

WP-03-02

PL EUDI Wallet Certification System

EUDI Wallet Unit Provisioning and Lifecycle

Requirements

VERSION 1.01

2026.06.12

Document reference	WP-03-02
Version	1.01
Status	FINAL
Date	02.06.2026
Document type	Certification Scheme — Process 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	EUDI Wallet unit provisioning and lifecycle management
Primary audience	EUDI Wallet Provider
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

Table of content	3
1 Scope.....	4
2 Legal Basis	5
2.1 Legal acts	5
2.2 Normative references	5
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 WP-03-01, WP-03-03, GP-01 and GP-02	8
5 Legal Requirements	10
5.1 Requirements derived from Regulation (EU) No 910/2014 as amended	10
5.2 Requirements derived from CIR (EU) 2024/2979.....	11
5.3 Requirements derived from CIR (EU) 2024/2981.....	12
5.4 Requirements derived from CIR (EU) 2015/1502.....	12
6 Provisions	14
6.1 User Account creation	14
6.2 Wallet Unit activation	14
6.3 PID binding with Wallet Unit.....	18
6.4 Wallet Unit maintenance	20
6.5 Common security and authentication factors	24
Annex A (Informative) — Mapping of Provisions to Legal Requirements.....	27
Annex B (Informative) — Wallet Unit lifecycle	29
6.6 Wallet Unit maintenance	33

1 Scope

- 1 The present document specifies the requirements for the provisioning and life-cycle management of Wallet Units within the EUDI Wallet ecosystem, for the purposes of certification under the eID Certification Scheme (GP-03).
- 2 This document applies to Wallet Providers that provide Wallet Solutions to Wallet Users.
- 3 This document covers the following processes:
 - Wallet Unit activation;
 - PID binding with Wallet Unit;
 - Wallet Unit maintenance.
- 4 The organisational and management system requirements applicable to Wallet Providers are specified in WZ-03-01 and WZ-03-03. The present document addresses the process-specific requirements for Wallet Unit provisioning and life-cycle management. The functional and security requirements for the Wallet Solution as a product are specified in GP-01 and GP-02.
- 5 The process described in this document covers the Wallet Provider and Wallet Unit obligations required to support the technical binding of PID to a specific Wallet Unit. It does not cover the issuance of PID itself, the uniqueness of PID, or the responsibility of the PID Provider for identity proofing and PID issuance, which are addressed in WP-03-01.
- 6 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 Wallet Provider conformity within the eID Certification Scheme (GP-03) as defined in ISO/IEC 17067.

2 Legal Basis

2.1 Legal acts

7 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) 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, 4, 6, 7, 9 and 13 thereof;
- III. 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 Article 8 thereof and Annex I thereto;
- IV. Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015, in particular Sections 2.1.1, 2.2.1 and 2.2.3 of the Annex thereto;
- V. 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;
- VI. Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. 2024 r. poz. 1275 z późn. zm.);
- VII. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.).

8 *NOTE: 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 considered. References to this guidance document are informative only.*

2.2 Normative references

- [18098] CEN/TS 18098:2026 - Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets
- [18098-4] FprCEN/TS 18098 — Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets, Part 4: Requirements for Wallet Provider (2025);

- [15408] ISO/IEC 15408-1:2022 — Common Criteria for Information Technology Security Evaluation — Part 1: Introduction and general model;
- [CEM2022] Common Evaluation Methodology for Information Technology Security Evaluation (CEM:2022), Revision 1;

3 Terms and Definitions

9 For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and G-02 (Vocabulary) apply, together with the following:

Eligibility fulfilment of policy-defined criteria by the User, User's device, Wallet Unit or Wallet Provider, as applicable, allowing the relevant process to continue.

Note to entry: Eligibility checks may concern legal, organisational, technical, security or compatibility criteria.

User Account account at the Wallet Provider system allowing the Wallet User to request management operations of the Wallet Unit after successful authentication

Wallet Unit activation process where the Wallet Unit is installed or configured, then bound to the User and the User's device, initialized and equipped with the required Wallet Unit attestations and Wallet keys

PID binding with Wallet Unit process where the Wallet Unit generates or provides information needed by the PID Provider to cryptographically bind PID to the Wallet Unit

Note to entry: PID issuance itself remains outside the process.

4 General Principles

4.1 Proportionality to risk

10 In accordance with Sections 2.1 and 2.2 of the Annex to CIR (EU) 2015/1502, all provisions in this document shall be understood as requirements at assurance level high. This implies a higher degree of rigour in the provisioning and life-cycle management processes than would be expected at assurance levels substantial or low.

11 Wallet Providers shall take due account of the risks specific to the Wallet Solutions they provide, including the risks listed in Annex I to CIR (EU) 2024/2981, when implementing the provisions of this document. The overall wallet provider 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. Certification bodies assessing conformity with this document shall be accredited against ISO/IEC 17065, complemented by ETSI EN 319 403-1, pursuant to G-05. Wallet Providers shall therefore ensure that their implementation of the provisions 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 wallet provider shall comply with the applicable national law. Where this document permits flexibility or defers to national arrangements, the Wallet 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 Wallet Provider considers that a recommendation ("should") is not applicable or feasible in its specific context, the Wallet Provider shall document and substantiate the reasons for the deviation.

4.5 Relationship with WP-03-01, WP-03-03, GP-01 and GP-02

15 This document defines requirements applicable to the Wallet Provider and Wallet Unit related processes. PID Provider obligations for identity proofing and PID issuance are defined in WP-03-01. Requirements for eID means and authentication mechanisms are defined in WP-03-03. Product-level Wallet

Solution functional and security requirements are defined in GP-01 and GP-02 and their subsidiary documents Compliance with requirements included in this document does not replace the requirements of those documents and vice versa.

5 Legal Requirements

16 *NOTE: This section lists, at a granular level, all legal requirements applicable to wallet providers in scope of this document. Each requirement is assigned a unique identifier for traceability. The provisions in Section 6 are mapped to these requirements. The listed requirements concern Wallet Unit activation, PID binding with Wallet Unit and Wallet Unit maintenance. Product-only or PID-issuance-only requirements are included only where they define a process boundary or a process prerequisite relevant to WP-03-02.*

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

Identifier	Requirement
REQ-910-01	European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to securely request, obtain, store, delete, share and present, under the sole control of the user, person identification data and electronic attestations of attributes. [Article 5a(4)(a)]
REQ-910-02	European Digital Identity Wallets shall enable the user to download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations. [Article 5a(4)(f)]
REQ-910-03	European Digital Identity Wallets shall enable the user to exercise the user's rights to data portability. [Article 5a(4)(g)]
REQ-910-04	European Digital Identity Wallets shall support common protocols and interfaces for issuance of person identification data. [Article 5a(5)(a)(i)]
REQ-910-05	Wallet Provider shall provide Mechanisms that allow verification of the authenticity and validity of European Digital Identity Wallets. 5a(8)(a)
REQ-910-06	The validity of the European Digital Identity Wallet shall be revocable upon explicit user request, where the Wallet security has been compromised, or upon death of the user / cessation of activity of the legal person. Art. 5a(9)
REQ-910-07	European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high. [Art. 5a(11)]
REQ-910-08	European Digital Identity Wallets shall ensure security by design. [Art. 5a(11)]
REQ-910-09	Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider. If the European Digital Identity Wallet is provided by private parties, the provisions of Article 45h(3) shall apply mutatis mutandis, requiring functional separation from other services. [Article 5a(14)]

Identifier	Requirement
REQ-910-10	Where a Wallet, validation mechanism or underlying eID scheme is breached or compromised in a way affecting reliability, provision and use of affected Wallets shall be suspended, and where justified or not remedied, withdrawn and revoked. [Article 5e]

5.2 Requirements derived from CIR (EU) 2024/2979

17 The following requirements are derived from Commission Implementing Regulation (EU) 2024/2979. Requirements that impose obligations primarily on the wallet unit as a product (Articles 3(1), 4(1), 4(3), 5, 8, 9(1)–(2), 10, 11, 12, 14) are addressed in GP-01 and GP-02 and are not listed below.

Identifier	Requirement
REQ-2979-01	Wallet providers shall, for each wallet unit, sign or seal at least one wallet unit attestation compliant with the requirements laid down in Article 6. The certificate used to sign or seal the wallet unit attestation shall be issued under a certificate listed in the trusted list. [Article 3(2)]
REQ-2979-02	Wallet providers shall ensure integrity, authenticity and confidentiality of the communication between wallet instances and wallet secure cryptographic applications. [Article 4(2)]
REQ-2979-03	Wallet providers shall ensure that each wallet unit contains wallet unit attestations. [Article 6(1)]
REQ-2979-04	Wallet providers shall ensure that the wallet unit attestations contain public keys and that the corresponding private keys are protected by a wallet secure cryptographic device. [Article 6(2)]
REQ-2979-05	Wallet providers shall inform wallet users of their rights and obligations in relation to their wallet unit. [Article 6(3)(a)]
REQ-2979-06	Wallet providers shall provide mechanisms, independent of wallet units, for the secure identification and authentication of wallet users. [Article 6(3)(b)]
REQ-2979-07	Wallet providers shall ensure wallet users have the right to request revocation of their wallet unit attestations, using the authentication mechanisms referred to in Article 6(3)(b). [Article 6(3)(c)]
REQ-2979-08	Wallet providers shall be the only entities capable of revoking wallet unit attestations for wallet units that they have provided. [Article 7(1)]
REQ-2979-09	Wallet providers shall establish a publicly available policy specifying the conditions and the timeframe for the revocation of wallet unit attestations. [Article 7(2)]
REQ-2979-10	Where wallet providers have revoked wallet unit attestations, they shall inform affected wallet users within 24 hours of the revocation, including the reason for the revocation and the consequences for the wallet user, in a manner that is concise, easily accessible and using clear and plain language. [Article 7(3)]

Identifier	Requirement
REQ-2979-11	Where wallet providers have revoked wallet unit attestations, they shall make publicly available the validity status of the wallet unit attestation in a privacy preserving manner and describe the location of that information in the wallet unit attestation. [Article 7(4)]
REQ-2979-12	The logs shall be accessible to the wallet provider, where it is necessary for the provision of wallet services, on the basis of explicit prior consent by the wallet user. [Article 9(5)]
REQ-2979-13	Wallet providers shall ensure integrity, authenticity and confidentiality of the logged information. [Article 9(3)]
REQ-2979-14	Wallet providers shall enable wallet users to export the logged information. [Article 9(7)]
REQ-2979-15	Wallet units shall, where technically feasible and excepting cases of critical assets, support secure export and portability of personal data of the wallet user, to allow the wallet user to migrate to a wallet unit of a different wallet solution in a way that ensures level of assurance high. [Article 13]

5.3 Requirements derived from CIR (EU) 2024/2981

18 *NOTE: The following requirements are derived from Commission Implementing Regulation (EU) 2024/2981. Requirements that impose obligations primarily on the wallet unit as a product are addressed in GP-01 and GP-02 and are not listed below.*

Identifier	Requirement
REQ-2981-01	Wallet Providers shall complement the scheme risk assessment with implementation-specific risks and treatment measures. [Article 4(4)d]
REQ-2981-02	Wallet providers shall establish, maintain and operate vulnerability management policies and procedures, including disclosure and registration of publicly known and remediated vulnerabilities. [Article 5]
REQ-2981-03	Wallet providers shall establish and implement policies and procedures for risk management, change management, vulnerability management and personnel management relevant to operation of the Wallet Solution. [Article 8(3)b]

5.4 Requirements derived from CIR (EU) 2015/1502

Identifier	Requirement
REQ-1502-01	Wallet Provider shall ensure the wallet user is aware of the terms and conditions related to the use of the electronic identification means. [Annex, Section 2.1.1, All levels, Element 1]

Identifier	Requirement
REQ-1502-02	Wallet Provider shall ensure the wallet user is aware of recommended security precautions related to the electronic identification means. [Annex, Section 2.1.1, All levels, Element 2]
REQ-1502-03	Wallet Provider shall ensure that the electronic identification means utilises at least two authentication factors from different categories. [Annex, Section 2.2.1, Level Substantial, Element 1]
REQ-1502-04	Wallet Provider shall ensure that the electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs. [Annex, Section 2.2.1, Level Substantial, Element 2]
REQ-1502-05	Wallet Provider shall ensure that the activation process includes mechanisms verifying that e electronic identification means has been delivered only into the possession of the person to whom it belongs.
REQ-1502-06	The Wallet Provider shall ensure mechanisms for suspending or revoking an electronic identification means in a timely and effective manner. [Annex, Section 2.2.3, All levels, Element 1]
REQ-1502-07	Wallet Provider shall implement measures that prevent unauthorised suspension, revocation and/or reactivation. [Annex, Section 2.2.3, All levels, Element 2]
REQ-1502-08	Wallet Provider shall implement mechanisms for reactivation only if the same assurance requirements as established before the suspension or revocation continue to be met. [Annex, Section 2.2.3, All levels, Element 3]
REQ-1502-09	Wallet Provider shall ensure that where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including offline analysis. 3Wallet Provider shall implement security controls to the authentication mechanisms and verification , so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with hig attack potential can subvert the authentication mechanisms.

6 Provisions

19 *NOTE 1: Description of the Wallet Unit lifecycle is provided in Annex B.*

20 *NOTE 2: All technical requirements are derived from the CEN/TS 18098(Working Draft).*

6.1 User Account creation

WPP-00

21 The Wallet Provider shall request from the User the evidence required to determine User eligibility for Wallet Unit provisioning. The Wallet Provider shall document the eligibility evidence accepted and the decision criteria applied. Where a User Account is created or used for Wallet Unit provisioning or lifecycle management, the Wallet Provider shall ensure that the authentication mechanism used by the Wallet User to access the User Account is commensurate with assurance level high. The authentication mechanism shall be documented and justified by a risk assessment.

22 [CEN/TS 18098-4 6.1.1, 6.1.2]

6.2 Wallet Unit activation

23 *NOTE: This section defines the core requirements for the Wallet Unit activation process executed by the Wallet Provider.*

WPP-01

24 The Wallet Provider shall make the Wallet Unit software application available to the user to enable the download and initiation of the local installation sequence.

25 [CEN TS 18098-4: REQ-6.2.1]

WPP-01a

26 Wallet Unit activation shall support secure onboarding interfaces required for eID-based onboarding under the electronic identification scheme. Where the identity proofing or authentication part is performed under WP-03-01 or WP-03-03, the Wallet Provider shall ensure that the Wallet Unit activation process exposes the required technical interfaces and preserves the security properties required for assurance level high.

27 [Reg. 910/2014 Art. 5a]

28

WPP-02

29 Upon the downloading and launching of the installation sequence by the user, the Wallet Provider shall perform a technical verification of the user's device. This verification shall check whether the device meets the mandatory hardware capabilities, security features, and deployment policies necessary for the operation of the Wallet Unit.

30 *[CEN TS 18098-4: REQ-6.3.2.2.2.1; REQ-6.3.2.2.2.2]*

WPP-02a

31 Where the device fails to meet the technical requirements evaluated under WPP-02, the Wallet Provider shall immediately terminate the activation process and notify the user of the device's failure to meet the required technical and eligibility criteria.

32 *[CEN TS 18098-4: REQ-6.3.2.2.2.2 REQ-6.3.2.2.2.3; REQ-6.3.2.2.2.4]*

WPP-03

33 Where the user's device is successfully verified, the Wallet Provider shall execute a mandatory device integrity check. This check shall confirm that the host operating system and system security structures have not been modified or compromised through mechanisms such as rooting or jailbreaking.

34 *[CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.2]*

WPP-03a

35 Where the device integrity verification under WPP-03 fails, the Wallet Provider shall immediately terminate the activation process and notify the user of the reason(s) why the device integrity checks failed based on the specification of the Wallet Solution.

36 *[CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.3]*

WPP-04

37 Once the device's integrity has been successfully verified, the Wallet Unit shall allow the user to select and configure the authentication factors used to protect the wallet. Supported methods include PINs, passwords, or device-supported biometrics.

38 *NOTE — The selected mechanisms are then used to strictly control access to the cryptographic keys stored in the Wallet Unit.*

39 *[CEN TS 18098-4: REQ-6.3.5.1]*

WPP-05

40 The Wallet Provider shall execute a cryptographic verification to validate the binding of the client application to the user's. This verification shall confirm that the application executes genuinely on the verified device, is not malicious, and has not been tampered with.

41 *[CEN TS 18098-4: REQ-6.3.3.1]*

WPP-06

42 Upon successful verification of the application binding, the Wallet Provider shall establish a formal cryptographic relationship linking the User, the user's device, and the Wallet Unit.

43 *[CEN TS 18098-4: REQ-6.3.5.1]*

WPP-07

44 Following the establishment of the cryptographic binding, the Wallet Provider shall initialize the core configuration layer of the Wallet Unit. During this configuration phase, the Wallet Provider shall maintain a secure communication channel that guarantees the absolute integrity, authenticity, and confidentiality of all transmitted data.

45 *[CEN TS 18098-4: REQ-6.4.2]*

WPP-07a

46 Where the wallet solution supports alternative logical or physical storage environments for Person Identification Data (PID), the Wallet Unit shall present the available storage options to the user (Present PID storage options, if applicable).

47 *[CEN TS 18098-4: REQ-6.4.1]*

WPP-07b

48 The Wallet Unit shall process and accept the preferred storage method selected by the user from the options presented under WPP-07a (Select option of the PID storage, if applicable).

49 *[CEN TS 18098-4: REQ-6.4.1]*

WPP-08

50 Upon completion of the configuration layer, the system shall initiate the cryptographic initialization sequence of the Wallet Unit (Initialisation of Wallet Unit).

51 *[CEN TS 18098-4: Clause 6.5]*

WPP-08a

52 The Wallet Unit shall generate localized cryptographic keys within the secure hardware environment of the device (WSCD), and the Wallet Provider shall securely retrieve the generated public keys from the Wallet Unit.

53 *[CEN TS 18098-4: REQ-6.5.1.1; CEN TS 18098-4: REQ-6.5.2.1]*

WPP-08b

54 The Wallet Provider shall retrieve the corresponding Proof of Association (PoA) and Proof of Possession (PoP) tokens for each generated key pair from the Wallet Unit.

55 *[CEN TS 18098-4: REQ-6.5.1.2; CEN TS 18098-4: REQ-6.5.2.2]*

WPP-08c

56 The Wallet Provider shall verify the validity and structural correctness of the received cryptographic proofs. If any verification step fails, the activation process shall be aborted, and no credentials shall be issued.

57 *[CEN TS 18098-4: REQ-6.5.1.3; CEN TS 18098-4: REQ-6.5.2.3]*

WPP-08d

58 Wallet keys and PID keys shall be stored in a WSCD and their cryptographic operations shall be executed in the same WSCD. Cryptographic keys should be stored in a local WSCD where technically feasible. Where cryptographic keys are stored in a remote WSCD, the Wallet Provider shall implement adequate security measures to limit the risk of key compromise. Communication between the WSCD and the WSCA shall be protected for integrity, authenticity and confidentiality.

59 *[CEN/TS 18098-4 10.7, 10.8, 10.9, 10.10]*

WPP-09

60 Upon successful validation of all cryptographic proofs, the Wallet Provider shall issue the Wallet Unit Validity Attestation (WUVA) to confirm the structural and operational validity of the Wallet Unit.

61 *NOTE — In strict compliance with data protection frameworks, the issued WUVA shall incorporate public keys, systemic device profiles, and Wallet Provider identifiers, but shall not contain personal data relating to the user or the prospective PID holder.*

62 [CEN TS 18098-4: REQ-6.5.1.4; CEN TS 18098-4: REQ-6.5.1.5]

WPP-09a

63 Concurrently, the Wallet Provider shall issue one or several Wallet Unit Trust Attestations (WUTA) containing the public keys, Wallet Provider and hardware/software (WSCA/WSCD) environment details, device profiles, and a cryptographic signature, while strictly excluding any personal data relating to the User or the PID Subject.

64 [CEN TS 18098-4: REQ-6.5.2.4; CEN TS 18098-4: REQ-6.5.2.5]

WPP-10

65 Following the successful issuance of both mandatory attestations, the Wallet Provider shall execute the finalization phase. The Wallet Provider shall accept all verified Proof of Possession (PoP) tokens for the generated keys and update all internal systemic registers.

66 [CEN TS 18098-4: Clause 6.6]

WPP-10a

67 Upon successful register updates and acceptance of the token, the system shall transition the operational status of the Wallet Unit to "Activated", thereby completing the onboarding sequence and fulfilling the mandatory prerequisite required to execute the subsequent PID binding process (7).

68 [CEN TS 18098-4: Clause 6.6]

6.3 PID binding with Wallet Unit

1 *NOTE 1: This section sets out the requirements for the initialization and configuration of the Person Identification Data (PID) binding with the Wallet Unit on the user's device.*

WPP-11

69 The Wallet Unit shall enable the user to trigger the sequence by initiating a request to bind the PID credential to the activated Wallet Unit.

70 [CEN TS 18098-4: Clause 7]

WPP-12

71 The Wallet Unit shall process and transmit the specific verification method selected by the user from the options presented by the PID Provider.

72 [CEN TS 18098-4: REQ-7.3.1]

WPP-13

73 Prior to the generation of the PID key, the Wallet Unit shall request the User to set the PID key authentication factors (knowledge-based, possession-based, or inherent).

74 *[CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3]*

WPP-14

75 Following authentication factor configuration, the Wallet Unit shall generate a cryptographic key pair dedicated exclusively to the PID credential.

76 *[CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3]*

WPP-15

77 The Wallet Unit shall generate and send a formal credential request payload to the PID Provider, incorporating the Wallet Unit Validity Attestation, the Wallet Unit Trust Attestation, the freshly generated PID public key, the Proof of Association (PoA), and the Proof of Possession (PoP).

78 *[CEN TS 18098-4: REQ-7.7.1; REQ-7.7.2; REQ-7.7.4; REQ-7.7.5]*

WPP-16

79 The Wallet Unit shall explicitly indicate to the PID Provider in its request for issuance of PID the expected PID format.

80 *[CEN TS 18098-4: REQ-7.7.8]*

WPP-17

81 The Wallet Provider shall collect from the Wallet Unit the expected format specified for the PID credential.

82 *[CEN TS 18098-4: REQ-7.7.9]*

WPP-17a

83 Upon successful collection of the expected format by the Wallet Provider, the PID shall be successfully bound to the Wallet Unit, and the system shall transition the operational status of the Wallet Unit to "operational".

84 *[CEN TS 18098-4: REQ-7.7.9]*

WPP-17b

85 PID binding with Wallet Unit shall establish the technical association between the
PID and the specific Wallet Unit. The uniqueness of PID and the legal
determination of the person represented by PID remain the responsibility of the
PID Provider and the electronic identification scheme under WP-03-01.

86 *[Reg. 910/2014 Art. 5a(5)(f)]*

6.4 Wallet Unit maintenance

87 *NOTE: This section sets out the requirements for the Wallet Unit lifecycle
maintenance, security incident management, and status modification of the Wallet
Unit..*

WPP-18

88 The Wallet Provider shall maintain continuous monitoring capabilities to detect
security incidents affecting the operational integrity of deployed Wallet Units.
The Wallet Provider shall regularly repeat client application genuineness checks,
device capability controls and device integrity controls during the lifespan of the
Wallet Unit and shall justify the control interval based on risk, threat intelligence,
update cadence and the security model of the Wallet Solution.

89 *[CEN/TS 18098-4 10.11, 10.12]*

WPP-19

90 Upon detection of a security incident, the Wallet Provider shall execute an
immediate problem analysis to determine the scope and impact of the issue.

91 *[CIR 2024/2981 Art. 5, 8, 18]*

WPP-20

92 The Wallet Provider shall evaluate whether the analyzed security incident
applies strictly to a single Wallet Unit, a group of Wallet Units, a Wallet Solution
component, a WSCA/WSCD component, a device family or a broader population
of Wallet Users.

93 *[CIR 2024/2981 Annex I risk treatment]*

WPP-20a

94 Where the security incident is determined not to apply to a single unit but
represents vulnerability or compromise with broader impact, the Wallet
Provider shall trigger a mass Wallet Unit Attestation revocation , Wallet Unit
invalidation, forced update, blocking, or other measures proportionate to the
risk.

95 *[Reg. 910/2014 Art. 5e; CIR 2024/2979 Art. 7].*

WPP-21

96 The Wallet Provider shall provide reporting channels to ingest lifecycle events, including scenarios where a smartphone is reported as lost, stolen, or damaged, or the User's will of discarding the service. *Such mechanisms shall be accessible independently of the affected Wallet Unit where necessary.*

97 *[Reg. 910/2014 Art. 5a(10); CIR 2024/2979 Art. 6(3)(b)]*

WPP-22

98 Upon receiving a reported lifecycle event, the Wallet Provider shall perform a problem analysis to evaluate the Wallet Unit status modification requirements. The decision and evidence supporting it shall be recorded.

99 *[CIR 2015/1502 Annex 2.2.3]*

WPP-23

100 Where the status change is confirmed as permanent, the Wallet Provider shall transition the specific Wallet Unit or Wallet Unit Attestation to an end-of-life, revoked or invalid status, as applicable, and shall update the relevant registers and status services.

101 *[CIR 2024/2979 Art. 7; Reg. 910/2014 Art. 5a(9)]*

WPP-23a

102 Where Wallet Unit Attestations are revoked, the Wallet Provider shall inform affected Wallet Users within 24 hours of the revocation, including the reason for the revocation and the consequences for the Wallet User, in a concise, easily accessible and clear manner. Where a Wallet Unit is withdrawn, suspended or otherwise restricted, the Wallet Provider shall provide appropriate user notification consistent with the security context.

103 *[CIR 2024/2979 Art. 7(3)]*

WPP-23b

104 Where Wallet Unit Attestations are revoked, the Wallet Provider shall make publicly available the validity status of the Wallet Unit Attestation in a privacy-preserving manner and shall describe the location of that information in the Wallet Unit Attestation.

105 *[CIR 2024/2979 Art. 7(4)]*

106 The Wallet Provider shall establish and maintain a publicly available policy specifying the conditions and timeframe for revocation of Wallet Unit

Attestations. The policy shall also describe the user request channel, independent user authentication mechanism and consequences of revocation.

107 *[CIR 2024/2979 Art. 7(2), 6(3)(c)]*

WPP-24

108 Where the status change is determined under WPP-23 not to be permanent, the Wallet Provider shall evaluate whether a temporary blocking or suspension is required.

109 *[CIR 2015/1502 Annex 2.2.3]*

WPP-24a

110 Where a temporary blocking is validated, the Wallet Provider shall apply a temporary restriction to the Wallet Unit for a designated period of time.

111 *[CIR 2015/1502 Annex 2.2.3]*

WPP-24b

112 The Wallet Provider shall implement measures to prevent unauthorised suspension, revocation, invalidation, reactivation or unblocking of Wallet Units and Wallet Unit Attestations. Such measures shall include secure user identification and authentication mechanisms independent of the Wallet Unit for user-initiated revocation requests.

113 *[CIR 2015/1502 Annex 2.2.3; CIR 2024/2979 Art. 6(3)(b)-(c)]*

WPP-25

114 The Wallet Provider shall continuously monitor the status of a temporarily blocked Wallet units to verify if the designated blocking time has elapsed.

115 *[CIR 2015/1502 Annex 2.2.3]*

WPP-25a

116 Where the monitored block time has not elapsed, the system shall maintain the temporary block on the Wallet Unit.

117 *[CIR 2015/1502 Annex 2.2.3]*

WPP-25b

118 Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met. Where the conditions for reactivation are not met or the blocking period expires without

remediation, the Wallet Provider shall route the flow to permanent invalidation or revocation as appropriate under WPP-23a.

119 [CIR 2015/1502 Annex 2.2.3]

WPP-26

120 The Wallet Provider shall implement a periodic key renewal process for the Wallet Unit triggered by the expiration of the defined key lifetime. *NOTE — This process governs how the system handles the rotation and regeneration of core cryptographic keys before their security profile degrades.*

121 [CEN/TS 18098-4 10.13 POS; CIR 2024/2981 Art. 8]

WPP-27

122 The Wallet Provider shall establish, maintain and operate vulnerability management, change management and update management policies and procedures. The Wallet Provider shall notify the certification body without undue delay of breaches, compromises, vulnerabilities or changes likely to affect conformity and shall prepare vulnerability impact analysis reports where required. Update mechanisms shall cover every software component of the Wallet Solution and underlying eID scheme within scope.

123 [CIR 2024/2981 Art. 5, 8, 18]

WPP-28

124 The Wallet Provider shall ensure integrity, authenticity and confidentiality of logged information. The logs shall be accessible to the Wallet Provider only where necessary for the provision of Wallet services and on the basis of explicit prior consent by the Wallet User. The Wallet Provider shall enable Wallet Users to export the logged information.

125 [CIR 2024/2979 Art. 9(3), 9(5), 9(7)]

WPP-29

126 Where technically feasible and except for critical assets, Wallet Units shall support secure export and portability of the Wallet User's personal data to allow migration to a Wallet Unit of a different Wallet Solution while preserving assurance level high.

127 [CIR 2024/2979 Art. 13; Reg. 910/2014 Art. 5a(4)(f)-(g)]

WPP-30

128 Relevant information produced during conformity assessment and information provided by the Wallet Provider as certificate holder shall be securely retained

and made available to the certification body or supervisory body upon request. Lifecycle events, status changes, updates, revocations, reactivations and evidence supporting decisions shall be logged and retained according to the certification scheme and applicable law.

129 *[CIR 2024/2981 Art. 19]*

6.5 Common security and authentication factors

WPP-31

130 The Wallet Provider shall ensure that verification of fulfilment of all assurance level high requirements by the Wallet Unit and by the Wallet Provider processes is based on suitable certifications or other suitable evidence. Such evidence shall be documented, traceable and made available to the conformity assessment body.

131 *[CEN/TS 18098-4 9.1]*

WPP-32

132 Where TLS is used during Wallet Unit activation, PID binding or Wallet Unit lifecycle management, the Wallet Provider shall use at least TLS version 1.2 and follow the required cypher suites. Only cryptographic algorithms recognised as secure by ENISA Agreed Cryptographic Algorithms should be used.

133 *[CEN/TS 18098-4 9.2, 9.3, 9.4]*

WPP-33

134 The Wallet Unit shall include additional security measures to protect collected personal data beyond device manufacturer or operating system security. The additional security measures protecting personal data shall be security certified or otherwise evidenced as suitable for assurance level high in accordance with the certification scheme.

135 *[CEN/TS 18098-4 10.1, 10.2]*

WPP-34

136 The Wallet Provider shall ensure that the Wallet Unit is designed so that PID key authentication factors are independent from Wallet Unit authentication factors and from User device authentication factors. A successful authentication to the device or to the Wallet Unit shall not automatically satisfy the authentication requirement for use of the PID key.

137 *[CEN/TS 18098-4 11.1, 11.2]*

WPP-35

138 The Wallet Provider shall ensure that at least one Wallet Unit authentication factor is set and that each Wallet Unit authentication factor is resistant to an attacker with high attack potential. The Wallet Provider shall ensure that use of the PID key requires multi-factor authentication using at least two factors from different categories, and that each PID key authentication factor is resistant to an attacker with high attack potential.

139 *[CEN/TS 18098-4 11.3, 11.4; CIR 2015/1502 Annex 2.2.1]*

WPP-36

140 Where a PIN or password is used as a Wallet Unit authentication factor, account authentication factor or PID key authentication factor, the Wallet Provider shall implement and document a PIN/password complexity policy. The PIN or password shall consist of at least 6 digits or 6 characters and shall allow a maximum of 3 false authentication attempts before blocking or equivalent protective action. The Wallet Provider shall clearly inform the Wallet User of good practices for choosing and managing the PIN or password.

141 *[CEN/TS 18098-4 11.5, 11.6, 11.7]*

WPP-37

142 Where a possession-based authentication factor is used, the Wallet Provider shall ensure that it is resistant to high attack potential against manipulation and duplication, is tamper-resistant, and provides cryptographic functions for secure execution of the authentication protocol. Where PIN/password or biometrics are used as PID key authentication factors, the Wallet Provider shall ensure that the Wallet Unit stores, manages and verifies those factors in the same WSCA/WSCD that stores, manages and uses the corresponding PID key.

143 *[CEN/TS 18098-4 11.10, 11.11]*

WPP-38

144 Where biometrics are used as Wallet Unit authentication factors or PID key authentication factors, the Wallet Provider shall ensure that the Wallet Unit provides biometric performance and security consistent with the relevant ISO/IEC or CEN standards required to reach assurance level high. Where the Wallet Provider uses inherent authentication factors as account authentication factors, the Wallet Provider shall not store the reference biometrics.

145 *[CEN/TS 18098-4 11.13, 11.14]*

WPP-39

146 Where PIN/password or biometrics are used as Wallet Unit authentication factors or PID key authentication factors, the Wallet Unit should ensure, or at least clearly advise the User, that these factors are different from those used to unlock or authenticate to the User's device.

147 *[CEN/TS 18098-4 11.12 C-RECO]*

Annex A (Informative) — Mapping of Provisions to Legal Requirements

Provision	Legal Requirements
WPP-00	CEN/TS 18098-4 6.1.1, 6.1.2
WPP-01	CEN TS 18098-4: REQ-6.2.1
WPP-01a	CEN TS 18098-4: Clause 7
WPP-02	CEN TS 18098-4: REQ-6.3.2.2.2.1; REQ-6.3.2.2.2.2
WPP-02a	CEN TS 18098-4: REQ-6.3.2.2.2.2 REQ-6.3.2.2.2.3; REQ-6.3.2.2.2.4
WPP-02b	CEN/TS 18098-4 6.3.2.1.1, 6.3.2.1.2
WPP-03	CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.2
WPP-03a	CEN TS 18098-4: REQ-6.3.2.2.3.1; REQ-6.3.2.2.3.3
WPP-04	CEN TS 18098-4: REQ-6.3.5.1
WPP-05	CEN TS 18098-4: REQ-6.3.3.1
WPP-06	CEN TS 18098-4: REQ-6.3.5.1
WPP-07	CEN TS 18098-4: REQ-6.4.2
WPP-07a	CEN TS 18098-4: REQ-6.4.1
WPP-07b	CEN TS 18098-4: REQ-6.4.1
WPP-07c	CEN/TS 18098-4 10.1, 10.4, 10.6
WPP-08	CEN TS 18098-4: Clause 6.5
WPP-08a	CEN TS 18098-4: REQ-6.5.1.1; CEN TS 18098-4: REQ-6.5.2.1
WPP-08b	CEN TS 18098-4: REQ-6.5.1.2; CEN TS 18098-4: REQ-6.5.2.2
WPP-08c	CEN TS 18098-4: REQ-6.5.1.3; CEN TS 18098-4: REQ-6.5.2.3
WPP-08d	CEN/TS 18098-4 10.7, 10.8, 10.9, 10.10
WPP-09	CEN TS 18098-4: REQ-6.5.1.4; CEN TS 18098-4: REQ-6.5.1.5
WPP-09a	CEN TS 18098-4: REQ-6.5.2.4; CEN TS 18098-4: REQ-6.5.2.5
WPP-10	CEN TS 18098-4: Clause 6.6
WPP-10a	CEN TS 18098-4: Clause 6.6
WPP-10b	CEN/TS 18098-4 Clause 6.6; CIR 2015/1502 Annex 2.1.1
WPP-11	CEN TS 18098-4: Clause 7
WPP-12	CEN TS 18098-4: REQ-7.3.1
WPP-13	CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3
WPP-14	CEN TS 18098-4: REQ-7.7.2; REQ-7.7.3
WPP-15	CEN TS 18098-4: REQ-7.7.1; REQ-7.7.2; REQ-7.7.4; REQ-7.7.5
WPP-16	CEN TS 18098-4: REQ-7.7.8

Provision	Legal Requirements
WPP-17	CEN TS 18098-4: REQ-7.7.9
WPP-17a	CEN TS 18098-4: REQ-7.7.9
WPP-17b	CEN TS 18098-4: REQ-7.7.10
WPP-17c	Scope clarification for CEN/TS 18098-4 Clause 7
WPP-17d	CEN/TS 18098-4 8.1.1
WPP-17e	Scope boundary: PID Provider obligations remain in WP-03-01
WPP-18	CEN/TS 18098-4 10.11, 10.12
WPP-19	CIR 2024/2981 Art. 5, 8, 18
WPP-20	CIR 2024/2981 Annex I risk treatment
WPP-20a	Reg. 910/2014 Art. 5e; CIR 2024/2979 Art. 7
WPP-21	Reg. 910/2014 Art. 5a(10); CIR 2024/2979 Art. 6(3)(b)]
WPP-22	CIR 2015/1502 Annex 2.2.3
WPP-23	s
WPP-23a	CIR 2024/2979 Art. 7(3)
WPP-23b	CIR 2024/2979 Art. 7(4)
WPP-24	CIR 2015/1502 Annex 2.2.3
WPP-24a	CIR 2015/1502 Annex 2.2.3
WPP-25	CIR 2015/1502 Annex 2.2.3; CIR 2024/2979 Art. 6(3)(b)-(c)
WPP-25a	CIR 2015/1502 Annex 2.2.3
WPP-25b	CIR 2015/1502 Annex 2.2.3
WPP-26	CEN/TS 18098-4 10.13 POS; CIR 2024/2981 Art. 8
WPP-27	CIR 2024/2981 Art. 5, 8, 18
WPP-28	CIR 2024/2979 Art. 9(3), 9(5), 9(7)
WPP-29	CIR 2024/2979 Art. 13; Reg. 910/2014 Art. 5a(4)(f)-(g
WPP-30	CIR 2024/2981 Art. 19
WPP-31	CEN/TS 18098-4 9.1
WPP-32	CEN/TS 18098-4 9.2, 9.3, 9.4
WPP-33	CEN/TS 18098-4 10.1, 10.2
WPP-34	CEN/TS 18098-4 11.1, 11.2
WPP-35	CEN/TS 18098-4 11.3, 11.4; CIR 2015/1502 Annex 2.2.1
WPP-36	CEN/TS 18098-4 11.5, 11.6, 11.7
WPP-37	CEN/TS 18098-4 11.10, 11.11
WPP-38	CEN/TS 18098-4 11.13, 11.14
WPP-39	CEN/TS 18098-4 11.12 C-RECO

Annex B (Informative) — Wallet Unit lifecycle

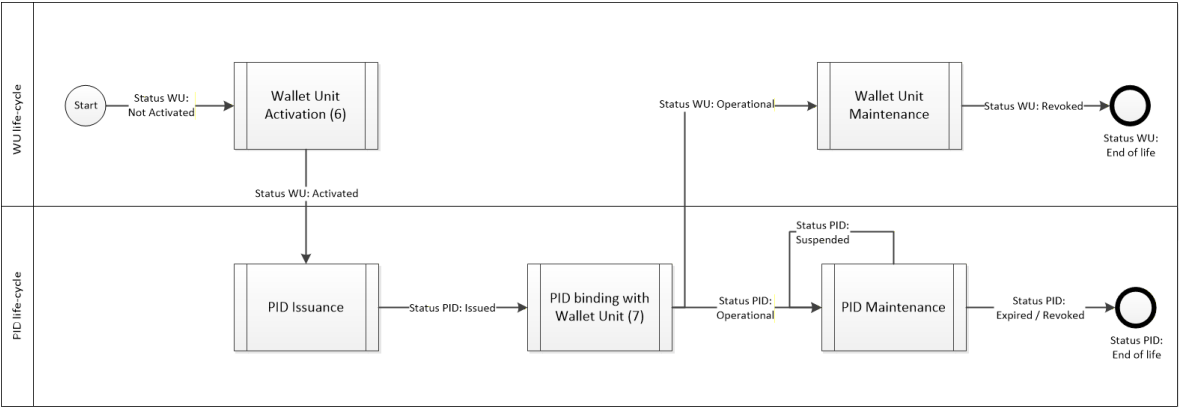
A. General

148 The Wallet Provider provides and operates the Wallet Solution that forms the technical foundation of the European Digital Identity Wallet. The wallet unit, once provisioned and activated on the user's device, serves as the user's means of electronic identification at assurance level high and as the secure container for person identification data and electronic attestations of attributes.

149 The Wallet Provider is responsible for the whole wallet provisioning process, including any parts delegated to third parties. The Wallet Provider remains responsible for the fulfilment of all requirements of this document as if it had performed the activities itself.

150 *NOTE: Numbers used in subsequent figures refer to CEN TS 18098-4 Requirements for Wallet and PID Providers; this document is currently at early stage of development the figures and accompanying description are subject to change in the future.*

151 **Figure 1** illustrates the Wallet Unit lifecycle and its relationships to the PID of respective Wallet User and shows how the application activation step link with the issuance and management of the user's digital identity.



152

Figure 1 Relationship between PID and Wallet Unit in their lifecycles

153 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 Wallet Unit of the PID holder (User).

154 The architecture of EUDI Wallet solution enforces a strict sequential dependency: successful execution of the Wallet Unit Activation (6) process is a mandatory prerequisite to proceed with the PID Binding with Wallet Unit (7) step. Once this binding is completed, the Wallet Unit status transitions to operational, and both tracks enter their respective maintenance phases (Wallet Unit Maintenance and PID Maintenance).

155 The architecture enforces a strict sequential dependency: successful execution of the Wallet Unit Activation (6) process is a mandatory prerequisite to proceed with the PID Binding with Wallet Unit (7) step. Once this binding is completed, the Wallet Unit status transitions to operational, and both tracks enter their respective maintenance phases (Wallet Unit Maintenance and PID Maintenance).

156 B. Wallet Unit activation

156 This section sets out the requirements for the initialization and configuration of the Wallet Unit on the user's device. The structural sequence and flow of the activation phase are illustrated in **Figure 2**.

157 *NOTE 1: Some steps of the process are performed automatically by the Wallet Unit or other part of the Wallet Provider back-end system supporting the Wallet Unit configuration. Such actors are considered as performing actions on behalf of the Wallet Provider.*

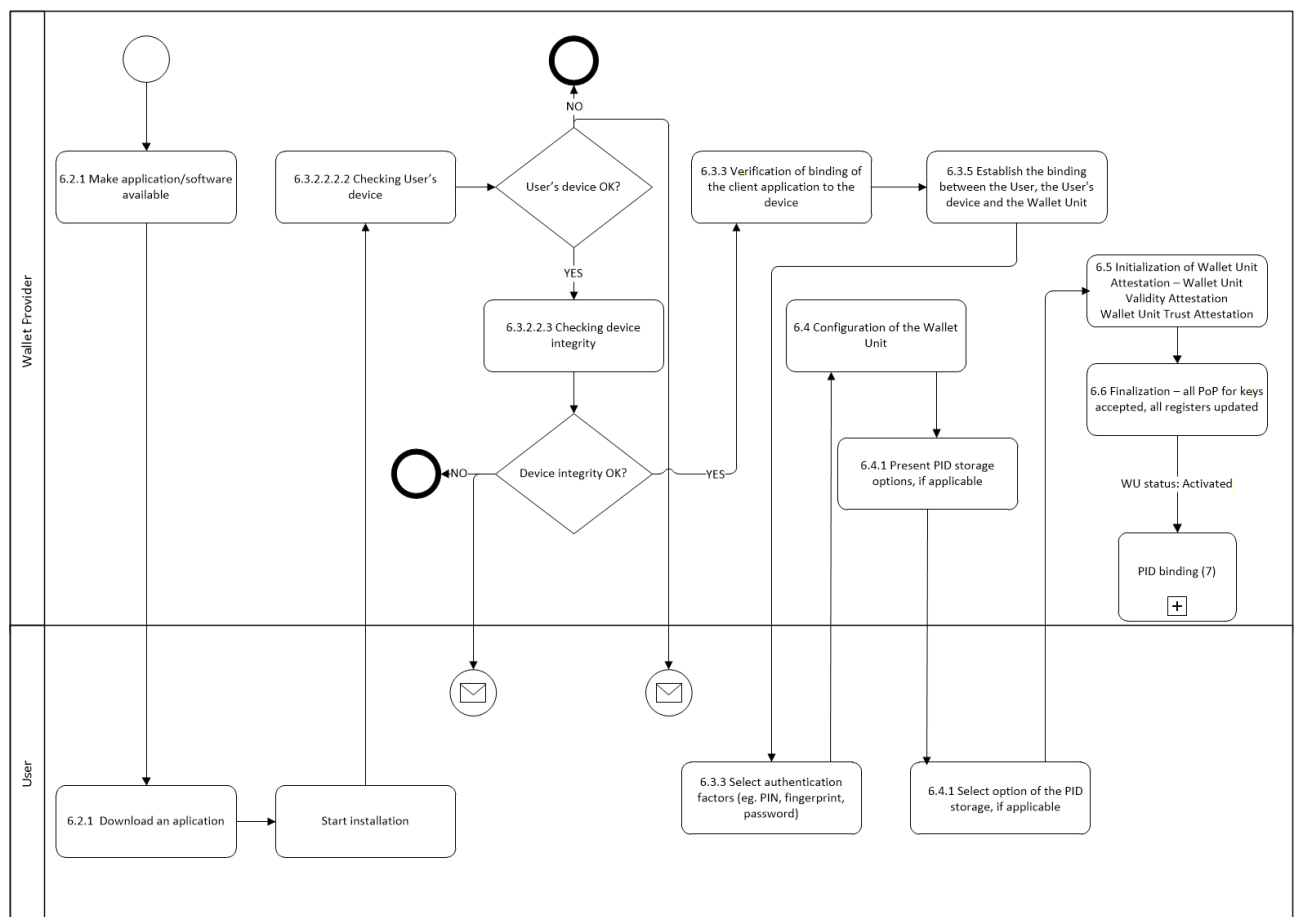


Figure 2 Wallet Unit Activation process

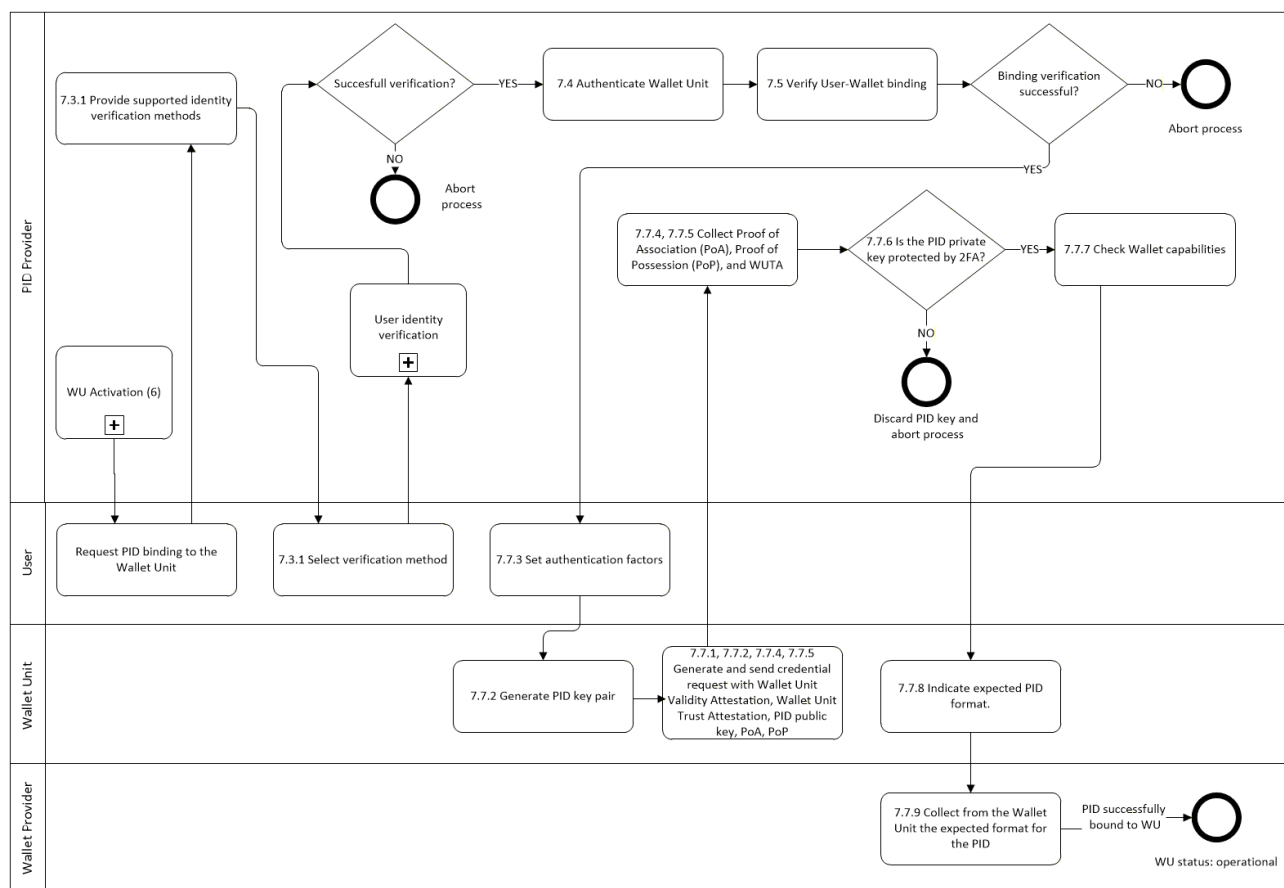
158 The activation process is executed by two actors establishing a coordinated sequence of actions between the Wallet Provider and the User.

159 The Wallet Provider makes the Wallet Unit software application available to the user to enable the download and initiation of the local installation sequence.

- 160 *NOTE: If verification checks performed by the Wallet Provider fail the process is aborted, and appropriate information is sent to the user.*
- 161 Upon the downloading and launching of the installation sequence by the user, the Wallet Provider performs a technical verification of the user's device. This verification check whether the device meets the mandatory hardware capabilities, security features, and deployment policies necessary for the operation of the Wallet Unit.
- 162 Where the user's device is successfully verified, the Wallet Provider executes a device integrity check. This check confirms that the host operating system and system security structures have not been modified or compromised through mechanisms such as rooting or jailbreaking.
- 163 Once the device's integrity has been successfully verified, the application shall allow the user to select and configure the authentication factors used to protect the wallet unit. Supported methods include PINs, passwords, or device-supported biometrics.
- 164 *NOTE 2: The selected mechanisms are then used to strictly control access to the cryptographic keys stored in the Wallet Unit.*
- 165 The Wallet Provider executes a cryptographic verification to validate the binding of the application to the user. This verification shall confirm that the application executes genuinely on the verified device, is not malicious, and has not been tampered with.
- 166 Upon successful verification of the application binding, the Wallet Provider establishes a formal cryptographic relationship linking the User, the user's device, and the Wallet Unit.
- 167 Following the establishment of the cryptographic binding, the Wallet Provider initializes the core configuration layer of the Wallet Unit.
- 168 Where the Wallet Solution supports alternative logical or physical storage environments for Person Identification Data (PID), the application presents the available storage options to the user (Present PID storage options, if applicable).
- 169 Upon completion of the configuration layer, the Wallet Unit initiates the cryptographic initialization sequence of the Wallet Unit (Initialisation of Wallet Unit).
- 170 The Wallet Unit generates localized cryptographic keys within the secure hardware environment of the device (WSCD), and the Wallet Provider retrieves the generated public keys from the Wallet Unit.

- 171 The Wallet Provider retrieves the corresponding Proof of Association (PoA) and
Proof of Possession (PoP) tokens for each generated key pair from the Wallet
Unit.
- 172 The Wallet Provider verifies the validity and structural correctness of the
cryptographic proofs received. If any verification step fails, the activation process
shall be aborted, and no credentials shall be issued.
- 173 Upon successful validation of all cryptographic proofs, the Wallet Provider shall
issue the Wallet Unit Validity Attestation (WUVA) to confirm the structural and
operational validity of the Wallet Unit.
- 174 *NOTE 3: In strict compliance with data protection frameworks, the issued WUVA
shall incorporate public keys, systemic device profiles, and Wallet Provider
identifiers, but shall not contain personal data relating to the user or the
prospective PID holder.*
- 175 Concurrently, the Wallet Provider issues one or several Wallet Unit Trust
Attestations (WUTA) containing the public keys, Wallet Provider and
hardware/software (WSCA/WSCD) environment details, device profiles, and a
cryptographic signature, while strictly excluding any personal data relating to the
User.
- 176 Following the successful issuance of both mandatory attestations, the Wallet
Provider executes the finalization phase. The Wallet Provider accept all verified
Proof of Possession (PoP) tokens for the generated keys and updates all internal
systemic registers.
- 177 Upon successful register updates and token acceptance, the system changes a
status of the Wallet Unit to "Activated", thereby completing the Wallet Unit
activation phase and fulfilling the mandatory prerequisite required to execute
the subsequent PID binding process (7).

c. PID binding with Wallet Unit



6.6 Wallet Unit maintenance

178 The maintenance process is presented in **Figure 4**.

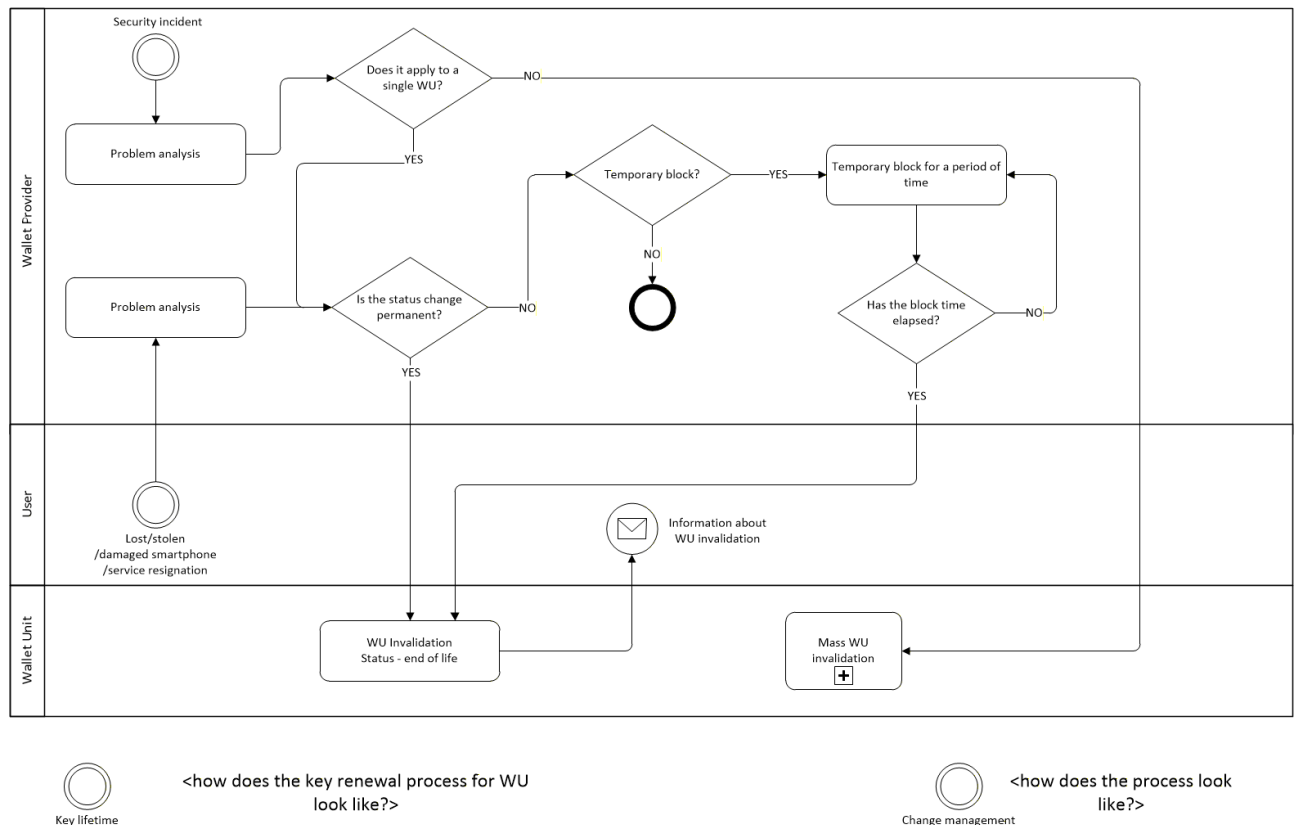


Figure 4 Wallet Unit Maintenance

- 179 The maintenance process is executed across three operational tracks involving the Wallet Provider, the User, and the PID Provider.
- 180 The Wallet Provider maintains continuous monitoring capabilities to detect security incidents affecting the operational integrity of deployed Wallet Units.
- 181 The Wallet Provider provides reporting channels to ingest lifecycle events, including scenarios where a smartphone is reported as lost, stolen, or damaged, or upon the formal submission of a service resignation.
- 182 Upon detection of a security incident, the Wallet Provider executes an immediate problem analysis to determine the scope and impact of the issue.
- 183 The Wallet Provider determines whether the analyzed security incident applies strictly to a single Wallet Unit.
- 184 Where the security incident is determined not to apply to a single unit but represents a vulnerability that could have a broader impact, the Wallet Provider triggers massive Wallet Unit invalidation.
- 185 If the Wallet Provider responds to the User request (e.g., a smartphone is lost, stolen or damaged, or the User discards the service) the Wallet Provider starts the process of invalidation, and appropriate message is sent to the PID Provider.

- 186 Upon receiving a reported lifecycle event, the Wallet Provider performs a problem analysis to determine the status modification requirements i.e., if the status change required is permanent.
- 187 If the status change is confirmed as permanent, the system initiates transitioning the Wallet Unit to an end-of-life status.
- 188 If the status change is determined not to be permanent the Wallet Provider decides whether a temporary blocking is required. In such case the Wallet Provider shall apply a temporary restriction to the Wallet Unit for a designated period.
- 189 Once the monitored block time has elapsed, the system automatically routes the flow to execute the permanent invalidation sequence under WPP-23a.
- 190 *NOTE: periodic renewal process for the Wallet Unit keys are not covered yet except some high-level statements*
- 191 The Wallet Provider implements a periodic key renewal process for the Wallet Unit triggered by the expiration of the defined key lifetime. *NOTE — This process governs how the system handles the rotation and regeneration of core cryptographic keys before their security profile degrades.*