EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-CS-part3

NL EUDI Wallet Certification System

NL FITCEM Cybersecurity Certification Scheme
Evaluation Instruction for Evaluation Laboratories
NI002

RC1.0

2026.10.25

Document reference	NL-CS (part3)
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 (part1, part2, part4) NL-CS-WI & NL-CS-WI-conditions NL-WSCA & NL-WSCA-conditions

NI002 instructs Evaluation Laboratories on how to perform the FITCEM evaluation tasks for the European Digital Identity Wallet at assurance level high, and what to record. It is the document that [NP001] section 7 lists as the general FITCEM evaluation task instructions for laboratories. It adds no requirement to [NP001]; where a requirement is stated here it is drawn from [NP001], [EN 17640] or [NP002] and the source is named. Items marked [proposed] are drafting proposals of this document and are not yet decided.

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	For publication

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

Contents

Document control 2
1. Introduction 5
1.1 Purpose 5
1.2 Scope 5
1.3 Involved roles 5
1.4 Conventions 5
2. General rules for the evaluation 6
2.1 Assurance level, task set and time 6
2.2 Evaluator competence 6
2.3 Pinning and tool control 6
3. Evidence checklist 7
4. Task instructions 9
4.1 Product identity verification (NP001 section 6.2.1) 9
4.2 Completeness check (EN 17640 6.1) 9
4.3 FIT Security Target evaluation (EN 17640 6.4) 9
4.4 Development documentation (EN 17640 6.5) 10
4.5 Evaluation of TOE installation (EN 17640 6.6) 10
4.6 Conformance testing (EN 17640 6.7) 10
4.7 Penetration testing (EN 17640 6.10) 11
4.8 Extended cryptographic analysis (EN 17640 6.12) 11
4.9 Delta assessment (NP001 section 6.6 and Annex C) 12
4.10 Findings and the termination rule 12
4.11 Evaluation Technical Report (EN 17640 Annex G) 12
5. Evaluation review meetings (optional) 13
Annex A: ETR outline [proposed] 14
Annex B: References 15
Annex C: FOR REVIEW and placeholder register 17

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

1. Introduction

1.1 Purpose

This instruction tells the Evaluation Laboratory what to do, in which order and with what output, for each evaluation task that [NP001] requires. It supports the fixed time premise of FITCEM: because the time budget per task is fixed, the laboratory needs a stable description of what the task consists of and what counts as done.

1.2 Scope

This instruction applies to evaluations of the European Digital Identity Wallet Instance at assurance level high under the NL FITCEM scheme, for the architecture variants admitted in [NP001] section 2.3. Today that is the remote WSCA-WSCD variant under [PP-WI-REMOTE]. It does not cover the audit of the product developer's operational processes ([NI003]), the certification decision, or the procedures of [NP002].

1.3 Involved roles

Role	Entity	Responsibility
Evaluator	Evaluation Laboratory	Performs the evaluation tasks, produces the evaluator evidence and the ETR. Acts under the responsibility of the CB ([NP001] section 3.3).
Certifier	Certification Body	Reviews the evaluation activities, issues the mandatory guidance and the evaluation plan, chairs evaluation review meetings, reviews the ETR and any delta assessment.
Product developer	Applicant	Delivers the evidence checklist, the test samples and accounts, and the source code; answers evaluator questions.

1.4 Conventions

"Shall" marks a requirement that comes from [NP001], [NP002] or [EN 17640]. "Should" marks a recommendation of this instruction. Clause numbers of [EN 17640] are given as "[EN 17640] 6.x" and were checked against the standard text held in the project. Epistemic tags in square brackets follow [NP001]: [established], [inferred], [assumption], [unknown].

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

2. General rules for the evaluation

2.1 Assurance level, task set and time

- The assurance level is high and this is mandatory ([NP001] section 5.1). The required tasks are [EN 17640] 6.1, 6.4, 6.5, 6.6, 6.7, 6.10 and 6.12, together with the product identity verification ([NP001] section 6.2.1) and, where it applies, the delta assessment ([NP001] section 6.6).
- Each task has a fixed time budget set in the evaluation plan ([NP001] section 5.3). The evaluator shall record the time spent per task and report any deviation in the ETR. More functionality raises the probability of findings within the budget; it does not extend the budget.
- The evaluator shall not reduce testing because a requirement has been covered by functional conformity testing, except where [NP001] section 6.6 and the Protection Profile expressly permit reuse ([NP001] section 6.2).
- A finding, vulnerability or non-conformity within the budget is handled under section 4.10.

2.2 Evaluator competence

[EN 17640] states a competence requirement per task (for example knowledge of the TOE domain and of secure development processes for 6.5; the ability to observe installation as an end user would for 6.6). Those statements apply. [NP001] section 3.3 requires the laboratory to maintain evaluator competence "at or above the level required by this document", and the competence requirements document NI-COMP-001 was removed from the scheme in the current [NP001].

2.3 Pinning and tool control

The evaluator shall record the exact versions of the Protection Profile, of each OWASP MAS deliverable used, of the platform and devices, and of every tool and script used in the evaluation. Scripts and test tools shall be kept under configuration control and identified by version, because [NP001] section 6.6 only permits their reuse in a delta assessment on that condition.

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

3. Evidence checklist

This is the scheme-specific checklist that [EN 17640] 6.1 and 6.5 refer to. The Protection Profile and the OWASP profile are not complete, so the list is a baseline that the Protection Profile can extend. The checklist "source" column states whether the item is required by [EN 17640], by [NP001], or is [proposed] here.

#	Evidence item	Content	Source
E1	FIT ST (Wallet Security Specification)	Final version, claiming conformance to the Protection Profile; instantiates its operations; mirrors the environmental requirements table; identifies the functional certificate; states the TOE boundary and the architecture variant.	[NP001] 4.1, 2.4, 6.2
E2	Functional certificate and report	The functional certificate or attestation for the same product and exact version, with the functional conformity assessment report where available.	[NP001] 3.4, 6.2
E3	Specification of the functionality	At the level of the interfaces and their parameters, including the interfaces with the WSCA-BE, the WSCD and the Wallet Provider backend.	[EN 17640] 6.5.2
E4	Development process documentation	Including vulnerability and patch management.	[EN 17640] 6.5.2
E5	Design documentation	At the level of the modules of the module decomposition of the Protection Profile: wallet core; WSCA/WSCD interface; optional remote signing module; presentation and proximity interface; modules specific to the architecture variant.	[EN 17640] 6.5.2; [NP001] 5.4
E6	Security architecture description	Self-protection, secure communication channels, key management, attestation handling (Wallet Instance Attestation, Key Attestation), resilience mechanisms (obfuscation, anti-deobfuscation, integrity, debug and platform state detection, screen protection).	[EN 17640] 6.5.2; [NP001] 6.6
E7	Source code	Complete source code of the Wallet Instance, with its build instructions. Failure to provide it counts as an evaluation failure.	[NP001] 3.4; scheme decision
E8	Setup and User Guide (SUG)	How to install, configure and use the Wallet Instance securely, in the language fixed in the evaluation plan.	[EN 17640] 6.6
E9	Test samples and access	Installable builds identical to the production release, target devices or access to them, and test accounts or a working backend, including the WSCA-BE and WSCD access needed to operate the TOE.	[EN 17640] 6.6.4.1 (backend example)
E10	Product identification data	Application identifier, version name, version code, build or release identifier, signing certificate fingerprint, and a cryptographic digest of the delivered package.	[NP001] 6.2.1
E11	Third-party components	Libraries and SDKs with versions, as used in the build.	[proposed]; needed for [NP001] Annex C item 6

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

#	Evidence item	Content	Source
E12	Update mechanism description	How updates are produced, signed, distributed and verified, per software component.	[IR 2981] Annex IX
E13	Risk assessment	The product developer's risk assessment for the specific architecture.	[NP002] 2.3
E14	Assurance information for components outside the TOE	WSCD certificate and report; WSCA-BE assurance information where outside the TOE.	[NP001] 2.4, 5.4
E15	Test to requirement mapping inputs	The product developer's own test evidence, if any, for the Protection Profile requirements.	[proposed]

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

4. Task instructions

Each subsection states the aim and the clause of [EN 17640], the scheme-specific actions, and what the evaluator records. The work units of [EN 17640] apply in addition and are not repeated.

4.1 Product identity verification (NP001 section 6.2.1)

Performed together with the completeness check. The evaluator shall:

1. obtain the functional certificate and, where available, the functional conformity assessment report, from the product developer or the issuing body;

2. record the product name, product identifier, version identifier and build or release identifier as stated on the functional certificate;

3. determine the same identifiers from the evaluated product itself, by inspection of the delivered package and its metadata, and not solely from the declaration of the product developer. At minimum: the application identifier, the version name and version code declared in the package, and the signing certificate fingerprint of the delivered package;

4. where a cryptographic digest of the delivered product is available, record it and compare it with any digest recorded in the functional conformity assessment;

5. state explicitly whether the identifiers from the certificate and from the product are identical;

6. where they are not identical, record the differences and apply the delta assessment of section 4.9;

7. confirm that the functional certificate was valid at the date of the check.

Output: a positive, negative or delta identity result in the ETR. The CB does not take a positive decision without a positive result or a delta conclusion it has accepted.

4.2 Completeness check (EN 17640 6.1)

Aim: verify that all evidence of section 3 is present. Missing or incomplete items are recorded as findings and communicated to the CB; the evaluator shall not proceed with a task whose evidence is missing unless the evaluation plan says otherwise. Output: the completed checklist, with the delivery date of each item and the version of each document.

4.3 FIT Security Target evaluation (EN 17640 6.4)

Aim: verify that the FIT ST is well constructed, consistent and a suitable basis for the evaluation. No access to the TOE is needed. Because a Protection Profile is mandatory, work unit 1b applies; work unit 1a (a FIT ST not based on a Protection Profile) does not.

- Confirm that all operations of the Protection Profile have assigned values in the FIT ST ([EN 17640] 6.4.4.2).
- Confirm that the FIT ST claims conformance to the Protection Profile and to the version pinned in the evaluation plan, and that the environmental requirements table of the Protection Profile is mirrored and not restated or altered ([NP001] section 2.4).

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

- Confirm that the TOE boundary is unambiguous and that the WSCA-BE and WSCD are placed as the Protection Profile places them ([NP001] section 2.1).
- Confirm that the FIT ST is free of contradictions with the SUG and the other design documents, understandable to the end customer, and not misleading about security properties ([EN 17640] 6.4.4).
- Confirm that the functional certificate is identified by issuing body, certificate identifier, date of issue, validity period, and product and version covered ([NP001] section 6.2).
- Confirm that the cryptographic algorithms listed are in the set approved by the scheme [placeholder, see section 4.8].

Output: verdict and the list of inconsistencies found.

4.4 Development documentation (EN 17640 6.5)

Aim: assess the development documentation and evidence against the checklist entries. [EN 17640] advises schemes to keep this task as light as possible; the evaluator shall check that the documentation is complete according to the checklist ([EN 17640] 6.5.4.1) and analyse the entries listed in [EN 17640] 6.5.2: specification of functionality, development process documentation including vulnerability and patch management, design at module level, the description of the security architecture, and the source code. The source code is used to support the penetration testing and the extended cryptographic analysis; any further source code review beyond what the Protection Profile requires is not part of this task.

Output: verdict per checklist item, and the list of gaps.

4.5 Evaluation of TOE installation (EN 17640 6.6)

- Check that every system needed to install and use the TOE is present and correctly set up. The set-up may be done together with the product developer and is itself not part of the evaluation; the evaluation does not proceed until it is complete ([EN 17640] 6.6.4.1).
- Install the Wallet Instance from the distribution channel or package that the delivered product identity identifies, following the SUG in the language of the FIT ST. Record the platform, device and operating system versions.
- Record in the ETR whether the TOE is operating as described in the FIT ST (secure state) after set-up. If not, use general expert knowledge to reach the secure state and record each step that differs from the SUG.
- Check that the SUG follows the scheme requirements, and determine how hard it is to leave the secure state and whether the user is warned ([EN 17640] 6.6.4.2 and 6.6.4.3).

4.6 Conformance testing (EN 17640 6.7)

Aim: verify that the TOE complies with the security claims of the FIT ST. At assurance level high the coverage is complete and the acceptance criteria are defined by the scheme ([EN 17640] Table D.2; Annex C of [EN 17640] on acceptance criteria).

1. Determine the security requirements to be tested, from the FIT ST and the Protection Profile: the Functional Security Requirements (FSR) and the Resilience Security Requirements (RSR).

2. Define the test cases, each with preparation, steps, expected result and the explanation of when it is a fail.

3. Record each test with its target requirement. A test without a recorded target requirement does not contribute to assurance ([NP001] section 4.3). The mapping is many to many: one test may give evidence for several requirements.

4. Execute the tests and record, for each failed test, the test case, the expected result and the observed result. Where no test case can be specified for a requirement, give an alternative proof of correct implementation.

5. Record the testing strategy and results in the ETR.

4.7 Penetration testing (EN 17640 6.10)

Aim: a sampling test strategy based on the Flaw Hypothesis Methodology that the TOE does not contain vulnerabilities of the class of known vulnerabilities. This task is a superset of vulnerability testing ([EN 17640] 6.9). The methodology of [EN 17640] 6.10.2.2 applies: gather information, hypothesise flaws, exclude attacks that require too much effort or that the FIT ST context excludes, test, and record.

- Information gathering includes the evaluator's own evidence from the earlier tasks, public vulnerabilities applicable to the product, unexpected behaviour during conformance tests and inconsistencies found in the FIT ST.
- The test set is built on OWASP MAS, as pinned in the evaluation plan ([NP001] section 4.4): the working baseline for the wallet at assurance level high is L2 + R + P with the EUDI Wallet profile on top, subject to the open point of [NP001] section 4.4. The evaluator shall not reproduce OWASP content in the ETR; it references it.
- The attack potential is determined per [EN 17640] Annex F. The expected resistance, and the depth of the vulnerability analysis, are the placeholder of [NP001] section 5.1 (working position AVA_VAN.3).
- The platform is tested only as far as [NP001] sections 2.2 and 2.4 allow. The Wallet Instance's mechanisms that detect and reject platform states which do not meet the environmental requirements are security controls that are evaluated ([IR 2981], Annex IV, section 4). The scope of platform testing is an open point of [NP001] section 2.2.
- Use validated tools where possible; analyse the coverage of tools and add manual tests where needed ([EN 17640] 6.9.4.4 for the corresponding vulnerability testing work unit).
- The hours basis of [TP-WI-BB] organises the effort per requirement and is not an evaluation test specification. The allocation of the fixed budget to [EN 17640] tasks is open in [NP001] section 5.3.

Output: the test plan with the hypotheses and the reasons for excluding attacks; for each test its result; for each failed test the assessed attack potential; the residual risks.

4.8 Extended cryptographic analysis (EN 17640 6.12)

[PLACEHOLDER] method of the task. The scheme has not yet fixed the cryptographic catalogue or methodology for the extended cryptographic analysis. The cryptographic annex is deferred, per the project record, to a later draft of the [EN 17640] Protection Profile of the Wallet Instance. Until it is issued, the evaluator shall record the cryptographic specification as evidence ([EN 17640] 6.4.2), review the algorithms and protocols of the FIT ST for suitability, and propose the method to the CB for approval in the evaluation plan.

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

4.9 Delta assessment (NP001 section 6.6 and Annex C)

The delta assessment applies where the submitted product differs from the product covered by the functional certificate, or from a previously certified product. It is part of the ETR, within the fixed time budget of the affected tasks. The evaluator shall:

1. record the evidence of [NP001] Annex C, items 1 to 20, and state why any item that is not applicable is not applicable. Annex C is not reproduced here;

2. obtain from the product developer a description of all changes between the baseline and the changed product, not only the changes the developer considers security relevant, and corroborate its completeness independently (source difference, binary difference, dependency manifest comparison or other), stating the residual uncertainty (Annex C items 4 and 5);

3. determine, for each change, the affected assets, threats, requirements and modules and whether it touches an environmental requirement or an interface to a certified component (Annex C items 8 to 12);

4. decide for each previous test and analysis whether it remains valid, and perform replacement tests for those that do not (Annex C items 13 to 15);

5. re-assess the attack potential in the light of the change and of vulnerabilities disclosed since the baseline, and consider the elapsed time (Annex C items 16 and 17);

6. reach one of the conclusions covered, partially covered or not covered, with the reasoning, and record the residual risk and the evaluators' identity and qualification (Annex C items 18 to 20).

The delta assessment shall not be used where the change alters the TOE boundary, the assumptions on the operational environment, the environmental requirements, or the identity or version of a certified component on which the product depends. The changes listed in [NP001] section 6.6 shall not be concluded as covered without new analysis and testing of the affected requirements. Where the analysis cannot be completed within the budget the conclusion is not covered. Tools and scripts from earlier evaluations may be reused only where they are identified by version, retained under configuration control and shown to run against the changed product; record this under Annex C.

4.10 Findings and the termination rule

[NP001] section 5.2 gives the working position that a finding within the fixed budget terminates the evaluation and that the full trajectory is re-run after remediation. Until the rule is settled the evaluator shall, on identifying a finding, stop the task concerned only on instruction of the CB, report the finding to the CB without undue delay, and record the time spent so that the cost of a restart can be stated. Severity differentiation and the interaction with a partially covered delta conclusion are to be settled.

4.11 Evaluation Technical Report (EN 17640 Annex G)

The ETR follows Annex G of [EN 17640] and the content required by [NP002] section 4.7. It is submitted to the CB when all tasks are complete. A recommended outline is in Annex A.

5. Evaluation review meetings (optional)

Evaluation review meetings (ERM) are optional ([NP001] section 6.1, phase 5; [NP002] section 4.6). The CB decides in the evaluation plan whether to hold them and when. The following is [proposed] as the form when the CB holds them. It follows the idea of progressive review used in the Dutch EUCC practice, in which the evaluator presents evidence to the certifier in meetings and a checklist of evaluator actions is populated progressively until all verdicts are pass; the content is rewritten for the FITCEM tasks and no Common Criteria assurance class is used.

Meeting	Goal	Deliverables of the evaluator
ERM1, understanding	The evaluator demonstrates understanding of the Wallet Instance and its TOE boundary, and the CB challenges it.	Completeness check result (4.2) and identity result (4.1); FIT ST evaluation result (4.3); summary of the development documentation (4.4) in the evaluator's own words with references, not copied material; the module decomposition as understood; the evaluator's checklist of actions, populated for ERM1.
ERM2, test plan	The evaluator presents the test to requirement mapping, the conformance test plan and the penetration test plan with the flaw hypotheses and exclusions, and the CB challenges soundness before the testing effort is spent.	Installation result (4.5); conformance test plan and mapping (4.6); penetration test plan and hypotheses (4.7); cryptographic analysis approach (4.8); the time used per task; updated checklist.
Final ERM, results	The evaluator presents the results of the tests and the analysis, and the CB questions the interpretation.	Test results and failed-test analysis; findings and their severity; delta assessment where applicable (4.9); WSCD and other certificate records; completed checklist with verdicts; draft ETR.

The certifier shall challenge the evaluator on understanding at ERM1, on the soundness of the plan at ERM2, and on the analysis of results at the final ERM. The evaluator shall not rely on a meeting to substitute for the recording obligations of [EN 17640], [ISO/IEC 17025] or [ISO/IEC 17065]. The CB documents the outcome of each meeting.

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

Annex A: ETR outline [proposed]

#	Section	Content
1	Identification	Product, version, build, identifiers of E10, Protection Profile and version, functional certificate identifiers, laboratory, CB, evaluation plan reference and date.
2	Summary	Verdicts per task, findings, conclusion on the security claims and on conformance to the Protection Profile.
3	Product identity	Result of section 4.1; delta assessment if any (4.9).
4	Environment	Platforms, devices, tools and versions; OWASP MAS versions; WSCD and other certificate records (identity, version, validity).
5	Task reports	One section per task of [EN 17640] 6.1, 6.4, 6.5, 6.6, 6.7, 6.10 and 6.12, with the work units, the time spent and any deviation.
6	Mapping	Test to requirement mapping with the module and the kind of test.
7	Findings	Every finding, with its severity, status and, where relevant, assessed attack potential.
8	Residual risks and limitations	For the certification report.
9	Evaluators	Identity and qualification of the evaluators.

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

Annex B: References

External documents are referred to in the text by their reference tag. Versions, editions and dates are given only in this table.

Reference	Document	Version or date
[NP001]	NP001-EUDIW-C, NL FITCEM EUDI Wallet Certification Scheme (complete scheme)	0.9.4 for review, 24 October 2026
[NP002]	NP002, Scheme Procedures	0.9.4 for review, 24 October 2026
[NI002]	NI002, Evaluation Instruction for Evaluation Laboratories	0.9.4 for review, 24 October 2026
[NI003]	NI003, Audit Instruction for Operational Processes	0.9.4 for review, 24 October 2026
[PP-WI-REMOTE]	FITCEM Protection Profile for EUDI Wallet Instance supported by a remote WSCA-WSCD (FITCEM-PP-WALLET-INSTANCE-for-REMOTE-WSCA-WSCD)	0.2d, 20 August 2026, draft
[PP-WI-DRAFT]	EN 17640 Protection Profile of the Wallet Instance (project draft; cryptographic annex pending)	Draft 0.6 reviewed; 0.7 pending
[TP-WI-BB]	Black-Box Penetration Testing Plan for the Wallet Instance, with effort estimate. Effort basis, not an evaluation test specification	1.0, 16 October 2026
[EN 17640]	EN 17640, Fixed-time cybersecurity evaluation methodology for ICT products (FITCEM)	2022
[EN 17927]	EN 17927, Security Evaluation Standard for IoT Platforms (SESIP)	2023
[ISO/IEC 15408]	ISO/IEC 15408, Evaluation criteria for IT security (Common Criteria)	2022
[ISO/IEC 18045]	ISO/IEC 18045, Methodology for IT security evaluation	2022
[ISO/IEC 17025]	EN ISO/IEC 17025, Competence of testing and calibration laboratories	2017
[ISO/IEC 17065]	EN ISO/IEC 17065, Requirements for bodies certifying products, processes and services	2012
[ISO/IEC 17067]	EN ISO/IEC 17067, Fundamentals of product certification	2013
[ISO/IEC 30111]	EN ISO/IEC 30111, Vulnerability handling processes	2019
[ISO 19011]	EN ISO 19011, Guidelines for auditing management systems (informative)	Edition not pinned
[EUCC-NI002]	Dutch NCCA EUCC scheme document NI002, Content and presentation of evaluation review meetings (reference only, Common Criteria terms)	1.0
[EUCC-NI003]	Dutch NCCA EUCC scheme document NI003, EUCC licensing evidence (reference only)	Dated 04-10-2024

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

Reference	Document	Version or date
[NSI002]	NSI002, Content and presentation of evaluation review meetings, EUDI Wallet certification using FITCEM (outside the NP001 document set)	1.0
[IR 2981]	Commission Implementing Regulation (EU) 2024/2981, certification of European Digital Identity Wallets (national certification schemes)	OJ L, 4.12.2024
[IR 2979]	Commission Implementing Regulation (EU) 2024/2979, integrity and core functionalities of European Digital Identity Wallets	2024
[IR 848]	Commission Implementing Regulation (EU) 2025/848, registration of wallet-relying parties	2025
[OWASP MAS]	OWASP MASVS, MASWE, MASTG, MAS testing profiles (L1, L2, R, P) and the EUDI Wallet profile	MASVS 2.1.0; MASWE 1.0; MASTG current; EUDI Wallet profile draft, not released
[ARF]	EUDI Wallet Architecture and Reference Framework, including the Functional Conformance Assessment Framework	Version to be pinned

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

Annex C: FOR REVIEW and placeholder register

Section	Point	Origin
2.2	Evaluator competence requirements after removal of NI-COMP-001	[NP001] section 3.3
2.3	Who holds the scripts and tools between and after evaluations	[NP001] section 6.6
3	Checklist extension from the Protection Profile	[PP-WI-REMOTE]
4.6	Test set and mapping table	[NP001] sections 4.3, 4.4
4.7	Attack potential expectation; platform test scope; budget allocation per task	[NP001] sections 5.1, 2.2, 5.3
4.8	Cryptographic catalogue and method for task 6.12	[EN 17640] PP annex pending
4.10	Termination rule and severity	[NP001] section 5.2
5	Evaluation review meeting content, agreed with certifiers	NI002