EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-SYS-01

NL EUDI Wallet Certification System

RC1.1

2026.10.31

Intern gebruik

Document reference	NL-SYS-01
Version	RC1.1
Status	Release Candidate
Date	31/10/206
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	State	Date
RC1.0	First Consolidated Version following European Collaboration and Refinement Discussion with BZK-Policy Department and Legal.	Release Candidate Draft	2026-10-20
RC1.1	Release Candidate for publication following review round NL Certification System Mngt Board	Release Candidate	2026-10-31

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

Table of Content

1 Introduction 5

2 Legal and normative documents 8

3 Governance and stakeholder relationships 9
3.1 Stakeholders 9

4 Mandatory elements of the scheme definition based on ISO/IEC 17067 13
4.1 Scheme ownership 13
4.2 Scope and objectives 14
4.3 Elements of the scheme according to ISO/IEC 17067 16

5 Scheme life cycle management 19
5.1 Conditions for participation of CABs in the certification scheme 19
5.2 General rules on certification processes 19
5.3 Assurance evidence from external sources 19
5.4 Surveillance 20
5.5 Post-certification obligations of certificate holders 20
5.6 Changes to the object of top-level certification 21
5.7 Dealing with non-conformities 22
5.8 Suspension, termination, withdrawal or expiration of certificates 22
5.9 Complaints and appeals 23
5.10 Retention of records 23
5.11 Periodic review of the certification scheme 24
5.12 Scheme maintenance 24

6 Conformity assessments methods, specifications, and reporting overview 25
6.1 General 25
6.2 Required elements to be defined within conformity assessment methods 25
6.3 Mandatory elements of reports 25
6.4 Conformity assessment template dedicated to certification schemes 26

7 Conformity analysis 28
7.1 Conformity with eIDAS regulation and relevant implementing acts 28
7.2 Conformity with (EU) Cybersecurity Act (Article 54(1) - Elements of European cybersecurity certification schemes 34

Annex A Conformity assessment methods and techniques 37
A.1. Terms relating to conformity assessment 37
A.2. Methods relating to evaluation 37
A.3. Various types of attestations 38

Annex B Description of supported Wallet Solution architectures in the Dutch national wallet certification system 39

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

1 Introduction

1 This document serves as a high-level framework that explains the EUDI Wallet certification system, ensuring its conformity with related regulations.

2 The certification system is based on the concept and content of the certification system described in ISO/IEC 17067 (see Figure 1).

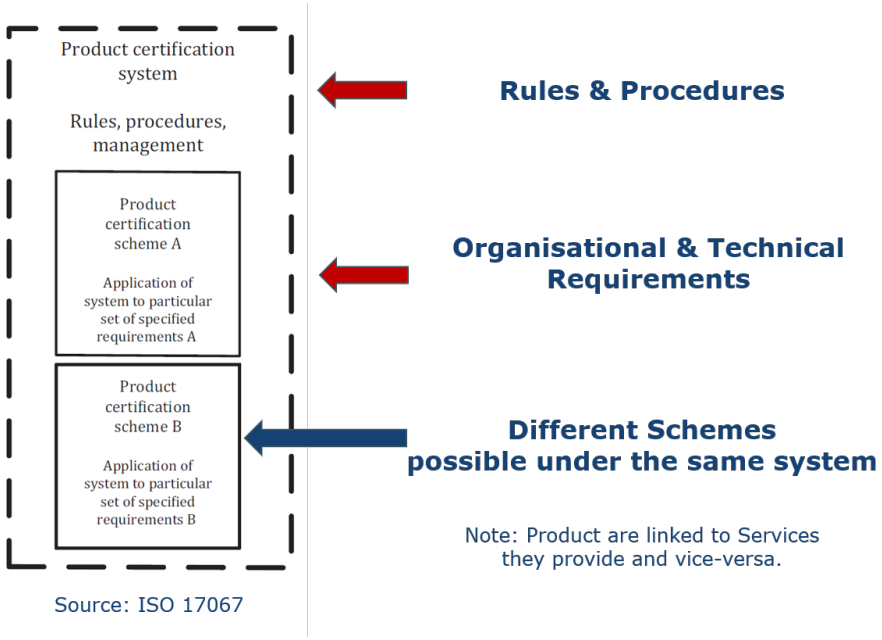


Figure 1 Certification system concept applied to the national EUDI Wallet schemes

3 *NOTE 1: The terms "EUDI wallet" and "European Digital Identity Wallet" are used as synonyms.*

4 *NOTE 2: According to ISO/IEC 17000: "scheme" and "program" are synonyms.*

5 The NL EUDI Wallet certification system aims to provide interested parties with information on the top-level certificate issuance in regards to European Digital Identity Wallets and the NL electronic identification scheme under which they are provided (Figure 2), in accordance with Regulation (EU) 2014/910 modified by 2024/1183 Article 5d(1).

6 A top-level certificate under the NL National eID Scheme will be subject to the applicant wallet provider to satisfy the applicable requirements of the certification scheme; to provide the required underlying certificates; and to demonstrate that it meets the national admission-conditions as set in National law.

7 All the underlying certificates indicated in Figure 2 and underlying certification schemes shall comply with ISO/IEC 17067 and ISO/IEC 17065.

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

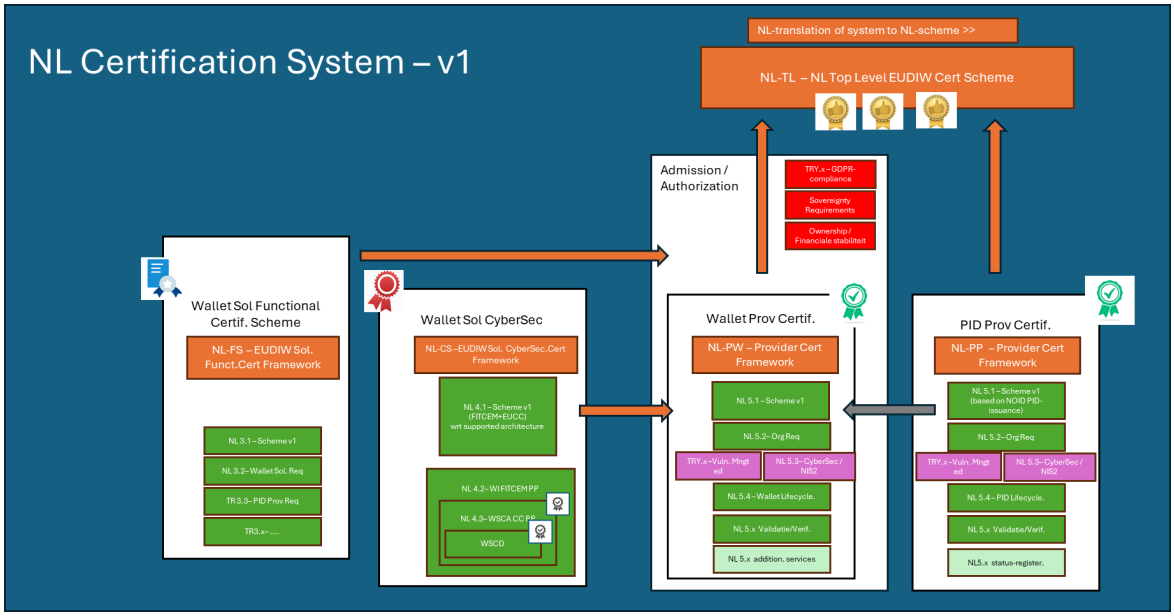


Figure 2 Set of certificates/declarations of conformity resulting from implementation of the national EUDI Wallet certification system

8 The figure illustrates the structural composition of the EUDI Wallet certification system, showing how the different certification schemes – functional, cybersecurity, and eID – combine to form the overall EUDI Wallet Provider Certificate (which will be issued per Wallet Provider).

9 Visually, the diagram is organized as a layered, modular architecture.

(a) On the bottom / left side:

- Functional certification of the Wallet Solution represents the set of conformity assessment activities related to wallet functionality as per Regulation (EU) 2014/910 modified by 2024/1183 (and related Implementing Acts) as-well-as compliance to onboarding flows requirements and compliance to PID issuance flow requirements. The expected activities for this certification mostly consist of product evaluation with functional testing.

(b) On the bottom / middle

- Cybersecurity certification of the Wallet Solution consists of at least two distinct external cybersecurity certification components i.e.: 1) the WSCA certificate and the WSCD certificate, both following the EUCC cybersecurity scheme, and 2) cybersecurity evaluation of Wallet Unit (Wallet Instance in combination with the WSCA/WSCD), based on a FITCEM evaluation scheme (in compliance with EN 17640:2022). The expected activities for this certification mostly consist of product evaluation with security testing.

(c) On the bottom / right hand sides:

- The wallet provider certification and the PID provider certification focus on the requirements for these providers outside the product certifications. This includes the technical, procedural and organizational requirements applicable to the services and service providers. The expected activities for this certification mostly consist of process evaluation and auditing

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

(d) On the top:

- The NL Top Level Certification reflects the overall certificate of "The wallet and the eID-scheme under which the wallet is provided" as mentioned in the regulation. This is the certificate The Netherlands needs to provide to Europe for each combination of wallet and eID-scheme (PID-provider).
- As the figure indicates, this certificate can only be issued if *and* the PID Provider has an activate certificate *and* the Wallet Provider has an active certificate *and* the Wallet provider demonstrates that it meets the national admission-conditions as set in National law.

10 Overall, the figure conveys how the certification system is architected as an integrated model, where several independent but interlinked certification schemes contribute to a harmonized and interoperable European Digital Identity Wallet certification outcome.

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

2 Legal and normative documents

11 In order to carry out certification of European Digital Identity Wallets, a certification system is established regarding compliance with Regulation (EU) 2014/910 modified by 2024/1183 on the basis of EN ISO/IEC 17067 and EN ISO/IEC 17065 standards and operated under the conformity assessment system as described in Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

12 The NL EUDI Wallet Certification System and its schemes will demonstrate compliance with the following documents:

(a) Regulation (EU) 2014/910 modified by 2024/1183 Functional framework (Article 5a) and respective Commission Implementing Regulations:

- EU 2024/2977
- EU 2024/2979
- EU 2024/2982

(b) Certification Rules (Article 5c of with Regulation (EU) 2014/910 modified by 2024/1183) and the Implementing Regulation (EU) 2024/2981

(c) European Cybersecurity Certification scheme as specified in EUCC as defined in the Commission Implementing Regulation (EU) 2024/482

(d) Article 54 of the EU 2019/881 Cybersecurity Act

(e) Article 8(3) of EU 910/2014 on eID and trust services for electronic transactions along with Commission Implementing Regulation (EU) 2015/1502

(f) Regulation (EU) 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products(..), in particular Articles 4 and 5.

13 In addition, the EUDI Wallet Certification System will comply with:

(a) [Placeholder for references to NL national law when available]

3 Governance and stakeholder relationships

3.1 Stakeholders

14 This section briefly describes the stakeholders involved in the NL EUDI Wallet Certification System, their roles and responsibilities.

3.1.1 System Owner

15 **Role:** Top-level governance body of the certification system.

16 **Owner:** Minister of Economic Affairs
(in close concertation with Minister of the Interior)

17 **Responsibilities:**

- Define the overall rules of the certification system.
- Define the overall evaluation methods and requirements
- Maintain and update system documentation and make it available to all relevant stakeholders
- Ensure the overall system complies with ISO/IEC 17067 and legal requirements
- Notify the certification system to the EDICG for opinions and recommendations as required in the regulation.
- Cooperate with other EU Member States operating an EUDI Wallet certification system to ensure a level playing field towards a future EU certification system

3.1.2 Top-Level Scheme Owner

18 **Role:** Governance of Top Level Certification Scheme

19 **Owner:** Minister of Economic Affairs
(in close concertation with Minister of the Interior)

20 **Responsibilities:**

- Define elaborate scheme requirements
- Maintain scheme-specific documentation and make it available to all relevant stakeholders
- Ensuring compliance with the NL Certification System rules/methods/requirements
- Supervision of certification activities
- Compliance of certified services with national and EU legal frameworks
- Post-certification monitoring, particularly following incidents or vulnerabilities

21 *NOTE: The roles of System Owner and Top level Scheme Owner can be combined.*

3.1.3 Subordinate Scheme Owners

22 **Role:** Governance of subordinate certification schemes for specific products or services

23 **Owners:** For some subordinate schemes, individual CABs may propose their own scheme if legal requirements allow and if their scheme is in full compliance with NL Certification System, top-level scheme and set requirements for the subordinated schemes (methods and related requirements). Where EUCC is available and mandated, the legal ownership of the EUCC scheme applies

24 **Responsibilities:**

- Define practical scheme details and operations
- Maintaining scheme-specific documentation and make it available to all relevant stakeholders
- Ensuring compliance with the rules/methods/requirements of the NL Certification System and all overarching schemes applicable to the subordinate scheme
- Supervision of certification activities
- Post-certification monitoring, particularly following incidents or vulnerabilities

3.1.4 National Accreditation Body (NAB)

25 **Role:** Ensures trust and competence of Conformity Assessment Bodies (CABs).

26 **Responsibilities:**

- Accredit CAB-CB according to ISO/IEC 17065 or other standards, if required by the scheme
- Accredit CAB-ITSEF according to ISO/IEC 17025, in respective certification schemes
- Verify competence, impartiality, and consistent application of certification rules
- Act under the EU's overarching accreditation framework (Regulation 765/2008).

3.1.5 Conformity Assessment Body (CAB-CB)

27 **Role:** Performs or subcontracts conformity assessment activities.

28 **Responsibilities:**

- Conduct or subcontract evaluations, audits, or testing
- Produce or validate test reports, evaluation reports, and certification documentation
- Support decision-making on conformity findings.

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

3.1.6 Conformity Assessment Body (CAB-ITSEF)

29 **Role:** Performs evaluation or testing activities.

30 **Responsibilities:**

- Conduct evaluations or testing
- Produce test reports, evaluation reports, and evaluation documentation
- Support the CAB-CB decision-making on conformity findings.

3.1.7 Applicant / Certificate Holder

31 **Role:** An entity seeking certification or possessing the certificate. Typically, the EUDI Wallet provider, PID provider or their subcontractors and suppliers

32 **Responsibilities:**

- Submit the application for certification
- Provide all required technical, procedural, and security documentation
- Continuously maintain conformity throughout operation (including post-certification obligations).

33 *NOTE: each certificate applicant/holder is responsible for the costs related to the certification process and maintenance of their own certificate*

3.1.8 European Digital Identity Cooperation Group (EDICG)

34 **Role:** EU-level coordination and harmonization of the European Digital Identity Framework

35 **Responsibilities:**

- Support consistent implementation of the EUDI Wallet framework across Member States.
- Facilitate cooperation between national authorities, including on supervision, incident handling, and cross-border interoperability.
- Provide guidance to ensure uniform application of certification-related requirements.
- Assist the European Commission in monitoring and improving the functioning of the European Digital Identity ecosystem.

3.1.9 Supervisory Authority (SA)

36 *NOTE: SA may not be merged with the System/Scheme Owner role. Different organizational units of the Ministry of Digital Affairs have been assigned to these roles.*

37 **Role:** Supervisory and oversight function, according to EU and national law

38 **Responsibilities:**

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

- Supervision of Trust Framework (see NL-SYS-03)
- Cross-border cooperation and notification processes.

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

4 Mandatory elements of the scheme definition based on ISO/IEC 17067

4.1 Scheme ownership

39 *NOTE: the text is relevant for System Owner and Scheme Owners.*

40 In accordance with Commission Implementing Regulation (EU) 2024/2981, Chapter II, Article 3(1) on the establishment of national certification schemes, Member States shall assign a Scheme Owner for each national certification system.

41 The owner of the top-level national EUDI wallet certification scheme is the Minister of Economic Affairs (in close concertation with Minister of the Interior).

42 The Top-Level Scheme owner and subordinate Scheme Owners need to:

(a) take on full responsibility for the objectives, the content and the integrity of the scheme;

(b) maintain the scheme and provides guidance when required;

(c) set up a structure for the operation and management of the scheme;

(d) document the content of the scheme;

(e) ensure that the scheme is developed by people competent in both technical and conformity assessment aspects;

(f) plan to protect the confidentiality of information provided by the parties involved in the scheme;

(g) operate and maintain the risk register defined in CIR (EU) 2024/2981;

(h) evaluate and manage the risks/liabilities arising from its activities;

(i) approve the scope of subcontracting activities outsourced by the certification body;

43 Scheme Owners may subcontract a defined part of their tasks to a third party. When subcontracting the third party, the Scheme Owner shall set out the duties and responsibilities of all parties by contract. Scheme owners shall remain responsible for all subcontracted activities performed by their subcontractors.

44 Scheme Owners shall monitor the compliance of CAB-CB with their obligations pursuant to Regulation (EU) 2014/910 modified by 2024/1183 and pursuant to the national certification schemes.

45 Scheme Owners shall perform their monitoring activities, if applicable, at least based on the following information:

(a) information coming from certification bodies (CAB-CB), testing laboratories (CAB-ITSEF), national accreditation bodies, and relevant market surveillance authorities, if applicable;

(b) information resulting from its own or another authority's audits and investigations;

(c) complaints and appeals received.

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

46 Scheme Owners shall manage the scheme during its life cycle and have procedures for reviewing and improving the scheme based on:

(a) information gathered from EUDI Wallet ecosystem stakeholders, including but not limited to CABs, Wallet Providers, other Member States and EUDI Wallet Cooperation Group;

(b) its own monitoring activities;

(c) the complaint and appeal processes;

(d) outcomes from internal procedures.

47 Scheme Owners shall maintain procedures or references to the applicable national legislation, which defines the mechanism to effectively lodge and handle complaints and appeals in relation to their implementation of the certification scheme or to a certificate of conformity issued. These procedures shall include the provision of information to the complainant about the progress of the proceedings and on the decision taken, and information to the complainant on the right to an effective judicial remedy.

48 The certification schemes shall contain provisions that all complaints and appeals that have not been resolved by the CAB-CB are sent to the Scheme Owner for assessment and resolution.

49 Scheme Owners shall inform NL Certification System / NL-Top-Level Certification Scheme Owner of revisions to the certification scheme. That notification shall provide adequate information to issue recommendations to the Scheme Owner and opinions about the updated certification scheme.

50 Where applicable, the NL Certification System / NL-Top-Level Certification Scheme Owner shall notify such changes to the EDICG. That notification shall provide adequate information for the Cooperation Group to issue recommendations and opinions about the updated certification scheme.

51 The Top-Level Scheme Owner shall publish a list of certified EUDI Wallet solutions along with information specified in CIR (EU) 2024/2981 Annex V and ensure this list remains accurate and current.

4.2 Scope and objectives

52 The NL EUDI Wallet Certification System addresses the object of certification defined in CIR 2024/2981, art. 3(2) and 3(3).

53 The certification system consists of the general approach of assessing the conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided as defined in CIR 2024/2981.

54 The legally required overall certification of "the digital identity wallet and the eID scheme under which the wallet is provided", is defined as one top-level scheme composing certificates from three distinct subordinate certification schemes (see Figure 3):

- European Digital Identity Wallet Functional Certification Scheme (NL-CS series)
- European Digital Identity Wallet Cybersecurity Certification Scheme (NL-CS series)

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

- National eID Scheme Certification Scheme (NL-P-P and NL-P-W series)

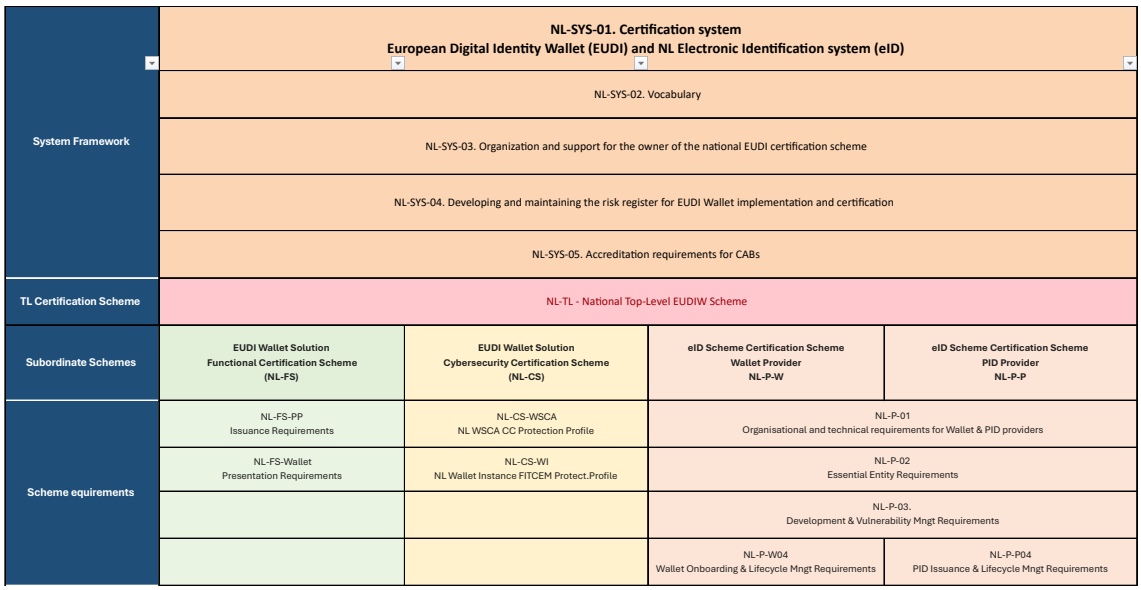


Figure 3 Structured view of NL EUDI Wallet certification system

55 This document provides an overview of how this structure, and its elements, are nested and meet the specific requirements of the relevant standards and regulations, to reach a top-level European Digital Identity Wallet certification.

56 Each certification scheme is building on top of necessary standards (international or European) or technical specification references that constitute a set of specified requirements for the scheme[1].

57 Each scheme is based on the ISO/IEC 17067 product[2] certification scheme type. The types assigned to EUDI Wallet certification scheme are the following (as defined in ISO/IEC 17067):

- European Digital Identity Wallet Functional Certification Scheme (Type 5);
- European Digital Identity Wallet Cybersecurity Certification Scheme (Type 5);
- National eID Scheme Certification Scheme (Type 6).

58 European Digital Identity Wallet Functional Certification Scheme (NL-FS series) lists a set of requirements and necessary information to allow conformity assessment to be performed on the software/hardware components of the EUDI Wallet Unit. It establishes one certificate /declaration of conformity for a specific wallet solution as provided by a wallet provider.

59 European Digital Identity Wallet Cybersecurity Certification Scheme (NL-CS series) provides requirements and necessary information to allow conformity assessment for a specific wallet solution as provided by a wallet provider.

60 eID Certification Scheme (NL-P-P- and NL-P-W- series) is an overarching scheme providing guidance and necessary information to allow conformity assessment to be

[1] In an absence of standards or technical specifications the content of relevant documents will use 'the best practice' approach and will be structured according to ISO/IEC 17007.

[2] ISO/IEC 17067 includes a note: In this International Standard the term "product" can also be read as "process" or "service", except in those instances where separate provisions are stated for "processes" or "services"

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

performed regarding the PID provider and EUDI wallet provider (see Figure 2). This scheme will reuse some of the results obtained after performing the respective wallet solution certification (cybersecurity and functional certification).

61 The structure of the scheme (see Figure 3) is divided into the following parts:

(a) Top-Level Scheme contains all elements to allow to issue a certificate for a wallet provider that has a certificate and that meets the admission criteria (and interfaces and coexists as per national scheme rules iuth the certified PID provider)

(b) The different sub-schemes: for Wallet Solution Functional Certification, for Wallet Solution Cybersecurity Certification, for certification of the conformity with te National eID scheme rules.

(c) The subordinate specific requirements for each these sub-schemes.

4.3 Elements of the scheme according to ISO/IEC 17067

62 This section is based on the provision of Commission Implementing Regulation (EU) 2024/2981, Article 4(3) let. (a) and presents a detailed analysis of conformity with the requirements for the certification scheme and three product certification schemes as specified in the standard, Section 6.5. All references used in this section are presented in Figure 3

	NL-FS	NL-CS	NL-P-P/W
Main evaluation activities	Testing	Testing	Audit
Accreditation standard for CAB-CB	ISO/IEC 17065	ISO/IEC 17065 augmented by EUCC program, where applicable	ISO/IEC 17065 augmented by ETSI EN 319 403-1 V2.3.1
Accreditation standard for CAB-ITSEF	ISO/IEC 17025	ISO/IEC 17025 augmented by EUCC program, where applicable	not relevant

Table 1. Accreditation requirements in NL EUDI Wallet certification system

a) **Scope of the scheme:** Both, the overarching NL Certification System described in this document (with reference to **NL-SYS-series**) and the top-level national scheme **(NL-TL)** and each sub-scheme **(NL-FS, NL-CS, NL-P-P/W)** clearly define their scope: functional conformity, cybersecurity conformity of the wallet solution, and certification of the National eID system, respectively.

b) **Selection of activities:** According to Commission Implementing Regulation (EU) 2024/2981, Article 9 (1), the certification shall be performed in compliance with ISO/IEC 17065. The evaluation activities are further divided in the evaluation methodology by techniques such as audit, inspection, demonstration and test – see Annex A. For application of evaluation activities in relevant certification schemes, see Table 1.

c) **Evaluation Methods & Procedures:** All relevant evaluation methods and procedures are specified in the individual subordinate Certifications Schemes (NL-TL, NL-FS, NL-FS and NL-P-P/W).

d) **Evaluation requirements:** These are specified in detail within the schemes in the requirements for the products or services plane. For instance, the product cybersecurity requirements consists of the following documents:

(a) NL-CS-Decomp. Decomposition - EUDI Wallet security requirements

(b) WP-CS-WI. FITCEM protection profile for the application - EUDI Wallet instance

(c) WP-CS-WSCA. EU CC Protection Profile for WSCA

e) **Requirements for certification bodies:** the system contains requirements for CABs[3] defined in relevant harmonized standards (see Table 1) and NL-SYS-05.

f) **Accreditation of CABs:** this document and, additionally, **NL-SYS-05** specify the accreditation requirements for CABs.

g) **Content of the declaration of conformity[4]:** The content of certificate of conformity for top-level certificate is included in CIR (EU) 2024/2981, Annex VII. Common content requirements are specified in NL-SYS-01. Scheme-specific provisions are set out in NL-TL, NL-FS, NL-CS and NL-P-P/W.

h) **Conditions under which the client may use the statement of conformity or marks of conformity in reference to certified objects** are defined in NL-SYS-03 document, and relevant sections of NL-TL, NL-FS, NL-CS and NL-P-P/W.

i) **Ownership of marks:** The procedures and technical organization of the System/Scheme Owner governance defined in NL-SYS-03 establishes the rules of using certificates of conformity and relevant marks which are used for the NL EUDI Wallet certification system. The rules of using the EU Trust Mark on certified EUDI Wallet solution are specified in relevant EU regulations

j) **Necessary resources:** The competency requirements for personnel of the CABs, and the necessary resources for evaluations and certifications are defined in NL-SYS-05

k) **Notification of results:** NL-SYS-01 (this document); further, procedures for notifying evaluation and surveillance results to the Scheme Owner are specified in NL-SYS-03.

l) **Handling of nonconformities:** NL-SYS-01 (this document) sets general rules; scheme-specific processes for addressing findings and non-conformities are specified in NL-TL, NL-FS, NL-CS, NL-P-P/W

m) **Surveillance procedures:** Surveillance activities are defined in CIR (EU) 2024/2981, Article 16. NL-TL, NL-FS, NL-CS, NL-P-P/W contain provisions regarding surveillance procedures.

n) **Access criteria:** The scope of documents of each certification scheme (NL-TL, NL-FS, NL-CS, NL-P-P/W) and accreditation requirements (NL-SYS-05) define the criteria (i.e., eligible CABs and stakeholders) for access to the scheme.

o) **Publication of certified products:** CIR (EU) 2024/2981 Annex V contains the content of publicly available information necessary for publishing a repository of certified products. Additionally, the NL Top-Level Scheme Owner publishes all

[3] In EUCC, two types of CABs are recognized: CAB-CB (certification bodies) and CAB-ITSEF (testing laboratories)

[4] All terms related to the statement of conformity i.e., declaration of conformity, certificate, certificate of conformity are synonyms in the context of the EUDI Wallet certification scheme.

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

certificates/declarations of conformity issued under NL EUDI Wallet Certification system.

p) **Contracts:** Respective certification scheme documents (NL-TL, NL-FS, NL-CS, NL-P-P/W) define the need for legally binding contracts between the CABs and the Applicants.

q) **Conditions for certification lifecycle:** NL-SYS-01 (this document) defines the conditions for granting, maintaining, renewing, suspending, or withdrawing certificates, further detailed in respective scheme documents (NL-TL, NL-FS, NL-CS, NL-P-P/W).

r) **Handling of complaints:** The issue is covered by the provisions of CIR (EU) 2024/2981 Article 17 and NL-SYS-01.

s) **Referencing the certified product** – NL-SYS01 (this document) and NL-SYS-03 contain rules for how clients can refer to the certification.

t) **Retention of records by the Scheme Owner and certification body:** NL-SYS-01 (this document) and respective scheme documents (NL-TL, NL-FS, NL-CS, NL-P-P/W) specify the requirements for record retention.

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

5 Scheme life cycle management

5.1 Conditions for participation of CABs in the certification scheme

63 Any CAB is required to successfully pass an accreditation process within the scope of relevant certification scheme. The CAB shall inform the Scheme Owner about the accreditation status without undue delay.

64 In duly justified cases, the CAB may start performing its evaluation or certification services according to the rules specified in NL-SYS-05, Section 10.

65 For evaluating requirement covered in the accreditation, the Scheme Owner shall rely on the NAB accreditation process as-well-as on surveillance towards accredited CABs.

66 The CAB shall inform the Scheme Owner of any change in the status of the CAB accreditation without undue delay.

5.2 General rules on certification processes

67 Top-Level Certification of the EUDI Wallet Provider shall be performed under NL-TL-certification scheme, building on relevant certificates or declaration of conformity from NL-TL, NL-FS, NL-CS, NL-P-P/W

68 While submitting the application for the top-level certificate, the Wallet Provider is required to submit all relevant certificates and corresponding certification reports for the respective subordinate certification schemes. The CAB-CB shall assess the scope and validity of these certificates and verify that the applicant meets the conditions to be recognized/admitted to operate as a wallet provider under the NL Wallet eID-scheme before issuing a top-level certificate

69 Dependencies among statuses of certificates issued are specified in relevant sections of respective certification scheme descriptions (NL-TL, NL-FS, NL-CS, NL-P-P/W).

70 It is

5.3 Assurance evidence from external sources

71 The CAB may rely on external assurance evidence in all certification schemes and in reference to the top-level certificate. The status of assurance cases shall be considered as the assurance outcome:

- **Full reliance.** The assurance evidence provides sufficient evidence that the requirement is met. No supplementary evaluation activities are required for this requirement. The CAB-CB shall document the basis for this determination.
- **Partial reliance**. The assurance evidence covers part of the requirement or provides a level of assurance that requires supplementation. The CAB-CB shall specify and perform the necessary supplementary evaluation activities as part of the evaluation.

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

- **No reliance.** The assurance evidence is not available, is not adequate, or does not cover the requirement. The CAB-CB shall perform its own evaluation of the requirement in full.

72 The CAB-CB shall document its evaluation and determination of reliance for each piece of assurance evidence as part of the evaluation records. The CAB-CB remains fully responsible for the certification decision regardless of the extent to which reliance is placed on external assurance evidence.

73 Acceptance of assurance evidence in the evaluation process may not contradict the requirement of ISO/IEC 17065, 7.4.5 related to the evaluation results related to certification completed prior to the application for certification.

5.4 Surveillance

74 The top-level certificate is subject to annual surveillance activities performed by the CAB-CB according to the rules specified in NL-SYS-03 certification scheme and considering the outcomes from surveillance activity specified under NL-FS, NL-CS, NL-P-P/W certification schemes

75 Surveillance activities relevant to the object of certification are specified in respective certification schemes.

5.5 Post-certification obligations of certificate holders

76 The certificate holder shall:

- comply with relevant European and national legislation related to the EUDI Wallet Solution including but not limited to CIR 2024/2981;
- establish, implement and maintain communication channels with CAB-CBs, CAB-ITSEFs if applicable, and the Scheme/System Owner to fulfill its notification obligations;
- ensure that essential information related to the secure use, certification and updates of the EUDI Wallet solution in relation to the certified service or the certified part of product is available to end users in an accessible and understandable language and is presented in a format which is appropriate to its function;
- establish, implement and maintain a continual process of identification, analysis and assessment of vulnerabilities that can affect the EUDI Wallet solution in relation to the certified service or the certified part of product or other products or services that support the EUDI Wallet solution;
- establish, implement and maintain vulnerability handling procedures and cooperate with the CAB-CB and the Scheme Owner in case the vulnerability is identified in relation to the certified service or the certified part of product, or other products or services that support the EUDI Wallet solution;

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

- publish or reference to publicly known vulnerabilities that can affect the EUDI Wallet solution, and relate to the certified service or certified part of the product, or other products or services that support the EUDI Wallet solution;
- ensure that published or referenced information:
  - clearly identify the vulnerability,
  - indicate the affected versions of the product, or the part of it, or any other product or service that supports the EUDI Wallet solution,
  - contain a description of the mitigating or updating measures that are available for relevant stakeholders,
  - does not contain any details that allow direct or indirect exploitation.
- use the mark of conformity in relation to the EUDI Wallet solution, the certified service or the product that contains certified parts, according to the rules provided in NL-SYS-03.

5.6 Changes to the object of top-level certification

77 Changes that have impact on the EUDI Wallet solution, thus on the top-level certificate shall be handled under the CAB-CB regular change management process which is a part of the certificate maintenance process (see Figure 4).

78 In case the process is initiated by the Certificate Holder the CAB-CB shall be notified accordingly and obtain the description of changes in the form of Impact Analysis Report (IAR).

79 The processes of IAR handling by the CAB-CB are described in respective certification schemes.

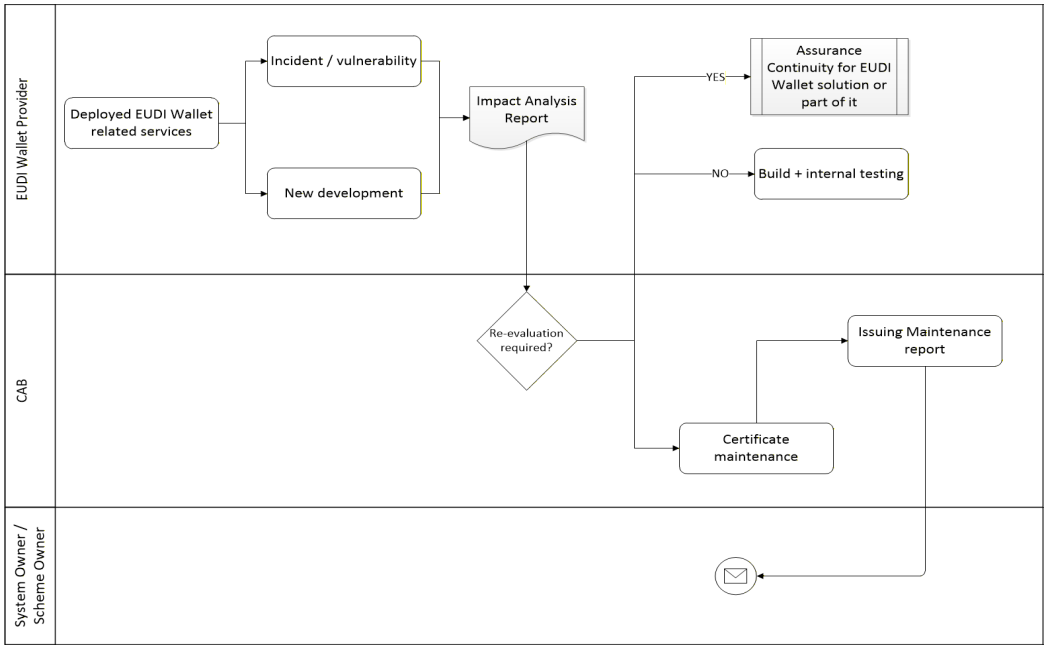


Figure 4 Change management process implemented in the certification system

80 Following the flow presented in Figure 4, any change that results from a security incident or vulnerability shall be handled by the CAB-CB with respect to the assurance continuity principle.

81 *NOTE: NL-SYS-03 contains the description of technical vulnerability handling from the Scheme Owner perspective*.

5.7 Dealing with non-conformities

82 Any non-fulfillment of specified requirement by the object of certification shall be considered as a nonconformity.

83 *NOTE: Due to different characteristics of nonconformities in certification schemes specific provisions are included in* NL-TL, NL-FS, NL-CS, NL-P-P/W*, respectively.*

84 The CAB-CB shall ensure that any non-compliance identified in relation to the certificate holder obligations are handled in accordance with the contract provisions and ISO/IEC 17065.

85 In case where the CAB-CB identifies that the certificate holder does not comply with the obligations imposed on the entity by the applicable European, or national regulations or contractual provisions, the CAB-CB shall:

- Formally notify the certificate holder of the existence of the non-compliance, describing:
  - the specific obligation - suspected or proven - to be breached,
  - available evidence,
  - possible impact on trust or maintenance of certification.
- Request from the certificate holder further clarifications of the case,
- In case the certificate holder clarification is not sufficient, establish a maximum period, which may not exceed thirty (30) calendar days, within the certificate holder shall:
  - propose appropriate corrective measures, and
  - commit to its execution within a reasonable time.

86 Upon failure to comply with the deadline, or unsatisfactory proposals, or failure to respond the CAB-CB enters the procedure of suspension of the certificate in accordance with section 5.8.

5.8 Suspension, termination, withdrawal or expiration of certificates

87 A certificate may be suspended or withdrawn as the result of finding nonconformities in certified object or part of it.

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

88 Where the certificate is withdrawn or terminated on request of the Certificate Holder, such action shall be final, and the certificate shall not be reinstated. The withdrawal of the certificate shall not automatically invalidate certificates issued for individual components, provided that such component certificates remain compliant with the applicable requirements.

89 Where the certificate is suspended, the certificate may be reinstated following a formal certification process. Such a process shall demonstrate that the causes leading to the suspension have been adequately addressed and resolved and that continued conformity with the certification requirements is ensured.

90 The CAB shall inform the Certificate Holder, the System Owner and the top-level scheme owner of the date of expiration certificate and take appropriate action toward re-certification without undue delay.

91 NOTE 1: Expiration of top-level certificate of one Wallet Provider and/or one Wallet Solution does not have any impact on validity of other certificates issued under the NL EUDI Wallet Certification System.

92 NOTE23: The CAB-CB follows requirements of ISO/IEC 17065 to ensure discontinuity of relationship between the product or service concerned and certification.

5.9 Complaints and appeals

93 Any certification decision, including decisions related to suspension or withdrawal of the certificate, may be appealed by a relevant stakeholder identified within the certification system, as well as by a user of an EUDI Wallet. Appeals shall be duly substantiated by reference to the applicable legal requirements, scheme requirements, or system requirements that are alleged not to be fulfilled.

94 An appeal shall be handled by relevant CAB-CB according to the CAB-CB publicly available procedures.

95 The Scheme Owner may not alter CAB decisions.

96 Any EUDI Wallet stakeholder may submit a complaint to the Scheme Owner regarding any aspect of NL EUDI Certification System.

97 A complaint may be handled under the provisions of administrative procedure regarding complaints and requests.

98 NOTE 1: NL-SYS-03 contains the description of complaint or appeal cases that are handled by the Scheme Owner.

99 NOTE 2: Respective scheme documents contain description of appeal cases that are handled by the CAB-CBs.

5.10 Retention of records

100 The validity period of top-level certificate and wallet provider and PID-provider certificate is four years (see NL-TL, NL-P-P/W).

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

101 The retention period of records created during the certification process shall be defined according to relevant legal requirements which will include provisions so that records related to NL-TL, NL-P-P/W and NL-FS/CS- certification shall --in addition to local backups-- also be given in custody at the Certification System Owner.

102 NOTE 1: It is recommended to specify the retention period for all relevant records that are created per each certification case as not less than five years after the certification validity has expired.

103 NOTE 2: The certification case encompasses all relevant CAB initiatives regarding the application or the certified product.

5.11 Periodic review of the certification scheme

104 The NL Certification System Owner shall perform periodic reviews of the EUDI Wallet certification system and certification schemes which operate under the system.

105 NOTE: Periodic review procedures for the Scheme Owner are specified in NL-SYS-03 document.

5.12 Scheme maintenance

106 In the case the review process (internal or in the form of peer review) identifies non-compliances in the scheme or the system performance does not meet defined criteria the Scheme Owner shall initiate the scheme maintenance process which could result in changes in the system or scheme themselves, including their documentation.

107 NOTE: The scheme maintenance process is described in NL-SYS-03.

108 When the certification system or top-level scheme introduces new or revised requirements the System Owner or Scheme Owner shall ensure this information is made available to all relevant stakeholders,

109 Following information from the System Owner or Scheme Owners, the CAB-CB shall ensure the changes that affect the client are communicated to all clients. The CAB-CB shall verify the implementation of the changes by its clients, if applicable, and shall take actions introduced by the scheme due to the changes.

110 NOTE 2: Possible actions toward changes affecting certification are presented in ISO/IEC 17065, 10.1.3.

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

6 Conformity assessments methods, specifications, and reporting overview

6.1 General

111 This chapter provides a unified overview of the conformity assessment toolbox that supports the EUDI Wallet certification scheme. It establishes the methods, competence requirements, decision criteria, and reporting rules that underpin all activities across the functional, cybersecurity, and national eID scheme certification schemes.

112 General description of applicable conformity assessment methods is contained in Annex A.

6.2 Required elements to be defined within conformity assessment methods

113 To ensure harmonized implementation, each method applied within the scheme shall explicitly define the following elements:

- Competence requirements: Competence shall be defined for all individuals involved in the assessment, based on the method which is applicable to relevant certification scheme.
- Outsourcing conditions: As a rule, outsourcing is not permitted unless explicitly allowed within the method's normative framework. Where permitted, the applicable requirements shall be described in relevant certification scheme.
- Pass/Fail criteria: For each assessment activity, the method shall define the applicable pass/fail criteria and describe their impact on the validity of the certificate.

6.3 Mandatory elements of reports

114 Mandatory elements of reporting shall be defined according to the conformity assessment method. The certification scheme can add other relevant requirements, if applicable.

115 Test reports include the following mandatory elements (see ISO/IEC 17025 for reference):

- Title: test report / report on sampling;
- Name and address of the testing laboratory;
- Location of performance of the laboratory activities;
- Unique identification that all its components are recognized as a part of a complete report, and a clear identification of the end;
- Name and contact details of the customer;
- Identification of the method;
- Dates of performance of the laboratory activity;
- Date of issue of the report;
- Statement to the effect that the results relate only to the items tested or sampled;
- Results with, where appropriate, the units of measurements;
- Identification of the person(s) authorizing the report;

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

- Clear identification when test results are from external providers, including customers.

116 The management system audit report shall include the following mandatory elements (see ISO/IEC 17021-1):

- Identification of the certification body;
- The name and address of the client and the client's management representative;
- The type of audit (e.g. initial, surveillance or recertification audit);
- The audit criteria;
- The audit objectives;
- The audit scope, particularly identification of the organizational or functional units or processes audited and the duration of the audit;
- Identification of the audit team leader, audit team members and any accompanying persons;
- The dates and places where the audit activities (onsite or offsite) were conducted;
- Audit evidence, findings and conclusions, consistent with the required elements of the audit;
- Any unresolved issues, if identified.

117 Documentation for product-, service- or process – related certification which is provided to the client shall include the following mandatory elements (see ISO/IEC 17065):

- The name and address of the certification body;
- The date certification is granted (the date shall not precede the date on which the certification decision was completed);
- The name and address of the client;
- The scope of certification;
- The term or expiry date of certification, if certification expires after an established period;

118 Additionally, the certification report for the object of conformity shall include specific information required by the certification schemes (see NL-TL, NL-FS, NL-CS, NL-P-P/W).

6.4 Conformity assessment template dedicated to certification schemes

119 To ensure consistent implementation of the certification schemes the table of basic characteristics of the scheme is introduced.

Subject	Description required	Required details
Object of conformity assessment	Clear identification of the component that is assessed	Reference to the composite model when relevant
Conformity assessment methodology	Choice of methodology out of the methodologies described in Annex A	Rationale to use this methodology
Impartiality criteria	Identification of impartiality criteria only when they add to the general impartiality criteria of the conformity assessment standard.	

Subject	Description required	Required details
Confidentiality criteria	Identification of confidentiality criteria only when they add to the general impartiality criteria of the conformity assessment standard.	
Competence requirements	People performing conformity assessment methods.	Specification of competence requirements or reference to relevant sources.
Pass/Fail Criteria	Pass/Fail criteria general description	Reference to relevant standard(s) or WM-0x documents
Certificate lifecycle	Suspension / withdrawal/renewal criteria when relevant	Condition description in all respective certification schemes
Reporting	Reporting elements reference to 6.3 + additional elements where required	Details on the format
Dependencies	Dependencies on other objects of conformity assessment	Description

7 Conformity analysis

7.1 Conformity with eIDAS regulation and relevant implementing acts

7.1.1 Conformity with implementing act (CIR (UE) 2024/2981)

120 The EUDIW Certification System and EUDIW Certification Scheme is designed to be fully compliant with the specifications and procedures established by the Commission Implementing Regulation (EU) 2024/2981 for the certification of European Digital Identity Wallets. The following analysis details how the requirements of the implementing act are met by the certification scheme structure.

121 **Article 1: Subject matter and scope**

122 Requirement**:** Sets the scope for a robust framework for the certification of wallets

123 Conformity: The entire certification system, governed by NL-SYS-01, is designed to establish such framework. The pillars (NL-TL; NL-FS, NL-CS, NL-P-P/W) collectively cover the full scope required for the certification of the EUDI wallet solution and its underlying eID system.

124 **Article 2: Definitions**

125 Requirement: Provides key definitions for the regulation.

126 Conformity: NL-SYS-02 (Vocabulary) is a dedicated document for establishing a set of terms relevant to the certification scheme. NL-SYS-02 incorporates all definitions from Article 2 of CIR (EU) 2024/2981 and adds relevant terms and their definitions, if necessary.

127 **Article 3: Establishment of national certification schemes**

128 Requirement 3(1): Member States shall assign a Scheme Owner.

129 Conformity: NL-SYS-01 assigns the System Owner/Scheme Owner and specifies responsibilities of these roles. This role will be assigned by national legislation.

130 Requirement 3(2): The object of certification shall be the provision and provisioning of wallet solutions and the national eID scheme under which they are provided.

131 Conformity: This is fully covered by the three-pillar structure:

- NL-FS Series: Covers the functional certification of the EUDI Wallet solutions.
- NL-CS Series: Covers the cybersecurity certification of the EUDI wallet solutions.
- GP-NLWP/PP Series: Covers the certification of the underlying eID scheme (aka the wallet providers and the PID providers)

132 Requirement 3(3): The object of certification shall include specific elements.

133 Conformity:

- Software components: Addressed by NL-FS-series, NL-CS-series (incl specific Wallet Instance FITCEM PP and WSCA PP PP) en Resilience requirements related to software development and the provisioning of essential services under the NL-P-P/W-series).
- Hardware components: Addressed by a Protection Profile for WSCD, certified externally.
- Processes that support the provision and operation of a wallet solution and explicitly referenced in CIR (EU) 2015/1502: Addressed in detail by the the NL-P-P/W-series notably the requirements on "Wallet Onboarding & LifeCycle Management" and "PID-issuance and lifecycle management).

134 **CHAPTER II NATIONAL CERTIFICATION SCHEMES**

135 Requirement 3(4): National certification schemes shall include a description of the specific architecture of the wallet solutions and of the electronic identification scheme under which they are provided.

136 Conformity:

137 See Annex B in this document.

138 Requirement 3(5): [Specific architecture of the wallet solution] within a scheme must define specific elements.

139 Conformity:

- the specific architecture of a wallet solution and of the electronic identification scheme: see Annex B of this document.
- the security controls associated with assurance levels set out in Article 8 of Regulation (EU) 2014/910 modified by 2024/1183: are defined in NL-P-P/W-series.
- evaluation plan(s) drawn-up in accordance with section 7.4.1 of EN ISO/IEC 17065;2012: The Certification System states the object of certification, provides a structured decomposition of the object of certification, including elements where component certifications are possible, sets the evaluation methodologies and lists a set of requirements (derived from various risk analysis) across NL-FS-, NL-CS and NL-P-P/W-series.
- the security requirements necessary to address the cybersecurity risks and threats listed in the risk register set out in Annex I: the methodology for developing and maintaining the risk register is included in NL-SYS-04; additionally, specific threats and risks are considered as a part of security problem definitions in respective Protection Profiles (NL-CS-series of documents) and audit framework documents (NL-P-W/PP series of documents).
- Mapping of controls: Elaborated on in the NL-P-P/W-series – cfr the requirements on "Wallet Onboarding & LifeCycle Management" and "PID-issuance and lifecycle management).
- Risk assessment justification: the methodology for developing and maintaining the risk register is included in NL-SYS-04; additionally, specific threats and risks are considered as a part of security problem definitions in respective Protection Profiles

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

(NL-CS-series of documents) and audit framework documents (NL-P-W/PP series of documents).

140 **Article 4: General requirements**

141 Requirement 4(1) & 4(2): Schemes shall cover functional, cybersecurity, and data protection requirements by using European cybersecurity certification schemes, where relevant.

142 Conformity: EUCC program defined in CIR (EU) 2024/2981 is used to certify specific components of the EUDI Wallet Unit; Composite Target of Evaluation (i.e., wallet instance + WSCA + WSCD and relevant interfaces), functionality EUDI Wallet and eID scheme will be certified under dedicated national certification schemes. If possible, certification schemes are based on relevant European or international standards or technical specifications

143 Requirements 4(3)(a): National certification schemes shall specify the elements listed in section 6.5 of ISO/IEC 17067:2013;

144 Conformity: see section 4.3 of NL-SYS-01 (this document)

145 Requirement 4(3)(b): National certification schemes shall be implemented as a type 6 scheme (ISO/IEC 17067).

146 Conformity: NL-SYS-01 (this document) explicitly states that the certification scheme is a type 6 scheme for the top-level certificate (NL-TL), which includes initial certification and subsequent surveillance activities regarding both the certified product and associated services. The certification processes are defined in NL-FS, NL-CS and NL-P-P/W. The surveillance framework is defined in NL-SYS-01 (this document).

147 Requirements 4(4(a), (c), (d): National certification schemes shall (define) requirements for eligible providers.

148 Conformity: The governance rules are defined in NL-SYS-01. The organizational and technical requirements are described in NL-WP -series for EUDI Wallet Providers and NL-P-P- series for PID Providers.

149 Requirement 4(4)(b): National certification schemes shall ensure that only the Trust Mark is used as mark of conformity.

150 Conformity: NL-SYS-03 defines relevant characteristics of the national mark and terms and conditions of its use. The Trust Mark as defined in Commission Implementing Regulation 2024/2981 will be used only for the top-level certificate.

151 Requirement 4(4)(e): National certification schemes shall define responsibilities and the legal action are established and include references to the applicable national legislation which defines the responsibilities and possible legal action, where certification under the scheme is being used fraudulently.

152 Conformity: subject to a dedicated Dutch National Regulation establishing NL EUDI Wallet Certification system.

153 **Article 5: Incident and vulnerability management**

154 Requirements 5(2) to (7) and (9) related to the certificate holders.

155 Conformity: These requirements are defined within the organizational requirements documents: NL-P-P/W-series03 related to respective providers.

156 Requirement 5(8) National certification schemes shall establish vulnerability disclosure requirements applicable to certification bodies.

157 Conformity: This requirement is included in NL-P-P/W-series.

158 **Article 6: Maintenance of national certification schemes**

159 Requirement 6 (1) (2): National certification schemes shall establish and implement processes for periodic review, maintenance, and management of changes.

160 Conformity: This is a core function of the Scheme Owner and the overall governance model, which is described in NL-SYS-01 (this document), and appropriate procedures are established in NL-SYS-03.

161 ***CHAPTER III - REQUIREMENTS RELATING TO SCHEME OWNERS***

162 **Article 7: General requirements**

163 Requirement 7(1) to (4): The national certification scheme shall define the responsibilities of the Scheme Owner.

164 Conformity: These responsibilities are described in NL-SYS-01, Section 4.1.

165 ***CHAPTER IV - REQUIREMENTS RELATING TO PROVIDERS***

166 **Article 8: General requirements**

167 Requirement 8(1)(2) and (4): National certification schemes shall contain cybersecurity requirements based on a risk assessment of each specific supported architecture.

168 Conformity: Relevant requirements are covered by the NL-CS series of documents as-well as the software development and essential entity requirements as listed in the NL-P-P/W-series.

169 Requirement 8(3): National certification schemes establish security criteria, which shall include the following requirements i.e. an extensive list of requirements for providers, including risk management, policies for changes, vulnerability handling, managing human resources, operating environment, etc.

170 Conformity: Relevant requirements are covered by the software development and essential entity requirements as listed in the NL-P-P/W-series.

171 Requirement 8(5): National certification schemes shall require that the following information and documentation is provided or otherwise made available to the certification body by the applicant for certification (..):

172 Conformity: the structure of application forms containing relevant information described in the Commission Implementing Regulation 2024/2981 are provided by CAB-CB based on NL-FS, NL-CS and NL-P-P/W provisions.

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

173 ***CHAPTER V - REQUIREMENTS RELATING TO CERTIFICATION BODIES***

174 **Article 9: General requirements**

175 Requirement 9(1), (2) and (3): Certification bodies shall be accredited by national accreditation bodies in accordance with EN ISO/IEC 17065:2012 provided that complies with accreditation requirements.

176 Conformity: The accreditation framework is defined in NL-SYS-01 (this document). All requirements pertaining to CABs (including surveillance activities) are consolidated and detailed in NL-SYS-05 (Accreditation requirements for CABs).

177 Requirements 10 and 11: related to subcontracting and notifications to the supervisory authority.

178 Conformity:

(a) Subcontracting rules are defined in relevant certification schemes operating under NL-SYS-01

(b) The scheme owner will be designated in a Dutch National Regulation that establishes NL EUDI Wallet Certification System.

179 Requirement 12: related to Incident and vulnerability management.

180 Conformity: Relevant requirements are covered by the NL-CS series of documents as-well as the software development and essential entity requirements as listed in the NL-P-P/W-series.

181 ***CHAPTER VI - CONFORMITY ASSESSMENT ACTIVITIES***

182 **Article 13: Evaluation activities**

183 Requirement 13(1) to (4): National certification schemes shall contain methods and procedures to be used by the conformity assessment bodies when conducting their evaluation activities (..)

184 Conformity: All evaluation methods and procedures are defined in Certification schemes (NL-TL, NL-FS, NL-CS, NL-P-P/W).

185 **Article 14: Certification activities**

186 Requirement 14(1): National certification schemes shall set out an attestation activity for the purpose of issuing a certificate of conformity (..)

187 Conformity: This requirement is addressed in NL-TL, NL-FS, NL-CS, NL-P-P/W that contain relevant certification scheme specifications.

188 Requirement 14(2): The certification assessment report may be made available to the European Digital Identity Cooperation Group and to the European Commission.

189 Conformity: By virtue of sharing the NL Certification System and NL EUDIW Certification Scheme to the EDICG.

190 **Article 15: Complaints and appeals**

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

191 subject to national law

192 **Article 16: Surveillance activities**

193 Requirement: Surveillance activities shall be implemented by certification bodies.

194 Conformity: General framework is defined in NL-SYS-01, Section 5.4. Detailed specifications are implemented in all certification schemes (NL-TL, NL-FS, NL-CS, NL-P-P/W).

195 **Article 17: Consequences of non-compliance**

196 Requirement: National certification schemes shall set out the consequences of non-conformity a certified wallet solution and of the electronic identification scheme under which they are provided, with the requirements set out in Commission Implementing Regulation 2024/2981

197 Conformity: Appropriate consequences are referred to in NL-SYS-01 (this document), see Section 5.8.

198 ***CHAPTER VII - CERTIFICATION LIFECYCLE***

199 **Article 18: Certification lifecycle**

200 Requirement 18(1): The validity of certificates of conformity issued under national certification schemes shall be subject to regular evaluation activities by the certification body (..)

201 Requirement 18(2): National certification schemes shall contain a process for the recertification of wallet solutions and the electronic identification scheme under which they are provided, upon request of the holder of the certificate of conformity before the expiry of the initial certificate of conformity.

202 Requirement 18(3): National certification schemes shall contain a process for managing changes in a certified wallet solution and the electronic identification scheme under which they are provided.

203 Requirement 18(4): National certification schemes shall contain a process for special evaluations in accordance with PN-EN ISO/IEC 17065. That process for special evaluations shall include a selection of activities to be performed to address the specific issue that triggered the special evaluation.

204 Requirement 18(5): National certification schemes shall set out rules related to the cancellation of a certificate of conformity.

205 Conformity: All processes included in Article 18 are specified in NL-TL, NL-FS, NL-CS and NLWP/PP-certification schemes.

206 ***CHAPTER VIII - RECORDKEEPING AND PROTECTION OF INFORMATION***

207 **Articles 19: Retention of records**

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

208 Requirement 19(1): National certification schemes shall contain requirements for certification bodies concerning a record system for all relevant information produced in connection with the conformity assessment activities.

209 Conformity: General rules are provided in NL-SYS-01. These requirements are imposed on CABs in NL-TL, NL-FS, NL-CS and NLWP/PP certification schemes.

210 Requirement 19(2) and (3): National certification schemes shall set out requirements for the holder of the certificate of conformity to store the following information securely for the purpose of Commission Implementing Regulation 2024/2981 (..)

211 Conformity: Relevant obligations for the certificate holders are included in NL-SYS-01 (this document) and relevant application forms defined by CAB-CB based on certification scheme provisions (NL-TL, NL-FS, NL-CS and NLWP/PP).

212 **Article 20: Protection of information**

213 Requirement: (..) all persons or organizations that are granted access to information in the execution of activities under the national certification scheme shall be required to ensure the security and protection of trade secrets and other confidential information, as well as preserving intellectual property rights, and take the necessary and appropriate technical and organizational measures to ensure this confidentiality.

214 Conformity: Will be achieved by appropriate procedures implemented by the Scheme Owner and CABs followed by confidentiality clauses included in the contracts between the CAB and the entity applied for a certificate.

7.2 Conformity with (EU) Cybersecurity Act (Article 54(1) - Elements of European cybersecurity certification schemes

215 The **NL-CS (Cybersecurity Certification Scheme)** is designed to be compliant[5] with Article 54(1) of the CSA.

216 A European cybersecurity certification scheme shall include at least the following elements:

217 **Subject matter and scope:** The scope of the scheme is defined in the introductory section of NL-CS.

218 **b) Purpose of the scheme:** The purpose is to certify the cybersecurity of the EUDI Wallet components.

219 **c) References to standards:** For the EUCC program Common Criteria/Common Evaluation Methodology, CC/CEM:2022 release 1 (ISO/IEC 15408:2022/ISO/IEC 18045:2022, respectively) apply; for the national cybersecurity certification scheme EN 17640:2022.

220 **d) Assurance levels:** The scheme explicitly targets a high assurance level, specifically AVA_VAN.5, for the EUCC related certifications, and assurance level "high" according to the definition contained in Regulation (EU) 2019/881 for the FITCEM related part of NL-CS (see Figure 5).

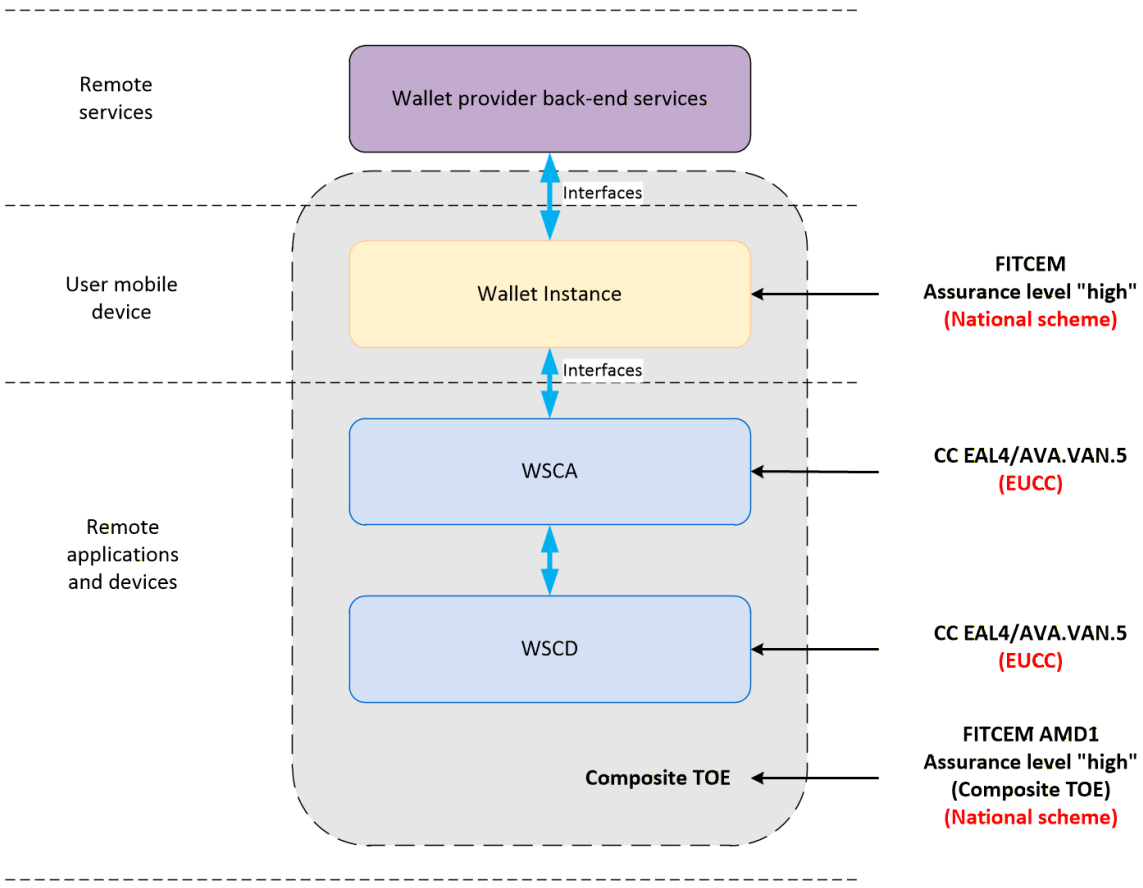


Figure 5 TOE concept for NL-CS

221 **e) Self-assessment:** The schemes are based on third-party evaluation by accredited CABs; self-assessment is not permitted for the required level of assurance.

222 **f) Requirements for CABs:** These are detailed NL-SYS-05 ensuring CABs have the technical competence to evaluate the specific requirements.

223 **g) Evaluation criteria and methods:** These are through the evaluation methods and PPs as describes in the NL-CS-series.

224 **h) Information from applicants:** This is specified in the NL-CS and relevant application forms.

225 **i) Marks or labels:** The governance model (NL-SYS-01) along with specific procedures in defines the conditions for the use of certification marks related to the NL-FS and NL-CS-02.

226 **j) Rules for monitoring compliance** are specified in NL-CS-certification scheme.

227 **k) Conditions for certification lifecycle** are specified in NL-CS certification scheme.

228 **l) Consequences of non-compliance:** The governance model contained in NL-SYS-01 establishes rules for handling certified products that are found to be non-compliant.

229 **m) Vulnerability reporting:** The governance model contained in NL-SYS-and further in NL-P-P/W establish rules on how to report and manage newly discovered vulnerabilities.

230 **n) Record retention:** The governance model contained in NL-SYS-01 specifies the rules for record retention by CABs. Additionally, specific provisions on record retention are in each certification scheme.

231 **o) Identification of other schemes:** The cybersecurity scheme (NL-CS) identifies the relationship between the different sub-schemes (EUCC-based and national cybersecurity certification scheme based on EN 17640).

232 **p) Content and format of certificates:** This will be defined by CAB-CB based on provisions included in NL-CS

233 **q) Availability of documentation:** The organizational requirements will mandate the period of availability for all relevant documentation according to CIR (EU) 2024/2981, Article 19.

234 **r) Maximum period of validity:** This is defined in the governance model contained in NL-SYS-01 (this document) for a top-level certificate, and each certification scheme for specific national certificates/declarations of conformity.

235 **s) Disclosure policy:** The governance model contained in NL-SYS-01 defines the policy for disclosing the status of certificates (issued, amended, suspended, withdrawn). Additionally, each certification scheme contains specific provisions on terms and conditions for the certificate lifecycles.

236 **t) Mutual recognition:** The EUCC related part – subject to automatic EU-wide mutual recognition based on the provision of CSA, the national cybersecurity certification scheme part – subject to further discussion among Member States.

237 **u) Peer assessment mechanism:** this is established as part of the governance model defined in NL-SYS-01 and the CSA provisions relevant to 'peer assessment' (assurance level 'high' is applied).

238 **v) Supplementary information:** NL-CS defines the procedures for providing supplementary cybersecurity information to users (see art. 55 of the CSA).

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

Annex A Conformity assessment methods and techniques

A.1. Terms relating to conformity assessment

NOTE: All definitions are taken from EN-ISO/IEC 17000:2020 unless otherwise stated.

239 **Conformity assessment** - demonstration that **specified requirements** *are* fulfilled

240 **Object of conformity assessment** - entity to which **specified requirements** apply

241 **Specified requirement** - need or expectation that is stated

NOTE to entry: Specified requirements can be stated in normative documents such as regulations, standards and technical specifications.

242 **Conformity assessment body** - body that performs conformity assessment activities, excluding **accreditation**

243 **Accreditation body** - body that performs **accreditation**

244 Whenever a requirement is assessed, the scheme documentation needs to identify the following elements:

(a) Conformity assessment type. In the context of EUDI Wallet certification scheme it is a choice among the following: evaluation and its sub-types (testing, audit, inspection, validation, verification, certification (managements systems, product/service/process), accreditation.

(b) Rationale for a choice of the method: considering the definitions of the methods and provisions of CIR (EU) 2024/2981.

A.2. Methods relating to evaluation

245 NOTE: EN-ISO/IEC 17065 defines general functions "Selection" and "Determination" in joined conformity assessment activity called "Evaluation".

246 **Testing** - determination of one or more characteristics of an **object of conformity assessment**, according to a procedure

NOTE: procedure is a specified way to carry out an activity or a process.

247 Audit - process for obtaining relevant information about an **object of conformity assessment** and evaluating it objectively to determine the extent to which **specified requirements** are fulfilled

NOTE entry: Examples of objects for an audit are management systems, processes, products and services.

248 **Inspection** - examination of **an object of conformity assessment** and determination of its conformity with detailed requirements or, based on *professional judgement, with general requirements*

NOTE 1 to entry: Examination can include direct or indirect observations, which can include measurements or the output of instruments.

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

NOTE 2 to entry (modified): Conformity assessment schemes can specify inspection as examination only.

249 **Validation** - confirmation of plausibility for a specific intended use or application through the provision of objective evidence that **specified requirements** have been fulfilled

*NOTE to entry: Validation can be applied to **claims** to confirm the information declared with the claim regarding intended future use.*

According to EN ISO/IEC 17029, **claim** is information declared by the client.

250 **Verification - c**onfirmation of truthfulness through the provision of objective evidence that **specified requirements** have been fulfilled

*NOTE to entry: Verification can be applied to **claims** to confirm the information declared with the claim regarding events that have already occurred or results that have already been obtained.*

A.3. Various types of attestations

251 **Attestation** - issue of a statement, based on a decision, that fulfilment of *specified requirements* has been demonstrated

252 NOTE 1 to entry (modified): The resulting statement is referred as a "statement of conformity".

*253 NOTE 2 to entry (modified): First-party attestation is called **declaration (of conformity)** while third-party attestation is distinguished by the terms **certification** and **accreditation**.*

254 **Certification** - third-party **attestation** related to an **object of conformity assessment**, except for **accreditation**

255 Several objects of certification are applied to the EUDI Wallet certification scheme, namely, management systems, products, services and processes.

256 According to EN-ISO/IEC 17021-1, Introduction: Certification of a management system provides independent demonstration that the management system of the organization:

a) conforms to specified requirements;

b) is capable of consistently achieving its stated policy and objectives;

c) is effectively implemented.

257 According to EN-ISO/IEC 17065, Introduction: Certification of products, processes or services is a means of providing assurance that they comply with **specified requirements** in standards and other normative documents.

258 **Accreditation** - third-party **attestation** related to a **conformity assessment body** conveying formal demonstration of its competence, impartiality and consistent operation in performing specific conformity assessment activities.

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

Annex B Description of supported Wallet Solution architectures in the Dutch national wallet certification system

A. High-level diagram of EUDI Wallet solutions

Under Certification System v1 only HSM-based architectures are accepted, whereby:

- the Wallet Instance runs on a mobile platform that meet established conditions and interacts with a Wallet Provider Backend (where the HSM-based WSCA/WSCD run)
- the Wallet Instance complies with the Wallet Instance FITCEM PP and the complies with WSCA CC PP as defined under NL-CS-series are accepted.

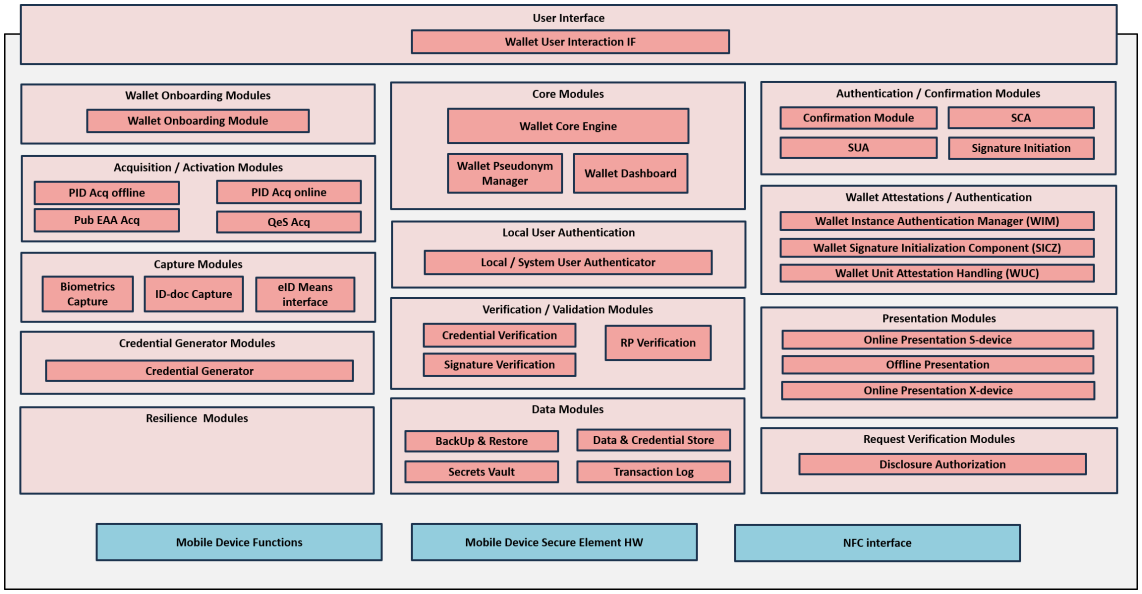


***Figure** 6 — Modular decomposition*
(independent of exact deployment – eg partially processing at WP-backend)

The visual above and table below provide a modular overview of the Wallet. The table thereby provides a link between the functional decomposition and the modular decomposition of the Wallet.

Module	Description of Modules	Functional decomposition
Wallet User Interaction IF	User interface visible on the User Device for login, authentication, consent, dashboard access and other Wallet functions.	Framework; Wallet Functions; WI/WSCA/WSCD Low Level Functions
Wallet Onboarding Module	Activates the first Wallet Instance and WSCA/WSCD, manages additional instances and deactivation.	Wallet Provider Interaction; WI/WSCA/WSCD Low Level Functions; Supporting Functions

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

Module	Description of Modules	Functional decomposition
PID Acq Offline	Requests PID issuance via a physical registration desk.	PID Provider Interaction; Issuance; WI/WSCA/WSCD Low Level Functions
PID Acq Online	Requests PID issuance online from a PID Provider.	PID Provider Interaction; Issuance
Pub EAA Acq	Requests public EAA issuance online.	PID Provider Interaction; Issuance
Biometrics Capture	Captures biometric data for issuance, enrolment or presentation.	PID Provider Interaction; Issuance; Presentation; WI/WSCA/WSCD Low Level Functions
ID-doc Capture	Reads ID cards/passports during offline enrolment.	PID Provider Interaction; Issuance
QeS Acq	Connects the Wallet to a remote Qualified Electronic Signature service.	Wallet Provider Interaction; Remote Signing; WI/WSCA/WSCD Low Level Functions
eID Means Interface	Invokes eID identification and authentication services.	PID Provider Interaction; Wallet Provider Interaction
Wallet Core Engine	Orchestrates interfaces between Wallet components and the platform.	Framework; WI/WSCA/WSCD Low Level Functions; Supporting Functions
Wallet Dashboard	User interface for data and log interaction.	Framework; Wallet Functions
Wallet Pseudonym Manager	Manages pseudonyms and their assignment to services.	Wallet Functions; PID Data Model; Presentation
Local / System User Authenticator	PIN-based local Wallet unlock.	WI/WSCA/WSCD Low Level Functions; Wallet Functions
Credential Verification	Validates attestations from Providers or Relying Parties.	PID Provider Interaction; Presentation; PID Data Model
RP Verification	Validates RP certificates.	Presentation; PID Provider Interaction
Signature Verification	Verifies electronic signatures and seals.	Presentation; Remote Signing; PID Provider Interaction
Backup & Restore	Backs up and restores Wallet data and credentials.	Supporting Functions; PID Data Model; Wallet Functions
Data & Credential Store	Stores and protects credentials, PID data and attributes.	PID Data Model; Supporting Functions
Secrets Vault	Secure storage of non-key confidential assets.	WI/WSCA/WSCD Low Level Functions; PID Data Model; Supporting Functions
Transaction Log	Maintains protected logs of Wallet interactions.	Supporting Functions; Wallet Functions
Confirmation Module	User confirmation of RP requests not requiring SCA/signature.	Presentation; Wallet Functions
SCA	Handles online strong customer authentication flows.	Wallet Provider Interaction; WI/WSCA/WSCD Low Level Functions
SUA	Handles online strong User authentication flows.	Wallet Provider Interaction; PID Provider Interaction; WI/WSCA/WSCD Low Level Functions

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

Module	Description of Modules	Functional decomposition
Signature Initiation	Confirms signing sessions with remote e-signing services.	Remote Signing; Wallet Provider Interaction
WIM	Obtains and uses Wallet Instance Attestations.	Wallet Provider Interaction; WI/WSCA/WSCD Low Level Functions
SICZ	Obtains and uses Wallet Unit Attestations.	Wallet Provider Interaction; WI/WSCA/WSCD Low Level Functions
WUC	Handles Wallet Unit Attestations.	Wallet Provider Interaction; PID Data Model; WI/WSCA/WSCD Low Level Functions
Offline Presentation	Presents PID/attestations via ISO 18013-5.	Presentation; Wallet Functions; PID Data Model
Online Presentation S-device	OID4VP presentation on the same device.	Presentation; PID Provider Interaction; Wallet Functions
Online Presentation X-device	OID4VP presentation via redirect or QR code.	Presentation; PID Provider Interaction; Wallet Provider Interaction
Disclosure Authorization	Checks intended use and disclosure policy compliance.	Presentation; PID Data Model; Wallet Functions
Request Verification	Verifies RP request integrity and authenticity.	Presentation; PID Provider Interaction
Credential Generator	Generates Wallet-level attestations such as mandates.	PID Data Model; Issuance; Wallet Functions
Resilience	Provides security mechanisms protecting the Wallet against compromise, analysis, insecure operating environments and attacks on sensitive assets.	Supporting Functions; WI/WSCA/WSCD Low Level Functions; Framework

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