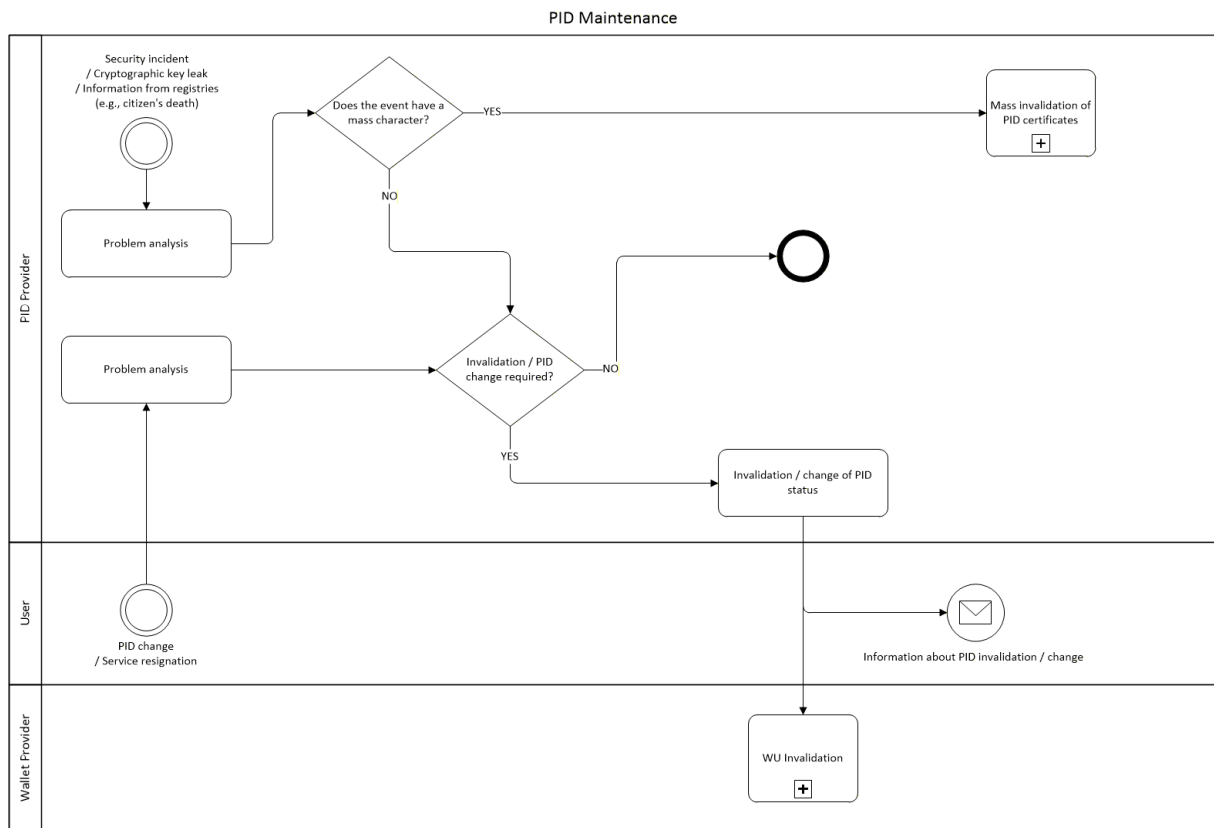


Figure 3 PID Maintenance phase

- 135 The maintenance process is executed across three operational tracks involving the PID Provider, the User, and the Wallet Provider.
- 136 The PID Provider responds to various triggers, including security incidents, cryptographic key leakage, or critical updates received from external official registries.
- 137 The PID Provider assesses whether the analysed security or registry event have a massive impact. In such cases the PID provider a massive invalidation of the affected PID attestations.
- 138 In case of some security incidents or changes to the credential status, the PID track permits the temporary suspension of the digital identity (Status PID: Suspended) while the Wallet Unit remains unaffected and operational on the user's device.
- 139 If the cause of the PID provider action is the User request (e.g., PID change, discarding the service) the PID is invalidated, and appropriate message is sent to the Wallet Unit.