EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-SYS-05

NL EUDI Wallet Certification System

Accreditation requirements for CABs

RC1.1
2026.10.31

Intern gebruik

Document reference	NL-SYS-05
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-TL, NL-FS-*, NL-CS-*, NL-PW-* and NL-PP-**

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	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

Introduction 6
1 Scope 7
2 References 8
2.1 Legal basis 8
2.2 Normative references 8
2.3 Peer documents 8
2.4 Subsidiary Documents 9
3 Terms and Definitions 10
3.1 General Terms 10
3.2 Specific Terms 10
4 General requirements 11
4.1 Legal and contractual matters 11
4.2 Management of impartiality 11
4.3 Liability and financing 11
4.4 Non-discriminatory conditions 11
4.5 Confidentiality 12
4.6 Publicly available information 12
5 Structural requirements 13
5.1 Organizational structure and top management 13
5.2 Mechanism for safeguarding impartiality 13
6 Resource requirements 14
6.1 Conformity Assessment Body personnel 14
6.2 Resources for evaluation 14
7 Process requirements 16
7.1 General requirements 16
7.2 Application 18
7.3 Application Review 18
7.4 Evaluation 19
7.5 Review 19
7.6 Certification decision 19
7.7 Certification documentation 19
7.8 Directory of certified products / services 20
7.9 Surveillance 20
7.10 Changes affecting certification 21
7.11 Termination, reduction, suspension or withdrawal of certification 22
7.12 Records 22
7.13 Complaints and appeals 23
8 Management system requirements 24
8.1 Options 24

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

8.2 General management system documentation 24
8.3 Control of documents 24
8.4 Control of records 24
8.5 Management review 24
8.6 Internal audits 24
8.7 Corrective actions 24
8.8 Preventive actions 24
9 Additional provisions regarding accreditation requirements for CAB-ITSEF .. 25
10 Transition 26
Annex A Competence requirements for the EUDI Wallet Certification 27

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

Introduction

1 The document aims to meet the general requirements of the international community to provide trust and confidence in European Digital Identity Wallet solutions including, amongst others, applicable requirements from Regulation (EU) 2024/1183.

2 The document is intended to support national accreditation bodies as specified in Regulation (EU) 765/2008 in applying ISO/IEC 17065 with extensions for the accreditation of Conformity Assessment Bodies (CABs) participating in the NL EUDI Wallet Certification Scheme.

3 The document does not repeat requirements from ISO/IEC 17065 but follows its document structure.

4 Additionally, the document incorporates requirements relating to the audit of management systems, as defined in ISO/IEC 17021-1 and ISO/IEC 27006-1. In addition, ETSI EN 319 403-1 will also be taken into account.

1 Scope

5 This document contains requirements for competence, consistent operation and impartiality of conformity assessment bodies performing evaluation and certification of European Digital Identity Wallets under Regulation (EU) 2024/2981, in addition to the requirements contained within ISO/IEC 17065 and ISO/IEC 17025, where relevant.

6 CAB-CB shall be accredited in accordance with ISO/IEC 17065 for the relevant certification schemes.

7 Additionally, in specific schemes, CAB-ITSEF shall be accredited in accordance with ISO/IEC 17025.

8 Both types of CABs shall be accredited by a national accreditation body appointed pursuant to Regulation (EC) No 765/2008.

9 Extensions to ISO/IEC 17065 specified in this document are applicable to all certification schemes, i.e., NL-TL, NL-FS, NL-CS and NL-P-P/W.

10 Extensions of ISO/IEC 17065 relevant to EUCC certification scheme apply to NL-CS, with limitation to the general software and network device area of competence.

11 Extensions to ISO/IEC 17065 that refer to ETSI EN 319 403-1 are applicable only to NL-P-P/W.

12 Additionally, Clause 9 specifies extensions to ISO/IEC 17025 which are relevant for CAB-ITSEF and are applicable to two certification schemes, i.e., NL-FS and NL-CS

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

2 References

2.1 Legal basis

13 The NL EUDI Wallet Certification System will have its foundation in a Dutch National Regulation.

2.2 Normative references

14 The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies, the latest edition of the referenced documents (including any amendments) applies.

15 ISO/IEC 17000, Conformity assessment — Vocabulary and general principles

16 ISO/IEC 17067, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes

17 ISO/IEC 17065, Conformity assessment — Requirements for bodies certifying products, processes and services

18 ISO/IEC 17021-1, Conformity assessment — Requirements for bodies providing audit and certification of management systems, Part 1: Requirements

19 ISO/IEC 17025, Conformity assessment — General requirements for the competence of testing and calibration laboratories

20 ISO/IEC 27006-1 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems, Part 1: General

21 EN ISO/IEC 19896-1, Requirements for the competence of IT security conformance assessment body personnel, Part 1: Overview and concepts

22 ISO/IEC 19896-3, Requirements for the competence of IT security conformance assessment body personnel Part 3: Knowledge and skills requirements for evaluators and reviewers according to the EN ISO/IEC 15408 series and EN ISO/IEC 18045

23 ETSI EN 319 403-1, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

24 EN 17640:2022 + A1:2026, Fixed-time cybersecurity evaluation methodology for ICT products (FITCEM)

2.3 Peer documents

25 NL-SYS-01. PL EUDI Wallet Certification system

26 NL-SYS -02. Vocabulary

27 NL-SYS -03. Organization and support for the owner of the national EUDI certification schemes

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

28 NL-SYS-04. Developing and maintaining the Risk Register for the EUDI Wallet implementation and certification

2.4 Subsidiary Documents

29 NL-TL NL Top Level EUDIW Certification Scheme

30 NL FS EUDI Wallet Solution Functional Certification Scheme

31 NL CS EUDI Wallet Solution Cybersecurity Certification Scheme

32 NL-P-P/W NL eID Scheme Certification Scheme

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

3 Terms and Definitions

3.1 General Terms

33 For the purposes of this document, all terms and definitions are provided in NL-SYS-02 Vocabulary. In addition, terms and definitions from EN ISO/IEC 17000 and ETSI EN 319 403-1.

3.2 Specific Terms

34 In addition, the following terms apply:

- **competence** - ability to apply knowledge, skills and experience as defined in the certification scheme to achieve intended result

  [SOURCE: ISO/IEC 24765:2017, 3.676 modified – the phrase "and relevant personal attributes," replaced with "experience"; the phrase "to achieve intended result" added]

- **assurance continuity –** an approach implemented in the certification system to maintain an assurance baseline in a certified object.

  [SOURCE: adopted from Commission Implementing Regulation No 2024/482, Annex IV]

- **assurance baseline** - refers to the culmination of activities performed by both the evaluator and developer resulting in a certified object, recorded or submitted as evidence and measurable by change to that evidence

  [SOURCE: Assurance continuity: CCRA requirements[1], 2.2 i) modified – 'TOE' replaced with 'object'.]

- **major change** – change that affect assurance baseline of the EUDI Wallet Solution

  [SOURCE: Adoption based on Assurance continuity: CCRA requirements, Chapter 3.]

- **minor change** - change that does not affect assurance baseline of the EUDI Wallet Solution

  [SOURCE: Adoption based on Assurance continuity: CCRA requirements, Chapter 3]

[1] https://www.commoncriteriaportal.org/files/operatingprocedures/CCDB-014-v3.1-2024-February-29-Final-Assurance_Continuity.pdf

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

4 General requirements

4.1 Legal and contractual matters

4.1.1 Legal responsibility

35 The requirements of ISO/IEC 17065, 4.1.1 apply.

4.1.2 Certification agreement

36 The requirements of ISO/IEC 17065, 4.1.2 apply. In addition, the following requirements apply.

- 4.1.2.1 The Applicant/Certificate Holder shall, upon request, make available to CAB-CB or the System Owner or the Supervisory Authority all information and any supporting documentation demonstrating continued compliance with the applicable certification requirements. The information shall be provided without delay.

4.1.3 Use of license, certificates and marks of conformity

37 The requirements of ISO/IEC 17065, 4.1.3 apply. In addition, the following requirements apply.

38 Only the mark of conformity defined in NL-TL applies. No additional marks of conformity shall be used under NL-FS, NL-CS or NL-P-P/W certification schemes.

39 4.1.3.2 The top-level CAB-CB shall be responsible for granting, suspending and withdrawing the right to use the mark of conformity in accordance with the certification decision.

4.2 Management of impartiality

40 The requirements of EN ISO/IEC 17065, 4.2 apply.

41 Additionally, requirements that are specific to the object of certification in respective certification schemes i.e., NL-TL, NL-FS, NL-CS and NL-P-P/W are included in these documents.

4.3 Liability and financing

42 The requirements of EN ISO/IEC 17065, 4.3 apply.

4.4 Non-discriminatory conditions

43 The requirements of EN ISO/IEC 17065, 4.4 apply.

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

4.5 Confidentiality

44 The requirements of EN ISO/IEC 17065, 4.5 apply. In addition, the following requirements apply.

- CAB-CBs shall provide certification reports to the NL National eID Certification System Owner and NL-TL Scheme Owner. The NL National eID Certification System Owner shall ensure custody over all certification-related evidences stemming for the NL-TS, NL-FS, NL-CS or NL-P-P/W certification.
- CAB-CB shall implement necessary and appropriate technical and organizational measures to ensure the confidentiality of all information obtained or generated in the performance of the certification activities, including information related to intellectual property rights. These measures shall apply to all personnel and other individuals granted access to such information.

4.6 Publicly available information

45 The requirements of EN ISO/IEC 17065, 4.6 apply.

5 Structural requirements

5.1 Organizational structure and top management

46 The requirements of EN ISO/IEC 17065, 5.1 apply.

5.2 Mechanism for safeguarding impartiality

47 The requirements of EN ISO/IEC 17065, 5.2 apply.

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

6 Resource requirements

6.1 Conformity Assessment Body personnel

6.1.1 General

48 The requirements of ISO/IEC 17065, 6.1.1 apply.

6.1.2 Management of competence for personnel involved in the certification process

49 The requirements of ISO/IEC 17065, 6.1.2 apply. In addition, the following requirements and guidance apply.

50 6.1.2.1 CAB-CB shall ensure and verify that they have knowledge of:

- detailed and technical knowledge of the relevant architectures of a wallet solution and of the electronic identification scheme;
- the application of specific standards related to the certification scheme according to 7.1.2;
- threats and risks relevant to the architectures;
- available security solutions and of their properties in accordance with the Annex to Implementing Regulation (EU) 2015/1502;
- activities related to functional and cybersecurity certification of components of the wallet solution and the associated electronic identification scheme;
- applicable national certification schemes.

51 Detailed requirements of competence of the personnel are included in Annex A (normative).

- 6.1.2.2 CAB-CB shall establish, implement and operate the competence management system for relevant personnel. The elements of competence, competency levels, knowledge, skills, and experience shall comply with the specific requirements contained in ISO/IEC 18896-1.
- 6.1.2.3 NL-CS: Extensions of ISO/IEC 17065 relevant to EUCC certification scheme apply to CAB-CB with limitation to the general software and network device area of competence.
- 6.1.2.4 NL-TL & NL-P-P/W: Additional requirements from ETSI EN 319 403-1, 6.1.2 regarding the audit process and related competences apply.

6.1.3 Contract with the personnel

52 The requirements of ISO/IEC 17065, 6.1.3 apply.

6.2 Resources for evaluation

6.2.1 Internal resources

53 The requirements of ISO/IEC 17065, 6.2.1 apply. In addition, the following requirements apply.

- 6.2.1.1 Requirements included in ETSI EN 319 403-1, section 6.2.1.1 shall be adopted in the following way:
  - "TSP" is replaced with "in the area of EUDI Wallet solution related services"

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

- 6.2.1.2 Requirements included in ETSI EN 319 403-1, section 6.2.1.2shall be adapted in the following way:
  - "TSP" and "trust services" are replaced with "EUDI Wallet solution related services"
- 6.2.1.3 Requirements included in ETSI EN 319 403-1, section 6.2.1.3 shall be adapted in the following way:
  - "TSP" is replaced with "EUDI Wallet Provider" or "PID Provider", where relevant,
- 6.2.1.4 Requirements included in ETSI EN 319 403-1, section 6.2.1.4 shall be adapted in the following way:
  - "TSP audits" is replaced by "audits of EUDI Wallet solution related services",
  - "trust services" is replaced "EUDI Wallet solution related services, including identity management",
  - "TSP" is replaced with "EUDI Wallet Provider" or "PID Provider", where relevant.
- 6.2.1.5 Requirements included in ETSI EN 319 403-1, section 6.2.1.5 shall be adapted in the following way:
  - "TSP assessments" is replaced with "ISMS assessments".
- 6.2.1.6 Requirements included in ETSI EN 319 403-1, section 6.2.1.6 shall apply.
- 6.2.1.7 Requirements included in ETSI EN 319 403-1, sections 6.2.1.7 and 6.1.8 shall be adapted in the following way:
  - "TSP" and "TSP trust service" are replaced with "EUDI Wallet solution related services"
- 6.2.1.9 Requirements included in ETSI EN 319 403-1, sections 6.2,1.9 shall be adapted in the following way:
  - "TSP audits" is replaced with "ISMS audits"

6.2.2 External resources

54 The requirements of ISO/IEC 17065, 6.2.2 apply. In addition, the following requirements apply.

55 6.2.2.1 CAB-CB may outsource evaluation activities according to a third-party body under the following conditions:

- all subcontractors performing evaluation activities shall, where applicable and appropriate for tasks performed, comply with relevant harmonised standards:
  - ISO/IEC 17025 for conformity testing and IT security evaluations
  - ISO/IEC 17021-1 for auditing
- full responsibility for all evaluation activities outsourced to other bodies shall be retained.
- appropriate measures shall be in place under the CAB-CB accreditation, including reliance on CAB-ITSEF accreditation in NL-FS and NL-CS
- establish procedures for the timing and method for informing the Scheme Owners of any outsourced evaluation activities.

56 In NL-FS and NL-CS, CAB-ITSEF accredited to ISO/IEC 17025 are required.

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

7 Process requirements

7.1 General requirements

57 The requirements of ISO/IEC 17065, 7.1 apply.

58 In addition, requirements of ETSI EN 319 403-1, 7.1 are adapted in the following way:

- "TSP and the trust service(s)" are replaced with "EUDI Wallet Provider and EUDI Wallet solution related services" or "PID Provider and EUDI Wallet solution related services, where relevant.

7.1.1 Object of certification

59 According to CIR (EU) 2024/2981 art 3(3), the object of certification includes the following elements:

- the software components, including settings and configurations of the wallet solutions and of the electronic identification scheme under which the wallet solutions are provided;
- the hardware components and platforms on which the software components referred to in point (a) run on or rely upon for critical operations, in cases where they are provided directly or indirectly by the wallet solution and electronic identification scheme under which they are provided and when they are required to meet the desired level of assurance for those software components;
- the processes that support the provision and operation of a wallet solution, including the user onboarding process as referred to in Article 5a of Regulation (EU) 2024/1183, covering at least enrolment, electronic means management and organisation pursuant to section 2.1, 2.2, and 2.4 of Annex I to Implementing Regulation (EU) 2015/1502.

7.1.2 Certification system framework

60 The certification system consists of multiple certification schemes, each covering defined aspects of the overall framework. For each object of certification, a specific certification scheme is established, including applicable product or service requirements. All schemes are based on ISO/IEC 17065 as the conformity assessment standard. The schemes are listed in Table 1.

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

Table 1 Certification system framework

Object to be certified	Certification scheme	Evaluation method	Product or service requirements	Applicant
Providing of the EUDI Wallet solution (Service)	NL-TL & NL-WP	Audit	NL-P-P/W-* specifications-	EUDI Wallet Provider
The issuing of PIDs to Wallet end users (Service)	NL-PP	Audit	NL-P-P-* specifications	PID Provider
Wallet solution cybersecurity (Product)	NL-CS	IT security evaluation	NL-CS-* - specifications	EUDI Wallet Provider
Wallet solution functional (Product)	NL-FS	Testing	NL-FS-*- specifications	EUDI Wallet Provider

For full list of specifications – see NL-SYS-NL

7.1.3 Certification hierarchy

61 Certification of the EUDI Wallet solution shall follow a certification hierarchy consisting of top-level certification supported by subsidiary scheme-level certifications granted to respective providers. The hierarchy is illustrated in Figure **1**.

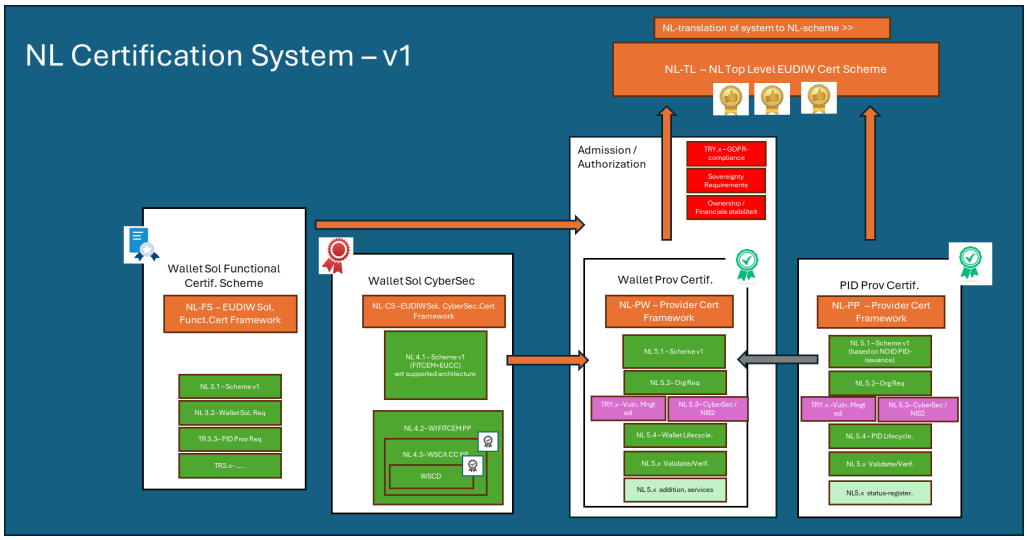


Figure 1 – Certificate Composition

62 Individual Wallet Providers authorized to be active in the national EUDI scheme shall hold a valid top-level certificate, whereby the Supervisory Authority shall ensure that it is notified to the European Commission in accordance with Article 5d of Regulation (EU) 2024/1183.

63 The top-level certificate shall cover Wallet Provider Certificate (in combination with the offered Wallet Solutions), the Wallet Provider's compliance with the admission criteria and the PID-provider Certificate. Otherwise stated, top-level certificate shall confirm the conformity of and the Digital Identity Wallets and the and the electronic

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

identification scheme under which they are provided (which includes certification and admission criteria).

64 Each actor within relevant scheme shall hold a valid certification covering the requirements applicable to its designated role. The allocation of requirements to roles is defined in the applicable certification scheme documents (NL-TL, NL-FS, NL-CS and NL-P-P/W series). Where an entity performs multiple roles, it shall hold certification for each product or service.

65 When performing evaluation activity towards the top-level certification, CAB-CB may rely on the scheme-level certifications as assurance information, in accordance with NL-SYS-01. Where such certifications are relied upon, CAB-CB shall verify their validity and scope and shall not re-evaluate requirements already covered by those certifications.

66 The top-level certification shall not be issued or maintained if their valid certification is lacking for any components included in the EUDI wallet solution (product or service).

67 The top-level certificate shall not be issued or maintained unless all elements of the object of certification specified in section 7.1.1 are covered by valid certificates.

7.1.4 Certification scheme

68 For each element of the object of certification, CAB-CB shall operate a certification scheme consistent with a Type 5 product certification scheme or a Type 6 service certification as defined in ISO/IEC 17067 as applicable. The certification process shall include:

- II. Determination of characteristics, through testing and audit (see 7.4);
- III. Review, the information and result of the evaluation (see 7.5);
- IV. Decisions on certification, granting, maintaining, extending, reducing, suspending and withdrawing certification (see 7.6);
- V. Attestation, licensing, issuing a certificate and granting the right to use certificates and marks (see 7.7);
- VI. Surveillance, evaluation of the operation of the process and audit of the management system (see 7.9).

7.2 Application

69 The requirements of ISO/IEC 17065, 7.2 apply.

7.3 Application Review

70 The requirements of ISO/IEC 17065, 7.3 apply. In addition, the following requirements apply.

- Where the applicable certification scheme requires the Applicant to hold valid certificates under other certification schemes, CAB-CB shall, as part of the application review, verify the existence, validity and scope of those certificates.
- In case evaluation and certification processes under NL-FS or NL-CS are in progress, based on the Applicant declaration, CAB-CB shall determine the status if

it does not restrict starting the process under NL-PW certification scheme. CAB-CB shall record the basis for its determination.

- In case evaluation and certification processes under NL-WP or NL-PP are in progress, based on the Applicant declaration, CAB-CB shall determine the status if it does not restrict starting the process under NL-TL certification scheme. CAB-CB shall record the basis for its determination

7.4 Evaluation

71 The requirements of ISO/IEC 17065, 7.4 apply.

72 In addition, the following requirements apply.

- Requirements included in ETSI EN 319 403-1, sections 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.5, shall be adapted in the following way:
  - "TSP" is replaced with "EUDI Wallet Provider" or "PID Provider", and provision of their services, where relevant,
  - "trust services" is replaced with "EUDI Wallet solution related services"

7.5 Review

73 The requirements of ISO/IEC 17065, 7.5 apply. In addition:

- The requirements of ETSI EN 319 403-1, 7.5 apply.

7.6 Certification decision

74 The requirements of ISO/IEC 17065, 7.6 apply.

7.7 Certification documentation

75 The requirements of ISO/IEC 17065, 7.7 apply.

76 In addition, the following requirements apply:

- The certification documentation shall contain the following:

  a) unique identification code;

  b) name and version of the object of certification;

  c) name of the electronic identification scheme and the Member State, where applicable;

  d) name, address and contact information of the Applicant;

  e) link to the website of the Applicant containing the information that is required to be made publicly available under the applicable certification scheme and, for Wallet Providers, WZ-03-01, Section 5.1.4, and WZ-03-03, Section 5.1.4;

  f) name, address and contact information of the CAB-CB;

  h) name of the Scheme Owner;

  i) references to Regulation (EU) 910/2014 and to Regulation (EU) 2024/2981;

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

j) reference to the public certification report;

k) reference to the standards used for the evaluation, including their versions; i.e. applicable version of each GP-series document against which the evaluation was performed;

m) the scope of the certification, including any limitations;

n) name of the EUDI Wallet provider or PID provider;

- the assurance level.
  - 7.7.2 CAB-CB shall issue a new certification documentation where an evaluation, including surveillance or re-evaluations, identifies changes to the object of certification. The new certification documentation shall retain the expiry date of the original certification documentation.

7.8 Directory of certified products / services

77 The requirements of ISO/IEC 17065, 7.8 apply.

78 In addition, the following requirements apply.

- 7.8.1 CAB-CB shall notify the Scheme Owner and Supervisory Authority of the issuance, termination (at the client's request), suspension and withdrawal of certificate.

7.9 Surveillance

79 The requirements of ISO/IEC 17065, 7.9 apply.

80 7.9.1 Requirements included in ETSI EN 319 403-1, 7.9 shall be adapted in the following way:

  - "TSP" is replaced with "EUDI Wallet Provider" or "PID Provider", and "provision of their service", where relevant.

81 In addition, the following requirements apply.

- 7.9.2 CAB-CB shall ensure that surveillance activities include verification that:

  a) the Certificate Holder complies with the applicable certification scheme specified in 7.1.2 and the national certification schemes;

  b) the certified object of certification continues to meet the requirements set out in 7.1.2 and in the national certification schemes;

- 7.9.3 CAB-CB shall also conduct surveillance activities based on the following information:

  a) information from national accreditation bodies, and relevant market surveillance authorities;

  b) information resulting from audits and investigations conducted by the certification body or other competent authorities;

  c) complaints and appeals.

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

- 7.9.4 CAB-CB may conduct special evaluations. A special evaluation may be initiated either at the request of the Certificate Holder or by CAB-CB in response to a specific issue, such as a vulnerability notification, or market surveillance authority.
- 7.9.5 The scope of a special evaluation shall be clearly defined and limited to the activities necessary to address the specific issue that triggered it.

7.10 Changes affecting certification

82 The requirements of ISO/IEC 17065, 7.10 apply.

83 In addition, the following requirements apply.

- 7.10.1 Requirements included in ETSI EN 319 403-1, sections 7.4.0-7.4.7 shall be adapted in the following way:
  - "TSP" is replaced with "EUDI Wallet Provider" or "PID Provider", and provision of their service, where relevant.
- 7.10.2 CAB-CB shall perform evaluation activities following changes to the certification scheme, including:
  - a revision of the certification scheme;
  - the publication of new specifications or standards; or
  - the publication of new versions of such specifications or standards,
- 7.10.3 CAB-CB shall take appropriate actions in accordance with information provided by the Scheme Owner.
- 7.10.4 CAB-CB shall perform evaluation activities following other changes affecting the certification, including:
  - the addition of a new wallet provider or PID provider to the scheme, or the removal of an existing wallet provider or PID provider from the scheme, if applicable;
  - a change in the identity or legal status of an existing wallet provider or PID provider within the scheme, if applicable;
  - material changes to the architecture or design of the wallet solution;
  - material changes to the enrolment or identity proofing processes;
  - significant security incident;
  - a suspension or withdrawal of certification of associated components certified by the same or other accredited certification bodies (see 7.1.3 and NL-SYS-03, Section 8.11)
  - material changes to the scheme risk register.
- 7.10.5 CAB-CB shall establish, implement and maintain a process for managing changes to the object of certification and to the conditions under which certification was granted.
- 7.10.6 CAB-CB shall determine whether changes to the object of certification or to the threat environment require additional evaluation activities. A special evaluation may also be initiated at the request of the Certificate Holder.
- 7.10.7 CAB-CB shall determine and implement appropriate actions in response to such changes. These actions shall include, as applicable:

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

- additional evaluation activities;
- review of the evaluation results;
- issuance of revised certification documentation;
- changes to surveillance activities.

- 7.10.8 CAB-CB shall record the rationale for excluding any of these actions.

7.11 Termination, reduction, suspension or withdrawal of certification

84 The requirements from ISO/IEC 17065, 7.11 shall apply.

85 In addition, the following requirements apply.

- 7.11.1 If the certification requirements are not met, CAB-CB shall:
  - inform the Certificate Holder of any non-conformity and require them to take appropriate remedial actions;
  - notify relevant market surveillance authorities when the non-conformity concerns applicable Union legislation;
  - ensure that the Certificate Holder is informed of the conditions for:
    - carrying out remedial actions.
    - suspension of the certification and restore the certification once the non-conformity has been resolved.
    - withdrawal of the certification.
- 7.11.2 CAB-CB shall suspend the certification without undue delay once it confirms that a reported security breach or compromise affects compliance with the applicable national certification scheme.
- 7.11.3 CAB-CB shall withdraw the suspended certification if the necessary corrective actions have not been completed within an appropriate timeframe.
- 7.11.4 CAB-CB shall withdraw the certification if an identified vulnerability has not have been resolved in a timely manner considering its severity and potential impact.
- 7.11.5 In addition, the following conditions shall provide as a basis for suspension or withdrawal:
  - the certification under the NL-FS, NL-CS or NL-PP/WP certification scheme is suspended or withdrawn, and no alternative certified wallet solution is available within the scheme;
  - the Scheme Owner is unable to demonstrate continued compliance with the governance requirements of NL-SYS-01 and/or NL-TL.

7.12 Records

86 The requirements of ISO/IEC 17065, 7.12 apply.

87 In addition, the following requirements shall apply.

- 7.12.1 Records shall be retained in accordance with NL-SYS-01, section 5.10.

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

7.13 Complaints and appeals

88 The requirements of ISO/IEC 17065, 7.13 apply.

89 In addition, the following requirements apply.

- 7.13.1 CAB-CB shall forward to the Scheme Owner any complaints or appeals that cannot be resolved for further assessment and resolution.

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

8 Management system requirements

8.1 Options

90 The requirements from ISO/IEC 17065, 8.1 shall apply.

8.2 General management system documentation

91 The requirements from ISO/IEC 17065, 8.2 shall apply.

8.3 Control of documents

92 The requirements from ISO/IEC 17065, 8.3 shall apply.

8.4 Control of records

93 The requirements from ISO/IEC 17065, 8.4 shall apply.

8.5 Management review

94 The requirements from ISO/IEC 17065, 8.5 shall apply.

8.6 Internal audits

95 The requirements from ISO/IEC 17065, 8.6 shall apply.

8.7 Corrective actions

96 The requirements from ISO/IEC 17065, 8.7 shall apply.

8.8 Preventive actions

97 The requirements from ISO/IEC 17065, 8.8 shall apply.

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

9 Additional provisions regarding accreditation requirements for CAB-ITSEF

98 For NL-FS and NL-CS, CAB-ITSEF shall be accredited to ISO/IEC 17025 within the scope resulting from the characteristics of the object of certification.

99 Additionally, the following requirements apply.

- CAB-ITSEF shall implement necessary and appropriate technical and organizational measures to ensure the confidentiality of all information obtained or generated in the performance of the certification activities, including information related to intellectual property rights. These measures shall apply to all personnel and other individuals granted access to such information. Certification of the CAB-ITSEF information security management system with the scope covering its laboratory activities is considered sufficient to meet this requirement.
- Extensions of ISO/IEC 17025 relevant to EUCC certification scheme apply to Nl-CS, with limitation to the general software and network device area of competence.
- Managing of personnel competence applicable to NL-FS and NL-CS shall comply with ISO/IEC 19896-1.

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

10 Transition

100 In the context of an accreditation process, CAB-CB may engage, under the supervision of the NAB and the Scheme Owner, in required certification activities that should be witnessed by the NAB.

101 In the context of accreditation, the CAB-ITSEF may engage, under the supervision of the NAB and the Scheme Owner, engage in the required conformity testing and cybersecurity evaluation activities, which should be witnessed by the NAB.

102 The issuance of certificates upon successful performance of all evaluation and certification activities requires that the CAB-CB is accredited.

103 The Applicant and all parties involved in these activities shall be fully aware of their status and accept the risks associated with the possibility that the CAB-CB or CAB-ITSEF may not ultimately be accredited.

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

Annex A Competence requirements for the EUDI Wallet Certification

104 *NOTE: All requirements are applicable to both CAB-CB and CAB-ITSEF unless otherwise stated.*

A.1 Foundational Principles

105 CAB-CBs shall demonstrate the capability to perform system-level certification based on heterogeneous assurance inputs, without re-certifying components. This includes:

- Integrating external certifications, test reports, and assurance artefacts into a coherent system-level judgment,
- Applying risk-based reasoning where assurance is partial, indirect, or inherited,
- Ensuring traceability between system requirements and supporting evidence, regardless of origin.

106 This requirement IS NOT applicable to CAB-ITSEF.

A.2 Competence framework

A.2.1. Interpretation of external certifications

107 CAB shall be able to:

- Assess scope, assurance level, and applicability of third-party certifications,
- Interpret Security Targets, Protection Profiles, and certification reports,
- Identify limitations, assumptions, and residual risks in external evaluations.

108 CAB-ITSEF shall be able to evaluate Security Targets and Protection Profiles.

A.2.2. Composition and Assurance Integration Competence

A.2.2.1. Evidence Integration

109 CAB shall:

- Combine heterogeneous assurance artefacts (certifications, test results, audit reports) into a unified assessment,
- Ensure consistency across different assurance sources.

A.2.2.2. Dependencies and Trust Analysis

110 CAB-CB shall:

- Identify trust dependencies between components and services,
- Evaluate whether assumptions made in one component certification remain valid in the composed system.

A.2.2.3. Composition Risk Management

111 CAB shall:

- Assess emergent risks arising from component interaction,
- Validate that interfaces and integrations do not invalidate existing assurances.

A.2.3. Regulatory Mapping and Coverage Analysis

A.2.3.1. Requirement Traceability

112 CAB shall:

- Map European Identity Wallet requirements to available assurance evidence,
- Maintain bidirectional traceability between requirements and demonstration of conformity of components and services.

A.2.3.2. Gap Identification and Treatment

113 CAB shall:

- Identify coverage gaps in external certifications or assurance evidence.
- Define compensating controls, additional evidence, or targeted evaluations.

A.2.4. Technical Cybersecurity Competence

A.2.4.1. Evaluation of Technical Evidence

114 CAB shall be capable of:

- Assessing system architecture and trust boundaries,
- Assessing secure design and implementation practices,
- Performing vulnerability assessments and assessing penetration test results,
- Performing ISMS assessment.

115 CAB-ITSEF shall be capable of performing vulnerability assessment, devising and performing penetration tests.

A.2.4.2. Cryptographic and Trust Services Expertise

116 CAB shall:

- Understand cryptographic mechanisms and key management,
- Evaluate resistance to advanced attack scenarios (e.g., high attack potential),
- Assess secure communication and identity-binding mechanisms

117 CAB-ITSEF shall be capable of performing evaluation of cryptographic mechanisms and key management.

A.2.5. Lifecycle and Supply Chain Assurance

A.2.5.1. Secure Lifecycle Assessment

118 CAB shall assess:

- Development, integration, deployment, and maintenance processes,

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

- Vulnerability handling, secure update and patch management mechanisms.

A.2.5.2. Supply Chain and Third-Party Risk

119 CAB shall:

- Assess supplier trustworthiness and dependency risks,
- Verify integrity of manufacturing, provisioning, and distribution processes.

A.2.6. ICT Services and Operational Security Assessment

A.2.6.1. Service-Level Assurance

120 CAB shall:

- Asses the evaluation of operational environments supporting the wallet,
- Assess identity, authentication, and trust service integration.

A.2.6.2. Management Systems and Compliance

121 CAB shall be competent in assessing:

- Information Security Management Systems aligned with standards such as EN ISO/IEC 27001, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, CIS Critical Security Controls, relevant ETSI standards.
- Regulatory frameworks that include NIS2 Directive.

A.2.7. Reporting, Traceability, and Justification

A.2.7.1. Structured Reporting

122 CAB shall:

- Produce clear, structured, and auditable assessment reports,
- Ensure traceability from findings to evidence and requirements.

123 CAB-ITSEF shall produce clear structured and traceable technical reports based on findings to evidence and requirements.

A.2.7.2. Justification of Certification Decisions

124 CAB shall:

- Clearly justify how external evidence supports certification claims,
- Explicitly document assumptions, limitations, and residual risks.

A.2.8. Independence, Impartiality, and Governance

A.2.8.1. Impartial Use of External Evidence

125 CAB shall:

- Evaluate third-party evidence without undue reliance or bias,
- Maintain independence from component developers and certifiers or evaluators, where relevant.

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

A.2.9. Stakeholder Coordination and Ecosystem Awareness

A.2.9.1. Multi-Party Coordination

126 CAB shall effectively interact with:

- Wallet providers,
- Third-party certification bodies or testing laboratories,
- National authorities (e.g., cybersecurity certification authorities)

A.2.9.2. Vulnerability and Incident Handling

127 CAB shall:

- Verify processes for vulnerability disclosure and remediation,
- Ensure alignment with coordinated vulnerability disclosure practices.

A.2.10. Continuous Assurance and Post-Certification Activities

A.2.10.1. Ongoing Compliance

128 CAB-CB shall:

- Follow defined mechanisms for surveillance, reassessment, and change management

129 CAB-ITSEF shall cooperate with CAB-CB in post-certification activities.

A.2.10.2. Residual Risk and Monitoring

130 CAB-CB shall:

- Evaluate and document residual risks at EUDI Wallet level and document the result of the evaluation
- Recommend monitoring and mitigation strategies.

131 This requirement IS NOT applicable to CAB-ITSEF.

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