EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-CS-part4

NL EUDI Wallet Certification System

NL FITCEM Cybersecurity Certification Scheme
Audit Instruction for Operational Processes
NI003

Document reference	NL-CS (part4)
Version	RC1.0
Status	Release Candidate
Date	25/10/2026
Document type	FITCEM Certification Scheme Audit Instruction for Operational Processes
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, part3) NL-CS-WI & NL-CS-WI-conditions NL-WSCA & NL-WSCA-conditions

NI003 instructs the Certification Body on the audit of the product developer's operational processes that maintain the security of the certified wallet: version control, change management, update delivery and vulnerability management. [NP001] section 6.1 (phase 4) refers to it as the audit instruction, and section 7 lists it as the instruction for the audit of developer operational processes. Criteria marked [proposed] are drafting proposals of this document, derived from the sources named, 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	Aligned to [NP001] and [NP002].

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. Audit principles 6
3. Audit types and schedule 7
4. Audit criteria 8
4.1 Version control (VC) 8
4.2 Change management (CM) 8
4.3 Update delivery (UD) 8
4.4 Vulnerability management (VM) 9
4.5 Continued validity of the certification basis (CV) 10
5. Audit procedure 11
5.1 Planning 11
5.2 Document review 11
5.3 Sampling of records 11
5.4 Interviews and observation 11
5.5 Findings 11
5.6 Audit report 12
6. Auditor competence 13
Annex A: Audit checklist 14
Annex B: Audit report outline [proposed] 16
Annex C: References 17
Annex D: FOR REVIEW and placeholder register 19

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

1. Introduction

1.1 Purpose

A certificate of conformity says something about one version of the wallet. The product developer keeps the wallet secure afterwards through its operational processes. [NP001] section 2.2 therefore scopes the management system element of the scheme to the processes directly relevant to the security maintenance of the certified product, and states that general information security management systems are not part of the certification decision. This instruction states what the CB audits in those processes, how, and how findings feed the certificate.

1.2 Scope

- The four processes of section 4: version control, change management, update delivery, and vulnerability management. Annex IX of [IR 2981] names version control, update and vulnerability management; [NP001] section 2.2 names change management, vulnerability management and update delivery. This instruction covers all of them [see the review point below].
- The continued validity of the functional certificate and of the assumptions and certificates the certification relies on (section 4.5).
- The initial audit (design and existence of the processes, not yet operating effectiveness), the annual surveillance audits (operating effectiveness) and the audit within recertification.

Out of scope: general information security management, software development lifecycle assurance, conformity with the Cyber Resilience Act as a whole ([NP001] section 2.2), and the evaluation tasks of [NI002].

1.3 Involved roles

Role	Entity	Responsibility
Lead auditor	Certification Body	Plans and leads the audit, decides on the findings, signs the audit report. Competent per section 6.
Auditor	Certification Body	Performs audit activities under the lead auditor.
Auditee	Product developer	Provides the process documentation and the records, and makes the process owners available.
Technical support	Evaluation Laboratory	May support the CB with technical questions on the evidence, under the CB's responsibility. [Proposed; [NP001] section 3.2 assigns the audit to the CB and does not mention laboratory support.]

1.4 Conventions

"Shall" marks a requirement taken from [NP001], [NP002], [IR 2981] or [EN 17640], with the source named. Criteria marked [proposed] are drafting proposals. Epistemic tags follow [NP001].

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

2. Audit principles

The audit is evidence based. The auditor shall verify statements by records and, where the audit type requires it, by observation or interview; a process description alone does not demonstrate operating effectiveness. The audit is performed by persons independent of the process audited and of the evaluation, in line with the impartiality required of the CB by [ISO/IEC 17065]. [ISO 19011] (guidelines for auditing management systems) is a useful informative reference for audit practice; this instruction does not make it normative [inferred suitability, not checked against the standard text].

Confidential information of the product developer obtained during the audit is protected under the CB's accreditation obligations. Source code and vulnerability details are shown to the auditor only as far as needed to verify the process.

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

3. Audit types and schedule

The schedule follows the reference schedule of Annex IX of [IR 2981] and [NP002] section 7.1. The Regulation makes the schedule a recommendation; any other schedule must keep the certificate validity within five years and each evaluation within 12 months of the previous year's.

Year	Audit type	Auditor verifies	Audit stages
0	Initial audit ([NP001] section 6.1, phase 4)	That the four processes exist and are designed to meet the criteria of section 4. Operating effectiveness is not assessed [Annex IX: maintenance processes excluding their operating effectiveness].	Document review; walk-through with process owners.
1, 2, 3	Surveillance audit	Operating effectiveness of at least version control, update and vulnerability management; evaluation of changes impacting the security of the product, using the delta assessment of [NP001] section 6.6.	Document review; record sampling; interviews.
4	Audit within recertification	Operating effectiveness of the maintenance processes, with the criteria applied to the whole period since the last full evaluation.	As surveillance, plus reconsideration of the design of the processes.
Any	Special audit	Triggered under [NP002] section 7.3, for instance after a vulnerability, a suspension or a change concluded as not covered. Scope set by the CB.	As the CB determines.

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

4. Audit criteria

The criteria below are what the processes shall achieve. Each has an identifier, used in the audit report and in Annex A. Evidence examples are indicative.

4.1 Version control (VC)

ID	Criterion	Source
VC1	Every release of the certified Wallet Instance is uniquely identified by application identifier, version name, version code and build or release identifier, and these match the identifiers on the functional certificate and in the FIT ST.	[NP001] 6.2, 6.2.1
VC2	The source code and build configuration of every release are held under version control with traceable history and controlled access, so that the delivered package can be related to a source revision.	[proposed]; supports [NP001] Annex C items 1 to 5
VC3	The signing key and the signing process are controlled, and a change of the signing key is notified to the CB before it is used.	[NP001] 6.6 (signing key change)
VC4	The list of third-party components, libraries and SDKs per release is maintained.	[proposed]; [NP001] Annex C item 6

4.2 Change management (CM)

ID	Criterion	Source
CM1	Planned changes to the certified product are notified to the CB before implementation.	[NP001] 3.4; [NP002] 7.4
CM2	Every change is recorded with a description of all differences, not only those the developer considers security relevant, so that a delta assessment is possible.	[NP001] Annex C item 4
CM3	Each change is assessed for security impact, including against the list of changes in [NP001] section 6.6 that shall not be concluded as covered without new analysis: the user authentication protocol or factors, the interface with the WSCA-BE or WSCD, key handling, attestation handling, resilience mechanisms, trusted list and revocation handling, target platform API level, signing key, distribution channel.	[NP001] 6.6
CM4	Changes to the TOE boundary, to the assumptions on the operational environment, to the environmental requirements or to the identity or version of a certified component are identified as such and are not treated as covered by delta assessment.	[NP001] 6.6
CM5	Changes to the target platform and to the variants for categories of end user devices are tracked, because wallet instances are expected to need frequent updates.	[IR 2981] Annex IV, section 5

4.3 Update delivery (UD)

ID	Criterion	Source
UD1	The product has a feature to perform updates of each software component, and the update process is described and operated as described.	[IR 2981] Annex IX

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

ID	Criterion	Source
UD2	Updates are produced from controlled builds, signed with the controlled key, and the integrity and authenticity of an update is verified before installation.	[proposed]
UD3	The distribution channel is the one stated in the FIT ST and any change of channel is notified ([NP001] section 6.6).	[NP001] 6.6
UD4	The time between availability of a security update and its delivery to users, and the share of users on supported versions, are monitored.	[proposed]
UD5	The Wallet Instance's mechanism for verifying, per wallet unit, that the platform satisfies the assumptions on the end user device remains effective after updates, including the minimum platform version.	[IR 2981] Annex IV, section 4; [NP001] 2.4

4.4 Vulnerability management (VM)

ID	Criterion	Source
VM1	The product developer has a vulnerability management policy and procedures that take into account [ISO/IEC 30111], and that meet the requirements of Annex I to the Cyber Resilience Act as required by Article 5(7) of [IR 2981].	[IR 2981] Art. 5(3), 5(7); [NP001] 3.4, 6.4
VM2	Sources of vulnerability information (public databases, dependency advisories, platform security bulletins, researcher reports) are monitored and the monitoring is evidenced.	[proposed]
VM3	Each vulnerability is assessed for severity and impact in the context of the certified wallet.	[NP001] 6.4
VM4	Critical vulnerabilities and active exploits are notified to the CB within 24 hours of discovery, and high-severity vulnerabilities within 72 hours. Other vulnerabilities and changes are notified within the timeline of the scheme.	[NP001] 3.4, 6.4
VM5	A vulnerability impact analysis report is prepared for any vulnerability that affects the software components of the wallet, with the content of Article 5(5), and transmitted to the CB without undue delay.	[IR 2981] Art. 5(5), 5(6)
VM6	Remediation is carried out commensurately with severity and potential impact, with remediation delays recorded.	[IR 2981] Art. 12(3); [EN 17640] 6.9.4.5
VM7	Publicly known and remediated vulnerabilities are disclosed and registered in the repositories of Annex V.	[IR 2981] Art. 5(9)

Evidence expectations drawn from [EN 17640] 6.9.4.5, which describes the evidence from the development process for vulnerability testing: vulnerability scan reports no older than three months; a sample of remediation actions annexed to the internal vulnerability management policy with remediation delays clearly indicated; and a risk management analysis covering at least the 12 months before the evaluation, with unambiguous version tracking. For the audit they are a reference for what a mature process leaves behind [inferred use].

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

4.5 Continued validity of the certification basis (CV)

ID	Criterion	Source
CV1	The functional certificate remains valid for the certified version, and its suspension, withdrawal or expiry is notified to the CB without undue delay.	[NP001] 3.4, 6.2
CV2	The product developer monitors the validity, version and certification status of the WSCD certificate and of other certificates recorded as environmental requirements, and notifies the CB of any change.	[NP001] 5.4, 6.6
CV3	The assumptions on the operational environment and the environmental requirements of the Protection Profile remain valid for the lifetime of the certificate.	[NP001] 2.4

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

5. Audit procedure

5.1 Planning

The lead auditor sends the product developer the audit plan with the scope, the criteria, the period to be covered, the documents and records requested, and the dates. For surveillance audits the period is the time since the last audit, and the request includes the change log, the vulnerability log, the notifications sent to the CB and the update release log for that period.

5.2 Document review

The auditor reviews the process documentation against the criteria and records for each criterion whether the design meets it. In the initial audit this is the principal activity.

5.3 Sampling of records

For operating effectiveness the auditor samples records of the period. [Proposed] sampling rule: all changes that the product developer or the CB classified as touching the list of [NP001] section 6.6; all vulnerabilities rated critical or high; all notifications to the CB; and a sample of other changes and vulnerabilities selected by the auditor, with the sampling basis stated in the report. The auditor traces each sampled change from request to release and to the next delta assessment, and each sampled vulnerability from discovery to notification, remediation and disclosure, checking the 24 and 72 hour limits against timestamps.

5.4 Interviews and observation

The auditor interviews the owners of the four processes and, where useful, observes a build or update release. The aim is to see that the people who operate the process know it and follow it.

5.5 Findings

The auditor records for each criterion: met, not met, or not applicable with the reason. [Proposed] classification of a not-met criterion:

Class	Meaning	Consequence
Major	A criterion is not met in a way that puts continued conformity in doubt, for example a missed 24 or 72 hour notification, a change that required a delta assessment and had none, or a process that does not exist.	Reported to the certifying function; may lead to suspension under [NP002] section 9.2. Remediation timeframe set by the CB.
Minor	A criterion is partly met, or a record is missing, without putting conformity in doubt.	Corrective action by a date set by the CB; verified at the next audit.
Observation	An improvement that does not concern a criterion.	Recorded; no action required.

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

5.6 Audit report

The CB issues an audit report to the product developer with the scope, the period, the criteria, the evidence examined, the sampling basis, the findings with their class, and the conclusion. A recommended outline is in Annex B. The report is an input to the certification decision ([NP002] section 6.1) in the initial audit, and to the surveillance report ([NP002] section 7.2) later. The CB keeps the records for the period set by the Scheme Owner ([NP001] section 3.2).

6. Auditor competence

The auditor shall have the competence required by [ISO/IEC 17065] for certification personnel, knowledge of the wallet and its threat model, and knowledge of secure software maintenance and vulnerability handling for mobile applications ([NP001] section 3.2).

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

Annex A: Audit checklist

One row per criterion. The columns for the initial audit and the surveillance audit say what the auditor looks for.

ID	Criterion (short)	Initial audit: look for	Surveillance audit: look for
VC1	Release identifiers	Process description of release identification	Release log against functional certificate and FIT ST for each release in the period
VC2	Source and build control	Repository and access control description	Sample trace from delivered package to source revision
VC3	Signing key control	Key management description	Records of key use; any key change and its notification
VC4	Third-party components	Component inventory process	Inventory per release; changes since last audit
CM1	Notification before implementation	Change notification procedure	Notifications against release log
CM2	Complete change description	Change record template	Sampled change records against source differences
CM3	Security impact assessment	Assessment procedure and list of [NP001] 6.6 changes	Sampled assessments; changes of the listed kinds and their delta assessments
CM4	Boundary and environment changes	Procedure to identify them	Any such change in the period and how it was treated
CM5	Platform and variant tracking	Procedure	Platform and API level changes in the period
UD1	Update feature per component	Update mechanism description	Update release log; evidence of updates delivered
UD2	Signed, verified updates	Release and verification description	Sampled release signing records
UD3	Distribution channel	Channel description	Evidence of channel for each release
UD4	Update timeliness	Monitoring approach	Time from fix availability to delivery for sampled security updates
UD5	Platform assumption verification	Description of the mechanism	Evidence it was retained and functional after updates
VM1	Policy per [ISO/IEC 30111] and CRA Annex I	The policy and procedures	Policy review dates; operation as described
VM2	Monitoring of sources	Source list and method	Monitoring records for the period
VM3	Severity and impact assessment	Method	Sampled assessments
VM4	24 and 72 hour notification	Notification procedure and contacts	Timestamps of discovery and notification for sampled vulnerabilities

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

ID	Criterion (short)	Initial audit: look for	Surveillance audit: look for
VM5	VIAR	Template and procedure	VIARs of the period; transmission date
VM6	Remediation commensurate with severity	Remediation targets	Remediation delays recorded for sampled vulnerabilities
VM7	Disclosure in Annex V repositories	Disclosure procedure	Registrations in the period
CV1	Functional certificate validity	Monitoring approach	Current status; any change and its notification
CV2	Certificates of environmental components	Monitoring approach	Status of WSCD and other certificates; any change and its notification
CV3	Assumptions remain valid	Monitoring approach [placeholder]	As the Protection Profile states

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

Annex B: Audit report outline [proposed]

#	Section	Content
1	Identification	Product, version, certificate identifier, CB, product developer, audit type, period covered, dates, auditors.
2	Scope and criteria	Processes and criteria identifiers audited; exclusions with reasons.
3	Evidence and sampling	Documents and records examined, sampling basis, interviews held.
4	Results per criterion	Met, not met (class), or not applicable with reason.
5	Changes in the period	Changes examined and the delta conclusions reached or required.
6	Conclusion	Whether the processes meet the criteria; recommended actions; input to the certification decision or to the surveillance report.

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

Annex C: 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 D: FOR REVIEW and placeholder register

Section	Point	Origin
1.2	Names of the processes; licensing evidence has no home in [NP001]	[NP001] sections 2.2, 3.3, 7
4.4	VM1: CRA Annex I against the scope exclusion of [NP001] section 2.2	[NP001] section 2.2; [IR 2981] Art. 5(7)
4.5	CV3: what must be monitored	[PP-WI-REMOTE], [NP001] section 2.4
5.5	Finding classes and remediation timeframes	[NP001] section 6.5; EZU review
6	Auditor competence criteria	[NP001] section 3.2

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