EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-FS

EUDI Wallet Functional Certification Scheme

RC 1.0

2026-11-06
~~2026.11.05~~

Document reference	NL-FS
Version	RC1.0
Status	Release Candidate
Date	2026-11-06
Document type	Framework document
Parent framework	none
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	European Digital Identity Wallets and the electronic identification scheme under which they are provided
Primary audience	System/Scheme Owner, CABs, EUDI Wallet providers, PID Provider
Secondary audience	EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Subsidiary Documents	NL Certification System Documents

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

History of changes			
Version	Change	Status	Date
RC1.0	First consolidated version	Release Candidate Draft	2026-11-06

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

Table of Contents

1 Scope 6
1.1 Object of certification 6
1.2 Out of scope 6
1.3 Document structure 6

2 Legal basis 8

3 Normative references 9

4 Terms and definitions 10

5 Certification scheme documentation structure 11
5.1 The NL-FS document series 11
5.1.1 Purpose and structure 11
5.1.2 Document map 11
5.2 Relationship to NL-SYS-1 11
5.3 Relationship to the NL-CS, NL-P-P/W and NL-TL 12
5.4 Scheme type 12
5.5 Use of certification and marks of conformity 12

6 Evaluation methodology 13
6.1 General 13
6.2 Evaluation scope 14
6.3 Implementation Conformance Statements 14
6.4 Evidence requirements 16

7 Test case development methodology 17
7.1 Developing test cases 17
7.2 Test cases 18
7.2.1 Test case definition 18
7.2.2 Coverage of test cases 18
7.2.3 Traceability 18

8 Certification process 19
8.1 Initial certification 19
8.2 Surveillance 19
8.3 Recertification 19
8.4 Certificate requirements 20

9 Evaluation methods 21
9.1 Requirements evaluated by testing 21
9.1.1 Test framework 21
9.1.2 Test tooling 21
9.1.3 Test execution 21
9.1.4 Test outcome 22
9.1.5 Test evidence 22
9.2 Reference test case specifications 22
9.3 Requirements evaluated by inspection 23

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

Annex A (normative) Test case specification details 24
A.1 General 24
A.2 Test case grouping and test case identifiers 25
A.3 Profiles 26
A.4 Preconditions 26
A.5 Informative example 26

Annex B (normative) Feature list for inclusion in certificates for functional conformance 28

Annex C (informative) Test Framework Design Principles 30
C.1 General 30
C.2 Functional design principles 30
C.3 Output requirements 30
C.4 Qualified test environment 31

1 Scope

1.1 Object of certification

The present document specifies the certification scheme for functional conformity of EUDI Wallet components within the Dutch EUDI Wallet Certification System. It establishes the evaluation methodology and conformity assessment procedures that accredited certification bodies shall apply when certifying the functional conformity of components for which certification is required under Regulation (EU) No 910/2014 and its implementing acts. These components include a wallet solution and a PID issuance service.

Note: The rationale for the inclusion of a PID issuance service as a component to be certified under the scheme is that CIR 2024/2981, Article 3 (3) (c) states that "the object of certification shall include the processes that support the provision and operation of a wallet solution, including the user onboarding process" and shall cover electronic identification means management. According to the referenced Implementing Regulation (EU) 2015/1502, electronic identification means management includes issuance, delivery and activation of the eID means. This implies that PID issuance is part of the object of certification.

In the context of this certification scheme, the object of certification is the functional behaviour of the wallet solution or the PID issuance service — namely, that it correctly implements the protocols, interfaces, data formats, and other functional requirements laid down in the applicable implementing acts and in the technical specifications referenced therein.

The following entities are subject to functional certification under this scheme:

(a) wallet providers, in respect of their wallet solution;
(b) PID providers, in respect of their PID issuance services.

1.2 Out of scope

This document does not address the cybersecurity certification of the wallet solution or the PID issuance service; that is the subject of the NL-CS series (EUDI Wallet Security Certification Scheme). Neither does it address the certification of the wallet providers in conjunction with the eID scheme under which their wallets are provided; that is covered by the NL-P-W and NL-TL documents.

1.3 Document structure

This document covers the following:

- Chapter 2 specifies the legal basis underlying this functional certification scheme
- Chapter 3 contains a list of normative references
- Chapter 0 defines terms and definitions used in this document
- Chapter 5 describes the certification scheme documentation structure
- Chapter 6 describes the evaluation methodology
- Chapter 7 focuses on the methodology to be used for developing test cases
- Chapter 8 describes the certification process to be followed by the certification body
- Chapter 9 details the evaluation methods to be used during certification
- Annex A (normative) specifies requirements for the test case specification to be developed or referenced by the certification body

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

- Annex B (normative) specifies the feature list for inclusion in certificates for functional conformance
- Annex C (informative) describes design principles for test frameworks to be used or qualified by the certification body.

This document does not specify any test cases. Neither does this document define the certification scope for individual objects of certification. Instead, the certification scope and requirements for functional conformance for wallet solutions are defined in NL-FS-W and for PID issuance services in NL-FS-P.

2 Legal basis

The certification scheme and framework defined in this document are established pursuant to the following legal instruments:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183 of 11 April 2024 ("eIDAS"), in particular Article 5a thereof.
- Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets ("CIR 2024/2977").
- Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards the integrity and core functionalities of European Digital Identity Wallets ("CIR 2024/2979").
- Commission Implementing Regulation (EU) 2024/2981 laying down rules for the application of Regulation (EU) No 910/2014 as regards the certification of European Digital Identity Wallets ("CIR 2024/2981"), in particular Article 3 and Annex III thereof.
- Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 as regards protocols and interfaces to be supported by the European Digital Identity Framework ("CIR 2024/2982").

Article 3 of CIR (EU) 2024/2981 requires Member States to establish national certification schemes for EUDI Wallet solutions, while Annex III of CIR 2024/2981 requires conformity assessment of functional requirements defined in CIR 2024/2977, CIR 2024/2979 and CIR 2024/2982.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document applies.

(a) ISO/IEC 17000, Conformity assessment — Vocabulary and general principles
(b) ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services
(c) ISO/IEC 17067:2026, Conformity assessment — Fundamentals of and guidelines for conformity assessment schemes
(d) NL-SYS-01, *EUDI Wallet Certification System — Certification System Requirements*
(e) NL-SYS-02, *EUDI Wallet Certification System — Vocabulary*
(f) NL-FS-W, *EUDI Wallet Functional Certification Scheme - Wallet Solution Conformance*
(g) NL-FS-P, *EUDI Wallet Functional Certification Scheme – PID Issuance Service Conformance*

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17065, ISO/IEC 17067 and NL-SYS-02 apply.

In particular, the following terms defined in NL-SYS-02 are used throughout this document: *wallet solution, wallet unit, wallet instance, wallet provider, PID provider, person identification data, functional conformity, object of certification, test framework and certification body.*

For the purposes of this document, the definitions given in Article 2 of CIR 2024/2979 and CIR 2024/2981 also apply.

5 Certification scheme documentation structure

5.1 The NL-FS document series

5.1.1 Purpose and structure

The NL-FS document series specifies the functional certification of EUDI Wallet components. The series is structured around an object-based grouping: A separate document defines the certification scope and ICS for each object of certification under NL-FS: wallet solutions are addressed in NL-FS-W; PID issuance services in NL-FS-P.

5.1.2 Document map

Table 1 lists the documents of the NL-FS.x series and identifies, for each document, the stakeholders that rely on the document for their certification.

Document	Title	Function	Relied on by
NL-FS	Scheme, Framework, methodology and evaluation rules	This document. The functional conformity scheme and framework that governs the application of all other NL-FS.x documents.	Wallet providers and PID providers, certification bodies
NL-FS-W	Wallet solution conformance	Defines the certification scope for the wallet solution; specifies the ICS template to be completed by wallet providers.	Wallet providers; certification bodies
NL-FS-P	PID issuance system conformance	Defines the certification scope for the PID provider; specifies the ICS template to be completed by PID providers.	PID providers; certification bodies

5.2 Relationship to NL-SYS-1

NL-SYS-01 specifies the common requirements on the certification body, including qualification, competence and process requirements. It builds upon ISO/IEC 17065 and adds scheme-specific requirements. It defines the common certification process, including application, evaluation, certification decision, surveillance, and re-certification. NL-SYS-01 is applicable for both functional and cybersecurity testing of products (i.e., wallet units and PID issuance services), as well as for eID scheme conformity.

The present document (NL-FS) specifies the certification scheme that the certification body shall apply for the functional conformity of products specifically, as opposed to product security conformity or eID scheme conformity. Together, NL-SYS-01 and the NL-FS series define the complete framework for conformity assessment of a wallet solution and a PID issuance service to the relevant functional requirements in the legal texts. The present document specifies the functional scheme-specific aspects of the evaluation framework and certification process.

5.3 Relationship to the NL-CS, NL-P-P/W and NL-TL

Within the certification hierarchy of the EUDI Wallet Certification System, a certification under the NL-FS is a product certification. It certifies the functional conformity of the wallet solution or of the PID issuance service. The NL-CS series is the parallel product certification addressing the cybersecurity of the wallet solution. The NL-FS and NL-CS series are assessed and certified independently of each other; neither replaces the other.

Product certifications provide assurance input to the higher levels of the certification hierarchy:

(a) a NL-FS certificate held by a wallet provider, covering the wallet solution it provides, is relied upon in the certification of that wallet provider under NL-P-W;
(b) a NL-FS certificate held by a PID provider, covering the data formats and interfaces relevant to its PID issuance service, is relied upon in the certification of that PID provider under the NL-P-P.
(c) Finally, the NL-P-W certificate held by a wallet provider and the NL-P-P certificate held by a PID Provider are relied upon under the top-level NL-TL certification.

The verification that a provider holds a valid NL-FS (and NL-CS) certificates for their producs, and the assessment of their scope and currency, is performed within the certification process described in NL-P-W (for wallet providers) and NL-P-P (for PID Providers). The certification bodies operating at the NL-P-W or NL-P-P level verify the validity and scope of the NL-FS and NL-CS certificates and does not re-evaluate the requirements already covered by them.

In turn, the verification that the providers hold valid NL-P-W or NL-P-P certificates is performed within the certification process described in NL-TL. The certification body operating at the NL-TL level verifies the validity and scope of the NL-P-W and NL-P-P certificates and does not re-evaluate the requirements already covered by them.The certification hierarchy and the obligations of each role within it are defined in NL-SYS-01 and in the NL-TL series.

Where a NL-FS certificate is suspended, withdrawn, or expires, the consequences for the certifications that rely upon it follow from the certification hierarchy defined in NL-SYS-01 and NL-TL.

5.4 Scheme type

This certification scheme follows the Type 6 model as defined in ISO/IEC 17067, which includes initial testing and evaluation, surveillance, and periodic re-evaluation. The common Type 6 scheme elements are specified in NL-SYS-01, in accordance with Article 4(3), point (a) of CIR (EU) 2024/2981.

5.5 Use of certification and marks of conformity

A certification issued under this scheme is internal assurance information within the certification hierarchy of the Dutch EUDI Wallet Certification System. A NL-FS certificate does not, of itself, confer the right to use the EU Digital Identity Wallet Trust Mark.

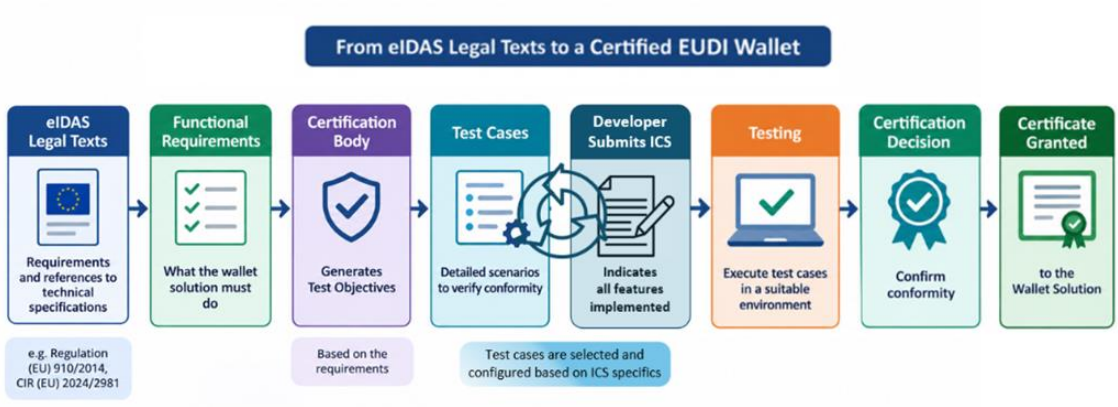
6 Evaluation methodology

6.1 General

This section provides an overview of the evaluation methodology that the certification body applies when evaluating the functional conformity of the object of certification with the requirements of the NL-FS series.

The certification body is responsible for the conformity assessment in accordance with the requirements of ISO/IEC 17065 and NL-SYS-01. The certification body shall be accredited in accordance with the latest version of ISO/IEC 17065 for the scope of this certification scheme by a national accreditation body appointed pursuant to Regulation (EC) No 765/2008.

The evaluation activities under this scheme are part of the common certification process defined in NL-SYS-01 and shall follow the common process requirements set out there. This section specifies only the aspects specific to the functional conformity scheme. These aspects are illustrated in the following figure.



Prior to any certification of a specific object of certification, the following activities take place (see the four left-most boxes in the figure):

(a) The functional requirements to be certified can be found in the eIDAS Regulation, the associated implementing acts, and the technical specifications referenced therein. For wallet solutions, these requirements are further identified in NL-FS-W. For PID issuance services, the functional requirements are identified in NL-FS-P.

(b) The certification body derives test objectives and test cases from the functional requirements, using the methodology specified in chapter 7 below. The certification body specifies all test cases necessary to test an object of certification against the applicable requirements in the Regulation and its implementing acts, as well as the technical specification referenced therein. The certification body creates this test case specification either directly or by reference to an existing suitable test standard, such as European Commission's Functional Conformance Assessment Framework (FCAF). As part of test case development, the certification body also develops or references the necessary Implementation Conformance Statement template(s), see section 6.3. Every test case contains a Profiles field that indicates which ICS statement(s) should have been answered with 'Yes' for that test case to be applicable. Please refer to Annex A and to the informative example in Annex A.5.

(c) Preferably, the certification body, directly or through an appropriately qualified outsourced partner, implements these test cases in an automated conformance test tool.

Subsequently, for each certification of a specific object of certification, the following activities take place (see the four right-most boxes in the figure):

(d) The developer of the object of certification declares the features implemented by the object of certification by filling out the Implementation Conformance Statement (ICS) template specified in NL-FS-W or NL-FS-P (as applicable), and by filling out additional ICS templates defined at the level of individual technical specifications that are supported by the object of certification. See section 6.3 for more information about ICSs and how they are used. The certification body shall guide the developer in completing the ICSs, to ensure they are filled out completely and correctly.
(e) The certification body, directly or through an outsourced partner, executes the applicable tests cases against the object of certification. The certification body uses the ICSs completed by the developer to evaluate which test cases are applicable. Where the certification body uses an outsourced partner, the partner shall be an ISO/IEC 17025-accredited testing laboratory. Where the certification body has developed or qualified an appropriate conformance test tool, the certification body may be able to rely on test execution evidence generated by the developer instead of a test laboratory; however, in this case the certification body shall obtain assurance that all applicable test cases are executed against the object of certification in a reliable and repeatable manner, by qualified and independent personnel.
(f) The certification body evaluates the evidence resulting for test case execution, to determine whether a certificate of conformance can be issued.

6.2 Evaluation scope

For a wallet solution, the certification body shall evaluate the functional behaviour at its external interfaces towards users, PID providers, attestation providers, relying parties, and infrastructure components such as Trusted Lists and revocation services, as required by the applicable implementing acts.

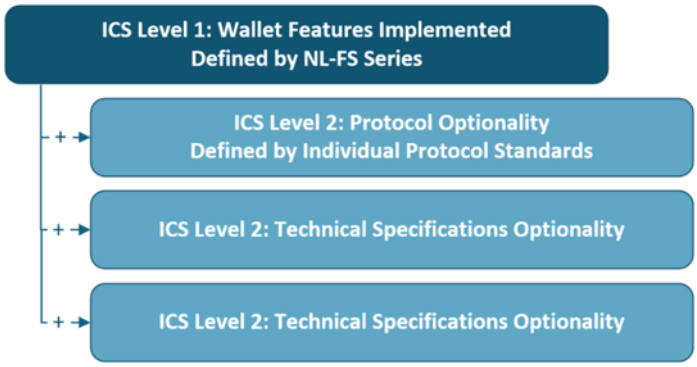
For a PID issuance service, its functional behaviour shall be evaluated at its external interface towards a wallet solution. The conformity of the person identification data it issues — the attributes, their data model and their encodings — is evaluated against the formats required by the applicable implementing acts, in particular CIR (EU) 2024/2977.

The certification body evaluates, for each applicable test objective and test case, whether the outcome is a pass.

The certification decision shall be either Pass or Fail. The certification body shall take the certification decision in accordance with the common process of NL-SYS-01.

6.3 Implementation Conformance Statements

Implementation Conformance Statements are declarations, by the developer of an object of certification, regarding the features that are supported or not supported by the object of certification. They consist of a series of statements that must be answered with Yes or No.



As shown in the figure above, this document distinguishes between two levels of Implementation Conformance Statement:

- First, NL-FS-W and NL-FS-P include conformance requirements and a corresponding ICS for wallet solutions and PID issuance services (respectively). This enables modularity of the certification regarding the features mandated in the legal instruments. By completing this ICS, a developer indicates to the certification body which of the legally mandated features are implemented in their wallet solution or PID issuance service.
- Secondly, every test case specification for one of the technical specifications required in the legal instruments will come with its own ICS[1]. Examples of these are the already existing ICS in ISO/IEC 18013-6 and the ICS that is part of the FCAF. In contrast to the ICSs in NL-FS-W and NL-FS-P, these ICSs cover only the optional features in their base standards. Objects of certification are not allowed to pick and choose from mandatory features of these standards, as this will directly impact interoperability. These technical specification-level ICSs are not included in the NL-FS-W and NL-FS-P documents, as they are an integral part of the test case specifications that must be developed or referenced by the certification body.

Developers shall complete and submit the ICS defined by NL-FS-W for any wallet solution to be certified and the ICS defined by NL-FS-P for any PID issuance service to be certified. In addition, the developer shall complete and submit the ICS applicable to each technical specification supported by the object of certification.

For example,

- If a wallet solution supports proximity presentations, the wallet provider indicates this when completing the ICS in NL-FS-W. Additionally, since proximity presentations use the attestation format and protocol specified in ISO/IEC 18013-5, the wallet provider completes the ICS included in ISO/IEC 18013-6 (which contains a test case specification for ISO/IEC 18013-5). Note that this assumes that the certification body has referenced ISO/IEC 18013-6 as the test case specification for testing wallet solutions against ISO/IEC 18103-5.
- If the wallet solution supports remote presentations of SD-JWT VC-formatted attestations using the protocol specified in OpenID4VP, the wallet provider again indicates this when completing the ICS in NL-FS-W. Additionally, the wallet provider completes the corresponding ICS(s) in the FCAF (again assuming that the certification body referenced the FCAF as the test case specification for testing wallet solutions against SD-JWT VC and OpenID4VP).

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

A submitted ICS shall as a minimum:

(a) identify the object of certification unambiguously, including its name, version and build identifier;
(b) declare, for each statement in the ICS, whether that statement is true or false for the object of certification.

6.4 Evidence requirements

In case the certification body did not execute the tests itself, the testing laboratory (or the developer, see section 6.1 (d)) shall provide the certification body with the evidence required by the common process of NL-SYS-01, together with the evidence specific to this scheme. The scheme-specific evidence comprises, in outline:

(a) a description of the object of certification sufficient to identify it unambiguously, including its build identifier, version and Software Bill of Materials reference, and a description of its configuration at the time of testing;
(b) the ICS in NL-FS-W or NL-FS-P (as applicable), as filled out by the developer for the object of certification;
(c) the ICS for each applicable technical specification, as filled out by the developer for the object of certification;
(d) (a reference to) the test case specification(s), including version numbers, used for testing;
(e) the qualified conformance test tool used for test execution, including its version, if applicable;
(f) any other details about the test environment necessary to be able to replicate test results, for example the brand, make, and OS version of any test device used for the installation a wallet unit that is the object of certification;
(g) an indication, preferably determined automatically by a test tool, of all test cases that are applicable for the object of certification, based on the ICS;
(h) for all test cases that are applicable, the reports of their execution, including a verdict per test case. In addition, the report shall include all details of the communication between the conformance test tool and the object of certification, and shall clearly indicate the exact reason for any verdict that is not Passed;
(i) supporting documentation enabling the certification body to verify the authenticity and completeness of the test evidence.

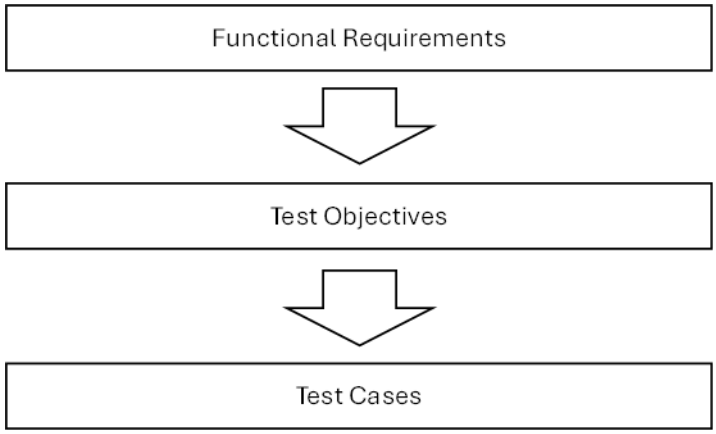
7 Test case development methodology

7.1 Developing test cases

The certification body uses the functional requirements to derive or references test objectives and test cases. The certification body shall be competent to develop or reference test objectives and test cases, ensuring their correctness and adequacy.

The scheme does not prescribe a particular set of test objectives and tests cases but recognises that the European Commission's Functional Conformance Assessment Framework (FCAF) may provide a suitable reference set of test objectives and test cases in the future.

Certification bodies shall ensure test case specifications are developed as follows:



NL-FS-W identifies the functional requirements for wallet solutions by referencing the applicable legal texts and referenced technical specifications, NL-FS-P does the same for PID issuance services. Functional requirements originate strictly from the regulatory sources (the eIDAS Regulation and its implementing acts) only.

Test objectives are detailed, natural-language statements of what is to be tested. These are derived by analysing the functional requirements line-by-line to identify text that is testable. Test objectives shall be granular and specific, expressing a single purpose, ensuring that there is no ambiguity on the item to be tested.

Example test objectives include:

- "Verify that the Wallet does not present an attestation to a Relying Party if the request includes a Wallet Relying Party Registration Certificate with an invalid signature, when using OpenID4VP presentation."
- "Verify that the Wallet presents an attestation containing a single attribute, if it receives a DCQL-query requesting two attributes, of which one is not present in the held attestation, for an attestation in mdoc format."

Test cases shall be written to address each functional requirement, including both positive and negative test cases. Test cases should be atomic, meaning the execution of one test case will have no bearing on the execution of any other test cases. This will allow functional conformance test reports to clearly identify where non-conformities exist in the implementation.

7.2 Test cases

7.2.1 Test case definition

Test cases shall treat the object of certification as a "black box", testing only the externally observable behaviour.

The test case format and test case contents shall comply with the requirements in Annex A.

7.2.2 Coverage of test cases

The certification body shall create or reference test cases that test positive and negative scenarios for each functional requirement in the legal instruments and the standards referenced therein.

The certification body shall create or reference test cases to exercise different usage scenarios that may be applicable to a functional requirement. For example, for a remote attestation presentation, test cases should provide coverage of different EAA types and formats applicable to the object of certification.

7.2.3 Traceability

The certification body shall a create a traceability matrix showing full coverage of the functional requirements in scope for the certification. The traceability matrix shall list each requirement identifier or section number containing functional requirements in the base specification and shall indicate which test case(s) cover that requirement or section. Coverage shall be as specific as possible. The traceability matrix shall be consistent with the information in the References section in each test case, see Annex A.

8 Certification process

8.1 Initial certification

The initial certification shall follow the common process set out in NL-SYS-01 and shall include a full evaluation of the object of certification against all test objectives applicable to it, as determined by the profile and ICS under the methodology of Section 6.

8.2 Surveillance

Surveillance activities shall be performed in accordance with the certification cycle set out in NL-SYS-01. Surveillance under this scheme shall take into account the rate of change of the inputs on which a functional certification depends: the NL-FS.x subordinate documents, the technical specifications referenced from the applicable implementing acts, and the implementing acts themselves.

A surveillance evaluation shall be triggered, as a minimum, where any of the following occurs:

(a) a change to the object of certification that affects its functional behaviour or the features declared in its ICS.
(b) a change to the applicable implementing acts, or to a technical specification referenced from them, that materially affects the functional requirements certified;
(c) a change to a test case specification that alters, adds or removes applicable test cases;

Where a change to the applicable implementing acts introduces new or amended functional requirements, or a change to test case specifications introduces new or amended test cases applicable to the object of certification, a transition arrangement shall apply. The details of this arrangement, including the period within which certified products must be brought into conformity, and the treatment of certificates issued against the superseded requirements or based on the superseded test cases, shall be defined by the certification system. Such transition arrangements are a matter of the management of the certification system and are not specified in this document.

8.3 Recertification

Recertification shall include a re-evaluation of the object of certification against the test objectives applicable at the time of recertification and shall follow the common recertification process defined in NL-SYS-01.

Recertification is performed against the versions of the NL-FS.x documents and test case specifications current at the time of recertification. Where the object of certification comprises components that can be tested individually, and a component is unchanged since the previous certification together with the test objectives applicable to it, the re-evaluation of that component may rely on the evidence from the previous certification, provided that evidence remains valid and the certification body is able to verify its continued applicability. Test objectives that are new or amended since the previous certification, and components that have changed, shall be evaluated in full.

8.4 Certificate requirements

The requirements of ISO/IEC 17065, clause 7.7 apply. In addition, the following requirements and guidance apply.

The certificate shall contain the following:

(a) a unique identifier for the certificate;
(b) name and version of the object of certification;
(c) from Annex B, the Certificate Feature Table (Table 2) filled out with the relevant Feature Descriptions (Table 1) as derived by the certification body from the ICSs submitted by the developer;
(d) a reference to the completed ICS form from NL-FS-W or NL-FS-P, as applicable, plus references to the completed ICS forms for each of the applicable technical specification;
(e) name of the wallet eID scheme, its owner and the Member State, where applicable;
(f) name, address and contact information of the client;
(g) link to the website of the client containing the information that is required to be made publicly available according to the requirements of ISO/IEC 17065, 4.6;
(h) name, address and contact information of the certification body;
(i) where different from the certification body, name of the conformity assessment body that performed the evaluation, together with information on its accreditation;
(j) references to Regulation (EU) No 910/2014 and to CIR (EU) 2024/2981;
(k) a reference to the public evaluation report, if applicable;
(l) a reference to the evaluation report;
(m) a reference to the test case specification(s), standards and other normative documents used for the evaluation, including their versions;
(n) a description of the test environment or test framework, including any information necessary to enable the reproduction of test results underlying the certification decision, with as a minimum:
    a. name and version of any (qualified) test tool used for testing,
    b. brand, make, and OS version of any test device used for installing wallet units under test.
(o) name of the wallet provider or PID provider, as applicable;
(p) the issuance date of the certificate;
(q) the expiry date of the certificate, which shall not be later than 5 years after the issuance date.

The certification body shall ensure that the ICS forms referenced in the certificate are publicly available for the entire validity period of the certificate.

The certification body shall issue new certification documentation where an evaluation, including surveillance or special evaluations, identifies significant changes to the object of certification. The new certification documentation shall retain the expiry date of the original certification documentation.

9 Evaluation methods

9.1 Requirements evaluated by testing

9.1.1 Test framework

Testing shall be conducted in a controlled environment (called the test framework) that ensures testing is impartial and reproducible.

Testing of wallet solutions shall be performed using clearly defined test devices, operating systems, and configurations, in line with the information provided by the developer in the completed ICS.

Where a wallet solution includes wallet units for multiple OS versions (e.g. iOS and Android), the certification body shall treat these wallet units as separate objects of certification.

Note: This is because these wallet units are, in fact, different mobile applications, having different code bases.

Supporting systems, such as Trusted Lists, shall be sourced by the certification body. Prior to testing these lists will need to be populated with the necessary certificates or attestations to support the testing, aligned with the ICS.

9.1.2 Test tooling

For test execution, the certification body should require the use of tooling that can interact with the object of certification over the defined external interfaces. Such tools shall be able to provide the object of certification with both valid and invalid inputs and to receive the object's response.

Where used, such test tools shall execute the test case specification(s) created or referenced by the certification body. Test tools shall log all necessary information required to assess the outcome of the test including a full trace of messages sent to and from the object of certification.

Additionally, tools should play a role in analysing the logs from the abovementioned test tools, providing a verdict for each test step in each test case executed. The functions of providing inputs and receiving responses on the one hand and analysing the correctness of these responses on the other hand, can also be combined in a single test tool.

Where test tools are used, the certification body is responsible to qualify these tools as being fit for purpose.

9.1.3 Test execution

Test execution should be performed by the certification body (directly or through an appropriately qualified outsourced partner) but may also be done by the developer of the object of certification.

Where the certification body performs the tests, it shall be responsible for collecting and reviewing test evidence.

Where the developer performs the tests, it shall use a testing tool that has been qualified by the certification body as being fit for purpose. The developer shall submit the logs and verdicts for each test cases, produced by the test tool, to the certification body for review.

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

9.1.4 Test outcome

The testing outcome of each test case that is executed shall be expressed as one of the following:

- **Pass** — every applicable functional requirement is complied with by the object of certification. This has been established by the executing the applicable test case(s), each test case producing a pass result.
- **Fail** — the object of certification does not comply with one or more applicable functional requirements.

The testing outcome of any test case that is not executed shall be expressed as one of the following:

- **Not applicable** – in case the object of certification, per the completed ICS, does not fulfil the conditions expressed in the profiles for the test case (see Appendix A.3).
- **Inconclusive** – in case one or more of the preconditions for the test case (see Appendix A.4) could not be fulfilled during test execution. The certification body shall investigate the reason for any Inconclusive test cases.

9.1.5 Test evidence

Regardless of who executes the tests, the certification body shall record comprehensive test results including:

- Version of object of certification, operating systems and devices
- A record of each test executed including
    - Timestamp
    - Test result – e.g., pass, fail, not applicable, inconclusive
    - Details on the specific step where a test case failed, with the detailed reason for failure
    - Details on the specific reasons for which a test case is deemed not applicable
    - Details on the specific reasons for which a test case is inconclusive
    - Trace of inbound and outbound messages (i.e. inputs into the object of certification and its responses) from the test execution of each test case

The certification body shall use these test results to determine the certification result.

9.2 Reference test case specifications

The certification body may decide to reference the European Commission's Functional Conformance Assessment Framework (FCAF), but this is not mandatory. If the certification body references the FCAF or any other external test case specification, it shall:

- Review the test case specification to determine the correctness and adequacy of the coverage of the test cases it contains.
- Review the suitability of the test objectives and test cases for object of certification.
- In case any gaps in coverage or bugs were found, report these to the organisation responsible for maintaining the test case specification to ensure these are corrected. Where corrections are not made (I time), develop additional test cases to such issues.
- Record the version of the test case specification being referenced, to ensure that the certification body can assess the impact on functional conformance testing of any changes that may occur in subsequent versions.

9.3 Requirements evaluated by inspection

Certain functional requirements within the scope of certification will be evaluated via inspection by a human tester, rather than by an automated test tool. These requirements mainly involve the behaviour of the object of certification on its user interface. Examples of this include requirements on the information shown by the wallet to its user in various circumstances, especially when asking for user approval during presentation of an attestation.

Although such requirements are evaluated by inspection, the certification body shall ensure that in all other aspects, they are treated in the same way as requirements evaluated by testing. In particular, such functional requirements shall be covered by appropriate test cases complying with the requirements in this document.

Note that test cases carried out by means of inspection will require the use of test tools (commonly called simulators) interacting with the object of certification. This is to ensure that the object of certification is brought into the state required to allow the human tester to carry out the relevant inspection. For example, if the test objective is to validate that a wallet correctly informs the user in case the registration certificate of a relying party does not cover the requested attributes, a test tool is needed to send a corresponding presentation request to the wallet.

Annex A (normative) Test case specification details

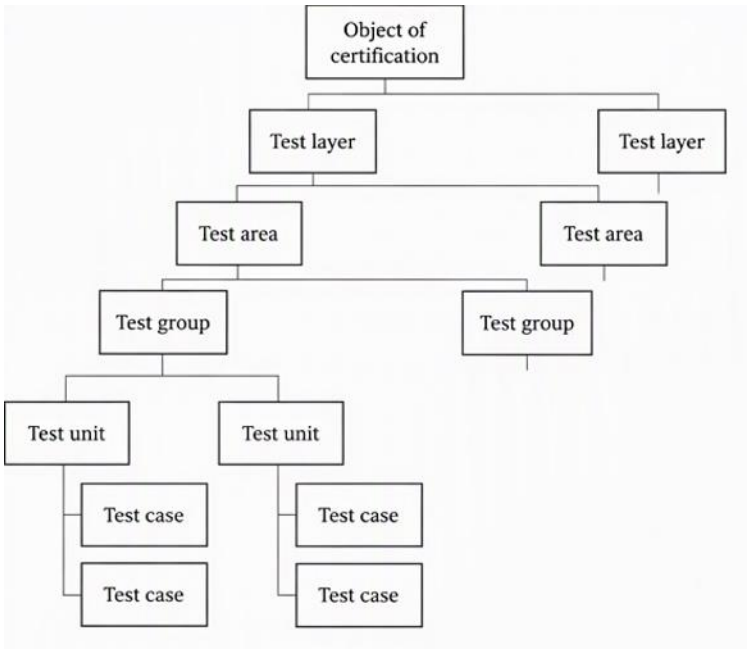
A.1 General

Each test case shall contain at least the following, or equivalent, information. All fields shown below shall be present in each test case:

Test case identifier	Uniquely identifies the test case. See A.2.
Objective	Specifies the test objective of this test case in natural language. The test objective shall clearly reflect the functional requirement(s) tested.
References	References the functional requirement(s) addressed by this test case, by means of a requirement identifier or section number in the base specification. References shall be as specific as possible. References shall be complete; for instance, if the main referenced section of the base specification references other sections or other specifications, and information from these sections or specifications was used to construct the test case, all of these sections and specifications shall be referenced.
Profiles	Defines the profile(s) for which the test case is applicable. See A.3.
Preconditions	Defines the state in which the object of certification needs to be before the test case can be executed, See A.4.
Test scenario	Defines the test steps that shall be taken during test execution. Each step shall cover a simple, exactly defined operation that must be performed by the tester or by a test tool. The steps shall be performed in the order listed. Each test step is defined by the following information:
	— Test step ID: a consecutive number, uniquely identifying each test step and the execution order in the test case. — Description: defining the operation that must be executed for this step. — Configuration data: optionally specifying input data required to perform this test step.
Expected results	Separate pass criteria for each test step in the test scenario. Note that this implies that the number of expected results shall exactly match the number of test steps in the Test scenario. Pass criteria shall be clear and precise, so that a tester or test tool can objectively decide whether a pass criterium is met or not. The analysis of the observed result in comparison with the expected result shall leade to a verdict of the test step, e.g. "Pass" or "Fail". The results of the individual test steps and the overall result of the test case shall be included in the test report.

A.2 Test case grouping and test case identifiers

The party creating the test case specification shall create a logical grouping of test cases, based on functional area each test case is covering. To create such a logical grouping, this party shall define a multi-level group structure. This structure may consist of, for example, test layers, test areas, and test groups, where each test layer contains zero or more test areas, and each test area contains zero or more test groups, as illustrated the figure below.



The party creating the test case specification shall clearly describe the test grouping, meaning which test layers, test areas, and test groups are used. Note that this document does not prescribe a specific number of levels to be used; for example, the party creating the test case specification may decide to not use test groups or to distinguish another layer (called test units, for instance) within a test group.

Once the logical grouping of test cases is established, test case identifiers shall be formed in the following manner:

OoC_TestLayer_TestArea_TestGroup_TestUnit_##, where:

- OoC represents the object of certification for which the test case is applicable, e.g. Wallet Solution, PID, PID Issuance Service, etc. The exact names used for the object of certification will depend on the base specification being tested. In addition, it is possible to have test cases whose object of certification is a specific artifact, such as an access certificate. The party creating the test case specification shall clearly describe the values that can be used for OoC in the test case IDs.
- TestLayer, TestArea, TestGroup and TestUnit are the names of the test layer, test area, test group, and test unit to which the test case belongs. Generally, to prevent names from becoming too long, abbreviations should be used in the test case identifiers.
- ## is a two-digit decimal number.

Note that not all components need to be present in each test case identifier. For example, if the specific test layer to which the test case belongs is not further divided into test areas, the test case identifier will be formed as OoC_TestLayer_##

A.3 Profiles

Profiles are defined for identifying optional functionality. If a profile is present in a test case, it means that the test case must be executed only if the object of certification complies with the conditions expressed in the profiles. This enables the tester or the automated test tool to select which tests must be executed for that object of certification This selection is based upon comparing the profile of the test case to the information in the Implementation Conformance Statement filled out by the developer or tester, see also NL-FS-W and NL-FS-P.

The certification body shall ensure there is a direct correspondence between each profile included in each test case and an individual statements in one of the ICSs (see section 6.3). This ensures that during test execution, the applicability of each test case for a particular object of certification can be assessed based on the information provided in the ICS.

For example, the ICS in NL-FS-W for a wallet solution contains a statement "wallet solution supports proximity attestation presentations". All test cases that are only applicable for wallet solutions that support proximity transactions shall therefore contain a profile stating "applicable if wallet solution supports proximity attestations presentations".

If no profile is listed in a test case, the test case shall be executed on all objects of certification. If one or more profiles are specified and the object of certification, according to its ICS, does not match with all of the specified profiles, the test shall be skipped and shall be marked as Not Applicable in the test report.

Note that if no profile is applicable for a test case, the Profile field shall not be omitted; it shall be present and empty.

A.4 Preconditions

- Preconditions define the state in which the object of certification needs to be before the test case can be executed. Preconditions can apply, among others, to:
- any action that must have taken place;
- conditions that must be fulfilled, for example the correct encoding of a request;
- the presence of a certain CA certificate as a trust anchor in the object of certification;
- the availability, in the test tool, of certain end-entity certificates and associated private keys.

If the preconditions listed in the test case cannot be fulfilled during test execution, test execution shall be skipped, and the test case shall be marked as Inconclusive in the test report.

Note that if no precondition is applicable for a test case, the Precondition field shall not be omitted; it shall be present and empty.

A.5 Informative example

As an example of a test case complying with the requirements in this Annex, below the test case mDL_MS_DE_DRWifi_02 from ISO/IEC 18013-6 Appendix 2, section 2.1.4.2 is reproduced.

Notes to the example:

- The **test case ID** is formed in the manner described above, using the test case grouping specified in Annex A.1 of the ISO/IEC 18013-6 main document

- As shown in the **Profile** field, this test case is applicable for any wallet that supports proximity transactions and that additionally
    - supports device engagement using QR code
    - does not support device retrieval using Wi-Fi Aware

  When applying for certification, the wallet provider completes the ICS included in the ISO/IEC 18013-6 main document, Annex B.1. Specifically, by answering ICS statements 47 and 56 in that document with Yes or No, the wallet provider provides the information necessary for the certification body to determine the applicability of this particular test case.
- The **Technology** field is an ISO-specific field that does not have to be present in test cases complying with this Annex A.

2.1.4.2 Test case mDL_MS_DE_DRWiFi_02

Test case ID	mDL_MS_DE_DRWiFi_02
System under test	mdoc
Purpose	This test case verifies that, if device engagement took place via QR code and the mdoc does not support Wi-Fi Aware as a device retrieval method, there is no DeviceRetrievalMethod array having type = 3 (Wi-Fi Aware) in the DeviceRetrievalMethods array.
Reference	ISO/IEC 18013-5:2021, 8.2.1.1
Technology	[DE-QR], [DT-WiFi-Aware]
Profile	mdoc supports device engagement using QR code. mdoc does not support device retrieval using Wi-Fi Aware.
Preconditions	A) The DeviceEngagement structure communicated by the mdoc was retrieved using QR code. B) The DeviceEngagement structure passed all Common_CBOR test cases.
Test scenario	1. Verify the presence of a DeviceRetrievalMethod data item having type = 3 (Wi-Fi Aware) in the DeviceRetrievalMethods array.
Expected results	1. The array is not present.

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

Annex B (normative) Feature list for inclusion in certificates for functional conformance

The certification body shall use Table 1 to populate Table 2 below. The certification body shall include Table 2 in the certificates for functional conformance it issues, as required in section 8.4.

Code	Service
PROX	Proximity Presentation
RPSD	Remote Presentation - Same Device
RPCD	Remote Presentation - Cross Device
ISSU	Issuance
QES	Qualified Signature
PSEU	Pseudonym
DASH	Dashboard / Transaction Log
PORT	Portability
EDP	Embedded Disclosure Policies
SUA	Strong User Authentication

Code	Object Type
PID	PID
QEAA	QEAA: <list of attestation types>
PUBEAA	PUBEAA: <list of attestation types>
EAA	EAA: <list of attestation types>
DPA	Data Protection Authority Request
ERASE	Data Erasure Request

Code	Transport
OPVP	OpenID4VP
ISO5	ISO/IEC 18013-5
ISO7	ISO/IEC 18013-7
OPVI	OpenID4VCI
NLISS	Dutch-Specific Issuance Spec
ACV	Access Cert Verification
RCV	Registration Cert Verification

Code	Format
MDOC	ISO/IEC 18013 mdoc
SDJ	SD-JWT VC
REDIR	Redirects

Code	Wallet Engagement
QR	QR Code
NFC	NFC
DCAPI	DCAPI

Code	Device Retrieval
NFC	NFC
BLE	BLE
WIFI	WiFi Aware

Table 1 Feature Descriptions

Service	
Object Type	
Transport	
Format	

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

Wallet Engagement	
Device Retrieval	

Table 2 Certificate Feature Table

Annex C (informative) Test Framework Design Principles

C.1 General

This annex provides guidance on the design principles that a test framework satisfies in order that its outputs may be used as evidence in a certification under this scheme.

C.2 Functional design principles

A test framework used for the generation of evidence in a certification under this scheme satisfies the following principles:

Determinism — given the same implementation under test, the same ICSs, the same test framework version and the same test data (if applicable), the test framework shall produce the same result on each execution.

Well-defined dependencies — every dependency of the test framework is declared by the test framework and reproducible by the certification body. Where a test objective concerns interaction with an external service, that service is represented in the test framework by a declared, reproducible counterpart. The test framework does not depend, as a condition of execution, on any external service that is not declared and reproducible.

Reproducible test data sets — where needed, the test framework includes, or refers to, specific versions of test data sets, which are reproducible across executions. Where test data are generated rather than fixed, the generation procedure and seed shall be documented and reproducible.

Taken together, these principles provide assurance that the outcome of a test execution depends only on the implementation under test, the declared inputs, and the identified versions, so that the certification body can independently reproduce and verify the developer's results.

C.3 Output requirements

A test framework used for the generation of evidence in a certification under this scheme produces structured output that includes, for each test case executed:

(a) the unambiguous identifier of the test case;
(b) the version anchors of the test case specification, of the test framework, of the implementation under test;
(c) the result of the execution of each test step as well as of the test case as a whole (pass, fail, not applicable, inconclusive) and, where relevant, the reason for the result;
(d) sufficient information to reproduce the execution.

C.4 Qualified test environment

The certification body may verify the authenticity and completeness of test results by relying on a qualified test environment. For the purposes of the NL-FS series, a test environment is qualified where:

(a) the executions of the test framework are correct and represent the behaviour of the object of certification at its observable interfaces;
(b) the executions of the test framework are deterministic, reproducible, and traceable;
(c) the executions of the test framework comply with the relevant test case specifications;
(d) the integrity and authenticity of its output can be established by the certification body, such that the certification body can rely on the reported results as corresponding to test executions actually performed against the object of certification.

Where these conditions are met, the certification body may rely on the output of the test framework as a means of verifying test results, to the extent it judges proportionate, without itself reproducing each execution. The certification body's reliance on a qualified test environment does not diminish its responsibility for the certification decision.