EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-CS-part1

NL EUDI Wallet Certification System

NL FITCEM Cybersecurity Certification Scheme
Scheme Specification
NP001-EUDIW

RC1.0

2026.10.25

Document reference	NL-CS (part1)
Version	RC1.0
Status	Release Candidate
Date	25/10/2026
Document type	FITCEM Certification Scheme Scheme Specification
Parent framework	NL-SYS-01, NL-SYS-02, NL-SYS-03, NL-SYS-04, NL-SYS-05 NL-TL
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	European Digital Identity Wallet Solutions
Primary audience	Scheme Owners, Evaluation Laboratories; CABs, EUDI Wallet providers
Secondary audience	EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Related & Subsidiary Documents	NL-CS (part2, part3, part4) NL-CS-WI & NL-CS-WI-conditions NL-WSCA & NL-WSCA-conditions

This is the complete NL FITCEM scheme for the European Digital Identity Wallet in a single document. It contains scheme policy, roles, the security requirements approach, the evaluation methodology and the certification process, and does not depend on other scheme documents for its normative content.

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

Version	Date	Summary of change
RC1.0	24 October 2026	Clean up for publication

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

Contents

The table of contents is a Word field. Right click and Update Field to populate it.

Document control 2
1. Introduction 5
1.1 Purpose and scope 5
1.2 Regulatory and normative basis 5
1.3 Relationship to other schemes 6
1.4 Terminology 6
2. Target of Evaluation 8
2.1 In scope 8
2.2 Out of scope 8
2.3 Architecture variants and admitted Protection Profiles 8
2.4 Assumptions on the operational environment 9
3. Roles and responsibilities 10
3.1 Overview of scheme parties 10
3.2 Certification Body 10
3.3 Evaluation Laboratory 11
3.4 Product developer / sponsor 12
3.5 National Accreditation Body 12
4. Security requirements approach 13
4.1 Protection Profile 13
4.2 Security requirements 13
4.3 Test to requirement mapping 13
4.4 Required test set 14
5. Evaluation methodology 15
5.1 Methodology and assurance level 15
5.2 Fixed time evaluation and the finding termination rule 15
5.3 Evaluation effort 15
5.4 Module decomposition and composition 16
6. Certification process 17
6.1 Process overview 17
6.2 Functional certificate prerequisite 17
6.2.1 Verification of product identity by the Evaluation Laboratory 18
6.3 Certificates and publication 18
6.4 Incident and vulnerability management 18
6.5 Certificate suspension and withdrawal 19
6.6 Changed products: delta assessment 19
6.7 Scheme maintenance and version transitions 20
7. Related scheme documents 21
Annex A: Glossary 22
Annex B: References 24
Annex C: Delta assessment evidence checklist 26

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

1. Introduction

1.1 Purpose and scope

This document is the complete evaluation and certification specification for the European Digital Identity Wallet under the NL FITCEM Cybersecurity Evaluation and Certification Scheme, operated by the Scheme Owner. It covers scheme policy, roles, the security requirements approach, the evaluation methodology and the certification process in a single document.

The scheme provides a framework for the independent cybersecurity evaluation and certification of the European Digital Identity Wallet using the fixed time evaluation methodology (FITCEM) of EN 17640:2022, augmented with evaluation methodology from Common Criteria (ISO/IEC 15408) and SESIP (EN 17927). The assurance level is high and this is mandatory; substantial is not sufficient.

This document applies to the Certification Bodies, Evaluation Laboratories and product developers operating under this scheme.

1.2 Regulatory and normative basis

Instrument	Relevance
Reg. (EU) 2024/1183 (amended eIDAS)	European Digital Identity framework.
Regulation (EU) 2019/881 (CSA)	Cybersecurity Act. Assurance levels and the role of the national cybersecurity certification authority.
Comm. Impl. Reg. (EU) 2024/2979	Integrity and core functionalities of the wallet.
Comm. Impl. Reg. (EU) 2024/2981, Annex II	Assurance level information requirements applicable to this scheme.
Comm. Impl. Reg. (EU) 2024/2981, Annex IX	Periodic post certification surveillance cycle.
Comm. Impl. Reg. (EU) 2024/2981, Section IV	Threat catalogue for wallets (TRnn identifiers). Threat reference used by the OWASP MAS EUDI Wallet profile and therefore by the test to requirement mapping of section 4.3.
Comm. Impl. Reg. (EU) 2025/848	Registration of wallet-relying parties. Bounds the relying party interface assumptions of the Protection Profile.
EUDI Wallet Architecture and Reference Framework (ARF)	Architecture reference, and the Functional Conformance Assessment Framework (FCAF) that produces the functional certificate required by section 6.2.
EN 17640:2022 (FITCEM)	The fixed time evaluation methodology applied by this scheme.
EN 17927:2023 (SESIP)	Accepted alternative evaluation methodology and source of the assurance component semantics used by this scheme.
EN ISO/IEC 17065:2012; 17025:2017	Requirements for the Certification Body and the Evaluation Laboratory.

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

Instrument	Relevance
EN ISO/IEC 17067:2013	Product certification scheme type. This scheme is a Type 5 scheme.
EN ISO/IEC 30111:2019	Vulnerability handling processes.
Regulation (EC) No 765/2008	Accreditation and market surveillance.
OWASP MASVS v2.1.0, MASWE v1.0, MASTG	Source of the required test set. See section 4.4.

1.3 Relationship to other schemes

This scheme is a national FITCEM-based cybersecurity certification scheme. It is designed to be compatible with and complementary to the EU cybersecurity certification framework under the CSA, including the EUCC and the future EUDI Wallet scheme(s). Certificates issued under FITCEM-based schemes are recognised assurance information under the criteria of Annex II of Commission Implementing Regulation (EU) 2024/2981.

Certification under this scheme is a cybersecurity certification. It is not a functional conformity assessment and does not substitute for one; section 6.2 makes a functional certificate a precondition for a certificate of conformity under this scheme.

1.4 Terminology

Term	Meaning
FITCEM	Fixed time evaluation methodology of EN 17640:2022.
FIT PP / WPP	The Wallet Protection Profile; equivalent of a Protection Profile.
FIT ST / WSS	The product specific security specification (Wallet Security Specification); equivalent of a Security Target.
WSF / WSFI	Wallet Security Functions and their interfaces; equivalent of TSF and TSFI.
WI	Wallet Instance. The application installed on the User device; the TOE under [PP-WI-REMOTE].
WIA	Wallet Instance Attestation. Attestation about a Wallet Instance, obtained from the Wallet Provider and used in credential issuance.
WSCA / WSCA-BE	Wallet Secure Cryptographic Application, and its backend variant executing on Wallet Provider infrastructure.
WSCD	Wallet Secure Cryptographic Device. In the remote architecture, a certified remote HSM.
TOE	Target of Evaluation. The product, or defined portion of it, subject to evaluation.
ETR	Evaluation Technical Report, per Annex G of EN 17640:2022.
Functional certificate	Certificate, or equivalent attestation, of conformity with the functional requirements applicable to the wallet. See section 6.2.

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

Term	Meaning
KA	Key Attestation. Attestation about a WSCD and a key, used in credential issuance.
Delta assessment	Demonstration that a changed product is sufficiently covered by previous and new analysis and testing. See section 6.6 and Annex C.

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

2. Target of Evaluation

2.1 In scope

- The Wallet Instance and its security functions (WSF) and interfaces (WSFI).
- Wallet core functionalities per Commission Implementing Regulation (EU) 2024/2979.
- The application's use of platform security services, under the assumptions of section 2.4.
- Positive tests, which verify that the functionality is present and behaves as specified, and vulnerability tests, which probe whether the functionality can be defeated.
- The Wallet Secure Cryptographic Application (WSCA) and the Wallet Secure Cryptographic Device (WSCD), only to the extent that the applicable Protection Profile places them inside the TOE. Under the current draft Protection Profile they are not in the TOE: the Wallet Instance is a standalone TOE and the WSCA-BE and WSCD are part of the operational environment, subject to the environmental requirement that key protection and cryptographic operations are performed inside a certified WSCD/WSCA.

2.2 Out of scope

- Server side and back office components, and their interfaces beyond the assumptions stated in the Protection Profile.
- Conformity with the Cyber Resilience Act, software development lifecycle assurance, and ISMS type certification, which are addressed under separate regimes.
- The underlying mobile platform and operating system, which are subject to assumptions and only light verification.

The management system element of this scheme is scoped specifically to processes directly relevant to the certified product's security maintenance: change management, vulnerability management, and update delivery. General information security management systems are assessed under separate schemes and are not part of the certification decision under this scheme.

2.3 Architecture variants and admitted Protection Profiles

Different secure element architectures lead to different decompositions and different test sets. The scheme states, per admitted Protection Profile, which architecture is allowed and the related evaluation effort.

Architecture variant	Admitted Protection Profile
Remote WSCA-WSCD (remote HSM)	[PP-WI-REMOTE] v0.2d, draft. Wallet Instance as standalone TOE; WSCA-BE and WSCD in the operational environment. [TP-WI-BB] gives the title as "EN 17640 FITCEM PROTECTION PROFILE for EUDI Wallet Instance in the remote HSM architecture"; identification and version to be confirmed.
Embedded secure element	[None admitted. Protection Profile required before certification.]
eSIM based	[None admitted. Protection Profile required before certification.]
No dedicated secure element	[Not admitted at assurance level high.]

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

2.4 Assumptions on the operational environment

The Protection Profile section 3.3 carries an environmental requirements table classifying each requirement as Logical, Procedural or Logical/Procedural and assigning it to the User or to the Wallet Provider. It covers the COTS platform (security services, integrity checking, trusted distribution, minimum OS and keystore, OS-level user authentication, sandboxing and secure boot, detection of insecure operational modes), the certified WSCD/WSCA, the mTLS availability of the Wallet Provider backend and WSCA/WSCD, account creation and identity proofing, protection of authentication secrets, trusted list and revocation list availability, and Wallet Provider responsibility for lifecycle maintenance and continued certification.
That table is normative and shall be mirrored, not restated, in the FIT ST.

3. Roles and responsibilities

3.1 Overview of scheme parties

Party	Role	Normative basis
Scheme Owner	Owns and governs the scheme; approves and publishes this document; maintains the register of authorised CBs and issued certificates; issues guidance and interpretations; maintains the central vulnerability register.	[to be confirmed]
Certification Body (CB)	Manages the certification process; bears responsibility for laboratory evaluation activities; issues certificates; issues mandatory guidance to laboratories.	EN ISO/IEC 17065:2012
Evaluation Laboratory	Performs FITCEM evaluation tasks under CB responsibility; fulfils EN ISO/IEC 17025:2017.	EN ISO/IEC 17025:2017; EN 17640:2022
Product Developer / Sponsor	Submits the product for certification; provides evaluation evidence; complies with post-certification obligations.	CSA; this document
National Accreditation Body	Accredits CBs (EN ISO/IEC 17065) and may accredit laboratories (EN ISO/IEC 17025) for the relevant scope.	Reg. (EC) No 765/2008
Market Surveillance Authorities	Oversight of certified products in the market.	National legislation; CSA

3.2 Certification Body

CBs operating under this scheme shall be accredited by the National Accreditation Body pursuant to Regulation (EC) No 765/2008 in accordance with EN ISO/IEC 17065:2012 with a scope covering certification of the European Digital Identity Wallet at assurance level high. Minimum competence requirements are:

- A minimum of two years of active certification experience under EN ISO/IEC 17065:2012 accreditation at assurance level high.
- Technical knowledge of the wallet, its threat model, and the applicable evaluation methodology.
- For CBs wishing to develop or co-develop the technical content of this scheme: a minimum of five years of active certification experience at assurance level high.

The CB shall:

- Manage and oversee the complete certification process for each evaluation project, from application through certificate issuance and ongoing surveillance.
- Review and approve the FIT ST submitted by the product developer.
- Plan evaluations in accordance with this document and issue the evaluation plan.
- Engage Evaluation Laboratories and bear full responsibility for all evaluation activities they perform.

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

- Guarantee that the fixed time budget allocated per evaluation task is adequate and consistent with section 5.3.
- Issue mandatory written guidance to each Evaluation Laboratory specifying evaluation requirements, quality criteria, time budgets per task, and reporting standards.
- Issue, maintain, suspend and withdraw certificates of conformity.
- Conduct initial and periodic audits of product developer operational processes.
- Report all incidents and vulnerabilities, regardless of severity, to the Scheme Owner.
- Review each delta assessment under section 6.6 and accept or reject its conclusion.
- Handle complaints and appeals in the first instance.
- Maintain records of all certification activities for the period specified by the Scheme Owner.

3.3 Evaluation Laboratory

Evaluation Laboratories shall fulfil the requirements of EN ISO/IEC 17025:2017 with a scope covering the evaluation activities for the European Digital Identity Wallet at assurance level high. Compliance shall be demonstrated by one of:

- Accreditation under EN ISO/IEC 17025:2017 by the National Accreditation Body pursuant to Regulation (EC) No 765/2008 with a scope covering FITCEM-based evaluation activities for the European Digital Identity Wallet. This is the primary and preferred method.
- Where a laboratory does not hold standalone accreditation: the engaging CB demonstrates, through its own EN ISO/IEC 17065:2012 accreditation arrangements, that the laboratory fulfils EN ISO/IEC 17025:2017 for the evaluation activities performed, with the CB's accreditation scope explicitly covering those activities.

Laboratory licensing floor (proposed). To be licensed to perform evaluations under this scheme, an Evaluation Laboratory shall hold EN ISO/IEC 17025:2017 accreditation with an accredited scope covering either (a) Common Criteria evaluation (ISO/IEC 15408 with ISO/IEC 18045) at EAL4 with AVA_VAN.3, or at a higher level, or (b) SESIP evaluation (EN 17927) at SESIP level 3, or at a higher level. The accredited scope shall include the evaluation of mobile applications. A laboratory without such a scope shall not be licensed under this scheme.

The scheme does not accept accreditation under EN ISO/IEC 17020, 17021 or 17029 as a substitute. Evaluation Laboratories shall:

- Perform all evaluation tasks assigned in the evaluation plan, in accordance with EN 17640:2022, this document, and the mandatory guidance issued by the CB.
- Act under the responsibility of the engaging CB at all times; the Evaluation Laboratory does not hold an independent certification role.
- Prepare the ETR per Annex G of EN 17640:2022 and the reporting requirements of this document.
- Participate in Evaluation Review Meetings as required.
- Report all identified vulnerabilities to the CB without undue delay.
- Verify and record the identity of the product and its exact version against the functional certificate, per section 6.2.1, and perform any delta assessment required under section 6.6.
- Maintain evaluator competence at or above the level required by this document.

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

3.4 Product developer / sponsor

Before evaluation the product developer shall:

- Select an authorised CB and submit a certification application with all required documents.
- Provide the FIT ST claiming conformance to the applicable Protection Profile.
- Provide all evaluation evidence required by the evidence checklist.
- Provide source code to the Evaluation Laboratory as required by the applicable Protection Profile.
- Provide a risk assessment for the specific product architecture.
- Provide the functional certificate, and where available the associated functional conformity assessment report, for the same product and the exact same version as the product submitted (section 6.2).

After certification the product developer shall:

- Notify the CB of critical vulnerabilities and active exploits within 24 hours of discovery, and of high-severity vulnerabilities within 72 hours.
- Establish and maintain a vulnerability management policy and procedures in accordance with EN ISO/IEC 30111:2019, and prepare Vulnerability Impact Analysis Reports where relevant.
- Notify the CB of all planned changes to the certified product prior to implementation.
- Maintain the functional certificate for the lifetime of the certificate of conformity, and notify the CB without undue delay if it is suspended, withdrawn or expires.
- Cooperate with the CB in all surveillance evaluations.
- Use only the scheme's Trust Mark [to be confirmed] as the mark of conformity.

3.5 National Accreditation Body

The National Accreditation Body accredits CBs under EN ISO/IEC 17065:2012 and Evaluation Laboratories under EN ISO/IEC 17025:2017 for the relevant scope, in accordance with Regulation (EC) No 765/2008.

4. Security requirements approach

4.1 Protection Profile

Security requirements for the European Digital Identity Wallet are derived from a threat assessment and are expressed in the applicable Protection Profile. The FIT ST submitted by the product developer claims conformance to the Protection Profile and instantiates it for the specific product.

The applicable Protection Profile at the date of this version is: FITCEM Protection Profile for EUDI Wallet Instance supported by a remote WSCA-WSCD, identification FITCEM-PP-WALLET-INSTANCE-for-REMOTE-WSCA-WSCD, version 0.2d, 20 August 2026, draft. It is referenced as [PP-WI-REMOTE] in Annex B and applies to the remote WSCA-WSCD architecture variant only; see section 2.3. The testing plan [TP-WI-BB] refers to the profile under the title "EN 17640 FITCEM PROTECTION PROFILE for EUDI Wallet Instance in the remote HSM architecture"; see the note below.

4.2 Security requirements

The Protection Profile splits the requirements into Functional Security Requirements (FSR) and Resilience Security Requirements (RSR), with a module decomposition. The FSR set covers protected channels to the WSCA-BE and Wallet Provider, local OS-based multi-factor authentication, the WSCA/WSCD-level Remote User Authentication Protocol, key attestation handling, revocation lists and installation. The RSR set covers monitoring, data sanitation, secure coding, key management, cryptography, random numbers, screen protection, payload encryption, focus and foreground handling, PIN entry, debug, obfuscation and anti-deobfuscation, operational modes, device attestation, integrity and user privacy. They are inserted here by reference on issue of the Protection Profile and are not reproduced or invented in this document.

4.3 Test to requirement mapping

FITCEM relies on an explicit mapping between the required tests and the security requirements. This mapping is the part of the methodology that most often fails when it is left implicit. It must be performed and recorded, not assumed. Every required test is mapped to the requirement it exercises; a test run without a recorded target requirement does not contribute to assurance under this scheme.

The draft Protection Profile already carries a mapping of each FSR and RSR to OWASP MAS. That mapping shall be re-keyed to MASWE v1.0 identifiers before issue, because the OWASP EUDI Wallet profile is built on MASWE and the OWASP requirement tables carry both a MASWE identifier and the Commission Implementing Regulation (EU) 2024/2981 Section IV threat identifier (TRnn). Keying the mapping to MASWE and TRnn gives this scheme an externally maintained coverage argument for its fixed scope. The full mapping table (test, target requirement, module, positive or vulnerability test, evidence expected) is inserted here on issue.

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

4.4 Required test set

The required test set is built on OWASP MAS. OWASP MAS material is referenced only; this scheme does not reproduce its content. The evaluation plan pins the version of every OWASP deliverable used and records its draft status where applicable.

Reference	Application
OWASP MASVS v2.1.0	Baseline mobile application security verification standard. Its categories structure the required test set.
OWASP MASWE v1.0	Weakness enumeration keyed to the MASVS categories. Required tests and the mapping of section 4.3 are identified by MASWE identifier, so that the mapping is stable across MASTG revisions.
OWASP MASTG	Test procedures for the required tests. Current version at the date the evaluation plan is issued.
OWASP MAS testing profiles	The profile set is L1 (essential security), L2 (advanced security), R (baseline resilience) and P (baseline privacy). The baseline combination for the wallet at assurance level high is L2 + R + P. [FOR REVIEW, see note below.]
OWASP MAS EUDI Wallet profile (W)	Additional wallet specific profile, applied on top. Built on MASWE and dual-keyed to the Commission Implementing Regulation (EU) 2024/2981 Section IV threat identifiers, with per-profile applicability (EUDIW-L1, EUDIW-L2). Announced deliverables are the "EUDI Wallet MAS Profile" and its "Practical Guidelines". Draft as at the date of this version and not yet normative.

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

5. Evaluation methodology

5.1 Methodology and assurance level

Evaluation is performed under FITCEM (EN 17640:2022), using CC or SESIP methodology. The assurance level for the EUDI Wallet is high (CC AVA_VAN.3/SESIP3 equivalent) and this is mandatory; substantial is not sufficient for the wallet. Source code shall be available as indicated in the Protection Profile. The complete wallet is expected to resist attackers with high attack potential. Trust service providers may begin at substantial and increment, but the wallet itself is high.

5.2 Fixed time evaluation and the finding termination rule

Evaluation is performed within a fixed evaluation time budget. The treatment of findings within that budget is a defining property of FITCEM.

5.3 Evaluation effort

This section fixes the evaluation effort, in person days. Under FITCEM the effort is fixed rather than scaled to functionality; more functionality raises the probability of findings within the fixed budget rather than extending the budget. The delta assessment of section 6.6 is performed within the fixed budget of the affected evaluation tasks.

The black-box penetration testing plan [TP-WI-BB] provides the black-box testing effort for the Wallet Instance against the profile. It is an estimate to support effort setting and does not define the evaluation test specification. Hours are split into test execution and analysis, and investigation and script or tool creation. Conversion to person days uses 8 hours per person day [assumption, to be confirmed]. Per requirement figures are in [TP-WI-BB] and are not reproduced here.

Group	Req.	Test execution and analysis (h)	Investigation and scripting (h)	Total (h)	Person days (8 h)
FSR covering T.USER_IMPERSONATION	7	136	158	294	36.75
FSR covering LEAKED_PRESENTATION_DATA	7	98	118	216	27
FSR, standard priority	8	78	102	180	22.5
FSR subtotal	**22**	**312**	**378**	**690**	**86.25**
RSR, mandatory	13	258	304	562	70.25
RSR, recommended	6	76	98	174	21.75
Mandatory total (all FSR and mandatory RSR)	**35**	**570**	**682**	**1252**	**156.5**
Total including recommended RSR	**41**	**646**	**780**	**1426**	**178.25**

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

5.4 Module decomposition and composition

The wallet is decomposed into a mandatory wallet core plus optional modules, so that requirements and effort can be attached per module. Every wallet has a wallet core that can acquire and present attestations; other modules are optional and change the requirements and the effort.

- Wallet core (mandatory): attestation acquisition and presentation.
- WSCA / WSCD cryptographic device interface.
- Remote electronic signing module (optional).
- Presentation and proximity interface module.
- Optional modules per wallet architecture (HSM backed, embedded secure element, eSIM).

Composition rules for product components already evaluated under other schemes are applied per this document and the applicable Protection Profile. Common Criteria and SESIP certifications can be reused under the responsibility of the Certification Body. Where the Protection Profile places the WSCD in the operational environment, its certificate is an environmental requirement rather than a composition input, and the Evaluation Laboratory shall record its identity, version and validity.

6. Certification process

6.1 Process overview

The certification process follows the Type 5 certification system structure of EN ISO/IEC 17067:2013, combining third-party type testing with assessment of the product developer's maintenance processes and ongoing post-certification surveillance.

#	Phase	Key activities
1	Application	Developer selects an authorised CB; submits application with FIT ST, risk assessment, evaluation plan proposal, functional certificate and prerequisite documentation.
2	Evaluation planning	CB reviews the application; agrees the evaluation plan with developer and laboratory; confirms the laboratory scope covers the required activities; pins the versions of referenced external specifications.
3	FITCEM evaluation	Laboratory performs the evaluation tasks per EN 17640:2022 and this document, within the fixed time budget, under CB responsibility, including the product identity verification of section 6.2.1.
4	Process audit	CB conducts the initial audit of developer operational processes per the audit instruction (NI003).
5	Evaluation Review Meeting	Optional. The CB reviews laboratory and developer findings, resolves open issues, and confirms evaluation completeness. In person or virtual.
6	Certification decision	CB certifying function reviews the ETR, any delta assessment, and the audit reports; takes the certification decision; issues the Certificate of Conformity and the Certification Report.
7	Post-certification	Periodic surveillance; change management; special evaluations triggered by changes or vulnerabilities; recertification.

6.2 Functional certificate prerequisite

A functional certificate is mandatory. A certificate of conformity shall not be issued under this scheme unless a valid functional certificate exists for the same product.

"The same product" means the same product identity and the same version. The product name, product identifier, version identifier and build or release identifier stated on the functional certificate shall be identical to those stated in the FIT ST and on the certificate of conformity issued under this scheme.

For the European Digital Identity Wallet the functional certificate is the output of the functional conformity assessment performed under the Functional Conformance Assessment Framework of the ARF. Where that assessment is issued as an attestation rather than a certificate, that attestation is the accepted form, provided it identifies the product and version unambiguously.

The functional certificate shall be valid at the date of the certification decision. Where it is suspended, withdrawn or expires, the product developer shall notify the CB without undue delay and the CB shall assess the consequences for the certificate of conformity in accordance with section 6.5.

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

The FIT ST shall identify the functional certificate by issuing body, certificate identifier, date of issue, validity period, and the product and version it covers. The Certification Report shall record the same identifiers.

Functional conformity does not substitute for any part of the security evaluation. The Evaluation Laboratory shall not reduce testing on the basis that a functional requirement has been tested under the functional conformity assessment, except where section 6.6 and the applicable Protection Profile expressly permit reuse.

6.2.1 Verification of product identity by the Evaluation Laboratory

The Evaluation Laboratory shall verify, and record in the ETR, that the product submitted for evaluation is the same product, at the same version, as the product covered by the functional certificate. The Evaluation Laboratory shall:

- obtain the functional certificate and, where available, the associated functional conformity assessment report, from the product developer or the issuing body;
- record the product name, product identifier, version identifier and build or release identifier as stated on the functional certificate;
- record the same identifiers as determined from the evaluated product itself, by inspection of the delivered package and its metadata, and not solely from the product developer's declaration; the identifiers recorded from the product shall include at minimum the application identifier, the version name and version code declared in the application package, and the signing certificate fingerprint of the delivered package;
- where a cryptographic digest of the delivered product is available, record that digest and compare it against any digest recorded in the functional conformity assessment;
- state explicitly whether the identifiers recorded from the certificate and from the product are identical;
- where they are not identical, record the differences and apply section 6.6;
- confirm that the functional certificate was valid at the date of the identity check.

The CB shall not take a positive certification decision where the Evaluation Laboratory has not recorded a positive identity result, or, where section 6.6 applies, has not recorded a positive delta conclusion reviewed and accepted by the CB.

6.3 Certificates and publication

Upon a positive certification decision the CB issues a Certificate of Conformity and publishes a Certification Report, and notifies the Scheme Owner for inclusion in the public register. The maximum certificate validity period is five years. Post-certification surveillance follows the periodic cycle consistent with Annex IX of Commission Implementing Regulation (EU) 2024/2981.

6.4 Incident and vulnerability management

Party	Obligation
Product developer	Notify the CB of critical vulnerabilities and active exploits within 24 hours; of high-severity vulnerabilities within 72 hours; of other changes and vulnerabilities per the timeline in this document. Maintain a vulnerability management policy per EN ISO/IEC 30111:2019. Prepare Vulnerability Impact Analysis Reports for relevant vulnerabilities.

Party	Obligation
Certification Body	Assess all developer notifications and Vulnerability Impact Analysis Reports and determine the required actions. Report all incidents and vulnerabilities to the Scheme Owner. Decide on certificate suspension or withdrawal where conformity is at risk.
Scheme Owner	Maintain the central vulnerability register, coordinate vulnerability response for certified products, and issue guidance to CBs and developers as necessary.

6.5 Certificate suspension and withdrawal

The CB may suspend a certificate where continued conformity is in doubt pending remediation. The CB shall withdraw a certificate where non-conformity is permanent, unremediated within the required timeframe, or where the developer ceases to maintain the certified product. Loss of the functional certificate is a trigger for assessment under this section.

6.6 Changed products: delta assessment

Where the product submitted for certification differs from the product covered by the functional certificate, or from a product previously certified under this scheme, the Evaluation Laboratory may demonstrate that the changed product is sufficiently covered by the combination of the previous analysis and testing and the new analysis and testing performed on the change.

The Evaluation Laboratory shall produce a delta assessment, which forms part of the ETR and shall reach one of the following conclusions.

Conclusion	Meaning
Covered	The change affects neither the security problem definition, the security requirements, the module decomposition, nor the validity of the previous vulnerability analysis and test results. The previous evaluation results remain applicable in full.
Partially covered	The change affects an identified subset of the above. That subset has been re-analysed and re-tested on the changed product; the previous results remain applicable for the remainder.
Not covered	The change is such that the previous results cannot be relied upon. A full evaluation is required.

Conclusions "covered" and "partially covered" shall be substantiated by all of the evidence listed in Annex C. The CB shall review the delta assessment and may reject the conclusion and require the change to be treated as "not covered".

A delta assessment shall not be used where the change alters the TOE boundary, the assumptions on the operational environment, the environmental requirements of the applicable Protection Profile, or the identity or version of a certified component on which the product depends. A change that alters the architecture variant of section 2.3, or that moves a function across the TOE boundary, shall be concluded "not covered".

The following changes shall not be concluded "covered" without new analysis and testing of the affected requirements:

- any change to the Remote User Authentication Protocol, to the derivation or handling of the knowledge factor, or to the possession factor held on the User device;
- any change to the interface with the WSCA-BE or the WSCD, or to the identity, version or certification status of the WSCD;
- any change to key generation, key storage, key usage policy, or to the set of keys listed in the Protection Profile;
- any change to attestation handling, including Wallet Unit Attestation, Wallet Instance Attestation and Key Attestation;
- any change to a resilience mechanism, including obfuscation, anti-deobfuscation, debug detection, integrity verification, platform state detection and screen protection;
- any change to the trusted list, revocation list or trust anchor handling;
- any change to the target platform API level, the signing key, or the distribution channel.

Where the change results in a version for which no functional certificate exists, section 6.2 applies and the certificate of conformity shall not be issued until a functional certificate covering that version is available. The delta assessment may be prepared in advance of that certificate.

The delta assessment is performed within the fixed evaluation time budget set for the affected evaluation tasks. Where it cannot be completed within that budget, the conclusion shall be "not covered".

Tool reuse: Scripts and test tools from a previous evaluation may be reused in a delta assessment only where they are identified by version, are retained under configuration control, shown to be still applicable for state-of-the-art attacks at the high level at the time of certification, and are shown to run against the changed product. This shall be recorded in the evidence of Annex C.

6.7 Scheme maintenance and version transitions

The Scheme Owner periodically reviews and revises this document, and revises it when the Protection Profile, the OWASP MAS deliverables, the regulatory basis, or the architecture set changes. For each revision, transition arrangements shall be published specifying:

- the effective date of the new version;
- timelines for new certifications under the revised version;
- re-evaluation obligations and simplification provisions for currently certified products;
- interaction of version transitions with ongoing surveillance obligations.

The Scheme Owner shall notify the relevant EU Cooperation Group of revisions where required.

7. Related scheme documents

Doc. ID	Type	Description	Status
NP001-EUDIW-C	Scheme	This document. Complete scheme for the European Digital Identity Wallet in one document.	v0.9.4 for review
NP002	Scheme procedures	Detailed certification procedures.	Planned
NI002	Evaluation instruction	General FITCEM evaluation task instructions for laboratories.	Planned
NI003	Audit instruction	Instruction for the audit of developer operational processes.	Planned

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

Annex A: Glossary

Term	Definition
ARF	EUDI Wallet Architecture and Reference Framework.
Baseline evaluation	The previous evaluation whose analysis and test results are relied upon in a delta assessment.
CB / Certification Body	Body accredited under EN ISO/IEC 17065:2012 responsible for managing the certification process and issuing certificates.
Delta assessment	Documented demonstration that a changed product is sufficiently covered by previous and new analysis and testing. Section 6.6; evidence in Annex C.
ETR / Evaluation Technical Report	Report produced by the Evaluation Laboratory summarising all evaluation activities, verdicts and findings.
Evaluation Laboratory	Testing laboratory fulfilling EN ISO/IEC 17025:2017 and performing FITCEM evaluation tasks under the responsibility of the CB.
FCAF	Functional Conformance Assessment Framework of the ARF. Produces the functional certificate or attestation required by section 6.2.
FSR	Functional Security Requirement of the Protection Profile. See section 4.2 and [TP-WI-BB].
FIT PP / WPP	Wallet Protection Profile.
FIT ST / WSS	Product specific security specification (Wallet Security Specification).
FITCEM	Fixed time evaluation methodology, EN 17640:2022.
Functional certificate	Certificate, or equivalent attestation, of conformity with the functional requirements applicable to the wallet. Mandatory. Section 6.2.
MASWE	OWASP Mobile Application Security Weakness Enumeration.
RSR	Resilience Security Requirement of the Protection Profile, mandatory or recommended. See section 4.2 and [TP-WI-BB].
Scheme Owner	Party that owns and governs the scheme. Identity [to be confirmed].
SESIP	Security Evaluation Standard for IoT Platforms, EN 17927.
SUG / Secure User Guide	Document describing how to install, configure and use the TOE securely.
TOE / Target of Evaluation	The product, or defined portion of it, subject to the FITCEM evaluation.
TR1	The certification system against which the scheme is admitted and supervised.
Trust Mark [to be confirmed]	The mark of conformity for products certified under this scheme.
VIAR	Vulnerability Impact Analysis Report.
WI	Wallet Instance. The application installed on the User device; the TOE under [PP-WI-REMOTE].

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

Term	Definition
WSCA / WSCA-BE	Wallet Secure Cryptographic Application, and its backend variant.
WSCD	Wallet Secure Cryptographic Device; in the remote architecture, a certified remote HSM.
WSF / WSFI	Wallet Security Functions and their interfaces.

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

Annex B: References

Reference	Document
[ARF]	EUDI Wallet Architecture and Reference Framework, including the Functional Conformance Assessment Framework (FCAF). [Version to be pinned.]
[CSA]	Regulation (EU) 2019/881 — Cybersecurity Act.
[eIDAS2]	Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014.
[EN 17640]	EN 17640:2022 — Fixed-Time Evaluation Methodology for ICT Products (FITCEM).
[EN 17927]	EN 17927:2023 / GlobalPlatform GPD_SPE_140 — Security Evaluation Standard for IoT Platforms (SESIP).
[ENISA-EUDIW]	Draft candidate EU cybersecurity certification scheme for European Digital Identity Wallets, ENISA. Draft.
[EUCC]	Commission Implementing Regulation (EU) 2024/482 — EUCC scheme.
[IR 2979]	Commission Implementing Regulation (EU) 2024/2979 — integrity and core functionalities of European Digital Identity Wallets.
[IR 2981]	Commission Implementing Regulation (EU) 2024/2981 — certification of European Digital Identity Wallets. Section IV contains the threat catalogue (TRnn).
[IR 848]	Commission Implementing Regulation (EU) 2025/848 — registration of wallet-relying parties.
[ISO/IEC 15408]	ISO/IEC 15408-1/2/3:2022 — Evaluation criteria for IT security (Common Criteria).
[ISO/IEC 17025]	ISO/IEC 17025:2017 — Competence of testing and calibration laboratories.
[ISO/IEC 17065]	ISO/IEC 17065:2012 — Requirements for bodies certifying products, processes and services.
[ISO/IEC 17067]	ISO/IEC 17067:2013 — Fundamentals of product certification.
[ISO/IEC 18045]	ISO/IEC 18045:2022 — Methodology for IT security evaluation (CEM).
[ISO/IEC 30111]	ISO/IEC 30111:2019 — Vulnerability handling processes.
[OWASP MASVS]	OWASP Mobile Application Security Verification Standard (MASVS) v2.1.0. https://mas.owasp.org/MASVS
[OWASP MASWE]	OWASP Mobile Application Security Weakness Enumeration (MASWE) v1.0. https://mas.owasp.org/MASWE
[OWASP MASTG]	OWASP Mobile Application Security Testing Guide (MASTG), current version. https://mas.owasp.org/MASTG
[OWASP MAS Profiles]	OWASP MAS testing profiles L1, L2, R and P.

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

Reference	Document
[OWASP MAS-EUDI]	OWASP MAS EUDI Wallet profile (W), with deliverables "EUDI Wallet MAS Profile" and "EUDI Wallet MAS Profile — Practical Guidelines". Draft; not released as at the date of this version.
[PP-WI-REMOTE]	FITCEM Protection Profile for EUDI Wallet Instance supported by a remote WSCA-WSCD, identification FITCEM-PP-WALLET-INSTANCE-for-REMOTE-WSCA-WSCD, version 0.2d, 20 August 2026, draft. The applicable Protection Profile for the remote WSCA-WSCD architecture variant. [TP-WI-BB] gives the title as "EN 17640 FITCEM PROTECTION PROFILE for EUDI Wallet Instance in the remote HSM architecture"; identification to be confirmed.
[TP-WI-BB]	Black-Box Penetration Testing Plan for the Wallet Instance (WI-TOE), version 1.0, 16 October 2026, with effort estimate (file title: HOURS ESTIMATE WI FITCEM Wallet Instance BLACK BOX TESTPLAN for Time Estimation). Prepared to support effort estimation; not an evaluation test specification.
[Reg-765/2008]	Regulation (EC) No 765/2008 on accreditation and market surveillance.

Annex C: Delta assessment evidence checklist

This annex lists the evidence the Evaluation Laboratory shall record to substantiate a delta assessment under section 6.6. Where an item is not applicable, the delta assessment shall state why.

#	Evidence item
	Identification
1	The baseline: product, version, build identifier, the evaluation results relied upon, their date, the Evaluation Laboratory that produced them, and the certificate identifier where applicable.
2	The changed product: product, version, build identifier, and the delivery from which it was obtained.
3	The status of the functional certificate for both the baseline and the changed product.
	Description of the change
4	A product developer supplied change description covering all changes between baseline and changed product, not only those the developer considers security relevant.
5	The Evaluation Laboratory's independent corroboration of the completeness of that description, the means used (source difference, binary difference, dependency manifest comparison, or other), and the residual uncertainty.
6	Third-party components, libraries and SDKs added, removed or changed, with versions.
7	Changes to the build toolchain, signing keys, hardening or obfuscation configuration, and target platform API level.
	Impact analysis
8	For each change, the affected assets, threats and security requirements, by the identifiers used in the Protection Profile and in the FIT ST.
9	The modules of the module decomposition affected by each change.
10	Whether the change affects any assumption on the operational environment or any environmental requirement.
11	Whether the change affects an interface to a component certified under another scheme, including the WSCD.
12	Whether the change affects mechanisms relied upon in the previous vulnerability analysis, in particular resilience mechanisms.
	Reuse justification
13	For each previous test case and analysis activity relied upon, a statement that it remains valid for the changed product, with the reason.
14	For each previous result not relied upon, the replacement analysis or test performed on the changed product.
15	The new test cases executed on the changed product, their results, and the tooling and platform versions used.

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

#	Evidence item
16	A re-assessment of the attack potential required to exploit any weakness identified, in the light of the change and of publicly known vulnerabilities disclosed since the baseline evaluation.
17	A statement on whether the elapsed time since the baseline evaluation, and the evolution of the attack state of the art in that period, affect the validity of the reused results.
	Conclusion
18	The conclusion under section 6.6, with the reasoning connecting items 8 to 17 to that conclusion.
19	The residual risk and any limitation to be carried into the Certification Report.
20	The identity and qualification of the evaluators who performed the delta assessment.

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

Colofon

NL FITCEM Cybersecurity Evaluation and Certification Scheme – NP001-EUDIW-C EUDI Wallet Scheme v0.9.4 for review

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