EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

Ensuring High Assurance of EUDI Wallets
& the NL National eID Scheme

NL-P-04P

NL EUDI Wallet Certification System

PID Lifecycle Specification (part1)

RC1.0

2026.11.01

Document reference	NL-P-04P (part1)
Version	RC1.0
Status	Release Candidate Draft
Date	01/11/2026
Document type	Requirements (PID Issuance & Lifecycle Management)
Parent framework	NL-SYS-01 NL-P-P
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	PID Providers under the NL EUDI Wallet Certification System
Primary audience	PID Providers, CABs and Scheme Owners
Secondary audience	Wallet Providers, Supervisory bodies, accreditation bodies and EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Related Documents	NL-P-01 NL-P-02 NL-P-03

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Version	**RC1.0**	State	Date
RC1.0	Transmission of working doc into Certification System Template	Release Candidate	2026-10-31

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Table of Contents

1 Introduction 5
1.1 Foreword 5
1.2 Scope 5
2 References 7
2.1 Normative References 7
2.2 Informative References 7
3 Terms & Abbreviations 8
3.1 Terms 8
3.2 Abbreviations 9
3.3 Model Verbs 10
3.4 Notations 10
3.5 Symbols 10
4 Relation to Resilience & High Assurance 11
4.1 Resilience 11
4.2 High Assurance 12
5 Lifecycle Event: PID Initial Issuance 15
5.1 Pre-Issuance Requirements and Eligibility 15
5.2 Wallet Unit Verification 17
5.3 User Identity Verification 19
5.3.1 General Requirements 19
5.3.2 Identity Proofing Using a Digital Identity Document 20
5.4 PID Issuance Request and Authorisation 24
5.5 PID Generation and Signing 26
5.6 Secure PID Delivery 28
5.7 Post-Issuance Status Service Registration 29
6 Lifecycle Event: PID Batch Replenishment 39
6.1 Replenishment Triggers and Threshold 39
6.2 Batch Request and Issuance Protocol 42
6.3 Offline Fallback 45
6.4 Exhausted Credential Cleanup 45
7 Lifecycle Event: PID Renewal 47
7.1 Renewal Triggers and Conditions 47
7.2 Re-identification Requirements 48
7.3 Renewal Request and Authorisation 48
7.4 PID Generation and Signing 49
7.5 Delivery of the PID 49
Annex A (informative): PID State Diagram 51
Annex B (informative): Risk Register Cross-Reference 54

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

1 Introduction

1.1 Foreword

The European Digital Identity Wallet (EUDIW) is a new concept introduced by Regulation (EU) 2024/1183 (eIDAS 2) that enables European citizens, residents and businesses to use a digital identity wallet for identification, authentication, and storage of electronic attestations of attributes. The EUDIW framework introduces novel security, privacy, and interoperability challenges that require clear, well-structured technical requirements.

The Person Identification Data (PID) is the central credential of the EUDIW, acting as the digital identity of its holder. The PID is treated as an object governed by the state model defined in the Architecture and Reference Framework (ARF).

Its lifecycle encompasses multiple stages, from initial issuance through to expiry, revocation or deletion, each presenting distinct security risks and operational requirements. In the present document, "PID" denotes the Logical PID unless a Technical PID is expressly meant; a batch comprises multiple Technical PIDs of the same Logical PID.

This specification addresses the initial issuance, the batch replenishment and the renewal of the PID. It establishes security requirements that the PID Provider must implement to ensure that PID issuance, batch replenishment and renewal processes meet the eIDAS Assurance Level High corresponding to the requirements set out in Commission Implementing Regulation (EU) 2015/1502.

This specification was developed to define security requirements to cover the risks that can arise during the initial issuance and the renewal of the PID. It is intended to serve as a normative basis for conformity assessment of PID Provider solutions with respect to PID issuance and renewal processes.

The requirements defined in this specification are risk-based and have been derived from an analysis of applicable legislation, reference frameworks, and threat models relevant to the EUDIW ecosystem. A companion risk register documents the risk analysis underpinning the requirements and is maintained as a separate document.

This specification is intended to be used by PID Providers as a normative framework for implementation, and by Conformity Assessment Bodies (CABs) as a basis for audit and conformity assessment of PID Provider solutions.

1.2 Scope

This specification defines requirements for the initial issuance and the renewal of the PID within the European Digital Identity Wallet framework. The PID is treated as an object, governed by the state model defined in the Architecture and Reference Framework. The processes covered by this specification meet the requirements for assurance level high as laid down in Commission Implementing Regulation (EU) 2015/1502.

This specification covers the following lifecycle events:

- PID Initial Issuance: requirements governing the initial issuance of a PID to a Wallet Unit under sole control of the subject of the PID, from pre-issuance eligibility verification through to the PID being stored and active in the Wallet Unit;

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- PID Batch Replenishment: requirements governing the silent, autonomous re-issuance of additional once-only Technical PIDs to a Wallet Unit when the available Technical PIDs fall below a defined threshold or when their attribute values change at the Authentic Source, without user action and without renewed identity proofing of the user;
- PID Renewal: requirements for the re-issuance of a PID when it approaches the end of its validity period. Renewal always requires renewed identity proofing of the user.

The following are explicitly out of scope of this specification:

- PID lifecycle events after issuance (revocation, expiry and deletion), which are covered in a separate specification;
- PID Provider organisational, security and policy requirements;
- PID data model requirements;
- processes at the Authentic Source level;
- requirements regarding the Wallet Unit or Wallet Instance lifecycle;
- Relying Party requirements.

NOTE: This specification does not preclude implementations from imposing additional requirements beyond those specified herein, provided such requirements do not conflict with the provisions of this specification or applicable regulatory requirements.

2 References

2.1 Normative References

The following referenced documents are indispensable for the application of this specification.

Reference	Document
[1]	Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
[2]	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.
[3]	Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets.
[4]	Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules as regards the certification of European Digital Identity Wallets
[5]	ETSI TS 119 472-3: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 3: Profiles for issuance of EAA or PID"
[6]	ARF Technical Specification TS10, "Data Portability and Download (Export)", https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts10-data-portability-and-download-(export).md
[7]	PID Lifecycle Events specification: "PID Lifecycle Events Specification" (companion specification defining the PID revocation, expiry and deletion lifecycle events), latest version.

2.2 Informative References

The following referenced documents are not essential for the application of this specification but may assist the reader in understanding the context and background of the requirements defined herein.

Reference	Document
[i.1]	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.
[i.2]	European Digital Identity Wallet Architecture and Reference Framework, Version 3.0.0 (2026-07-21) or later, published by the European Commission.
[i.3]	ETSI SR 001 262: ETSI drafting rules
[i.4]	ISO 37003:2025, "Fraud control management systems — Guidance for organizations managing the risk of fraud".
[i.5]	PID Issuance Assessment Checklist, companion deliverable to this specification (to be issued).

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

3 Terms & Abbreviations

3.1 Terms

For the purposes of this specification, the following definitions apply. Terms defined in eIDAS [1] and the Architecture and Reference Framework (ARF) [i.2] are used in accordance with those documents unless otherwise stated.

Term	Definition
Wallet Instance	The software application, including all its components, installed on a Wallet User's device, provided by a Wallet Provider.
Wallet Unit	A unique configuration of a Wallet Solution that includes one or more Wallet Instances, Wallet Secure Cryptographic Applications and Wallet Secure Cryptographic Devices, provided by a Wallet Provider to an individual Wallet User.
Wallet Instance Attestation (WIA)	An attestation issued by the Wallet Provider certifying that a Wallet Instance is a genuine instance of the Wallet Solution, and carrying the information required to determine its revocation status.
Key Attestation (KA)	An attestation issued by the Wallet Provider certifying, for one or more public keys, that the corresponding private keys are generated within and are non-extractable from an identified keystore, and describing the storage type and the security certification of that keystore.
Wallet Provider	A natural or legal person, or a public body, responsible for providing and operating an EUDIW solution.
Wallet Secure Cryptographic Device (WSCD)	A hardware or software component that provides a protected execution environment and secure storage for cryptographic keys and operations within the Wallet Unit.
Wallet Secure Cryptographic Application (WSCA)	The application component that manages cryptographic operations and secure storage within the WSCD.
Person Identification Data (PID)	A set of data enabling the identity of a natural or legal person to be established, issued by a PID Provider in accordance with eIDAS 2.
Logical PID	The Person Identification Data of a subject as a credential, independent of the individual instances issued to a Wallet Unit. A Logical PID is the type of PID, characterised by its attestation type and its attribute values. A Logical PID does not itself have a validity period or a revocation status; only its Technical PIDs do.
Technical PID	An individual issued instance of a Logical PID, stored in a Wallet Unit and presented to Relying Parties, with its own validity period and revocation status. A batch consists of multiple Technical PIDs that represent the same Logical PID, with the same attestation type and attribute values.
Administrative Validity Period	The period, maintained by the PID Provider for a Logical PID issued to a Wallet Unit, during which the PID Provider may issue further batches of Technical PIDs of that Logical PID to the Wallet Unit without renewed identity proofing of the person.
PID Provider	A Member State authority or body, or a private entity designated by a Member State, that issues PID to Wallet Units.
Electronic Attestation of Attributes (EAA)	A set of data in electronic form that allows attributes about a natural or legal person to be authenticated, issued by a (Qualified) Attestation Provider.
Conformity Assessment Body (CAB)	A body that performs conformity assessment activities in accordance with applicable standards and legislation.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Term	Definition
Activation	The process by which a Wallet Unit is initialised, configured, and bound to a specific Wallet Wallet User, device, and cryptographic key material, rendering it operational.
Suspension	A temporary, reversible disabling of a Wallet Unit by the Wallet Provider, preventing its use until the suspension is lifted.
Revocation	A permanent, irreversible invalidation of a Wallet Unit, after which the Wallet Unit cannot be reinstated.
Migration	The process of transferring the state of a Wallet Unit from one device to another while maintaining continuity of the Wallet Wallet User's wallet identity and credentials.
Key Material	Cryptographic keys and associated data generated, stored, and managed within the WSCD for the purpose of securing Wallet Unit operations.
Assurance Level	A classification of the degree of confidence in the claimed identity of a person or the integrity of a device, as defined in Commission Implementing Regulation (EU) 2015/1502.

3.2 Abbreviations

For the purposes of this specification, the following abbreviations apply:

Abbreviation	Expansion
ARF	Architecture and Reference Framework
CAB	Conformity Assessment Body
CIR	Commission Implementing Regulation
EAA	Electronic Attestation of Attributes
eIDAS	Electronic Identification, Authentication and Trust Services Regulation [1]
EUDIW	European Digital Identity Wallet
HSM	Hardware Security Module
PID	Person Identification Data
QTSP	Qualified Trust Service Provider
SE	Secure Element
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TSP	Trust Service Provider
WIA	Wallet Instance Attestation
KA	Key Attestation
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device

3.3 Model Verbs

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 23 of the ETSI Drafting Rules (Verbal forms for the expression of provisions) [i.3].

3.4 Notations

The requirements identified in the present document include:

a) requirements applicable to any EUDIW implementation. Such requirements are indicated without any additional marking;

b) requirements applicable to specific EUDIW implementations. Such requirements are marked by "[CONDITIONAL]" or indicated by clauses introduced by "[CONDITIONAL]".

The requirements in the present document are identified as follows:

<the 3 to 5 letters identifying the lifecycle> - < the clause number> - <2 digit number – incremental>

This identifier may be used in the companion Assessment Checklist to cross-reference individual requirements.

The lifecycle event identifiers are as follows:

Identifier	Lifecycle Event
ISS	PID Initial Issuance
REP	PID Batch Replenishment
REN	PID Renewal

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted at the start of a clause, the 2 digit number 00 is used.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for a deleted requirement is left and completed with "VOID".
- When a requirement is modified from the previous edition of the present document, the requirement number is amended by a capital 'X' letter.

3.5 Symbols

No symbols specific to this specification are defined. Mathematical and cryptographic notation follows standard conventions.

4 Relation to Resilience & High Assurance

4.1 Resilience

For the purpose of this specification, resilience refers to the ability of the PID issuance and PID lifecycle-management processes to maintain their intended security, integrity and trust properties when exposed to attacks, attempted fraud, compromise, operational failure or misuse. It does not refer to organisational resilience under NIS2 or product-development and vulnerability-handling obligations under the Cyber Resilience Act.

PID issuance and lifecycle management are security-critical processes because they determine whether Person Identification Data is issued to the correct person, bound to an authentic and trustworthy Wallet Unit, maintained on the basis of current and authoritative information, and revoked, expired or otherwise made unusable when the conditions for its continued use no longer apply. The attached specification treats PID as the central credential of the EUDI Wallet and identifies distinct risks throughout initial issuance, batch replenishment and renewal.

These processes are exposed to attackers with a high attack potential. Such attackers may have substantial expertise, resources and time and may combine technical attacks with identity fraud, social engineering, compromised devices, stolen or cloned identity documents, manipulation of issuance requests, interception or modification of communications, compromise of cryptographic keys, exploitation of exceptional lifecycle paths and abuse of legitimate support, recovery or revocation procedures. An attacker may also attempt to conceal the compromise by operating a second Wallet Unit while the rightful citizen's Wallet Unit continues to function normally.

The consequences of a successful attack may extend beyond the compromise of an individual process or technical component. An attacker could obtain a genuine PID in another person's name, bind a PID to cryptographic keys under the attacker's control, continue obtaining Technical PIDs through batch replenishment, renew a PID without the rightful citizen's involvement, prevent or delay effective revocation, or cause the PID Provider to rely on outdated or manipulated identity data. Such a compromise could enable unauthorised use of the citizen's digital identity and could remain undetected if the lifecycle processes are assessed only as separate transactions.

Resilience shall therefore be established through process requirements covering the complete PID lifecycle and the transitions between lifecycle events. These requirements shall ensure, as applicable, that:

- identity proofing and verification resist impersonation, replay, document cloning, relay, injection and manipulation;
- the authenticity, validity and status of identity evidence are established before a PID is issued or renewed;
- the PID is issued only to an authentic and appropriately trusted Wallet Unit;
- issuance, replenishment and renewal requests are fresh, authorised and cryptographically bound to the relevant Wallet Unit and PID;
- PID binding keys are generated and held in an appropriately protected cryptographic environment, and possession of the corresponding private keys is demonstrated;
- PID attributes are obtained from the applicable Authentic Source and remain complete, correct and current;

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- batch replenishment cannot be used to bypass renewed identity proofing, prolong a compromised PID relationship or supply an uncontrolled Wallet Unit indefinitely;
- renewal re-establishes the required identity assurance and does not rely solely on the continued possession of an existing Wallet Unit or credential;
- anomalous, repeated or conflicting issuance and lifecycle events are detected, recorded, investigated and responded to;
- the rightful citizen is informed, through an appropriate channel independent of the Wallet Unit, of security-relevant issuance and lifecycle events;
- compromise, loss of control or invalidity results in the appropriate restriction, suspension, revocation, expiry or termination of the affected PID; and
- audit information remains available to support detection, investigation, incident response and conformity assessment.

The attached specification already reflects this process-oriented approach through controls addressing genuine Wallet Instance Attestations, Wallet Trust Evidence, proof of possession, identity-document authenticity, replay protection, authorisation gates, independent citizen notifications, fraud indicators, batch limits, renewed identity proofing and revocation.

No single control is sufficient to ensure resilience. The requirements shall operate as mutually reinforcing safeguards across normal, exceptional and recovery paths. A strong initial identity-proofing process can be undermined by a weak replenishment or renewal process, just as secure PID generation can be undermined by incorrect key binding, insecure delivery, ineffective status management or delayed revocation.

The CAB shall therefore assess not only the design and correct implementation of individual controls, but also whether the PID Provider's processes collectively preserve the intended security properties across the applicable lifecycle events and transitions. This assessment shall consider whether an attacker with high attack potential could circumvent a control by selecting an alternative process path, combining weaknesses across different lifecycle events, or exploiting differences between initial issuance, batch replenishment, renewal and the post-issuance lifecycle processes.

4.2 High Assurance

The PID Provider is subject to the requirements applicable to assurance level High under Commission Implementing Regulation (EU) 2015/1502. That Regulation determines assurance levels by reference to the reliability and quality of enrolment, electronic identification means management, authentication, and management and organisation.

Accordingly, the PID issuance and lifecycle-management processes shall meet the requirements applicable to assurance level High and shall preserve the resulting level of assurance throughout the period in which the PID can be issued, replenished, renewed or otherwise used as part of the Wallet User's electronic identification means. Compliance shall not be limited to the initial identity-proofing decision. It shall extend to all process steps that can materially affect the relationship between:

- the identity established by the PID Provider;
- the rightful citizen to whom that identity relates;
- the PID issued in that citizen's name;
- the Wallet Unit to which the PID is issued; and

- the cryptographic keys and authentication mechanisms through which the PID can be used.

For initial issuance, the PID Provider shall establish with the reliability required for assurance level High that the person requesting the PID is the person whose identity is represented by the PID. The PID Provider shall also verify that the receiving Wallet Unit is authentic and sufficiently trustworthy, that the PID is bound to the intended Wallet Unit and dedicated PID binding key, and that delivery takes place only after the required authentication and authorisation steps have been completed. The attached specification gives effect to this through Wallet Unit verification, high-assurance trust evidence, proof of possession, key-provenance verification, identity proofing, secure authorisation and secure delivery requirements.

The PID issuance and lifecycle-management processes shall, in addition, ensure that the PID is placed and remains under the sole control of the rightful citizen. In the context of this specification, sole control means that the exercise of the PID and the cryptographic capabilities bound to it requires the involvement or authorisation of the correctly identified citizen and cannot be exercised independently by another person, device, Wallet Unit, provider or intermediary.

Sole control shall be established and preserved through a combination of identity, process and technical controls. These controls shall ensure that:

- identity proofing relates to the citizen for whom the PID is generated;
- the issuance decision is bound to the same identity-proofing session and authorised issuance transaction;
- the PID is issued only to the intended Wallet Unit;
- the PID is bound to a dedicated public key for which the intended Wallet Unit has demonstrated possession of the corresponding private key;
- the private key is generated and retained in an appropriately protected cryptographic environment and cannot be exported or independently exercised by the PID Provider;
- authentication of the citizen and the Wallet Unit is successfully completed before the PID is released;
- a PID cannot be issued silently to an additional Wallet Unit without the required detection, confirmation and notification controls;
- replenishment cannot transfer control to another Wallet Unit or continue after reliable evidence that the Wallet Unit is no longer under the citizen’s control;
- renewal includes renewed identity proofing at the assurance level required for initial issuance and proof that the request relates to the existing PID and Wallet Unit;
- changes to registered contact methods cannot be used to redirect authorisations and security notifications to an attacker; and
- the rightful citizen has an effective means to recognise and respond to unauthorised issuance or lifecycle events.

The sole-control objective is not satisfied merely because a valid PID has been technically delivered to a Wallet Unit. It requires reasonable assurance that the Wallet Unit and the PID binding keys are controlled by the same rightful citizen whose identity was established during identity proofing. A technically valid issuance to a genuine Wallet Unit would still fail this objective if that Wallet Unit were controlled by an attacker or if the issuance had been induced through impersonation, social engineering, unauthorised contact-method substitution or manipulation of the citizen.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Batch replenishment requires particular safeguards because it issues further Technical PIDs without renewed identity proofing. The attached specification therefore requires replenishment to remain within the Administrative Validity Period and to be cryptographically bound to the Wallet Unit holding the existing Logical PID. It also requires replenishment to stop when reliable information indicates that the Wallet Unit is no longer under the legitimate user's control. These controls are necessary to prevent a compromised Wallet Unit or stolen refresh mechanism from extending an attacker's control by continuously obtaining new Technical PIDs.

Renewal shall not be treated as a mere extension of technical validity. Because renewal establishes a new Administrative Validity Period, the PID Provider shall repeat identity proofing at the assurance level required for initial issuance and shall verify that the renewal request originates from the Wallet Unit holding the Logical PID concerned. The attached specification requires renewed identity verification and proof of possession of the private key corresponding to the existing PID binding public key.

The requirements for assurance level High and sole control are complementary. Assurance level High establishes the required confidence in the citizen's identity and in the processes supporting the electronic identification means; sole control ensures that the capabilities resulting from that identity relationship can be exercised only by the rightful citizen. A failure of sole control can therefore negate the practical value of correctly performed high-assurance identity proofing.

The CAB shall assess whether the PID issuance and lifecycle-management processes provide an end-to-end and continuously maintained chain of assurance. The assessment shall verify that assurance level High and sole control are preserved across initial issuance, batch replenishment, renewal and their interfaces with revocation, expiry and deletion. It shall also verify that exceptional, alternative and recovery paths do not permit the identity-proofing, binding, authentication, authorisation, notification or revocation controls of the normal process to be bypassed.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5 Lifecycle Event: PID Initial Issuance

Purpose of this chapter: Govern the initial issuance of a PID to a Wallet Unit under sole control of the subject of the PID. Ensure rigorous identity verification, secure cryptographic binding between the PID and the Wallet Unit, and secure delivery of the PID. This covers the full process from pre-issuance eligibility verification through to the PID being stored and active in the Wallet Unit. NOTE: The identity verification and the creation of the PID data are the responsibility of the PID Provider interacting with the Authentic Source. This chapter covers the technical requirements that govern the issuance interaction between the PID Provider and the Wallet Unit.

5.1 Pre-Issuance Requirements and Eligibility

ISS-5.1-01: The PID Provider shall not issue a PID to a Wallet Unit that already holds an active Logical PID issued by that PID Provider.

Guidelines

- *In practice, the PID Provider checks its own records for an active Logical PID already issued to the same Wallet Unit and does not issue a further one to that unit. This concerns a distinct Logical PID; issuing further Technical PIDs of the same Logical PID (for example during batch replenishment) is a separate operation and is not precluded by this requirement.*
- *Without this check a single Wallet Unit could accumulate several active Logical PIDs, giving an attacker who controls or clones the unit multiple parallel credentials and complicating later revocation.*
- *The check is commonly performed against the PID Provider's administration or status service, keyed on the Wallet Unit identifier recorded at issuance.*
- *A CAB verifies that a second issuance request from a unit already holding an active PID is refused, for instance by reviewing the issuance procedure and status records and testing the scenario.*

ISS-5.1-02: The PID Provider shall cancel a PID that has been generated but not issued within the maximum retention period defined in its documented issuance procedures, together with the personal data associated with that PID.

Guidelines

- *The PID Provider defines in its documented procedures how long a PID that was created but never delivered is retained, and removes both the PID object and its associated personal data once that period elapses.*
- *Retaining created-but-undelivered PIDs and their source data indefinitely widens the exposure window for a data breach and leaves orphaned credentials that could later be misused.*
- *This is typically realised by a scheduled clean-up driven by a timestamp recorded when the PID object is created, with the retention period fixed by a documented risk assessment.*
- *A CAB reviews the documented retention period and clean-up procedure, inspects retention timestamps, and confirms that expired created-but-unissued PIDs and their data are removed.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.1-03: [CONDITIONAL] Where a PID is generated in advance of issuance, the PID Provider shall re-verify, immediately before issuance, that no ground preventing issuance has arisen since the PID was generated, including loss of eligibility, a change in the attributes held by the authoritative population register, decease, a fraud signal, or the identity document having been reported lost or stolen.

Guidelines

- *Where a PID is produced some time ahead of the moment of issuance (for instance when creating PIDs in batches), the PID Provider repeats, immediately before release, the checks that could have changed in the interval, such as eligibility, register attributes, decease, fraud signals, or a lost or stolen document.*
- *A PID generated in advance can become invalid before it is delivered; without a fresh check an implementation could hand over a credential that no longer reflects the authoritative source or that relates to a compromised document.*
- *Implementations commonly re-query the authentic population register and the document status source at the point of release and compare the result against the state captured at generation time.*
- *A CAB verifies that release is blocked when a ground preventing issuance arises between generation and delivery, for instance by reviewing the pre-issuance re-verification step and testing a simulated occurrence.*

ISS-5.1-04: The PID Provider shall not issue a PID to a Wallet Unit of a Wallet Provider while an active Logical PID issued by that PID Provider in the name of the same person is held in another Wallet Unit of that same Wallet Provider, unless the Technical PIDs of that Logical PID have been revoked in accordance with **ISS-5.1-05**.

Guidelines

- *The PID Provider checks, before issuing, whether the person already has an active Logical PID in a Wallet Unit provided by the same Wallet Provider as the Wallet Unit now requesting a PID. If so, the PID Provider either refuses the issuance or issues only after the older Logical PID has been revoked.*
- *Without this check, an attacker who installs the wallet application of the same Wallet Provider on a second device and obtains a PID in the victim's name ends up with a working second Wallet Unit next to the victim's own, and nobody notices that the same person now holds two Wallet Units at one Wallet Provider.*
- *The PID Provider derives the Wallet Provider from the issuer of the Wallet Instance Attestation validated under **ISS-5.2-02** and compares it with the Wallet Provider recorded under **ISS-5.7-16** for the active Logical PIDs of that person. This requirement sets no maximum on the number Wallet Providers where a person holds a Wallet Unit. A refusal message to the Wallet Unit does not reveal the existence of the other Wallet Unit (see **ISS-5.7-19**).*
- *A CAB verifies this requirement by reviewing the documented issuance flow and the PID Provider's administration, for instance by inspecting the rule that compares the Wallet Provider of the requesting Wallet Unit with the Wallet Providers recorded for the person's active Logical PIDs, and by examining past issuance records for the absence of two active Logical PIDs of one person at one Wallet Provider.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.1-05: The PID Provider shall revoke the Technical PIDs referred to in **ISS-5.1-04** only after all other conditions for issuing the further PID have been met, including the confirmation required by **ISS-5.4-04** where that requirement applies.

Guidelines

- *The PID Provider revokes the older Logical PID of the same Wallet Provider as the last step before issuing the new one, and only once the person has confirmed the new issuance through the registered contact methods.*
- *If the older Logical PID were revoked as soon as a second Wallet Unit asks for a PID, an attacker could lock the victim out of the victim's own working Wallet Unit by starting an issuance at the same Wallet Provider without ever completing it.*
- *The PID Provider performs the revocation as part of the same transaction that issues the further PID, so that a failed or abandoned issuance leaves the existing Logical PID untouched. Revocation of the older Technical PIDs is recorded in the status mechanism of the PID Provider, as for other revocations (see **REP-6.1-04**).*
- *A CAB verifies this requirement by reviewing the issuance flow and its state handling, for instance by examining the point at which revocation of the older Logical PID is triggered and by inspecting records of abandoned issuance attempts that show the older Logical PID remained active.*

5.2 Wallet Unit Verification

ISS-5.2-01: The PID Provider shall verify, before issuing a PID, that the Wallet Unit presents a Wallet Instance Attestation that is valid, has not expired, and has not been revoked.

Guidelines

- *Before issuing, the PID Provider confirms that the Wallet Instance Attestation presented by the unit is currently valid, within its validity period, and not revoked.*
- *Accepting an expired or revoked Wallet Instance Attestation would let a decommissioned or untrusted wallet obtain a PID.*
- *Validation typically combines signature verification of the attestation with a freshness and status check against the issuer's revocation information.*
- *A CAB inspects the verification logic and tests issuance with expired and with revoked attestations to confirm both are rejected.*

ISS-5.2-02: The PID Provider shall verify, before issuing a PID, that the issuer of the Wallet Instance Attestation is present in the applicable trusted list.

Guidelines

- *The PID Provider confirms that the party that issued the Wallet Instance Attestation appears in the applicable trusted list before relying on the attestation.*
- *Without this check an attestation minted by an untrusted or rogue provider could be accepted as genuine.*
- *This is done by resolving the attestation issuer against the current trusted list published for the ecosystem.*
- *A CAB reviews the trusted-list resolution step and tests that an attestation from an issuer absent from the list is rejected.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.2-03: The PID Provider shall not issue a PID unless the Wallet Unit has provided the Wallet Trust Evidence required to establish that its cryptographic device satisfies the conditions for Assurance Level High.

Guidelines

- *The PID Provider requires Wallet Trust Evidence demonstrating that the unit's cryptographic device meets the conditions for high assurance before it issues a PID.*
- *Without evidence of a sufficiently strong device, a PID could be bound into a wallet whose key protection does not meet the required assurance level.*
- *The Wallet Trust Evidence is typically accompanying the attestation and is evaluated against the high-assurance device criteria.*
- *A CAB verifies that issuance is refused when the evidence does not establish high-assurance device properties, for instance by reviewing the evidence-evaluation step and testing the scenario.*

ISS-5.2-04: The PID Provider shall not bind a PID to a public key unless it has verified proof of possession of the corresponding private key as specified in CRED-REQ-PROC-4.6.2.1-0 of [5].

Guidelines

- *The PID Provider binds the PID to a public key only after the unit has proven that it holds the matching private key.*
- *Binding to a public key without proof of possession would allow a PID to be bound to a key the wallet does not actually control, enabling credential theft.*
- *A conformant implementation uses the key proof of the Credential Request defined in the referenced issuance profile: the Wallet signs a provider-issued nonce with the private key that the PID will be bound to (the proof-of-possession, or proofs-to-jwt, mechanism), and the PID Provider verifies that signature against the attested public key. A key-attestation-only variant, which carries no such signed proof, does not satisfy this requirement because it does not prove possession.*
- *A CAB verifies that issuance does not complete when proof of possession is absent or invalid, for instance by testing both scenarios.*

ISS-5.2-05: The PID Provider shall verify, using the key provenance attestation provided during issuance, that the PID binding key pair is generated and held in a cryptographic device certified at a level appropriate for Assurance Level High.

Guidelines

- *The PID Provider checks, using the key provenance attestation, that the PID binding key pair was generated and is held in a device certified at the level appropriate for high assurance.*
- *If the binding key were generated or stored outside a suitably certified device, the private key could be extracted or cloned, undermining the security of every later presentation.*
- *The key provenance attestation supplied during issuance is evaluated against the certification level recorded for the device.*
- *A CAB reviews the provenance-attestation check and confirms that keys not demonstrably held in an appropriately certified device are rejected.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.2-06: The PID Provider shall not rely on trusted-list data whose current validity cannot be confirmed when validating the Wallet Unit.

Guidelines

- *When validating the Wallet Unit the PID Provider uses trusted-list data whose current validity it can confirm, rather than a cached or unverifiable copy.*
- *Relying on stale trusted-list data could cause the PID Provider to trust an issuer that has since been removed or to miss a revocation.*
- *Implementations typically refresh the trusted list within a defined freshness window and verify the list's own signature and issue time before use.*
- *A CAB inspects the trusted-list handling configuration and confirms that outdated or unverifiable list data is not used for validation.*

5.3 User Identity Verification

5.3.1 General Requirements

ISS-5.3-01: The PID Provider shall verify that the unique identifier established for the subject during identity proofing corresponds to the identity that was authenticated in the same identity-proofing session.

Guidelines

- *The PID Provider confirms that the unique identifier it assigns to the subject belongs to the very identity that was authenticated in the same proofing session, so that the identifier and the proofed identity cannot become mismatched.*
- *If the identifier were taken from a different session or source, a PID could be issued carrying one person's identifier over another person's proofed identity.*
- *In the Netherlands the unique identifier is the BSN obtained through the polymorphic pseudonym-derivation step of the eID scheme; a conformant implementation derives it within the same authenticated session as the document authentication and ties it to that session's result.*
- *A CAB verifies that an identifier originating outside the current proofing session is not accepted, for instance by reviewing the session handling and testing the scenario.*

ISS-5.3-02: The PID Provider shall not introduce, into the PID or into the data it generates during issuance, any identifier or reused value — other than the PID attributes themselves — that would enable a third party to correlate separate Technical PIDs or issuance events independently of the attributes disclosed under the User's control from PID representations.

Guidelines

- *The PID Provider ensures that, apart from the PID attributes themselves, it places no identifier or reused value in the PID or in the issuance data that a third party could use to link separate Technical PIDs or issuance events.*
- *Even under selective disclosure, a non-attribute correlation handle left in the credential — such as a reused binding public key, a static credential serial, or reused salts — would let an attacker or colluding relying parties link two separate presentations that each reveal different attributes, establishing that both attributes belong to the same person even though no common identifying attribute was disclosed.*
- *Implementations avoid embedding document serial numbers, static issuance references, or other stable identifiers in credential data, using per-credential or salted values instead.*
- *A CAB verifies whether separate issuances for the same person share a correlatable value, for instance by inspecting the issued PID and the issuance data for stable identifiers.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5.3.2 Identity Proofing Using a Digital Identity Document

The requirements in the present clause apply where the identity proofing of the subject is performed by electronic authentication of a digital identity document, such as the electronic identity function of an identity card or a driving licence recognized as identity document AL High by the member state.

ISS-5.3-03: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall verify, during identity proofing, that the presented identity document chip is genuine and has not been cloned, using the chip's active authentication mechanism or an equivalent anti-cloning mechanism.

Guidelines

- *During identity proofing the PID Provider confirms that the document chip is authentic and not a clone, using the chip's active authentication or an equivalent anti-cloning mechanism.*
- *A cloned chip would let an attacker replay copied document data to impersonate the legitimate holder.*
- *This is achieved through the chip's challenge-response active authentication, or a chip-authentication mechanism of equivalent strength, executed live against the chip.*
- *A CAB verifies that authentication fails against a cloned chip, for instance by testing proofing with a simulated clone.*

ISS-5.3-04: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall accept the identity document only if validation of the issuer signature on the chip data against the country signing public key infrastructure returns a complete, fully-passed result.

Guidelines

- *The PID Provider accepts the document only when the issuer signature over the chip data validates completely against the country signing infrastructure, with no partial or failed result.*
- *Accepting a document whose signature only partly validates could admit forged or tampered chip data.*
- *Validation checks the document security object signature and its certificate chain to the country signing certificate authority, treating any incomplete result as a failure.*
- *A CAB verifies that documents with invalid or partially validating signatures are refused, for instance by testing both cases.*

ISS-5.3-05: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall establish that the identity document chip is read live during the identity-proofing session.

Guidelines

- *The PID Provider establishes that the chip is read live during the proofing session rather than from an earlier capture.*
- *A read that is not live would allow replay of previously captured chip data belonging to another person or session.*
- *Liveness is established through the interactive chip protocol executed in real time during the session, using session-bound challenges.*
- *A CAB verifies that the session does not complete when a previously captured chip readout is injected, for instance by testing that scenario.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.3-06: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall not accept a previously captured or stored chip readout in place of a live read of the identity document.

Guidelines

- *The PID Provider does not accept a stored or previously captured chip readout in place of a live read.*
- *Permitting stored readouts opens the door to replay attacks using data harvested from an earlier interaction.*
- *Implementations bind the accepted chip data to freshness values generated for the current session and reject data that lacks them.*
- *A CAB verifies that stored readout data is rejected, for instance by reviewing the freshness binding and testing the scenario.*

ISS-5.3-07: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document and a status service for that identity document is available, the PID Provider shall check the status of the presented identity document before completing identity proofing.

Guidelines

- *Where a status service exists for the document type, the PID Provider checks the presented document's status before completing proofing.*
- *Without a status check, a document that has been reported invalid at its source could still be used to obtain a PID.*
- *The provider queries the available document status service and treats a negative or unavailable status according to its documented policy.*
- *A CAB verifies that the status check is performed where a service exists and that a document flagged in that service is refused, for instance by testing the scenario.*

ISS-5.3-08: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall not complete identity proofing where the status check, or any other information available to it, indicates that the identity document is reported lost, stolen, or revoked.

Guidelines

- *The PID Provider does not complete identity proofing with a document that is reported lost, stolen, or revoked.*
- *Proceeding with a reported document would let a person in unlawful possession of it obtain a PID in the rightful holder's name.*
- *The reported status is obtained from the applicable document status source and, when positive, stops the proofing flow.*
- *A CAB verifies that proofing does not complete for a document in any reported blocking state, for instance by testing each state.*

ISS-5.3-09: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall complete identity proofing only after the chip of the identity document has confirmed successful verification of the document PIN.

Guidelines

- *The PID Provider completes proofing only after the chip has confirmed that the document PIN was verified successfully.*
- *Without confirmed PIN verification, mere possession of the document, without the holder's secret, would suffice to obtain a PID.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *The chip reports successful PIN verification within the authenticated session before proofing is treated as complete.*
- *A CAB verifies that identity proofing does not complete when the chip has not confirmed PIN verification, for instance by testing the scenario.*

ISS-5.3-10: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall protect the exchange in which the identity document is electronically authenticated against interception and modification by a party interposed between the identity document and the PID Provider.

Guidelines

- *In practice the PID Provider ensures that the data exchanged while the identity document is electronically authenticated cannot be read or altered by any component that merely carries the traffic between the document and the PID Provider.*
- *Without this protection, a party interposed between the document and the PID Provider could relay or alter a genuine authentication in real time, obtaining a PID in the legitimate holder's name or binding it to data that the attacker controls.*
- *Protection is commonly achieved with a channel that is end-to-end encrypted and integrity-protected between the document's secure chip and the PID Provider, so that intermediate components cannot access or modify the cleartext of the exchange.*
- *A CAB verifies that a party interposed between the document and the PID Provider can neither read nor modify the exchange, for instance by reviewing the channel design and testing the scenario.*

ISS-5.3-11: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall record the number of failed PACE or PIN-verification attempts that occurred, within the same identity-proofing session, before a successful attempt.

Guidelines

- *The PID Provider counts how many PACE or PIN-verification attempts failed within an identity-proofing session before the attempt that succeeded, and keeps that count.*
- *An attacker guessing or trying a small set of likely PINs against a lost, stolen, or borrowed document may eventually succeed within the chip's own retry limit; without a record of the failed attempts that preceded that success, the PID Provider would have no way to distinguish it from a legitimate user's single mistyped PIN.*
- *This count is available from the same PACE/PIN-verification exchange the identity-proofing session already performs and is written to the session record alongside the successful outcome.*
- *A CAB verifies that the count of failed PACE or PIN-verification attempts preceding success is recorded, for instance by reviewing session records and testing the scenario.*

ISS-5.3-12: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall flag, for investigation, an identity-proofing session in which the number of failed PACE or PIN-verification attempts before a successful attempt exceeds a defined threshold.

Guidelines

- *When an identity-proofing session shows more failed PACE or PIN-verification attempts before success than a threshold the PID Provider has defined, the PID Provider raises that session for investigation.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Without such a flag, a successful PIN-guessing attack would result in a PID being issued exactly as if the legitimate holder had authenticated normally, leaving no operational signal that anything unusual occurred.*
- *The threshold is set by the PID Provider's own fraud-management process, informed by the count kept under ISS-4.3-11.*
- *A CAB verifies that a failed-attempt count exceeding the defined threshold results in the session being flagged, for instance by reviewing the threshold configuration and testing the scenario.*

ISS-5.3-13: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall record the identity document's chip identifier together with the national identification number established during each identity-proofing session.

Guidelines

- *Each time the PID Provider completes identity proofing, it records the presented document's chip identifier alongside the national identification number the session established.*
- *A cloned or shared document chip could otherwise be presented across multiple identity-proofing sessions, each establishing a different national identification number, without the PID Provider ever recording the fact that the same chip identifier was involved each time.*
- *This pairs the chip identifier already read during identity proofing with the resulting national identification number in the PID Provider's administration.*
- *A CAB verifies that chip identifier and national identification number are recorded together for each identity-proofing session, for instance by reviewing the administration data and testing the scenario.*

ISS-5.3-14: [CONDITIONAL] If the PID Provider performs the identity proofing based on a digital identity document, the PID Provider shall flag, for investigation, an identity document chip identifier that has been recorded together with more than one distinct national identification number.

Guidelines

- *When the PID Provider's records show the same document chip identifier paired with more than one distinct national identification number, it raises that chip identifier for investigation.*
- *A cloned document, a shared document, or a compromised derivation step could each let one physical chip be used to obtain PIDs for more than one claimed identity; without cross-referencing across sessions, none of these would come to light.*
- *This check runs against the pairing already recorded under ISS-4.3-13 and can be performed at the time of each new identity-proofing session or on a periodic basis.*
- *A CAB verifies that a chip identifier recorded against more than one national identification number results in a flag, for instance by reviewing the cross-referencing mechanism and testing the scenario.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5.4 PID Issuance Request and Authorisation

ISS-5.4-01: The PID Provider shall reject an issuance request that does not contain a valid, unused freshness value bound to the authenticated wallet session.

Guidelines

- *The PID Provider rejects any issuance request that lacks a valid, single-use freshness value tied to the authenticated wallet session.*
- *Without a bound single-use freshness value, a captured issuance request could be replayed to obtain an unauthorised PID.*
- *A server-generated nonce or equivalent, bound to the session and consumed on first use, accompanies each request.*
- *A CAB verifies that a replayed request, and a request with a missing or reused freshness value, are both rejected, for instance by testing both cases.*

ISS-5.4-02: The PID Provider shall not authorise issuance unless every required pre-condition has been successfully completed, comprising Wallet Unit trust verification, user identity verification, and the eligibility check.

Guidelines

- *The PID Provider authorises issuance only when every prerequisite, namely unit trust verification, identity verification, the eligibility check, has been completed successfully.*
- *Authorising issuance with a skipped prerequisite could produce a PID that was never properly verified or consented to.*
- *A single authorisation gate checks the recorded outcome of each prerequisite step before issuance proceeds.*
- *A CAB verifies that issuance is blocked when any one prerequisite is incomplete, for instance by reviewing the authorisation gate and testing the scenario.*

ISS-5.4-03: The PID Provider shall log an issuance request rejected for failing a freshness or replay check, together with the reason for rejection.

Guidelines

- *Each time the PID Provider rejects an issuance request because it fails a freshness or replay check, it records that rejection and the reason in a log.*
- *Without this record, repeated replay attempts against the same Wallet Unit or credential would be invisible even though each individual attempt is correctly blocked, so a sustained attack would not be noticed until an issuance eventually succeeded through some other weakness.*
- *The rejection log entry is typically written by the same component that performs the freshness or replay check, capturing the check that failed and the request context.*
- *A CAB verifies that rejected replay or freshness-check failures are logged with their reason, for instance by reviewing log samples and testing the scenario.*

ISS-5.4-04: [CONDITIONAL] Where one or more contact methods are registered for a person, the PID Provider shall not authorise the issuance of a PID in that person's name to a Wallet Unit that does not yet hold a Logical PID of that person unless the person has entered in the issuance flow the one-time code that the PID Provider has sent through a registered contact method.

Guidelines

- *Issuance of a PID to a new Wallet Unit is confirmed with a one-time code that reaches the person through at least one of the contact methods registered earlier, so that the person actually decides whether a new Wallet Unit is set up in their name.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *An attacker who passes identity proofing with stolen or relayed credentials and installs a wallet on a device of the attacker's own gets a working PID in the victim's name, and the victim finds out only afterwards. Because the code goes only to the contact methods of the person, the attacker cannot complete the issuance without the cooperation of the person.*
- *The code is sent by text message to the registered mobile number or by e-mail to the registered address, and the person types it into the issuance flow. Registration and verification of contact methods is covered by **ISS-5.7-20** and **ISS-5.7-21**. A person who no longer has access to a registered contact method first replaces it as described in **ISS-5.7-24**. This requirement does not apply to renewal or replenishment of a Logical PID that is already held by the Wallet Unit.*
- *A CAB verifies this requirement by reviewing the issuance flow and the authorisation logic, for instance by examining that issuance to a new Wallet Unit is not authorised without a matching code from a registered contact method, and by inspecting records of past issuances for the presence of the code confirmation.*

ISS-5.4-05: The PID Provider shall ensure that every message that carries a one-time code under **ISS-5.4-04** names the Wallet Provider of the Wallet Unit concerned, states that a new Wallet Unit is being set up in the person's name, warns the person never to share the code with anyone, and contains no link, QR code, or telephone number to call.

Guidelines

- *The message that delivers the code tells the person which Wallet Provider the request comes from, that a new Wallet Unit is being set up, and that the code is never to be shared with anyone.*
- *A fraudster who has persuaded a victim to forward a code, for example by posing as a bank employee or as the government, depends on the victim not understanding what the code is for. A message that states what is about to happen, and that contains nothing to click or call, gives the victim the information to recognise the attempt and removes the fraudster's route to redirect the victim.*
- *The message is short and states the three facts in plain language, for instance the name of the Wallet Provider, the words that a new Wallet Unit is being set up in the person's name, and a sentence that if the code is asked for by another person, that the conversation with that person should be halted immediately as this is a very strong sign of fraud. The wording follows the communication charter that applies to the PID Provider and all Wallet Providers.*
- *A CAB verifies this requirement by reviewing the templates of the messages and the configuration that fills them, for instance by inspecting a sample of messages sent in the past, and by confirming that each contains the three required statements and no link, QR code or telephone number.*

ISS-5.4-06: The PID Provider shall invalidate a one-time code issued under **ISS-5.4-04** or **ISS-5.7-21** after its first successful use, after the end of a defined validity period, and after a defined number of failed entry attempts.

Guidelines

- *A one-time code works once, for a short time, and for a limited number of attempts.*
- *A code that stays valid after use, for a long time or for unlimited attempts is exposed to guessing, to reuse after the person has been talked into reading it out, and to replay against a later issuance.*
- *The PID Provider determines the validity period and the number of attempts as part of its risk assessment, and generates codes with sufficient entropy for the chosen limits.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *A CAB verifies this requirement by reviewing the design and configuration of the code service, for instance by inspecting the validity period and attempt limit that are set, and by examining records of issued codes that show invalidation after use, expiry or failed attempts.*

5.5 PID Generation and Signing

ISS-5.5-01: The PID Provider shall not generate a PID unless a complete and current set of the required attributes has been obtained from the authoritative population register.

Guidelines

- *The PID Provider generates a PID only once it holds a complete and current set of the required attributes obtained from the authoritative population register.*
- *Generating a PID from incomplete or outdated attribute data would issue a credential that misstates the person's authoritative identity.*
- *The provider retrieves the attributes from the authoritative register at issuance time and confirms completeness before generation.*
- *A CAB verifies that generation does not proceed with an incomplete attribute set, for instance by reviewing the register-retrieval step and testing the scenario.*

ISS-5.5-02: The PID Provider shall populate each mandatory PID attribute in accordance with the applicable national value convention, including the defined fall-back values where an attribute value is not available.

Guidelines

- *The PID Provider fills each mandatory PID attribute following the applicable national value convention, using the defined fall-back values where a value is unavailable.*
- *Inconsistent attribute population or ad-hoc handling of missing values would produce PIDs that relying parties cannot interpret reliably.*
- *A documented mapping from register fields to PID attributes, including the national fall-back values, drives population.*
- *A CAB reviews the attribute-mapping documentation and inspects issued PIDs for conformant values and fall-backs.*

ISS-5.5-03: The PID Provider shall not fetch, process, or store any optional attribute that has been excluded at national level.

Guidelines

- *The PID Provider does not fetch, process, or store any optional attribute that has been excluded at national level.*
- *Handling excluded attributes would collect or expose personal data beyond what is proportional.*
- *The set of permitted attributes is configured from national policy, and retrieval or storage of anything outside it is suppressed.*
- *A CAB verifies that excluded attributes are neither retrieved nor retained, for instance by reviewing the configured attribute set and testing the scenario.*

ISS-5.5-04: The PID Provider shall bind the PID to the dedicated PID binding public key provided for that PID and to no other key.

Guidelines

- *The PID Provider binds the PID to the dedicated PID binding public key provided for that PID and to no other key.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Binding to the wrong key, for instance a reused or unrelated key, would let a party other than the intended holder use the credential.*
- *The provider takes the binding public key from the proof-of-possession step of the same issuance and embeds only that key. The binding public key is the dedicated PID binding key whose generation and protection in the Wallet Unit's certified cryptographic device has been attested to the PID Provider, so that the PID is placed under the sole control of the User and bound to that Wallet Unit alone.*
- *A CAB verifies that a PID is not bound to any key other than the one presented for that issuance, for instance by inspecting the binding in issued PIDs and testing the scenario.*

ISS-5.5-05: The PID Provider shall sign the PID using a signing key whose certificate chains to a trust anchor published in the applicable trusted list.

Guidelines

- *The PID Provider signs the PID with a signing key whose certificate chains to a trust anchor published in the applicable trusted list.*
- *A signing key that is not anchored in the trusted list would produce PIDs that relying parties cannot validate as authentic.*
- *The signing certificate is issued under a chain terminating at a published trust anchor, and that chain is kept current.*
- *A CAB verifies the signing certificate chain against the trusted list and inspects a signed PID.*

ISS-5.5-06: The PID Provider shall use the PID signing key only within the authorised issuance process.

Guidelines

- *The PID Provider uses the PID signing key solely within the authorised issuance process and for no other purpose.*
- *Use of the signing key outside the controlled issuance process could produce unauthorised or forged PIDs.*
- *The signing key is held in a protected signing service whose invocation is restricted to the issuance workflow.*
- *A CAB reviews the access controls and usage logs for the signing key and confirms that its use is confined to PID issuance.*

ISS-5.5-07: The PID Provider shall set the validity period of the PID so that it does not exceed the maximum PID lifetime defined by national policy.

Guidelines

- *The PID Provider sets the PID validity period so that it does not exceed the maximum PID lifetime defined by national policy.*
- *An over-long validity period would keep a credential usable well beyond the point where its data or binding can be relied upon.*
- *The configured maximum lifetime from national policy caps the validity end date computed at generation.*
- *A CAB reviews the configured maximum and inspects issued PIDs for conformant validity periods.*

ISS-5.5-08: The PID Provider shall set the validity period of the PID so that it does not extend beyond the validity of the Wallet Unit to which the PID is issued.

Guidelines

- *The PID Provider sets the PID validity so that it does not extend beyond the validity of the Wallet Unit to which the PID is issued.*
- *A PID outliving its Wallet Unit could remain nominally valid in a unit that is no longer trusted.*
- *The validity end date is capped at the earlier of the national maximum and the Wallet Unit's own validity.*
- *A CAB inspects issued PIDs against the corresponding unit validity and confirms that the PID does not outlast the unit.*

5.6 Secure PID Delivery

ISS-5.6-01: The PID Provider shall not release a PID to the Wallet Unit before authentication of the Wallet Unit and of the holder has completed successfully.

Guidelines

- *The PID Provider releases the PID to the unit only after both the Wallet Unit and the holder have been authenticated successfully.*
- *Releasing before authentication completes could deliver a PID to an unverified unit or to someone other than the holder.*
- *A release gate withholds the PID until both authentication results are confirmed within the session.*
- *A CAB verifies that no PID is released when either authentication is incomplete, for instance by testing the scenario.*

ISS-5.6-02: The PID Provider shall deliver the PID to the Wallet Unit using the issuance protocol specified in [5].

Guidelines

- *The PID Provider delivers the PID over the issuance protocol defined in the referenced normative specification rather than over an ad-hoc channel.*
- *An unspecified delivery mechanism would lead to interoperability in the EUDIW ecosystem and could omit the mutual authentication and secure-channel properties that the standard issuance protocol guarantees, exposing the PID in transit.*
- *The delivery uses the issuance protocol profile named in the requirement, including its authentication and secure-transport provisions.*
- *A CAB verifies an issuance exchange for conformance with the referenced specification, for instance by reviewing the implemented protocol and testing the exchange.*

ISS-5.6-03: The PID Provider shall record the outcome of each issuance, including any refusal of the issued PID by the Wallet Unit and any case where the Wallet Unit does not respond.

Guidelines

- *The PID Provider records the outcome of each issuance, including any case where the unit refuses the issued PID or when the Wallet Unit does not respond anymore.*
- *Without recorded outcomes, refusals and failures would go untracked, hindering incident investigation and reconciliation.*
- *The outcome, including a refusal, is written to the issuance record as the exchange concludes.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *A CAB reviews issuance records and confirms that both successful and refused outcomes are captured.*

ISS-5.6-04: The PID Provider shall classify a PID that has left its systems as issued, regardless of whether the Wallet Unit confirms its acceptance.

Guidelines

- *The PID Provider treats any PID that has left its systems as issued, even if the unit has not confirmed acceptance.*
- *If a delivered PID were treated as never issued because acceptance was not confirmed, a credential that actually reached a unit could remain unaccounted for, for example when an acceptance message is lost.*
- *The provider marks the PID as issued at the point it leaves the provider boundary, independently of any later acceptance confirmation.*
- *A CAB verifies that a PID which has left the provider is recorded as issued when acceptance confirmation is withheld, for instance by reviewing the state model and testing the scenario.*

ISS-5.6-05: The PID Provider shall revoke a PID that it has classified as issued where the Wallet Unit reports that the PID was not accepted.

Guidelines

- *Where the unit reports that a PID it has classified as issued was not accepted, the PID Provider revokes that PID rather than cancelling it.*
- *Cancelling instead of revoking a PID that may in fact have reached a unit could leave a usable credential outside the revocation status, because a not-accepted report can be a false negative.*
- *On a not-accepted report for an issued PID, the provider drives it through the revocation path so that its status is published.*
- *A CAB verifies that a not-accepted report for an issued PID results in the PID being revoked and not cancelled, for instance by testing the scenario.*

5.7 Post-Issuance Status Service Registration

ISS-5.7-01: The PID Provider shall register each issued PID, including its identifier, its validity end date, and its status, in the PID Provider's administration and status service.

Guidelines

- *The PID Provider records each issued PID, with its identifier, validity period, and status, in its administration and status service.*
- *An unregistered PID could not be tracked or revoked, and its status could not be published to relying parties.*
- *Registration writes the identifier, validity, and status to the status service as part of completing issuance.*
- *A CAB reviews the status service contents and confirms that issued PIDs appear with the required fields.*

ISS-5.7-02: The PID Provider shall record, for each issued PID, the Wallet Unit to which that PID was issued.

Guidelines

- *The PID Provider records, for each issued PID, which Wallet Unit it was issued to.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Without this record the provider could neither prevent a second valid PID from going to the same unit nor detect that an additional wallet has been activated for the same person.*
- *The Wallet Unit identifier is stored alongside the PID record at issuance and used in later duplicate checks.*
- *A CAB inspects issuance records and confirms that the issuing-target Wallet Unit is captured for each PID.*

ISS-5.7-03: The PID Provider shall record the withdrawal of a PID that has already been delivered to a Wallet Unit as a revocation with a corresponding entry in the status service.

Guidelines

- *When a PID that has already been delivered is withdrawn, the PID Provider records the withdrawal as a revocation with a matching status-service entry.*
- *Recording a delivered PID's withdrawal as anything other than a revocation would leave relying parties unaware that the credential is no longer valid.*
- *The withdrawal of a delivered PID is routed to the revocation path, producing a published status change.*
- *A CAB verifies that withdrawal of a delivered PID produces a revocation entry in the status service, for instance by testing the scenario.*

ISS-5.7-04: The PID Provider shall record each issuance event in a tamper-evident log with sufficient detail to support conformity assessment and incident investigation.

Guidelines

- *The PID Provider records each issuance event in a log that is protected against tampering and detailed enough for conformity assessment and incident investigation.*
- *A log that could be altered, or that lacks detail, would undermine after-the-fact investigation and audit.*
- *Log entries are written to append-only or integrity-protected storage capturing the salient issuance facts and timestamps.*
- *A CAB reviews the log's integrity protection and confirms that entries carry sufficient investigative detail.*

ISS-5.7-05: The PID Provider shall notify the person identified in the PID, through a channel independent of the Wallet Unit, when a PID is issued in that person's name.

Guidelines

- *The PID Provider notifies the identified person, over a channel that does not depend on the Wallet Unit, whenever a PID is issued in that person's name.*
- *Without an independent notification, a PID issued fraudulently in someone's name could go unnoticed by the victim.*
- *The notification is sent over a channel the person holds independently of the wallet, such as an official government message box or a registered contact method.*
- *A CAB reviews the notification mechanism and confirms that an out-of-band notice is generated on issuance.*

ISS-5.7-05A: The PID Provider shall notify the person in whose name a PID was requested, through a channel independent of the Wallet Unit, when a request to issue a PID in that person's name does not result in issuance because identity proofing or another eligibility check failed, inviting that person to raise an alarm if they did not make the request.

Guidelines

- *The PID Provider sends an out-of-band notice not only when a PID is issued (ISS-4.7-05) but also when an attempt to obtain a PID in a person's name is made and does*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

not complete, for example because identity proofing failed, asking the person to report the attempt if they did not make it.

- *Without notice of a failed attempt, a fraudulent attempt that is stopped by proofing leaves no signal to the targeted person, so an attacker can retry or refine the attempt while the victim remains unaware that their identity is being targeted.*
- *The notice is sent over the same independent channel used for ISS-4.7-05, addressed to the person named in the request as held by the Authentic Source, and tells the person to raise an alarm if they did not initiate the request; the PID Provider applies rate and content safeguards so the notice itself cannot be used to probe or harass a person.*
- *A CAB verifies that a failed or refused issuance attempt generates an out-of-band notice to the named person with instructions to report an unrecognised attempt, for instance by testing a request that fails identity proofing.*

ISS-5.7-06: The PID Provider shall notify the identified person, through a channel independent of the Wallet Unit, when more than one Logical PID issued by that PID Provider is active in that person's name.

Guidelines

- *The PID Provider notifies the person, over a wallet-independent channel, when more than one PID that it has issued is active (has an ongoing valid Administrative Validity Period) in that person's name.*
- *Several active PIDs for one person can signal that a second wallet has been activated fraudulently, and a person left unaware cannot intervene.*
- *The provider detects the condition from its own active-PID records per person and triggers the notification.*
- *A CAB verifies that a notification is generated for the multiple-active-PID condition, for instance by testing the scenario.*

ISS-5.7-07: The PID Provider shall offer the person the opportunity to register one or more contact methods that are capable of delivering a notification to the person without delay.

Guidelines

- *The PID Provider gives the person the opportunity to register one or more contact methods able to reach them without delay.*
- *If notifications only reach a channel the person checks infrequently, an attacker's window to misuse a fraudulent PID before the person reacts is much longer.*
- *The provider offers registration of instantaneous channels, such as a mobile number for text messaging or an email address, in addition to any default channel.*
- *A CAB reviews the enrolment options and confirms that the person can register an instantaneous contact method.*

ISS-5.7-08: The PID Provider shall ensure that the notification referred to in **ISS-5.7-06** states explicitly that the activation of a further Wallet Unit that the person did not perform or authorise or that was done on request of someone else, may result in financial loss or identity theft to that person.

Guidelines

- *The PID Provider makes the notification about a further active wallet state plainly that an activation the person did not perform or authorise or that was done on request of someone else (potentially an attacker), can lead to financial loss or identity theft.*
- *A notice that does not convey the concrete consequences may be ignored or the attacker could easily convince the victim that the message can be safely disregarded, so the person fails to act on a genuine fraud signal. In the case of social engineering*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

the victim is under influence of the attacker and the message should be strong enough to make the victim realize he might be under attack and reconsider whether to continue to follow the instructions of the attacker.
- *The notification text names the potential harms in clear, plain language accessible to the recipient.*
- *A CAB inspects the notification content and confirms that the explicit harm statement is present.*

ISS-5.7-09: The PID Provider shall include, in the notification referred to in **ISS-5.7-06**, a means for the person to revoke the newly issued PID through a low-threshold procedure.

Guidelines

- *The PID Provider includes in that notification an easy, low-threshold way for the person to revoke the newly issued PID.*
- *If revoking a suspicious new PID were difficult, a person who recognises fraud might be unable to stop it quickly enough.*
- *The notification carries a direct, simple action, such as a single link or short procedure, that revokes the newly issued PID.*
- *A CAB reviews the notification and confirms that it provides a low-threshold revocation path for the newly issued PID.*

ISS-5.7-10: The PID Provider shall require the use of its standard revocation procedure to revoke any PID, other than the newly issued PID referred to in **ISS-5.7-09**, that is active in that person's name.

Guidelines

- *The PID Provider confines the low-threshold revocation offered in the notification to the newly issued PID, and requires any other PID active in the person's name to be revoked through the standard revocation procedure.*
- *If the low-threshold path could revoke the person's earlier legitimate PID, an attacker could use the notification itself to trick the victim into revoking their genuine credential and locking themselves out.*
- *The low-threshold action is scoped to the single new PID, while revocation of any pre-existing PID is directed to the normal, more deliberate revocation channel.*
- *A CAB verifies that the notification's low-threshold action cannot revoke a PID other than the newly issued one, and that any other PID requires the standard procedure, for instance by testing the scenario.*

ISS-5.7-11: The PID Provider shall record, for each national identification number, the number of Wallet Units to which a PID for that national identification number is currently issued and within its Administrative Validity Period, and the timestamps of each issuance and renewal request relating to that national identification number.

Guidelines

- *The PID Provider keeps a running count of active Logical PIDs and a timestamped history of issuance and renewal requests, indexed by national identification number.*
- *Without such a record, a Logical PID issued into an additional Wallet Unit under someone else's control, alongside the legitimate holder's own working Wallet Unit, would leave no trace an investigator could later use to notice that more than one active PID exists for the same person.*
- *This is typically implemented as an addition to the PID Provider's existing administration and status service, keyed by national identification number rather than by Logical PID identifier alone; the same record is drawn on for renewal requests under Chapter 6.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *A CAB verifies that the administration records active-Logical-PID counts and request timestamps per national identification number, for instance by inspecting the administration data model and issuing a test PID.*

ISS-5.7-12: The PID Provider shall flag, for investigation, a national identification number whose active-Logical-PID count or issuance-or-renewal-request rate exceeds a defined threshold.

Guidelines

- *When the count of active Logical PIDs, or the rate of issuance or renewal requests, for a given national identification number exceeds a threshold the PID Provider has defined, the PID Provider raises that identification number for investigation.*
- *An attacker who has obtained a genuine PID into an additional Wallet Unit relies on this pattern going unnoticed; without a threshold-based flag, the resulting anomaly in active-PID count would never be surfaced to anyone able to act on it.*
- *The threshold and the resulting investigative workflow are defined by the PID Provider's own fraud-management process; this requirement only constrains that some such threshold and flagging mechanism exists.*
- *A CAB verifies that exceeding the defined threshold results in the identification number being flagged, for instance by reviewing the threshold configuration and testing the scenario.*

ISS-5.7-13: The PID Provider shall record, where available to it, the network origin or locality indicator of each issuance or renewal request.

Guidelines

- *Where the PID Provider has access to a network origin or locality indicator for an issuance or renewal request, such as the requesting network's approximate location, it records that indicator with the request.*
- *Without any locality indicator on record, two issuance or renewal events for the same person occurring in quick succession from geographically implausible locations would look identical to two ordinary, unrelated requests.*
- *This depends on whatever network-origin information is already available to the PID Provider's issuance and renewal channel; it does not require introducing new means of locating the User.*
- *A CAB verifies that available network origin or locality indicators are recorded with issuance and renewal requests, for instance by reviewing request records and testing the scenario.*

ISS-5.7-14: The PID Provider shall flag, for investigation, two issuance or renewal requests relating to the same national identification number whose recorded network origin or locality indicators are inconsistent with the time elapsed between them.

Guidelines

- *When two issuance or renewal requests for the same national identification number carry locality indicators that could not both be genuine given the time between the requests, for example locations a person could not plausibly travel between in that time, the PID Provider raises that pair of requests for investigation.*
- *This pattern is a recognised indicator that one of the two requests originates from a party other than the legitimate holder, for example an attacker operating a duplicate Wallet Unit or impersonating the holder from elsewhere, while the holder's own genuine request continues undisturbed.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *The plausibility check compares the recorded locality indicators and elapsed time against a configured travel-speed assumption; it is only meaningful where locality indicators were captured under ISS-4.7-13.*
- *A CAB verifies that a geographically implausible pair of requests results in a flag, for instance by reviewing the plausibility-check configuration and testing the scenario.*

ISS-5.7-15: The PID Provider shall subject each case that this specification requires to be flagged for investigation to a defined investigation and response procedure.

Guidelines

- *The PID Provider handles every case that this specification requires to be flagged for investigation through a defined procedure that determines the response, rather than recording the flag and leaving it without follow-up.*
- *Flagging a suspected fraud or anomaly without a defined follow-up would leave the detection signal unacted upon, so the control would not reduce the risk it was introduced to address.*
- *The PID Provider maintains an investigation and response procedure, aligned with a recognised fraud-management framework such as ISO 37003 [i.4], that assigns each flagged case for assessment and defines the possible responses.*
- *A CAB verifies that flagged cases are routed to a defined investigation and response procedure, for instance by reviewing the procedure and tracing a flagged case through it.*

ISS-5.7-16: The PID Provider shall record, for each issued PID, the Wallet Provider that provided the Wallet Unit to which the PID was issued and the date of issuance.

Guidelines

- *For every PID, the PID Provider keeps the name of the Wallet Provider of the receiving Wallet Unit and the date on which the PID was issued, in addition to the Wallet Unit recorded under **ISS-5.7-02**.*
- *Without these two data, the PID Provider cannot tell a person which Wallet Units are active in their name, cannot recognise a second Wallet Unit at the same Wallet Provider, and cannot route a revocation request or a report to the Wallet Provider concerned.*
- *The PID Provider takes the Wallet Provider from the Wallet Instance Attestation validated under **ISS-5.2-01** and the date from the issuance event logged under **ISS-5.7-04**.*
- *A CAB verifies this requirement by reviewing the data model of the administration and by examining a sample of PID records for the presence of the Wallet Provider and the issuance date.*

ISS-5.7-17: The PID Provider shall state, in each notification referred to in **ISS-5.7-05** and **ISS-5.7-06**, the Wallet Provider and the date of issuance recorded under **ISS-5.7-16** for the Wallet Unit concerned.

Guidelines

- *Each notification names the Wallet Provider and the date, so the person can tell a Wallet Unit they know from one they do not.*
- *A notification that only says that a PID has been issued does not allow the person to tell their own new device from an attacker's device, and is easily dismissed as routine.*
- *The Wallet Provider and date are included in the notification text, for instance in the first sentence.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *A CAB verifies this requirement by reviewing the notification templates and by examining a sample of sent notifications for the presence of the Wallet Provider and the date.*

ISS-5.7-18: The PID Provider shall list, in the notification referred to in **ISS-5.7-06**, every Wallet Unit in which an active Logical PID is held in the person's name, stating for each the Wallet Provider and the date of issuance, and invite the person to revoke any Wallet Unit that is suspicious or no longer in use through the standard revocation procedure referred to in **ISS-5.7-10**.

Guidelines

- *The notification about a further Logical PID gives the person the complete picture: every active Wallet Unit with its Wallet Provider and issuance date, and an invitation to revoke those that are unknown or unused.*
- *If the person is told only about the newest Wallet Unit, an older fraudulent Wallet Unit, or one that was forgotten after a change of phone, stays active and unnoticed.*
- *The list is built from the data recorded under **ISS-5.7-16**. The invitation points to the revocation route to which the person authenticates, and does not offer a revocation link that works from a Wallet Unit.*
- *A CAB verifies this requirement by reviewing the notification templates and the logic that builds the list, and by examining a sample of notifications sent where more than one Logical PID was active.*

ISS-5.7-19: The PID Provider shall not disclose to a Wallet Unit, or offer through a Wallet Unit a means to revoke, any other Wallet Unit in which a PID is held in the name of the same person.

Guidelines

- *Information about, and revocation of, a person's Wallet Units is available to the person through channels that do not depend on a Wallet Unit, and never through a Wallet Unit itself.*
- *An attacker who has activated a Wallet Unit in the victim's name could otherwise see the victim's other Wallet Units and revoke them, which locks the victim out and leaves the attacker as sole holder.*
- *The PID Provider limits the issuance protocol responses to the Wallet Unit to what that Wallet Unit needs, and offers the overview and revocation of Wallet Units only through a route that is not a Wallet Unit, as described in the PID Lifecycle Events Specification [7].*
- *A CAB verifies this requirement by reviewing the interface descriptions of the issuance protocol and by inspecting the responses sent to a Wallet Unit, for instance to confirm that they contain no data about other Wallet Units of the person.*

ISS-5.7-20: The PID Provider shall, at the first issuance of a PID in a person's name, collect from the person both a mobile telephone number that is able to receive text messages and an e-mail address, and register them as contact methods under **ISS-5.7-07** unless the person explicitly declines.

Guidelines

- *At the first issuance, the person is asked for both a mobile number and an e-mail address, and both are registered unless the person declines.*
- *If no contact method is registered, the notifications and codes of the PID Provider can only reach a channel that the person checks rarely, and an attacker has a long window to use a fraudulent PID. Two independent channels reduce the risk that a single compromised channel hides the attack.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *The collection is part of the first-issuance flow, after identity proofing. Declining is recorded, so the PID Provider notifies through the channel of **ISS-5.7-05** only. A person who declined is offered registration again at each later issuance.*
- *A CAB verifies this requirement by reviewing the first-issuance flow and by examining the records of a sample of first issuances for the registered contact methods or the recorded refusal.*

ISS-5.7-21: The PID Provider shall register a contact method only after the person has entered a one-time code that the PID Provider has sent to that contact method.

Guidelines

- *A contact method is registered only after the person has shown that they have access to it by entering a code sent to it.*
- *An attacker who is allowed to register a contact method without proof of access can register a number or address of their own, so that every later warning and code reaches the attacker instead of the victim.*
- *The code follows **ISS-5.4-06**. The PID Provider repeats the verification whenever a contact method is added or replaced.*
- *A CAB verifies this requirement by reviewing the registration flow and by examining records of registered contact methods for the verification event.*

ISS-5.7-22: The PID Provider shall replace a registered contact method only after the person has entered a one-time code that the PID Provider has sent to the contact method that is being replaced, except where **ISS-5.7-24** applies.

Guidelines

- *A contact method is changed only with proof of access to the existing one.*
- *An attacker who has obtained a PID could otherwise replace the contact methods of the victim with their own, so that further warnings and codes no longer reach the victim.*
- *The code follows **ISS-5.4-06** and the new contact method is verified under **ISS-5.7-21**. A person who has no access to the contact method being replaced follows **ISS-5.7-24**.*
- *A CAB verifies this requirement by reviewing the contact-change flow and by examining records of past changes for the code confirmation.*

ISS-5.7-23: The PID Provider shall notify every contact method registered before a change, through that contact method, when a registered contact method has been replaced.

Guidelines

- *Whenever a contact method is replaced, the previous contact methods are told.*
- *Even a verified change is sometimes the result of social engineering; a notice to the previous contact gives the person the opportunity to see the change and to react.*
- *The notice states the date of the change and that the change was made. It does not contain the new contact details in full, so that it is useless to a person who intercepts it.*
- *A CAB verifies this requirement by reviewing the contact-change flow and by examining a sample of changes for the notification to the previous contact methods.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.7-24: The PID Provider shall, where the person has no access to a contact method that is to be replaced, replace it only after identity proofing in accordance with clause 4.3, at the same assurance level as required for initial issuance, has been completed for that person.

Guidelines

- *A person who has lost their phone number or e-mail address changes their contact details by proving who they are again.*
- *Without an alternative route, a person who lost a contact method would be locked out of every future issuance; with a weaker route, an attacker would use it to take over the contact methods.*
- *The route uses the same identity proofing as the initial issuance, and the notice of **ISS-5.7-23** still applies to the previous contact methods.*
- *A CAB verifies this requirement by reviewing the replacement route and by examining records of such replacements for the identity proofing event.*

ISS-5.7-25: The PID Provider shall flag, for investigation, a network origin indicator recorded under **ISS-5.7-13** that is linked to issuance or renewal requests for more than a defined number of distinct national identification numbers within a defined period.

Guidelines

- *The PID Provider flags a network origin from which requests for many different persons arrive in a short period.*
- *A fraudster who operates a farm of devices or an anonymising network to open Wallet Units in the name of many victims is not visible from any single request, but is visible when requests for many identities share the same origin.*
- *The number and the period are determined as part of the risk assessment. Flagged cases follow the procedure of **ISS-5.7-15**. The PID Provider sees the network origin only for its own issuances; it does not receive a device identifier, consistent with **ISS-5.3-02**.*
- *A CAB verifies this requirement by reviewing the detection rules and their configuration and by examining records of past flags and of the investigations that followed.*

ISS-5.7-26: The PID Provider shall limit the retention of the network origin indicators recorded under **ISS-5.7-13** to a period determined as part of its risk assessment.

Guidelines

- *Network origin data are kept only as long as the fraud detection needs them.*
- *Long-lived records of network origin build up a profile of where people are, long after the fraud detection has any use for it.*
- *Deletion of expired records is automatic. The retention period is long enough for the period used in **ISS-5.7-25**.*
- *A CAB verifies this requirement by reviewing the risk assessment and the retention configuration, and by examining that records older than the retention period are absent.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

ISS-5.7-27: The PID Provider shall use the network origin indicators recorded under **ISS-5.7-13** for no purpose other than the detection of fraud.

Guidelines

- *Network origin data serve fraud detection and nothing else.*
- *Data collected as a fraud control that are reused for other purposes, such as profiling or analytics, would turn the control into surveillance.*
- *Access to the records is limited to the staff and systems that operate the detection and investigation under **ISS**-5.7-15.*
- *A CAB verifies this requirement by reviewing the access rules and the documented purposes of the records, and by examining access logs.*

6 Lifecycle Event: PID Batch Replenishment

Purpose of this chapter: Govern the silent, autonomous replenishment of a Wallet Unit's supply of once-only Technical PIDs. When the number of unused Technical PIDs held by the Wallet Unit falls below a defined threshold, additional Technical PIDs are re-issued to the Wallet Unit without any user action and without renewed identity proofing, so that the Wallet User can continue to present a PID without interruption. This chapter covers the technical requirements that govern the batch replenishment interaction between the PID Provider and the Wallet Unit. NOTE: Batch replenishment does not re-verify the identity of the Wallet User; it relies on the identity proofing performed at the most recent initial issuance or renewal. Where renewed identity proofing is required (for example on expiry of the PID validity period), *the PID Renewal event applies instead.*

6.1 Replenishment Triggers and Threshold

REP-6.1-01: ISS-4.4-01 applies in this context as well.

REP-6.1-02: The PID Provider shall not replenish Technical PIDs to a Wallet Unit for which the Administrative Validity Period has ended.

Guidelines

- *Once the Administrative Validity Period has ended, the silent replenishment path is closed for that Wallet Unit, and obtaining a new PID afterwards requires a fresh issuance or renewal process that includes identity proofing.*
- *This prevents replenishment from being used to silently re-supply a person whose PID was revoked by a competent authority for fraud or loss of eligibility, bypassing the identity proofing at Assurance Level High that re-establishment demands.*
- *The revocation state is read from the PID Provider's own administration and status service, in which every Logical PID's status is maintained.*
- *A CAB verifies that a replenishment request referencing a revoked Logical PID is refused, by inspecting the status-service linkage and testing the flow against a revoked Logical PID.*

REP-6.1-03: The PID Provider shall verify, before issuing replenished Technical PIDs, that the attribute values of the Logical PID remain current.

Guidelines

- *Before replenishing, the PID Provider confirms that the Logical PID does not need to change, that is, that the attribute values it would place into the new Technical PIDs still match the authoritative record.*
- *Without this check, silent replenishment keeps creating Technical PIDs that carry attribute values which have since changed at the authoritative source, so the person continues to present out-of-date data long after the underlying facts changed.*
- *Currency can be confirmed by re-reading the authoritative population register, or by acting on a change notification from it.*
- *A CAB reviews how the PID Provider establishes attribute currency at replenishment and verifies that replenishment does not proceed with stale values when the source record has changed.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REP-6.1-04: The PID Provider shall revoke the outstanding Technical PIDs of a Logical PID when a revocation condition for that Logical PID is established.

Guidelines

- *A revocation condition for a Logical PID arises for cause, for example loss of eligibility, a security incident, or at the person's request. When such a condition is applicable, then it is applicable to all technical PIDs that are issued for that logical which means they all need to be revoked.*
- *Without this control, revoking a Logical PID would leave batch-issued copies of it valid and presentable, so a person or a Relying Party could continue to rely on a credential the PID Provider itself has already invalidated.*
- *Revocation is effected through the status service in which each Technical PID is registered under its Logical PID, while the detailed revocation procedure is governed by the PID lifecycle events specification.*
- *A CAB verifies that a revocation condition for a Logical PID results in every registered still valid Technical PID of it being set to revoked in the status service, for instance by testing the scenario against a Technical PID that has not yet reached the end of its own validity period.*

REP-6.1-05: The PID Provider shall not continue automatic replenishment to a Wallet Unit for which it has received an indication that the Wallet Unit or its device is no longer under the legitimate user's control.

Guidelines

- *On any reliable signal that the Wallet Unit or its device has been lost, stolen, or otherwise placed outside the legitimate user's control, the PID Provider stops the silent replenishment stream to that Wallet Unit.*
- *Without this control, a valid but misappropriated refresh token keeps yielding fresh batches to an attacker's device or a duplicate device indefinitely, because the victim's own wallet keeps working and nothing else signals a problem.*
- *Qualifying indications include revocation of the Wallet Instance Attestation, a reported loss or theft, or a fraud flag raised on the Logical PID, and the PID Provider treats continued replenishment as conditional on the absence of such an indication.*
- *A CAB verifies that replenishment stops after a loss, theft, or Wallet Unit revocation indication is recorded, for instance by reviewing which signals halt replenishment and testing the scenario.*

REP-6.1-06: The PID Provider shall not treat an indication that a Wallet Unit or its device is no longer under the legitimate user's control as qualifying under REP-5.1-05 unless the reliability of that indication has been established through a defined verification procedure.

Guidelines

- *Before an indication of lost control is allowed to halt replenishment under REP-5.1-05, the PID Provider passes it through a defined procedure that establishes whether the indication is genuine and attributable to a trustworthy source.*
- *Without this check, an attacker or an unreliable third party could fabricate or relay a false report that a Wallet Unit or its device is no longer under the legitimate user's control, causing the PID Provider to cut the legitimate user off from further Technical PIDs even though nothing is actually wrong.*
- *A defined verification procedure typically authenticates the reporting channel (for example the Wallet Provider, a government authority, or the user's own authenticated channel) and corroborates the content of the report before it is acted upon; qualifying indications and their expected sources are addressed in REP-5.1-05.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *A CAB verifies that an unauthenticated or uncorroborated report is not sufficient on its own to halt replenishment, for instance by reviewing the verification procedure and testing a fabricated report.*

REP-6.1-07: The PID Provider shall record the timestamp and the Technical-PID count of each batch replenishment performed for a Wallet Unit.

Guidelines

- *Each time the PID Provider replenishes a Wallet Unit's batch of Technical PIDs, it records when this happened and how many Technical PIDs were issued.*
- *Without this record, a Wallet Unit or device no longer under the legitimate user's control that continues to receive replenished batches on a stolen or replayed token would show no trace an investigator could use to notice the abnormal replenishment activity.*
- *This is typically an addition to the batch-replenishment processing already required, writing the timestamp and count to the PID Provider's administration alongside the existing token-verification outcome.*
- *A CAB verifies that batch-replenishment timestamp and count are recorded, for instance by reviewing the administration data and testing the scenario.*

REP-6.1-08: The PID Provider shall determine, as part of its risk assessment, a maximum batch size and a maximum number of outstanding Technical PIDs per Wallet Unit.

Guidelines

- *As part of its risk assessment, the PID Provider fixes an upper bound on the number of Technical PIDs issued in a single batch and on the number of outstanding Technical PIDs that a Wallet Unit may hold.*
- *Without a defined upper bound, there is no reference against which an excessive supply of Technical PIDs to a single Wallet Unit could be recognised or contained.*
- *The bounds follow from the once-only consumption rate over the PID validity period, balancing availability against privacy and abuse resistance, consistent with the reuse-policy parameters of the issuance protocol [5].*
- *A CAB verifies that the PID Provider has determined a maximum batch size and a maximum outstanding-count per Wallet Unit, for instance by reviewing the risk assessment and the resulting configured limits.*

REP-6.1-09: The PID Provider shall not exceed the maximum batch size or the maximum number of outstanding Technical PIDs per Wallet Unit, determined under REP-5.1-08, when replenishing a Wallet Unit.

Guidelines

- *When replenishing a Wallet Unit, the PID Provider stays within the maximum batch size and the maximum outstanding-count determined under REP-5.1-08.*
- *Enforcing the bounds prevents a compromised or misbehaving Wallet Unit from obtaining an unlimited supply of Technical PIDs, limiting the impact of a successful attack.*
- *Before issuing, the replenishment process checks the requested batch size and the Wallet Unit's current outstanding count against the determined limits and does not issue Technical PIDs beyond them.*
- *A CAB verifies that replenishment does not exceed the determined limits, for instance by testing a replenishment request that would exceed the maximum batch size or the maximum outstanding-count.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REP-6.1-10: The PID Provider shall, when it establishes that the attribute values held for a person by the Authentic Source have changed from those carried by the outstanding Technical PIDs of the Logical PID, revoke the outstanding Technical PIDs that carry the superseded values.

Guidelines

- *When the Authentic Source record for a person changes, the PID Provider revokes the Technical PIDs still outstanding that carry the superseded values, so that data the PID Provider no longer attests to can no longer be presented. The corresponding issuance of Technical PIDs carrying the new values is required by REP-5.1-11.*
- *Without this control, Technical PIDs carrying attribute values the PID Provider no longer attests to would remain valid and presentable, so a Relying Party could receive superseded data.*
- *The change is detected as part of the currency check of REP-5.1-03, by re-reading the Authentic Source or acting on a change notification from it; the revocation of the superseded Technical PIDs is effected through the status service in which each Technical PID is registered, while the detailed revocation procedure is governed by the PID lifecycle events specification. This replenishment does not repeat identity proofing, which is required only at renewal.*
- *A CAB verifies that a change in the Authentic Source attribute values results in every outstanding Technical PID carrying the superseded values being set to revoked, for instance by testing the scenario against the status service.*

REP-6.1-11: The PID Provider shall, when it establishes that the attribute values held for a person by the Authentic Source have changed from those carried by the outstanding Technical PIDs of the Logical PID, henceforth issue new Technical PIDs carrying the updated attribute values.

Guidelines

- *When the Authentic Source record for a person changes, the PID Provider henceforth issues Technical PIDs carrying the new attribute values to the Wallet Unit, so that current data remains available for presentation. This issuance accompanies the revocation of the superseded Technical PIDs required by REP-5.1-10.*
- *Without this control, new Technical PIDs could still contain data that is not valid anymore.*
- *The new Technical PIDs are issued through the batch replenishment path, carrying the attribute values confirmed current under REP-5.1-03; the change is detected as part of that same currency check, by re-reading the Authentic Source or acting on a change notification from it. This issuance does not repeat identity proofing, which is required only at renewal.*
- *A CAB verifies that a change in the Authentic Source attribute values results in replenished Technical PIDs carrying the new values being issued to the Wallet Unit, for instance by testing the scenario against the status service.*

6.2 Batch Request and Issuance Protocol

REP-6.2-01: ISS-4.6-02 applies also in the context of replenishment.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REP-6.2-02: The PID Provider shall verify the authenticity and integrity of the refresh token presented in a replenishment request.

Guidelines

- *Before acting on a replenishment request, the PID Provider checks that the refresh token was genuinely issued by it and has not been altered.*
- *Without this check, a forged or tampered token could drive the issuance of Technical PIDs without any valid entitlement behind them.*
- *Authenticity and integrity are established cryptographically, for example by verifying the PID Provider's own signature or protection over the token.*
- *A CAB verifies that a token failing authenticity or integrity verification is rejected and that no Technical PID is issued in that case.*

REP-6.2-03: The PID Provider shall verify that the refresh token is cryptographically bound to the Wallet Unit that holds the Logical PID to be replenished.

Guidelines

- *The PID Provider accepts the token only from the same Wallet Unit and secure cryptographic device that the Logical PID was originally issued to, by requiring a proof of possession that ties the request to a key already bound to that Logical PID.*
- *Without this binding, a token stolen from the legitimate holder could be used from a different device to obtain genuine Technical PIDs in the victim's name into a wallet the attacker controls.*
- *A conformant approach requires a proof of possession on the token exchange whose key matches a key bound to an existing Technical PID of the Logical PID, and this is the mechanism that substitutes for the absent identity proofing.*
- *A CAB verifies that a token presented without the matching device-bound proof of possession is rejected.*

REP-6.2-04: The PID Provider shall reject a replenishment request whose refresh token is expired or has been revoked.

Guidelines

- *The PID Provider checks the token's validity window and revocation state and declines any request presenting an expired or revoked token.*
- *Without this check, a token that is no longer valid for use, because it lapsed or was withdrawn after a security event, would still yield fresh Technical PIDs.*
- *The revocation state of refresh tokens is maintained by the PID Provider alongside the status of the Logical PID they relate to.*
- *A CAB verifies replenishment with an expired token and with a revoked token and confirms both are refused.*

REP-6.2-05: ISS-4.2-04 applies also in the context of replenishment.

REP-6.2-06: The PID Provider shall verify, using the key provenance attestation provided for a batch of replenished Technical PIDs, that the PID binding key pair of every Technical PID in that batch is generated and held in a cryptographic device certified at a level appropriate for Assurance Level High.

Guidelines

- *The PID Provider checks the key provenance evidence supplied with a replenishment batch and confirms it covers every Technical PID in that batch, each bound to a key generated and held in a device certified at the level appropriate for Assurance Level High.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Without this check, a batch could be accepted on provenance evidence that does not actually cover every key in it, so one or more Technical PIDs in the batch could carry a binding key generated or stored outside a certified device without being caught.*
- *Key provenance is typically established once per certified device or keystore and can cover the multiple keys generated for a single batch in that device; the check applies to the batch as the unit in which the evidence is supplied, while confirming it accounts for every Technical PID issued in it.*
- *A CAB verifies that a batch containing a Technical PID whose key is not covered by adequate provenance evidence is not issued, for instance by reviewing the provenance-evidence handling and testing the scenario.*

REP-6.2-07: ISS-4.5-05 applies also in the context of replenishment.

REP-6.2-08: VOID

REP-6.2-09: The PID Provider shall issue each replenished Technical PID as a credential that is distinct from every other Technical PID of the same Logical PID.

Guidelines

- *Each Technical PID in a batch is a distinct credential, so a Wallet Unit can choose to present a given Technical PID only once and to draw on the next Technical PID for the next presentation.*
- *Without distinctness, the use of different Technical PIDs would not avoid linkability.*
- *Distinct binding keys and registration per Technical PID allow single-use downstream.*
- *A CAB inspects a produced batch to confirm the Technical PIDs are mutually distinct.*

REP-6.2-10: The PID Provider shall not release a replenished Technical PID to the Wallet Unit before verification of the refresh token and validation of the Wallet Unit have completed successfully.

Guidelines

- *No Technical PID leaves the PID Provider until the refresh token has been verified and the requesting Wallet Unit has been validated.*
- *Without this ordering, Technical PID content could be released on the basis of an unverified token or to an unvalidated Wallet Unit, disclosing PID data prematurely.*
- *At replenishment the release gate rests on the token and Wallet Unit checks, since identity proofing and holder authentication are not repeated.*
- *A CAB verifies that no Technical PID is released when token verification or Wallet Unit validation has not completed successfully.*

REP-6.2-11: The PID Provider shall deliver each replenished Technical PID to the Wallet Unit over a channel that provides confidentiality, integrity, and endpoint authentication bound to the authenticated Wallet Unit.

Guidelines

- *Technical PIDs are delivered only over a channel that keeps them confidential, detects modification, and authenticates the endpoint as the Wallet Unit the replenishment was authorised for.*
- *Without such a channel, a party interposed on the replenishment exchange could intercept, alter, or redirect the delivered Technical PIDs.*
- *The channel's endpoint authentication is bound to the same authenticated Wallet Unit whose token and attestation were verified earlier in the flow.*
- *A CAB verifies that delivery fails when confidentiality, integrity, or endpoint authentication is absent, for instance by inspecting the transport configuration and testing the scenario.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REP-6.2-12: ISS-4.7-01 applies also in the context of replenishment.

REP-6.2-13: ISS-4.7-04 applies also in the context of replenishment.

REP-6.2-14: The PID Provider shall protect any exchange with the authentic source performed during replenishment against interception and modification.

Guidelines

- *Where replenishment involves contacting the authoritative source to confirm that attribute values remain current, that exchange is protected so it cannot be read or altered in transit.*
- *Without protection, an attacker interposed on the provider-to-source exchange could suppress or alter a change, causing replenishment to proceed with attacker-influenced or stale attribute values.*
- *Protection provides confidentiality, integrity, and authentication of both endpoints of the exchange with the authentic source.*
- *A CAB verifies the channel's behaviour when integrity or authentication is absent, for instance by inspecting the provider-to-source channel configuration and testing that behaviour.*

6.3 Offline Fallback

NOTE: A Wallet Unit that anticipates being temporarily unable to reach the PID Provider maintains continuity of use through the stock of once-only Technical PIDs already issued to it, and may manually trigger an out-of-cycle replenishment request before the anticipated period offline. Determining when to trigger such a request, and sizing its stock accordingly, is a Wallet Unit responsibility and is outside the scope of the present document. Where the Wallet Unit does trigger such a request, the requirements of clauses 5.1 and 5.2 apply to it in the same way as to a threshold-triggered request; no separate PID Provider obligation arises from the request being manually triggered.

6.4 Exhausted Credential Cleanup

REP-6.4-01: The PID Provider shall mark a Technical PID as expired or inactive in its administration once its technical validity period has ended or the Wallet Unit has reported that it was not accepted.

Guidelines

- *Once a Technical PID's technical validity period ends, or the Wallet Unit reports that a replenished Technical PID was not accepted, the PID Provider marks it as inactive in its administration, distinguishing it from the Technical PIDs still current and available for presentation.*
- *Without this, expired or refused Technical PIDs would remain indistinguishable from current ones in the administration, obscuring which Technical PIDs a Wallet Unit can still present and complicating status and expiry handling. The PID Provider has no general means of detecting that a Technical PID has actually been presented and used, since presentation happens directly between the Wallet Unit and a Relying Party without the PID Provider's involvement, and a Wallet Unit may request a further batch before its existing Technical PIDs are used up; use, as such, is therefore not a trigger for this requirement.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Marking a Technical PID as inactive changes its administrative state only; it does not remove the record of the Technical PID, its history, or the associated audit log entries, which remain available as required elsewhere in this clause.*
- *A CAB verifies that a Technical PID whose technical validity period has ended, or that was reported not accepted, is marked as inactive in the administration, for instance by reviewing the administration state against a Technical PID in each condition.*

REP-6.4-02: The PID Provider shall retain the audit log entries relating to a Technical PID for the defined retention period, including after that Technical PID has been marked as inactive in the PID Provider's administration.

Guidelines

- *The audit log entries about a Technical PID survive that Technical PID being marked as inactive and remain available for the whole defined retention period.*
- *Without this, a cleanup or state-management routine that also discarded log data would erase the evidence needed to investigate an incident or demonstrate conformity after a Technical PID is marked as inactive.*
- *This complements the requirement to create the log entries and the requirement that changes only the administrative state of a Technical PID, not its log history.*
- *A CAB verifies that log entries for a Technical PID marked as inactive are still present within the retention period, for instance by testing the scenario.*

REP-6.4-03: The PID Provider shall determine the retention period referred to in REP-5.4-02 as part of its risk assessment.

Guidelines

- *The PID Provider sets the retention period for audit log entries relating to a Technical PID as an outcome of its risk assessment.*
- *An arbitrary or unbounded retention period would either discard data needed for later investigation or retain personal data longer than justified, conflicting with data minimisation.*
- *The risk assessment weighs the need for after-the-fact investigation against data-minimisation obligations to fix a defined retention period.*
- *A CAB verifies that the retention period is defined and traceable to the risk assessment, for instance by reviewing the risk assessment and the configured retention setting.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

7 Lifecycle Event: PID Renewal

Purpose of this chapter: Enable secure re-issuance of a Logical PID when it is approaching expiry. *Renewal is treated as a lifecycle event distinct from initial issuance and always requires renewed identity proofing of the user.*

7.1 Renewal Triggers and Conditions

REN-7.1-01: The PID Provider shall not perform Batch Replenishment of a Logical PID after its Administrative Validity Period has ended without Renewal.

Guidelines

- *Batch Replenishment supplies Technical PIDs only within a current Administrative Validity Period; it cannot bridge the end of that period. Once the Administrative Validity Period has ended, the only way to obtain further Technical PIDs of the Logical PID is a Renewal, which repeats identity proofing and establishes a new Administrative Validity Period.*
- *Without this rule, Batch Replenishment, which does not repeat identity proofing, could keep supplying Technical PIDs indefinitely beyond the period the original identity proofing was intended to cover, so a Wallet Unit that had passed out of the legitimate user's control could continue to receive fresh PIDs without any renewed check.*
- *So that issuance is not interrupted, the PID Provider initiates the Renewal as the Administrative Validity Period approaches its end; the threshold for treating it as approaching its end is fixed in the PID Provider's documented issuance procedures. This complements REP-5.1-02, which states the same prohibition on the replenishment side.*
- *A CAB verifies that Batch Replenishment of a Logical PID whose Administrative Validity Period has ended is refused, and that further Technical PIDs are issued only after a Renewal with renewed identity proofing, for instance by testing a replenishment request submitted after the end of the Administrative Validity Period and confirming it is refused.*

REN-7.1-02: REP-5.1-02 applies also in the context of renewal.

REN-7.1-03: ISS-4.1-02 applies also in the context of renewal.

REN-7.1-04: ISS-4.1-03 applies also in the context of renewal.

REN-7.1-05: The PID Provider shall record the timestamp of each renewal request together with the outcome of the re-identification performed for that request.

Guidelines

- *The PID Provider keeps a timestamped record of every renewal request and whether the re-identification performed for it succeeded or failed.*
- *Without a timestamped record of renewal attempts and their re-identification outcome, a pattern such as repeated renewals shortly after each other, or a renewal immediately following a failed or borderline re-identification, would leave no trace for the PID Provider to later notice.*
- *This extends the renewal logging already required for tamper-evidence with the specific fields needed for pattern analysis: timestamp and re-identification outcome.*
- *A CAB verifies that renewal records include timestamp and re-identification outcome, for instance by reviewing the renewal log and testing the scenario.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REN-7.1-06: The PID Provider shall flag, for investigation, a Logical PID whose renewal requests show a frequency or a pattern relative to re-identification outcomes that exceeds a defined threshold.

Guidelines

- *When renewal requests for a Logical PID occur more frequently than a defined threshold, or show a pattern such as repeated attempts shortly after a failed re-identification, the PID Provider raises that Logical PID for investigation.*
- *A compromised credential or a re-identification step that can be gamed by repeated attempts would otherwise continue to be exploited through renewal indefinitely, because each individual renewal may pass its own checks even though the pattern across renewals is abnormal.*
- *The threshold and pattern definition are set by the PID Provider's own fraud-management process, informed by the records kept under REN-6.1-05.*
- *A CAB verifies that a renewal pattern exceeding the defined threshold results in the Logical PID being flagged, for instance by reviewing the threshold configuration and testing the scenario.*

7.2 Re-identification Requirements

REN-7.2-01: The PID Provider shall verify the identity of the person to whom the Logical PID was issued, applying the identity-proofing requirements of clause 4.3 at the same assurance level required for initial issuance, before renewing that Logical PID.

Guidelines

- *Renewal repeats, in full, an identity verification with a similar strength as for initial issuance; it does not rely on the identity established at a previous issuance or renewal, whichever ground triggered the current renewal.*
- *Without a fresh identity verification, a Wallet Unit no longer under the control of the person it was issued to, for example following theft, loss, or an unnoticed duplicate activation, could obtain a further, full-validity PID without passing the checks a new issuance would require.*
- *The identity verification performed for renewal uses a process and evidentiary requirements with the same strength as for initial issuance, applied at the time of the renewal request; it is not satisfied by referring back to records of an earlier verification.*
- *A CAB verifies that a renewal is preceded by a complete, fresh identity verification meeting the initial-issuance requirements, for instance by reviewing renewal-flow records and testing the renewal path against an incomplete or missing identity check.*

7.3 Renewal Request and Authorisation

REN-7.3-01: ISS-4.4-01 applies also in the context of renewal.

REN-7.3-02: The PID Provider shall not authorise a renewal unless the person's identity has been verified, no ground precluding renewal is present, and the request has been shown to originate from the Wallet Unit holding the Logical PID to be renewed.

Guidelines

- *The authorisation decision for a renewal is reached only once every one of its required pre-conditions has independently completed successfully.*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- *Without requiring every precondition, a flaw in server-side state handling could let a renewal reach authorisation despite an incomplete identity verification, an unresolved ground for refusal, or a request that did not actually originate from the legitimate Wallet Unit.*
- *Implementations commonly enforce this through explicit state tracking of each precondition, only permitting the authorisation step once all recorded states show completion.*
- *A CAB verifies that authorisation is refused when any one precondition has not completed, for instance by reviewing the authorisation logic and testing each precondition individually.*

REN-7.3-03: The PID Provider shall verify that a renewal request is bound to the Logical PID to be renewed by requiring proof of possession of the private key corresponding to the existing PID binding public key of that Logical PID.

Guidelines

- *The renewal request is shown to come from the same Wallet Unit that holds the Logical PID's existing binding key, through a proof-of-possession exchange, before the PID Provider proceeds with re-identification and renewal.*
- *Without this binding, an attacker holding a duplicate or separately-activated Wallet Unit in the victim's name could request renewal of the victim's Logical PID from a device the victim never controlled.*
- *A conformant implementation requires a proof of possession on the renewal request whose key matches the existing PID binding key of the Logical PID cited in the request.*
- *A CAB verifies that a renewal request lacking valid proof of possession of the existing binding key is refused, for instance by testing the scenario.*

7.4 PID Generation and Signing

REN-7.4-01: ISS-4.5-01 applies also in the context of renewal.

REN-7.4-02: REP-5.2-14 applies also in the context of renewal.

REN-7.4-03: ISS-4.5-02 applies also in the context of renewal.

REN-7.4-04: ISS-4.5-03 applies also in the context of renewal.

REN-7.4-05: ISS-4.5-04 applies also in the context of renewal.

REN-7.4-06: ISS-4.2-05 applies also in the context of renewal.

REN-7.4-07: ISS-4.5-05 applies also in the context of renewal.

REN-7.4-08: ISS-4.5-06 applies also in the context of renewal.

REN-7.4-09: ISS-4.5-07 applies also in the context of renewal.

REN-7.4-10: ISS-4.5-08 applies also in the context of renewal.

7.5 Delivery of the PID

REN-7.5-01: ISS-4.6-01 applies also in the context of renewal.

REN-7.5-02: ISS-4.6-02 applies also in the context of renewal.

REN-7.5-03: ISS-4.6-04 applies also in the context of renewal.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

REN-7.5-04: ISS-4.6-05 applies also in the context of renewal.

REN-7.5-05: ISS-4.7-01 applies also in the context of renewal.

REN-7.5-06: The PID Provider shall notify the identified person, over a channel that ensures the integrity and authenticity of the notification and is independent of the Wallet Unit, when their Logical PID has been renewed.

Guidelines

- *The PID Provider sends the person a notification, delivered independently of the Wallet Unit and protected against undetected alteration or spoofing, each time their Logical PID is renewed.*
- *Without an integrity- and authenticity-protected channel, a renewal notification could be suppressed or spoofed, so a person would not learn that their PID was renewed, for example following an unauthorised renewal from a duplicate Wallet Unit.*
- *This uses the same class of out-of-band channel, protected in the same way, as other notifications the PID Provider sends independently of the Wallet Unit.*
- *A CAB verifies that a renewal triggers the notification and that the channel used protects its integrity and authenticity, for instance by reviewing the notification mechanism and testing the scenario.*

REN-7.5-07: ISS-4.7-04 applies also in the context of renewal.

Annex A (informative): PID State Diagram

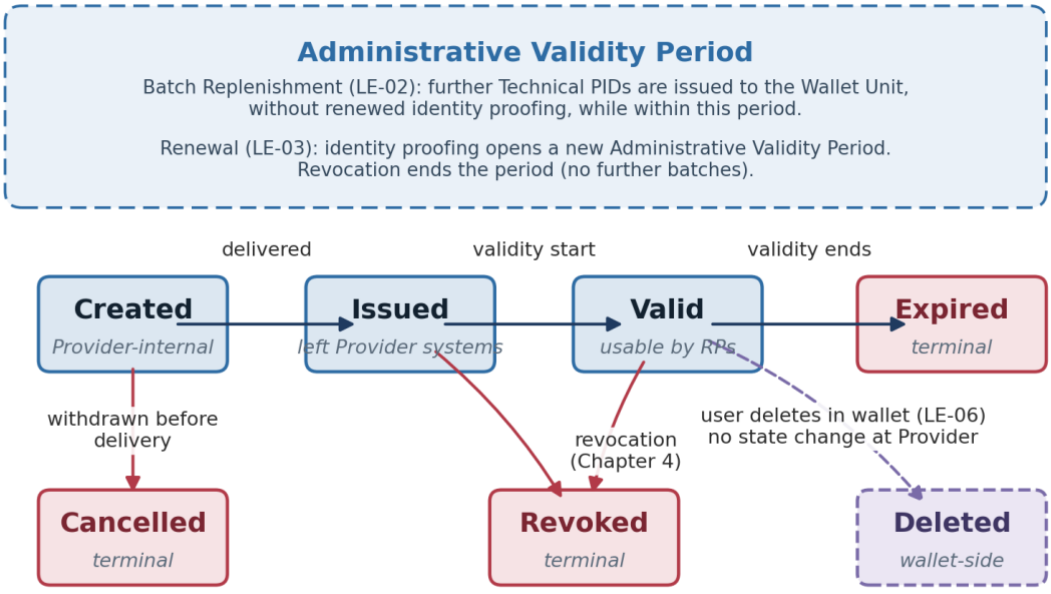
NOTE: This annex is informative and does not contain normative requirements.

The lifecycle events after issuance — PID revocation, expiry and deletion — are specified in the PID Lifecycle Events specification [7].

Overview

This annex proposes an updated Technical PID state model, built on the NOID/ARF baseline state model and revised for ARF v3.0.0 and for the lifecycle events foreseen in this specification (Initial Issuance, Batch Replenishment, and Renewal — LE-01, LE-02, and LE-03). Each state (Created, Issued, Valid, Expired, Revoked, Cancelled) applies to an individual Technical PID, and a seventh, Wallet-side state (Deleted) accounts for user-initiated deletion in the wallet. A Logical PID is only the type of PID and has no state of its own; whether the PID Provider may issue further Technical PIDs to a Wallet Unit without renewed identity proofing is governed by the Administrative Validity Period, not by any state of the Logical PID.

The diagram below is illustrative; the normative rules governing each transition are stated in the requirements of Chapters 4, 5, and 6 of this specification, referenced alongside each transition.



Each state applies to an individual Technical PID.
A Logical PID is only the type of PID and has no state of its own.

Definitions: Renewal, Batch Replenishment, Re-issuance, and Initial Issuance

Batch Replenishment: Batch Replenishment (LE-02) supplies further Technical PIDs of an existing Logical PID without renewed identity proofing, subject to the once-only-token and loss-of-control controls of Chapter 5. It also covers re-issuance with updated attribute values when these change at the Authentic Source, in which case the Technical PIDs carrying the superseded values are revoked (REP-5.1-10).

Renewal: Renewal (LE-03) always repeats identity verification at the assurance level required for initial issuance, and is triggered by the Administrative Validity Period approaching its end (REN-6.1-01). A change in the attribute values held by the Authentic Source is handled as Batch Replenishment (LE-02), not as a renewal, in line with the ARF.

Initial Issuance: Initial Issuance (LE-01) is the first PID issued to a Wallet Unit for a person or an issuance where a previous Logical PID for the same person exists but its Administrative Validity Period has ended and its Technical PIDs have been revoked. A fresh initial issuance — with full identity proofing — is then the only route back in.

Circumstance	Classification	Why
No previous Logical PID for the person	Initial Issuance (LE-01)	ISS-4.1-01
Existing Logical PID, unchanged attributes, more Technical PIDs needed	Batch Replenishment (LE-02)	REP-5.1-01 .. REP-5.1-08
Existing Logical PID, Administrative Validity Period approaching its end, no attribute change	Renewal (LE-03)	REN-6.1-01
Existing Logical PID, attribute values changed at the Authentic Source	Batch Replenishment (LE-02)	REP-5.1-03, REP-5.1-10
Existing Logical PID, Administrative Validity Period ended and previous Technical PIDs revoked	Initial Issuance (LE-01) only	REN-6.1-02, REP-5.1-02
Wallet Unit reports the PID as not accepted after delivery	Revocation of that PID (not a new lifecycle event)	ISS-4.6-05, REN-6.5-04
User deletes the PID in the wallet	Wallet-side Deletion (LE-06)	

States

State	Origin	Terminal?	Meaning
Created	PID Provider-internal (NOID)	No	PID generated at the Provider, before delivery to the Wallet Unit.
Issued	ARF-defined	No	PID has left the Provider's systems and been delivered to the Wallet Unit.
Valid	ARF-defined	No	Validity start date reached; the PID is usable. Batch Replenishment and Renewal keep the Logical PID in this state.
Expired	ARF-defined	Yes	Validity period has ended.
Revoked	ARF-defined	Yes	Permanently invalidated, whether Provider-initiated, User-initiated, or following a not-accepted report for a delivered PID.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

State	Origin	Terminal?	Meaning
Cancelled	PID Provider-internal (NOID)	Yes	Withdrawn before delivery (from Created only).
Deleted (Wallet-side)	Wallet-side, not a Provider state	No	User-initiated deletion in the wallet (LE-06).

Transitions Driven by Each Lifecycle Event

LE-01 (Initial Issuance) drives Created → Issued → Valid, or Created → Cancelled if withdrawn before delivery.

LE-02 (Batch Replenishment) adds further Technical PIDs within the Administrative Validity Period of an existing, Logical PID; the new Technical PIDs pass through Created → Issued → Valid like any others, and no state of the Logical PID changes because a Logical PID has no state of its own. Where the replenishment reflects changed attribute values, the Technical PIDs carrying the superseded values are additionally driven to Revoked (REP-5.1-10).

LE-03 (Renewal) issues further Technical PIDs after renewed identity proofing and opens a new Administrative Validity Period.

Delivered-PID withdrawal, at any point after Issued, drives that PID to Revoked, never to Cancelled (ISS-4.7-03).

A not-accepted report for a PID already classified as issued drives it to Revoked (ISS-4.6-05, REN-6.5-04).

User-initiated deletion in the wallet drives the Wallet Unit's copy to Deleted (Wallet-side). Since there is not notification to the PID Provider of this event, this is not leading to a change in state at the PID Provider side.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Annex B (informative): Risk Register Cross-Reference

Risk ID	Risk description	Requirements
R-01	Insufficient Wallet Unit trust verification	**ISS-5.2-01**, **ISS-5.2-02**, **ISS-5.2-03**
R-02	Trust list staleness or unavailability	**ISS-5.2-06**
R-03	Multiple PIDs per Wallet Unit	**ISS-5.1-01**, **ISS-5.7-02**, **ISS-5.1-04**, **ISS-5.1-05**, **ISS-5.7-16**
R-04	PID issuance after government-initiated revocation	**REP-6.1-02**
R-05	Fraudulent or cloned identity document accepted	**ISS-5.3-03**, REN-6.2-01
R-06	NFC + PIN authentication impersonation	**ISS-5.3-09**, ISS-4.3-11, ISS-4.3-12, ISS-4.7-13, ISS-4.7-14, **ISS-5.7-25**
R-08	National identifier (BSN) derivation integrity failure	**ISS-5.3-01**
R-09	Authentic source (BRP-V) lookup failure	**ISS-5.5-01**
R-10	Authentic source (BRP-V) vs. chip data inconsistency tolerated	**ISS-5.5-01**, REN-6.4-01
R-11	Mandatory PID attribute handling deviation	**ISS-5.5-02**
R-12	Disclosure of excluded optional attributes	**ISS-5.5-03**, REN-6.4-04
R-14	Incorrect cryptographic binding to wallet keys	**ISS-5.5-04**, REN-6.4-05
R-15	PID binding key not protected by qualified WSCD	**ISS-5.2-05**, **REP-6.2-06**, REN-6.4-06
R-16	PID signing key compromise or chain misconfiguration	**ISS-5.5-05**, **ISS-5.5-06**, **REP-6.2-07**, REN-6.4-07, REN-6.4-08
R-17	PID validity period misconfiguration	**ISS-5.5-07**, **ISS-5.5-08**, REN-6.4-09, REN-6.4-10
R-18	PID disclosure before completion of authentication	**ISS-5.6-01**, **REP-6.2-10**, REN-6.5-01
R-19	Insecure PID transport to Wallet Unit	**ISS-5.6-02**, **REP-6.2-11**, REN-6.5-02
R-20	Failure to handle Wallet Unit refusal of PID	**ISS-5.6-03**, **ISS-5.6-04**, **ISS-5.6-05**, REN-6.5-03, REN-6.5-04
R-21	Missing post-issuance status registration	**ISS-5.7-01**, **REP-6.2-12**
R-22	Replay of issuance request	**ISS-5.4-01**, **REP-6.1-01**, REN-6.3-01, ISS-4.4-03
R-23	Issuance authorisation logic bypass	**ISS-5.4-02**, REN-6.3-02
R-24	Insufficient audit logging of lifecycle events	**ISS-5.7-04**, **REP-6.2-13**, REN-6.5-07

Risk ID	Risk description	Requirements
R-25	Technical PID reuse / once-only constraint violation	**REP-6.2-09**
R-26	Exhausted Technical PIDs not cleaned up	**REP-6.4-01**
R-27	Renewal without renewed identity verification	REN-6.2-01
R-28	Outdated previous PID not invalidated after re-issuance with changed content	REP-5.1-10
R-29	Eligibility change not detected at renewal	REN-6.1-04
R-65	Insecure out-of-band notification channel to the User	REN-6.5-06
R-40	Linkability across PID issuance events	**ISS-5.3-02**, **ISS-5.7-26**, **ISS-5.7-27**
R-48	Proof-of-possession of the binding key not verified at issuance	**ISS-5.2-04**, **REP-6.2-05**, REN-6.3-03
R-50	Identity document chip issuer signature not fully validated	**ISS-5.3-04**
R-51	Replay or injection of a previously captured chip readout	**ISS-5.3-05**, **ISS-5.3-06**
R-52	Identity document status not checked (lost or stolen document accepted)	**ISS-5.3-07**, **ISS-5.3-08**
R-55	Batch replenishment without proper token verification	**REP-6.1-05**, **REP-6.2-01**, **REP-6.2-02**, **REP-6.2-03**, **REP-6.2-04**, REP-5.1-07, REP-5.1-08, REP-5.1-09
R-56	Withdrawal of an already-issued (pre-valid) PID misclassified as Cancelled instead of Revoked	**ISS-5.7-03**, , **ISS-5.6-05**
R-57	Orphaned Created PIDs not cleaned up	**ISS-5.1-02**, REN-6.1-03
R-58	Undetected withdrawal ground between PID creation and issuance (conditional)	**ISS-5.1-03**
R-59	Undetected duplicate Wallet Unit holding a genuine PID in the user's name	**ISS-5.7-05**, **ISS-5.7-02**, **ISS-5.7-06**, **ISS-5.7-07**, **ISS-5.7-08**, **ISS-5.7-09**, **REP-6.1-05**, **REP-6.2-03**, ISS-4.7-11, ISS-4.7-12, ISS-4.7-13, ISS-4.7-14, ISS-4.7-15, **ISS-5.4-04**, **ISS-5.4-05**, **ISS-5.4-06**, **ISS-5.7-16**, **ISS-5.7-17**, **ISS-5.7-18**
R-60	Social-engineered self-exclusion enabling an unmonitored attack window (secondary; primary in Revocation/Deletion)	**ISS-5.7-05**, **ISS-5.7-06**, **ISS-5.7-07**, **ISS-5.7-08**, **ISS-5.7-09**, ISS-4.7-10, ISS-4.7-15, **ISS-5.1-05**, **ISS-5.7-19**, **ISS-5.7-20**, **ISS-5.7-21**, **ISS-5.7-22**, **ISS-5.7-23**, **ISS-5.7-24**
R-61	Interception or modification of the identity-proofing exchange	**ISS-5.3-10**, REN-6.2-01
R-62	Stale attribute values propagated at batch replenishment	**REP-6.1-03**, **REP-6.1-04**
R-63	Insecure communication between the PID Provider and the authentic source	**REP-6.2-14**, REN-6.4-02

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Risk ID	Risk description	Requirements
R-66	Premature loss or deletion of audit log data	**REP-6.4-02**, REP-5.4-03
R-67	False or unreliable loss-of-control signal triggers wrongful revocation and blocks replenishment	, REP-5.4-03REP-5.1-05, REP-5.1-06
R-68	Anomalous renewal pattern undetected	REN-6.1-05, REN-6.1-06
R-69	Identity document or derived identifier reused across multiple distinct BSNs undetected	ISS-4.3-13, ISS-4.3-14

Colofon

v1.2
Trust Agency – Daalstraat 164, 1852 Beigem, Belgium – info@trust-agency.eu –
VAT: BE 0792.153.666 – bank account: BE84 0689 4647 1059