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 (part2)

RC1.0

2026.11.01

Document reference	NL-P-04P (part2)
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 Modal verbs terminology 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 Revocation 13
5.1 Revocation Triggers and Conditions 13
5.2 Revocation Procedures 16
5.3 Status Service Update 20
5.4 Wallet User Notification 23
6 Lifecycle Event: PID Expiry 25
6.1 Expiry Detection and Notification 25
6.2 Post-Expiry Behaviour 26
6.3 Pre-Deletion Security Measures 27
6.4 Expired PID Cleanup and Deletion 27
7 Lifecycle Event: PID Deletion 29
7.1 User-Initiated Deletion 29
7.2 PID Provider Notification 30
7.3 PID Revocation 30
Annex A (informative): PID State Diagram 31
Annex B (informative): Risk Register Cross-Reference 32

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 (an individual issued instance) is expressly meant; a batch comprises multiple technical PIDs of the same logical PID.

This specification addresses the lifecycle events of the PID after issuance: revocation by the PID Provider, expiry at the end of the validity period, and user-initiated deletion. It establishes security requirements that the PID Provider must implement to ensure that PID lifecycle management processes meet the eIDAS Assurance Level High corresponding to the requirements set out in Commission Implementing Regulation (EU) 2015/1502.

In developing these requirements, the following inputs have additionally been taken into account: the PID issuance and management process, the PID data model, and the applicable security requirements.

This specification was developed to define security requirements to cover the risks that can arise during the lifecycle events of the PID after issuance: revocation, expiry and deletion. It is intended to serve as a normative basis for conformity assessment of PID Provider solutions with respect to PID lifecycle management 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 deliverable.

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 lifecycle events of the PID after issuance within the European Digital Identity Wallet framework: revocation, expiry and user-initiated deletion. 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.

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

This specification covers the following lifecycle events:

- PID Revocation: requirements for the permanent invalidation of a PID by the PID Provider;
- PID Expiry: requirements for the natural end of the validity period of a PID;
- PID Deletion: requirements for the removal of a PID from the Wallet Unit at the initiative of the Wallet User.

The following are explicitly out of scope of this specification:

- PID initial issuance and PID renewal, 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) 2024/2981 of 28 November 2024 laying down rules as regards the certification of European Digital Identity Wallets
[4]	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.
[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]	ETSI TS 119 471: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Providers of Electronic Attestation of Attributes Services".
[8]	ETSI TS 119 472-1: "Electronic Signatures and Trust Infrastructures (ESI); Profiles for Electronic Attestation of Attributes; Part 1".
[9]	PID Issuance specification: Trust Agency, "PID Issuance Specification" (companion specification defining the PID initial issuance, batch replenishment and renewal 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

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 (PID instance)	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
WUA	Wallet Unit Attestation
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device

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

3.3 Modal verbs terminology

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
REV	PID Revocation
EXP	PID Expiry
DEL	PID Deletion

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 post-issuance PID lifecycle-management processes to preserve the security, integrity and trust properties of the PID when exposed to attack, attempted fraud, compromise, operational failure or misuse. In this document, resilience relates specifically to PID revocation, PID expiry and user-initiated PID deletion. It does not refer to organisational resilience under NIS2 or to product-development and vulnerability-handling obligations under the Cyber Resilience Act.

Following issuance, continued trust in a PID depends on reliable management of its validity and status. A PID that should no longer be relied upon must cease to be usable or accepted in accordance with the applicable lifecycle event. This requires a clear distinction between revocation, as the permanent and irreversible invalidation of one or more Technical PIDs by the PID Provider; expiry, as the natural end of the validity period of a Technical PID; and deletion, as removal of the PID and associated data and key material from the Wallet Unit at the initiative of the Wallet User.

These lifecycle processes may be targeted by attackers with a high attack potential, having substantial expertise, resources and time and potentially combining technical attacks with identity fraud, social engineering, compromised devices, insider actions, manipulation of status information and abuse of reporting or exceptional process paths. Such attackers may seek to prevent or delay revocation, fraudulently trigger revocation, keep expired or revoked Technical PIDs usable, manipulate status information, circumvent the termination of an Administrative Validity Period, or exploit differences between revocation, expiry and deletion.

A successful attack can undermine the assurance established during PID issuance. In particular, a revoked or expired Technical PID that continues to appear valid could be relied upon after the basis for that reliance has ended. Conversely, fraudulent revocation could deny the rightful citizen access to their digital identity. An incomplete or misunderstood deletion process could leave PID data or associated cryptographic material recoverable, or leave outstanding Technical PIDs valid while the Wallet User believes the PID has been invalidated.

The post-issuance lifecycle processes shall therefore incorporate process controls providing resilience against such threats. These controls shall ensure, as applicable, reliable identification and verification of revocation conditions; protection against fraudulent or unauthorised revocation; timely and complete revocation of all affected Technical PIDs; termination of the applicable Administrative Validity Period where required; timely publication of status information; prevention of reinstatement of revoked Technical PIDs; appropriate recording and notification of relevant lifecycle events; correct enforcement of expiry; and retention of records required for traceability, audit and investigation.

The CAB shall assess the individual requirements and their combined effectiveness across the post-issuance lifecycle. The assessment shall determine whether the processes for revocation, expiry and deletion collectively preserve the intended security properties of the PID and whether an attacker with high attack potential could circumvent the intended outcome by exploiting interfaces, delays, exceptional process paths, inconsistent status information or differences between the lifecycle events.

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

4.2 High Assurance

The PID Provider is subject to the requirements applicable to assurance level High under Commission Implementing Regulation (EU) 2015/1502. The assurance established through identity proofing and PID issuance shall be preserved throughout the subsequent lifecycle of the PID. Post-issuance lifecycle management shall therefore ensure that the continued validity and use of the PID remain consistent with the conditions under which it was issued and that a PID is no longer relied upon when those conditions no longer apply.

The lifecycle processes addressed in this Part 2 specification, namely revocation, expiry and user-initiated deletion, shall therefore protect both the continued reliability of the PID and the citizen's control over its use.

Revocation shall provide an effective means of terminating reliance on a PID where the conditions supporting its continued validity or legitimate use no longer apply. The process shall protect against both failure to revoke when revocation is necessary and unauthorised or fraudulent revocation. Where the basis for revocation has been reliably established, the affected PID shall cease to provide a valid basis for electronic identification.

Expiry limits the period during which the validity of a PID may be relied upon. A PID that has reached the end of its applicable validity period shall no longer be considered valid. Expiry shall be managed in a manner that preserves the distinction between the natural end of validity and revocation, while ensuring that continued use beyond the established validity conditions is prevented.

User-initiated deletion enables the rightful citizen to remove the PID and associated data from the Wallet Unit. Deletion shall be effective and shall remain clearly distinguished from revocation. In particular, where deletion from the Wallet Unit does not affect the status maintained by the PID Provider, the Wallet User shall be made aware that deletion does not by itself constitute permanent invalidation of the PID.

The post-issuance lifecycle processes shall furthermore preserve sole control by the rightful citizen. Sole control shall not be considered established only at the time of issuance; it shall remain protected for as long as the PID can be validly exercised. Where sole control is lost or can no longer be relied upon, the lifecycle processes shall enable the affected PID to be invalidated in a timely and effective manner.

The CAB shall assess whether the post-issuance lifecycle processes collectively preserve assurance level High and continued sole control by the rightful citizen, including whether their normal and exceptional process paths prevent continued or unauthorised reliance on a PID once the conditions supporting its validity or legitimate use no longer apply.

5 Lifecycle Event: PID Revocation

5.1 Revocation Triggers and Conditions

REV-4.1-01: When the PID Provider learns, from a reliable source, that the Wallet Unit to which it has issued Technical PIDs, or the device hosting that Wallet Unit, is no longer under the legitimate user's control, the PID Provider shall revoke the outstanding Technical PIDs it has issued to that Wallet Unit.

Guidelines

- *This establishes the primary revocation trigger: on a reliable indication that the Wallet Unit or its device has left the legitimate user's control — for example through loss, theft, or compromise — the Technical PIDs the PID Provider has issued to that Wallet Unit are revoked.*
- *Without this control, a lost, stolen, or compromised Wallet Unit could continue to present valid Technical PIDs, allowing an attacker or unauthorised holder to impersonate the subject towards Relying Parties.*
- *A reliable source may be the Wallet Provider, a government authority, or the legitimate user's own authenticated report; the reliability of the indication is itself subject to **REV-4.1-03**, and ending the silent issuance of further batches is required by **REV-4.1-06**.*
- *A CAB verifies that a reliable indication of lost control of the Wallet Unit or its device results in revocation of the Technical PIDs issued to it, for instance by tracing a sample indication through to revocation.*

REV-4.1-02: The PID Provider shall revoke the outstanding Technical PIDs it has issued to a Wallet Unit when a revocation condition applies, including loss of eligibility of the subject, the decease of the subject, confirmed fraud, or a substantiated request from the legitimate user.

Guidelines

- *Beyond loss of control of the Wallet Unit, the Technical PIDs issued to a Wallet Unit are also revoked when a condition affecting the person or the PID arises: the subject ceases to be eligible, the subject is deceased, fraud is confirmed, or the legitimate user requests revocation.*
- *Without this control, Technical PIDs could remain valid after the underlying entitlement has ended, so a Relying Party could continue to rely on identity data that no longer reflects the subject's status.*
- *The conditions listed are non-exhaustive; the PID Provider identifies the full set of revocation conditions applicable to the PID it issues as part of its policy, and the reliability of any condition reported by a third party is established under **REV-4.1-03**.*
- *A CAB verifies that each defined revocation condition, when established, leads to revocation of the affected Technical PIDs, for instance by reviewing the catalogue of revocation conditions and confirming that each maps to a revocation action.*

REV-4.1-03: The PID Provider shall not treat an indication that a revocation condition applies as a ground for revocation unless the reliability of that indication has been established through a defined verification procedure.

Guidelines

- *Before an indication is allowed to trigger revocation under **REV-4.1-01** or **REV-4.1-02**, the PID Provider passes it through a defined procedure that establishes whether the indication is reliable.*

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

- *Without this check, an attacker or an unreliable third party could fabricate or relay a false report and cause legitimate Technical PIDs to be revoked, denying the subject the service.*
- *A defined verification procedure typically authenticates the reporting channel — for example the Wallet Provider, a government authority, or the user's own authenticated session — and corroborates the indication before it is acted upon; an unauthenticated or uncorroborated report is not sufficient on its own to trigger revocation.*
- *A CAB verifies that an unverified indication does not on its own cause revocation, for instance by reviewing the verification procedure and confirming that indications are authenticated and corroborated before revocation.*

REV-4.1-04: When a revocation condition for a Logical PID is established, the PID Provider shall revoke every outstanding Technical PID of that Logical PID that it has issued to the Wallet Unit, including Technical PIDs issued through batch replenishment.

Guidelines

- *Revocation applies to every valid outstanding Technical PID that represents the affected Logical PID in the Wallet Unit, however it was issued, so that none is left valid.*
- *Without this control, revoking only some Technical PIDs would leave batch-issued instances of the same Logical PID valid and presentable, so a person or a Relying Party could continue to rely on a PID that should be invalid.*
- *A single Logical PID can be represented by multiple Technical PIDs held simultaneously by a Wallet Unit — in particular those provided through batch replenishment as described in the PID Issuance specification [9] — and the revocation applies to all of them; the mechanism by which each Technical PID is set to revoked is specified in clause 5.3.*
- *A CAB verifies that every outstanding Technical PID of the affected Logical PID is revoked, for instance by revoking on a condition where several batch-issued Technical PIDs exist and confirming that none remains valid.*

REV-4.1-05: The PID Provider shall revoke every outstanding Technical PID it has issued to a Wallet Unit when that Wallet Unit is revoked.

Guidelines

- *When the Wallet Unit that holds the Technical PIDs is itself revoked, those Technical PIDs can no longer be trusted; the PID Provider therefore revokes every Technical PID it issued to that Wallet Unit.*
- *Without this control, Technical PIDs would remain valid inside a Wallet Unit that is no longer trustworthy — for example a wallet whose Wallet Instance Attestation has been revoked after device compromise — so an attacker could keep presenting them.*
- *The Wallet Provider offers no facility to inform the PID Provider of a Wallet Unit revocation so the PID Provider establishes the Wallet Unit status itself through the periodic check required by **REV-4.2-06**.*
- *A CAB verifies that a revoked Wallet Unit leads to revocation of the Technical PIDs issued to it, for instance by tracing an invalidated Wallet Unit through to the revocation of its Technical PIDs.*

REV-4.1-06: The PID Provider shall end the Administrative Validity Period of a Logical PID issued to a Wallet Unit when it revokes the Technical PIDs of that Logical PID.

Guidelines

- *Revocation not only invalidates the outstanding Technical PIDs; it also closes the Administrative Validity Period, so that no further batches of Technical PIDs are issued silently to the Wallet Unit.*
- *Without ending the Administrative Validity Period, the PID Provider could keep replenishing fresh Technical PIDs to a Wallet Unit whose PIDs it has just revoked, defeating the revocation.*
- *Ending the Administrative Validity Period means that any future PID for the person requires a new initial issuance with full identity proofing, as described in the PID Issuance specification [9]; stopping automatic replenishment on a loss-of-control indication is also required there.*
- *A CAB verifies that a revocation closes the Administrative Validity Period, for instance by checking the status of the Administrative Validity Period in the systems of the PID Provider.*

REV-5.1-07: [CONDITIONAL] Where the authentic source provides event-driven notification of the decease of a person or of a loss of eligibility of a person, the PID Provider shall subscribe to that notification for each person in whose name a Logical PID is active and treat a received notification as an indication that a revocation condition applies under **REV-4.1-03**.

Guidelines

- *The PID Provider does not wait for the next periodic check but receives decease and eligibility events from the authentic source, as soon as the authentic source offers such events.*
- *A person who dies or loses eligibility keeps an active PID until the next periodic check, and someone with access to the Wallet Unit can use the PID in that period.*
- *The notification is verified under the defined verification procedure of **REV-4.1-03** before revocation, and is subscribed for persons for whom a Logical PID is active. The periodic check of **REV-4.2-07** continues to apply.*
- *A CAB verifies this requirement by reviewing the interface description with the authentic source and the subscription configuration, and by examining records of received events and of the revocations that followed.*

REV-5.1-08: The PID Provider shall, when the decease of a person has been established as a revocation condition, notify every Wallet Provider that provided a Wallet Unit to which a PID of that person was issued, so that each of them is able to revoke the Wallet Unit concerned.

Guidelines

- *When a person has died, the PID Provider informs all Wallet Providers that hold a Wallet Unit of that person, because only the PID Provider knows which Wallet Providers are involved.*
- *Revoking the PID alone leaves the Wallet Unit and the other attestations of the deceased person in it active, and the wallet can be used further for fraud.*
- *The PID Provider finds the Wallet Providers from the data recorded at issuance (see the PID Issuance Specification [9]). The Wallet Provider treats the notification as a request for permanent revocation of the Wallet Unit.*

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 procedure and its interface with the Wallet Providers, and by examining records of past decease cases for the notifications sent.*

5.2 Revocation Procedures

REV-4.2-01: The PID Provider shall determine, as part of its risk assessment, the maximum time within which the Technical PIDs are revoked after a revocation condition has been established.

Guidelines

- *The PID Provider sets a bound on how quickly revocation must be carried out once a verified revocation condition exists, and derives that bound from its own risk assessment.*
- *Without a determined maximum, revocation could be delayed indefinitely, leaving Technical PIDs that should be invalid in a usable state and prolonging the window in which they can be misused.*
- *The maximum time is bounded by the ceiling required by **REV-4.2-02**; within that ceiling the value depends on the sensitivity of the PID, the threats considered, and the capabilities of the status mechanism, and is documented as an outcome of the risk assessment. Where the reuse of batch-issued Technical PIDs is a factor, the reuse-policy parameters of ETSI TS 119 472-3 [5] inform this determination.*
- *A CAB verifies that a maximum revocation time has been determined and justified in the risk assessment, for instance by reviewing the risk assessment and the recorded parameter.*

REV-4.2-02: The maximum time determined under **REV-4.2-01** shall not exceed the maximum time for revoking an electronic attestation of attributes set out in ETSI TS 119 471 [7], clause 4.2.5.1.

Guidelines

- *The bound the PID Provider sets for carrying out a revocation may be shorter than, but never longer than, the maximum that ETSI TS 119 471 sets for revoking an electronic attestation of attributes.*
- *Without this upper limit, a PID Provider could set an arbitrarily long revocation time, leaving invalid Technical PIDs usable well beyond what the trust framework tolerates.*
- *The ceiling is the maximum for revoking an electronic attestation of attributes in ETSI TS 119 471 [7], clause 4.2.5.1.*
- *A CAB verifies that the determined maximum revocation time does not exceed the maximum in ETSI TS 119 471 [7], clause 4.2.5.1, for instance by reviewing the recorded parameter against that clause.*

REV-4.2-03: The PID Provider shall complete the revocation of the Technical PIDs within the maximum time it has determined under **REV-4.2-01**.

Guidelines

- *Once the maximum revocation time is set, the PID Provider carries out each revocation within that bound.*
- *Without this obligation, the determined maximum would be advisory only, and revocations could routinely exceed it, defeating the purpose of setting a bound.*
- *The time is measured from the point at which the revocation condition is established as reliable under **REV-4.1-03** to the point at which the revoked status is effective; propagation of that status through the status mechanism is addressed in clause 5.3.*

- *A CAB verifies that revocations are completed within the determined maximum, for instance by sampling revocation records and comparing the elapsed time against the parameter.*

REV-4.2-04: The PID Provider shall record, for each revocation, the identity of the revoked Technical PIDs, the revocation condition, the outcome of its verification, and the time of revocation.

Guidelines

- *Every revocation is logged with the information needed to account for why and when it was carried out.*
- *Without such a record, the PID Provider could not demonstrate that revocations were triggered by verified conditions and completed in time, nor investigate disputed or erroneous revocations.*
- *The record supports the verification obligation in **REV-4.1-03**, the timeliness obligation in **REV-4.2-03**, and any subsequent investigation of a wrongful or missed revocation; the retention period of the record is determined by the PID Provider as part of its risk assessment.*
- *A CAB verifies that revocation records capture the revoked Technical PIDs, the condition, its verification, and the time, for instance by inspecting a sample of revocation records.*

REV-4.2-05: The PID Provider shall not reinstate a Technical PID once it has been revoked.

Guidelines

- *Revocation is permanent: a revoked Technical PID cannot be returned to a valid state, and continued use of a PID requires the issuance of a new Technical PID.*
- *Without this constraint, revocation would be reversible in practice, undermining the certainty that Relying Parties place in a revoked status.*
- *Revocation is a terminal state for a Technical PID and is not reversible. Re-establishing a PID for the person after revocation follows the issuance process in the PID Issuance specification [9].*
- *A CAB verifies that no mechanism returns a revoked Technical PID to a valid state, for instance by reviewing the revocation procedure and confirming the absence of a reinstatement path.*

REV-4.2-06: The PID Provider shall periodically verify the validity status of each Wallet Unit to which it has issued Technical PIDs that have not reached a terminal state.

Guidelines

- *The PID Provider checks, at a regular interval, whether each Wallet Unit holding one of its still-valid Technical PIDs is itself still valid.*
- *Because the Wallet Provider does not proactively notify the PID Provider when a Wallet Unit is revoked, without this periodic check the PID Provider would never learn that a Wallet Unit had become invalid and would leave its Technical PIDs valid.*
- *The Wallet Unit status is obtained from the status mechanism published by the Wallet Provider for the Wallet Instance Attestation; where the check shows the Wallet Unit to be revoked, the PID Provider revokes the affected Technical PIDs under **REV-4.1-05**. The interval of the check is determined under **REV-4.2-07**.*
- *A CAB verifies that the PID Provider periodically checks Wallet Unit status for the wallets holding its valid Technical PIDs, for instance by reviewing the check procedure and its records.*

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

REV-4.2-07: The PID Provider shall determine the interval of the verification under **REV-4.2-06** as part of its risk assessment.

Guidelines

- *How often the Wallet Unit status is checked is set by the PID Provider on the basis of its risk assessment.*
- *Without a determined interval, checks could be too infrequent to detect an invalidated Wallet Unit in time, extending the period in which its Technical PIDs remain wrongly valid.*
- *The interval is chosen so that an invalidated Wallet Unit is detected quickly enough for the subsequent revocation to remain within the bound set under **REV-4.2-02**; it reflects the sensitivity of the PID and the update characteristics of the Wallet Unit status mechanism.*
- *A CAB verifies that a check interval has been determined and justified in the risk assessment, for instance by reviewing the recorded interval.*

REV-5.2-08: The PID Provider shall provide the person, after authentication at assurance level substantial or high as defined in [2] and through a means that is not a Wallet Unit, with an overview of every Wallet Unit to which a PID in that person's name has been issued, stating for each the Wallet Provider, the date of issuance and the status.

Guidelines

- *There is one place where a person sees all Wallet Units that are active in their name, with the Wallet Provider, the date and the status of each.*
- *Without an overview, a person cannot know that an attacker holds a second Wallet Unit in their name, or that an old Wallet Unit was never revoked after a change of phone.*
- *The overview is offered in an authenticated environment such as a government portal. The PID Provider builds it from its administration, because only the PID Provider sees the Wallet Units of a person across Wallet Providers.*
- *A CAB verifies this requirement by reviewing the design of the overview and its authentication, for instance by inspecting that the overview is not reachable from a Wallet Unit, and by examining a sample of overviews against the administration.*

REV-5.2-09: The PID Provider shall, on a request made by the person in the overview referred to in **REV-5.2-08**, revoke the Technical PIDs issued to the Wallet Unit concerned in accordance with **REV-4.1-05**.

Guidelines

- *From the overview, the person asks for revocation of any listed Wallet Unit, and the PID Provider revokes the PIDs issued to it.*
- *A person who cannot revoke a Wallet Unit that they recognise as unknown or stolen remains exposed until a support employee handles the case.*
- *The overview offers the request per listed Wallet Unit; the request is made in the authenticated environment of the overview and is never made available from a Wallet Unit. The request is treated as a request from the legitimate user under **REV-4.1-02**.*
- *A CAB verifies this requirement by reviewing the revocation flow and by examining records of past requests and of the revocations that followed.*

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

REV-5.2-10: The PID Provider shall forward a request under **REV-5.2-09** to the Wallet Provider that provided the Wallet Unit concerned, so that the Wallet Provider revokes the Wallet Unit.

Guidelines

- *The Wallet Provider is asked to revoke the Wallet Unit itself, as the PID Provider can revoke only the PIDs.*
- *If only the PIDs are revoked, the Wallet Unit and the other attestations in it stay usable, and the attacker keeps a working wallet.*
- *The request is sent through the interface that the Wallet Provider provides for requests from the PID Provider.*
- *A CAB verifies this requirement by reviewing the interface and by examining records of forwarded requests and of the Wallet Provider's confirmation.*

REV-5.2-11: The PID Provider shall provide a reporting point through which a person reports the loss, theft or compromise of a Wallet Unit without authenticating through any Wallet Unit.

Guidelines

- *The person can report a lost, stolen or compromised Wallet Unit to the PID Provider without using a Wallet Unit.*
- *A victim whose device is lost or in the hands of an attacker cannot use that Wallet Unit to report the problem.*
- *The reporting point is reachable by telephone and through the authenticated environment of **REV-5.2-08**, and can be combined with a national reporting point.*
- *A CAB verifies this requirement by reviewing the description of the reporting point and by examining that it works without a Wallet Unit.*

REV-5.2-12: The PID Provider shall forward a report received under **REV-5.2-11** to every Wallet Provider that provided a Wallet Unit to which a PID of the reporting person was issued.

Guidelines

- *A report reaches all Wallet Providers of the person at once.*
- *Without forwarding, the person has to find and call each Wallet Provider; in the meantime the Wallet Units at the other Wallet Providers stay active.*
- *The PID Provider uses the data recorded at issuance to identify the Wallet Providers (see the PID Issuance Specification [9]).*
- *A CAB verifies this requirement by reviewing the procedure and by examining records of past reports for the forwarded messages.*

REV-5.2-13: The PID Provider shall verify, before acting on a report under **REV-5.2-11** or on a request under **REV-5.2-09**, that the person making it is the person in whose name the PIDs were issued, by a means that does not depend on a Wallet Unit.

Guidelines

- *Reports and requests are acted on only after it is clear that they come from the person concerned.*
- *A reporting point without verification can be abused by anyone to revoke the Wallet Units of another person, which is itself a form of attack.*
- *The verification is proportionate to the risk, using assurance level substantial or high as defined in [2] for the overview, and a documented procedure for the telephone route. A report that cannot yet be verified is handled under **REV-4.1-03**.*

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 procedure and by examining records of past reports for the verification performed.*

REV-5.2-14: The PID Provider shall ensure that a revocation initiated by an employee of the PID Provider takes effect only after a second employee has approved it, and that both approvals are recorded in a tamper-evident log.

Guidelines

- *Revocation started by a helpdesk employee takes effect after a second employee agrees, and both approvals are logged.*
- *A single employee who is deceived by a caller, or who acts with bad intent, could revoke the PIDs of a person and lock that person out.*
- *The second approval is requested within the maximum time determined under **REV-5.2-15**. Revocation that the person requests through the overview is not initiated by an employee.*
- *A CAB verifies this requirement by reviewing the procedure and the supporting system, and by examining a sample of employee-initiated revocations for the two approvals.*

REV-5.2-15: The PID Provider shall determine, as part of its risk assessment, the maximum time within which the second approval under **REV-5.2-14** is given.

Guidelines

- *The PID Provider decides how long the second approval takes at most.*
- *If approval has no time limit, a revocation that protects a victim is held up, and the attacker keeps the Wallet Unit in use.*
- *The time follows the maximum time of **REV-4.2-01** and is realised through availability arrangements for approvers.*
- *A CAB verifies this requirement by reviewing the risk assessment and the documented maximum time.*

REV-5.2-16: The PID Provider shall ensure that the second approval under **REV-5.2-14** is given within the maximum time determined under **REV-5.2-15**.

Guidelines

- *Approvals are given within the maximum time.*
- *A time limit that is not enforced is no protection for the victim.*
- *The PID Provider monitors pending approvals and escalates those that approach the maximum time.*
- *A CAB verifies this requirement by reviewing the monitoring and by examining records of approval times.*

5.3 Status Service Update

REV-4.3-01: The PID Provider shall include in each Technical PID the reference to the status mechanism through which the revocation status of that Technical PID is made available, as required by ETSI TS 119 471 [7] and the attestation format profile ETSI TS 119 472-1 [8].

Guidelines

- *Each Technical PID carries a pointer to the status mechanism where its current revocation status can be checked.*
- *Without an embedded reference, a Relying Party receiving a Technical PID would have no reliable way to determine whether it has been revoked.*

- *The content and encoding of this reference are defined by ETSI TS 119 471 [7], clause 4.2.5.2, and the attestation format profile ETSI TS 119 472-1 [8], clause 4.2.11; the PID Provider includes them as required there. The identifier that locates the individual Technical PID within that mechanism is required by **REV-4.3-02**.*
- *A CAB verifies that every issued Technical PID contains a resolvable reference to its status mechanism, for instance by inspecting issued Technical PIDs.*

REV-4.3-02: The PID Provider shall include in each Technical PID the identifier or index that distinguishes that Technical PID within its status mechanism, as required by ETSI TS 119 471 [7].

Guidelines

- *In addition to the reference to the status mechanism, each Technical PID carries an index or identifier that singles it out within that mechanism.*
- *Without a distinct per-Technical-PID identifier, the status of an individual Technical PID could not be set or read independently, so the several Technical PIDs of one Logical PID could not be addressed separately from one another.*
- *ETSI TS 119 471 [7], clause 4.2.5.2, requires the Technical PID to carry both the status-mechanism reference and a per-attestation identifier or index; the PID Provider provides them as specified there. This lets all Technical PIDs of a Logical PID be revoked together (see **REV-4.1-04**) while each is addressed individually.*
- *A CAB verifies that each Technical PID has a unique index within its status mechanism, for instance by confirming that no two outstanding Technical PIDs share the same status index.*

REV-4.3-03: The PID Provider shall set the revocation status of a Technical PID in its status mechanism to revoked when that Technical PID is revoked.

Guidelines

- *Revocation of a Technical PID is made effective and visible by updating its status to revoked in the status mechanism.*
- *Without this update, a revoked Technical PID would still show a valid status, and Relying Parties checking the status mechanism would wrongly accept it.*
- *This is the mechanism through which the revocation required by clause 5.1 is carried out for each Technical PID; the delay permitted between the revocation decision and the visibility of the revoked status is bounded under **REV-4.3-06**.*
- *A CAB verifies that revoking a Technical PID results in its revoked status in the status mechanism, for instance by checking the published status before and after a revocation.*

REV-4.3-04: The PID Provider need not maintain revocation-status information for a Technical PID whose validity period is less than 24 hours, provided that this is stated in its PID provision policy.

Guidelines

- *Very short-lived Technical PIDs, valid for less than 24 hours, may be exempted from the revocation-status handling required for longer-lived Technical PIDs where the PID provision policy so provides.*
- *Maintaining revocation status for a Technical PID that expires within a day adds status-mechanism load and complexity for little benefit, because the Technical PID ceases to be valid on its own within the same window.*
- *This exemption follows ETSI TS 119 471 [7], clause 4.2.5.2, which allows revocation information to be omitted for attestations with a validity period of less than 24 hours*

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

where the practice statement so states, and ETSI TS 119 472-1 [8], clause 4.2.11; for such Technical PIDs, expiry rather than revocation is relied upon.

- *A CAB verifies that the exemption is applied only to Technical PIDs with a validity period of less than 24 hours, for instance by reviewing the validity periods of Technical PIDs excluded from status handling.*

REV-4.3-05: The PID Provider shall determine, as part of its risk assessment, the maximum delay between the revocation of a Technical PID and the availability of its revoked status in the status mechanism.

Guidelines

- *The PID Provider sets a bound on how long the revoked status may take to become visible to Relying Parties through the status mechanism, based on its risk assessment.*
- *Without a determined bound, status propagation could lag arbitrarily, so a revoked Technical PID might still appear valid to Relying Parties for an unpredictable period.*
- *The delay is bounded by the ceiling required by **REV-4.3-06**; within that ceiling the value reflects the sensitivity of the PID, the update and caching characteristics of the status mechanism, and the threats considered, and is documented as an outcome of the risk assessment.*
- *A CAB verifies that a maximum status-propagation delay has been determined and justified, for instance by reviewing the risk assessment and the recorded parameter.*

REV-4.3-06: The maximum delay determined under **REV-4.3-05** shall not cause the revoked status of a Technical PID to become available later than the maximum time for revoking and publishing the status of an electronic attestation of attributes set out in ETSI TS 119 471 [7], clause 4.2.5.1.

Guidelines

- *The revoked status of a Technical PID becomes visible to Relying Parties within the maximum that ETSI TS 119 471 sets for revoking and publishing the status of an electronic attestation of attributes, and the PID Provider may set a shorter bound.*
- *Without an upper limit, status propagation could be set so slowly that a revoked PID still appears valid long after it should, defeating revocation.*
- *The ceiling covers revocation and publication together, referring to ETSI TS 119 471 [7], clause 4.2.5..*
- *A CAB verifies that the determined propagation delay keeps the revoked status available within the maximum in ETSI TS 119 471 [7], clause 4.2.5.1, for instance by reviewing the parameter and testing status visibility after a revocation.*

REV-4.3-07: The PID Provider shall make the revoked status of a Technical PID available in the status mechanism within the maximum delay it has determined under **REV-4.3-05**.

Guidelines

- *The PID Provider ensures that each revoked status actually appears in the status mechanism within the bound it has set.*
- *Without this obligation, the determined maximum delay would be advisory, and revoked statuses could routinely take longer to appear, extending the window of misuse.*
- *The delay is measured from the effective revocation of the Technical PID under **REV-4.2-03** to the point at which a Relying Party querying the status mechanism obtains the revoked status.*
- *A CAB verifies that revoked statuses become available within the determined delay, for instance by measuring the interval between a revocation and its visibility in the status mechanism.*

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

5.4 Wallet User Notification

REV-4.4-01: The PID Provider shall notify the Wallet User when the Technical PIDs issued to that Wallet User's Wallet Unit are revoked.

Guidelines

- *When the Technical PIDs held by a Wallet Unit are revoked, the affected Wallet User is informed of the revocation.*
- *Without notification, the user could remain unaware that their PID no longer works and be unable to react, for example by requesting a new PID or reporting an erroneous revocation.*
- *Notification is provided regardless of the revocation condition, including revocations triggered by third-party indications; the channel and timing are addressed in **REV-4.4-02** and **REV-4.4-03**.*
- *A CAB verifies that a revocation results in a notification to the affected Wallet User, for instance by tracing a sample revocation to the corresponding notification.*

REV-4.4-02: The PID Provider shall deliver the revocation notification to the Wallet User through the government electronic mailbox (MijnOverheid Berichtenbox).

Guidelines

- *The revocation notification is sent through the designated government electronic mailbox, the MijnOverheid Berichtenbox.*
- *Without a designated, trusted channel, a notification could be spoofed or overlooked, and the user could not distinguish a genuine revocation notice from a phishing attempt.*
- *The MijnOverheid Berichtenbox is the channel chosen for official government communication to the citizen, so the user can rely on the authenticity of the message; where a subject cannot be reached through this channel, the PID Provider defines an equivalent trusted channel as part of its policy.*
- *A CAB verifies that revocation notifications are delivered through the designated government electronic mailbox, for instance by reviewing the notification configuration and a sample of sent notifications.*

REV-4.4-03: The PID Provider shall determine, as part of its risk assessment, the maximum time within which the Wallet User is notified after the Technical PIDs issued to that user's Wallet Unit are revoked.

Guidelines

- *The PID Provider sets a bound on how quickly the user must be notified after revocation, derived from its risk assessment.*
- *Without a determined bound, notification could be delayed to the point of being useless, leaving the user unable to act in time.*
- *No source fixes a figure; the value reflects how quickly the user is expected to need to act, for example to obtain a replacement PID, and the characteristics of the notification channel, and is documented as an outcome of the risk assessment.*
- *A CAB verifies that a maximum notification time has been determined and that notifications are sent within it, for instance by reviewing the risk assessment and sampling the interval between revocation and notification.*

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

REV-4.4-04: The revocation notification shall identify the revoked PID and state that it can no longer be used.

Guidelines

- *The notification tells the user which PID has been revoked and that it is no longer usable.*
- *Without clear content, the user could not tell which credential is affected or understand the consequence, reducing the notification's value.*
- *The notification is expressed in terms the user can understand and, where appropriate, indicates how to obtain a new PID; it need not disclose the detailed revocation condition where doing so would be inappropriate.*
- *A CAB verifies that the notification identifies the revoked PID and states that it is no longer usable, for instance by reviewing the notification template.*

REV-5.4-05: The PID Provider shall send the revocation notification referred to in **REV-4.4-01**, in addition to the government electronic mailbox, through a contact method registered by the person with the PID Provider.

Guidelines

- *A revocation is also announced on a contact method that the person registered, not only in the mailbox.*
- *A person who rarely opens the mailbox does not see that their PIDs were revoked, and an attacker who revoked them stays hidden.*
- *The registration of contact methods is specified in the PID Issuance Specification [9]. The notice contains no link, QR code or telephone number to call.*
- *A CAB verifies this requirement by reviewing the notification service and by examining a sample of revocations for the notices sent.*

REV-5.4-06: The PID Provider shall state in the revocation notification the Wallet Provider and the date of issuance of the Wallet Unit to which the revoked PIDs were issued.

Guidelines

- *The notice tells the person which Wallet Unit was affected.*
- *A notice that does not name the Wallet Unit does not allow the person to see whether their own Wallet Unit or an attacker's was revoked.*
- *The data are those recorded at issuance (see the PID Issuance Specification [9]).*
- *A CAB verifies this requirement by reviewing the notification templates and by examining a sample of notices.*

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

6 Lifecycle Event: PID Expiry

6.1 Expiry Detection and Notification

EXP-5.1-01: The PID Provider shall detect, in its administration, when the validity period of a Technical PID has ended.

Guidelines

- *The PID Provider keeps track of the validity period of every Technical PID it has issued and recognises when that period ends.*
- *Without expiry detection, the PID Provider would continue to treat an expired Technical PID as valid in its administration and status service, misrepresenting its status.*
- *Detection is based on the validity period recorded for each Technical PID at issuance; the consequences of detection are addressed in **EXP-5.1-02** and clause 6.4.*
- *A CAB verifies that the PID Provider detects the end of the validity period of its Technical PIDs, for instance by reviewing how expiry is determined and sampling expired Technical PIDs in its administration.*

EXP-5.1-02: The PID Provider shall cease to treat a Technical PID as valid in its administration once the validity period of that Technical PID has ended.

Guidelines

- *Once a Technical PID has expired, the PID Provider no longer records or reports it as valid.*
- *Without this, an expired Technical PID could still be presented as valid by the PID Provider's own administration or status service, so a Relying Party could wrongly accept it.*
- *Expiry is a terminal state distinct from revocation; the distinction between an expired and a revoked Technical PID is addressed in clause 6.2.*
- *A CAB verifies that expired Technical PIDs are no longer treated as valid, for instance by checking the recorded status of a sample of expired Technical PIDs.*

EXP-5.1-03: The PID Provider shall notify the Wallet User when the Administrative Validity Period of a Logical PID issued to that Wallet User's Wallet Unit is approaching its end.

Guidelines

- *Before the Administrative Validity Period ends — after which no further Technical PIDs can be issued without renewed identity proofing — the PID Provider informs the affected Wallet User so that the user can renew in time.*
- *Without advance notice, a user could be left without a valid PID once the last Technical PID expires or is used and no further batch can be issued, unable to renew before that point.*
- *The notification is delivered through the channel used for revocation notifications in clause 5.4; the wallet may additionally surface the approaching end to the user. How far in advance the notification is sent is determined under **EXP-5.1-04**. Renewal itself is specified in the PID Issuance specification [9].*
- *A CAB verifies that an approaching end of the Administrative Validity Period results in a notification to the affected Wallet User, for instance by tracing a sample nearing that point to the corresponding notifications.*

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

EXP-5.1-04: The PID Provider shall determine, as part of its risk assessment, how far in advance of the end of the Administrative Validity Period the notification under **EXP-5.1-03** is sent.

Guidelines

- *The lead time of the notification is set by the PID Provider on the basis of its risk assessment.*
- *Without a determined lead time, the notification could be sent too late for the user to act, or so early that it is ignored.*
- *The lead time reflects how long renewal typically takes and how disruptive an interruption in PID availability would be for the user.*
- *A CAB verifies that a lead time has been determined and justified, for instance by reviewing the risk assessment and the recorded parameter.*

6.2 Post-Expiry Behaviour

EXP-5.2-01: The PID Provider shall not revoke a Technical PID solely because its validity period has ended.

Guidelines

- *Natural expiry and revocation are different terminal states; the PID Provider does not mark a Technical PID as revoked merely because it has expired.*
- *Without this distinction, expired Technical PIDs would be recorded as revoked, misrepresenting why they are invalid and inflating revocation data with routine expiries.*
- *A Relying Party determines that an expired Technical PID is invalid from its validity period, not from its revocation status; the state model is described in Annex A.*
- *A CAB verifies that expiry does not cause a revocation entry, for instance by confirming that expired Technical PIDs are not recorded as revoked.*

EXP-5.2-02: The PID Provider need not maintain revocation-status information for a Technical PID after its validity period has ended.

Guidelines

- *Once a Technical PID has expired, the PID Provider is not required to keep publishing its revocation status.*
- *Maintaining revocation status for an already-expired Technical PID adds status-mechanism load for no benefit, because Relying Parties can already tell it is invalid from its validity period.*
- *This parallels the exemption for very short-lived Technical PIDs in **REV-4.3-04**; status resources for an expired Technical PID may be released once the retention rules in clause 6.4 allow.*
- *A CAB verifies that revocation status is not required to be maintained for expired Technical PIDs, for instance by reviewing when status entries for expired Technical PIDs are retired.*

6.3 Pre-Deletion Security Measures

EXP-5.3-01: The PID Provider shall retain, after the expiry of a Technical PID, only the personal data and records that remain necessary for status publication, audit, or legal obligations.

Guidelines

- *After a Technical PID expires, the PID Provider keeps only the data it still needs — for status, audit or legal reasons — and no more.*
- *Without this limitation, personal data for expired Technical PIDs would be retained beyond any need, increasing the impact of a data breach and conflicting with data-protection obligations.*
- *The records that remain necessary — for example audit logs and status entries — are retained under the retention rules in clause 6.4; everything else is removed under **EXP-5.4-01**.*
- *A CAB verifies that only necessary personal data and records are retained after expiry, for instance by reviewing what is kept against a documented retention justification.*

6.4 Expired PID Cleanup and Deletion

EXP-5.4-01: The PID Provider shall remove expired Technical PIDs from its administration in accordance with a defined cleanup procedure.

Guidelines

- *Expired Technical PIDs are removed from the PID Provider's administration through a documented, repeatable procedure rather than being left in place indefinitely.*
- *Without a cleanup procedure, exhausted and expired Technical PIDs accumulate as stale state in the PID Provider's administration, obscuring the true set of valid PIDs and complicating operations.*
- *The cleanup covers expired and exhausted Technical PIDs; removal from the Wallet Unit itself is the subject of user-initiated deletion in clause 7.1 and is not required here. The timing of removal is governed by **EXP-5.4-02**.*
- *A CAB verifies that expired Technical PIDs are removed under a defined procedure, for instance by reviewing the procedure and confirming that expired Technical PIDs are cleaned up.*

EXP-5.4-02: The PID Provider shall determine, as part of its risk assessment, the retention period after which expired Technical PID records are removed.

Guidelines

- *How long expired Technical PID records are kept before removal is set by the PID Provider on the basis of its risk assessment.*
- *Without a determined retention period, records could be removed too early to meet audit or legal needs, or kept so long that they become an unnecessary liability.*
- *The retention period reconciles the need to minimise data under **EXP-5.3-01** with the need to keep records required for audit and status publication under **EXP-5.4-03**.*
- *A CAB verifies that a retention period has been determined and justified, for instance by reviewing the risk assessment and the recorded parameter.*

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

EXP-5.4-03: The PID Provider shall not remove records that are required for audit or status-publication purposes before the end of their retention period.

Guidelines

- *Records still needed for audit or for publishing status are protected from the cleanup until their retention period ends.*
- *Without this protection, a routine cleanup could delete audit or status records prematurely, undermining traceability and the ability to investigate incidents.*
- *This complements the cleanup obligation in **EXP-5.4-01**: cleanup removes what is no longer needed but never the records still within their retention period set under **EXP-5.4-02**.*
- *A CAB verifies that audit and status records are not removed before their retention period ends, for instance by reviewing cleanup logs against the retention rules.*

7 Lifecycle Event: PID Deletion

Purpose of this chapter: Enable the Wallet User to remove a PID from the Wallet Unit at their own initiative.

NOTE: ARF requirement PAD_03 prohibits the Wallet Unit from notifying the PID Provider of a deletion. Since the PID Provider does not know when a PID is deleted from the Wallet Unit, it cannot act upon this lifecycle event and there are no requirements on the PID Provider, only on the capabilities of the Wallet Unit and the on the Wallet Provider.

7.1 User-Initiated Deletion

DEL-6.1-01: The Wallet Unit shall allow the Wallet User to delete a PID it holds, on the user's own initiative.

Guidelines

- *The Wallet User can, at any time and without involving the PID Provider, remove a PID from their Wallet Unit.*
- *Without a deletion capability, a user could not exercise control over the PIDs stored on their own device, contrary to the user-control principle of the EUDIW.*
- *Deletion removes the PID from the Wallet Unit; it does not, by itself, change the status of the corresponding Technical PIDs at the PID Provider, as set out in clause 6.3.*
- *A CAB verifies that the Wallet User can delete a PID from the Wallet Unit on their own initiative, for instance by exercising the deletion function and confirming the PID is removed.*

DEL-6.1-02: When a PID is deleted, the Wallet Unit shall erase the PID's attribute data and associated key material so that it cannot be recovered from the Wallet Unit.

Guidelines

- *Deleting a PID fully removes its attribute data and the key material bound to it from the Wallet Unit, leaving nothing recoverable.*
- *Without complete erasure, PID attributes or binding keys could remain on the device after deletion and be recovered, defeating the purpose of deletion and exposing personal data.*
- *Erasure covers the attribute values, metadata, and binding keys of the deleted PID held in the Wallet Unit; key material and data held by the PID Provider are outside the wallet and are governed by clause 5.3 and clause 5.4.*
- *A CAB verifies that deletion erases the PID's data and key material beyond recovery, for instance by inspecting the Wallet Unit state after a deletion.*

DEL-6.1-03: The Wallet Unit shall obtain confirmation from the Wallet User before deleting a PID.

Guidelines

- *A PID is deleted only after the user has explicitly confirmed the action.*
- *Without a confirmation step, a PID could be deleted by an accidental action, and — because deletion is irreversible in the wallet — the user would have to obtain a new PID.*
- *The confirmation guards against accidental deletion; the accompanying information that deletion does not revoke the PID is required by DEL-6.3-01.*

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

- *A CAB verifies that deletion requires explicit user confirmation, for instance by attempting a deletion and confirming it does not complete without confirmation.*

7.2 PID Provider Notification

DEL-6.2-01: The Wallet Unit shall not notify the PID Provider of a user-initiated deletion of a PID.

Guidelines

- *When the user deletes a PID from the Wallet Unit, the Wallet Unit sends no notification of that deletion to the PID Provider.*
- *A deletion notification would make deletion depend on connectivity to the PID Provider and would let the PID Provider observe when users remove PIDs from their own devices, without a corresponding benefit; the Architecture and Reference Framework [i.2] prohibits the Wallet Unit from notifying the PID Provider of a deletion.*
- *Because the PID Provider is not notified, a deletion does not change the state of the Technical PIDs at the PID Provider; the consequences for revocation are set out in clause 6.3.*
- *A CAB verifies that the Wallet Unit does not notify the PID Provider of a deletion, for instance by confirming that no deletion message is sent.*

7.3 PID Revocation

DEL-6.3-01: The Wallet Unit shall inform the Wallet User, when they delete a PID, that deletion does not revoke the PID and that revocation must be requested separately if required.

Guidelines

- *At deletion, the user is told plainly that removing the PID from the wallet does not invalidate it and that a separate revocation request is needed to do so.*
- *Without this information, a user who deletes a PID believing it is thereby invalidated — for example after being manipulated into 'removing' a compromised PID — would be left with valid Technical PIDs still usable.*
- *The revocation the user can request is the substantiated user request in REV-4.1-02; the deletion itself proceeds under clause 6.1.*
- *A CAB verifies that the user is informed at deletion that deletion does not revoke and that revocation is separate, for instance by reviewing the deletion dialogue.*

Annex A (informative): PID State Diagram

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

The PID lifecycle state model, including the states and transitions relevant to revocation, expiry and deletion, is defined in Annex A of the PID Issuance specification [9]. To avoid maintaining the state model in two documents, the present document does not reproduce it and refers to that annex.

Annex B (informative): Risk Register Cross-Reference

Risk ID	Risk description	Requirements
R-21	Missing post-issuance status registration	**REV-4.3-01**, **REV-4.3-03**
R-24	Insufficient audit logging of lifecycle events	**REV-4.2-04**
R-30	Revocation trigger not detected in time	**REV-4.1-01**, **REV-4.1-02**, **REV-4.2-01**, **REV-4.2-06**, **REV-5.1-07**, **REV-5.2-08**, **REV-5.2-09**, **REV-5.2-11**
R-31	Status service update failure on revocation	**REV-4.3-03**, **REV-4.3-05**, **REV-4.3-07**
R-32	Unauthorised revocation request accepted	**REV-4.1-03**, **REV-5.2-13**, **REV-5.2-14**, **REV-5.2-15**, **REV-5.2-16**
R-33	Wallet User not notified of revocation	**REV-4.4-01**, **REV-4.4-02**, **REV-4.4-03**, **REV-4.4-04**, **REV-5.4-05**, **REV-5.4-06**
R-41	PID revocation without reason	**REV-4.1-03**, **REV-4.2-04**
R-43	PID not revoked following Wallet Unit revocation	**REV-4.1-01**, **REV-4.1-04**, **REV-4.1-05**, **REV-4.1-06**, **REV-4.2-06**, **REV-4.2-07**, **REV-5.1-08**, **REV-5.2-10**, **REV-5.2-12**
R-44	Revocation not actioned within the maximum delay	**REV-4.2-01**, **REV-4.2-02**, **REV-4.2-03**, **REV-4.3-06**
R-45	Revoked PID reinstated	**REV-4.2-05**
R-46	Revocation not applied to all Technical PIDs of a Logical PID	**REV-4.1-04**, **REV-4.3-02**
R-47	PID status service unavailable or stale	**REV-4.3-04**, **REV-4.3-05**, **REV-4.3-07**
R-65	Insecure out-of-band notification channel to the User	**REV-4.4-02**
R-66	Premature loss or deletion of audit log data	**REV-4.2-04**, **EXP-5.4-03**
R-67	False or unreliable loss-of-control signal triggers wrongful revocation	**REV-4.1-01**, **REV-4.1-03**
R-34	PID expiry not detected by provider	**EXP-5.1-01**, **EXP-5.1-02**, **EXP-5.1-03**, **EXP-5.1-04**, **EXP-5.2-01**, **EXP-5.2-02**
R-36	Personal data or key material not minimised at end of PID life	**EXP-5.3-01**
R-26	Exhausted Technical PIDs not cleaned up	**EXP-5.4-01**, **EXP-5.4-02**
R-38	Deletion without corresponding revocation (accepted by design)	**DEL-6.2-01**
R-39	Incomplete Wallet Unit wipe on deletion	**DEL-6.1-01**, **DEL-6.1-02**
R-60	Social-engineered self-exclusion	**DEL-6.1-03**, **DEL-6.3-01**

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

Colofon

v1.1
Trust Agency – Daalstraat 164, 1852 Beigem, Belgium – info@trust-agency.eu –
VAT: BE 0792.153.666 – bank account: BE84 0689 4647 1059