

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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



NL-P-P

NL EUDI Wallet Certification System

PID Provider Certification Scheme

RC1.1

2026.10.31

Document reference	NL-P-P
Version	RC1.1
Status	Release Candidate
Date	27/10/206
Document type	Certification Scheme Scheme Specification (EN ISO/IEC 17067)
Parent framework	NL-SYS-01, NL-SYS-02, NL-SYS-03, NL-SYS-04, NL-SYS-05
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	European Digital Identity PID Providers (and the Wallet Solutions provided)
Primary audience	Scheme Owners, CABs, EUDI PID Providers
Secondary audience	EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Subsidiary Documents	NL-P-01, NL-P-02, NL-P-03, as well as NL-P-P04 and NL-P-P04b

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

Version	Change	State	Date
RC1.0	First Consolidated Version following European Collaboration and Refinement Discussion with BZK-Policy Department and Legal.	Release Candidate	2026-10-27
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 Foreword 6
2 Scope 7
3 Legal Basis 8
4 References 9
4.1 Standards and technical specifications 9
4.2 Parent documents 9
4.3 Peer documents 9
4.4 Subsidiary Documents 9
5 Terms and Definitions 10
6 Certification Scheme Structure 11
6.1 Object of Certification 11
6.2 Roles and Responsibilities 11
6.3 Mechanisms to ensure impartiality 12
6.4 Relationship to NL-P-W 12
6.5 Relationship to NL-P-01/02/03/04 Subsidiary Documents 12
6.6 Scheme Type 13
6.7 Use of certification and marks of conformity 13
7 Evaluation Framework 14
7.1 General 14
7.2 Scope of Evaluation 14
7.3 Evaluation Methods 15
7.4 Types of evidence 15
7.5 Proportionality 15
7.6 Acceptability and re-use of assurance evidence 16
7.7 Evaluation criteria 16
8 Certification Process 18
8.1 General 18
8.2 Preparation and application phase 18
8.3 Evaluation phase 18
8.4 Certification phase 19
8.5 Evaluation and certification efforts 19
8.6 Additional provisions 19
8.7 Certificate of conformity 20
8.8 Surveillance 20
8.9 Recertification 21
8.10 Suspension, Termination or Withdrawal of certificate 21
8.11 Implications of NL-P-P Certificate Changes 22
8.12 National legislation 22
8.13 Certification contracts 22
8.14 Costs 23
9 Final provisions 24
9.1 National legislation 24
9.2 Certification contracts 24
9.3 Costs 24

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

Annex A (Normative) — Allocation of Requirements to Subsidiary Documents 25
Annex B (Normative) Audit framework 27
Annex C (Normative) Minimum contents of an audit plan 37
Annex D (Normative)- Minimum contents of an audit evidence record 38
Annex E (Normative) Evaluation results matrix 39

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

1 Foreword

1 This document (NL-P-P) presents the specification for the PID Provider Certification Scheme, one of Certification Schemes within the NL EUDI Wallet Certification System. It defines the Certification Scheme — in the sense of ISO/IEC 17067 — the accredited and authorized Certification Body (CAB) shall apply when certifying the NL PID Provider.

2 This document should be read in conjunction with the NL Certification System overarching documents, notably NL-SYS-01.

3 NL-P-P is primarily addressed to the CAB that conducts the certification activities related to the PID provider under the NL Certification System. The PID Provider should read this document in conjunction with the applicable NL-P-* subsidiary documents, which specify the requirements it shall meet.

4 This document is part of the NL-P-*, which operates within the NL Certification System (Governance). It should especially be read in conjunction with NL-SYS-01 (NL EUDI Wallet Certification System) and NL-SYS-03 (Organization and support for the owner of the national EUDI certification system).

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

2 Scope

5 The document specifies the Certification Scheme for the PID Provider that is to be certified as the "foundational trust anchor" of the Dutch National eID Scheme ("Stelsel").

6 The object of certification is the PID Provider, comprising the organizational arrangements and processes of the PID Provider that are related to the issuance and lifecycle management of the PID to certified wallets of respective citizens.

7 The object of certification encompasses all services that support the provision and operation of services that support the controlled issuance and lifecycle management related to PIDs and transversal services that support the trust in the overall eID national scheme (like user dashboard and notification in order to combat fraud).

8 NL-P-P establishes the evaluation methodology (by reference to normative Annex B), the service requirements (see requirements in the subsidiary documents) and the conformity assessment procedures that accredited CABs shall apply when certifying the PID provider of the NL National eID scheme ("Stelsel"). It is intended to be read in conjunction with NL-SYS-05, which specifies the accreditation requirements on the certification bodies themselves.

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

3 Legal Basis

9 The Certification Scheme defined in this document is established pursuant to the following legal instruments:

1) Regulation (EU) 910/2014, in particular Articles 5a and 5c.
2) Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 on the certification of European Digital Identity Wallets, in particular Articles 3–5, 8, 12–14 and 19 and Annexes I–VII.
3) Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 on the integrity and core functionalities of European Digital Identity Wallets.
4) Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 on person identification data issued to European Digital Identity Wallets.
5) Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on assurance levels for electronic identification means, the Annex, Section 2.4.
6) Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 on cybersecurity risk-management measures.
7) Commission Implementing Regulation (EU) 2026/798 of 7 April 2026 laying down rules for the application of Regulation (EU) 910/2014 of the European Parliament and of the Council as regards reference standards and specifications for the remote onboarding of users to the European Digital Identity Wallets by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures where the combination meets the requirements of assurance level high
8) Regulation (EU) 765/2008 on accreditation and market surveillance, in particular Articles 4 and 5.

10 In addition, the EUDI Wallet Certification Scheme will comply with:

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

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

4 References

4.1 Standards and technical specifications

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

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

4.2 Parent documents

13 NL-SYS-01. NL EUDI Wallet certification system

14 NL-SYS-02. Vocabulary

15 NL-SYS-03. Organization and support for the owner of the national EUDI certification system

16 NL-SYS-04. Developing and maintaining the risk register for EUDI Wallet implementation and certification

17 NL-SYS-05. Accreditation requirements for CABs

4.3 Peer documents

18 NL-FS. EUDI Wallet Functional Certification Scheme

19 NL-CS. EUDI Wallet Cybersecurity Certification Scheme

4.4 Subsidiary Documents

20	NL-P-01	Org. and Techn. requirements for Wallet & PID providers
21	NL-P-02	Essential Entity Requirements
22	NL-P-03	Development & Vulnerability Mngt Requirements
23	NL-P-P04	PID Issuance & Lifecycle Mngt Requirements
24	NL-P-P04b	Fraud Mngt Requirements

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

5 Terms and Definitions

25 For the purposes of this document, all terms and definitions are provided in NL-SYS-02 Vocabulary.

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

6 Certification Scheme Structure

6.1 Object of Certification

26 The object of certification under this scheme is the PID Provider that issue PIDs in the NL National eID scheme ("stelsel"), as referred to in Article 5c(1) of Regulation (EU) 2024/1183. The certification covers both the scheme-level governance arrangements and the operational services provided by the PID Provider.

27 The CAB shall assess the conformity of the object of certification against the set of requirements established in the subsidiary documents, as allocated in Table 1 below.

28 *NOTE: In the context of NL-P-P certification scheme only a certification body that is accredited and also authorized under Dutch law is eligible as CAB.*

Table 1 Allocation of requirements documents to roles

Document	Title
NL-P-01	Organisational and technical requirements for Wallet & PID providers
NL-P-02	Essential Entity Cyber Resilience Requirements
NL-P-03	Development & Vulnerability Mngt Requirements
NL-P-P04	PID Issuance & Lifecycle Mngt Requirements
NL-P-P04b	Fraud Mngt Requirements

6.2 Roles and Responsibilities

6.2.1 Overview of the scheme stakeholders

29 The overview of the roles and responsibilities is presented in Table 2.

Table 2 Overview of Roles and Responsibilities

Role	Responsibilities	Normative basis
Scheme Owner	Owns and supervises the scheme; authorises CABs; maintains certificate register; monitors the scheme.	ISO/IEC 17067
CAB	Plans, performs and documents the evaluation; issues the certification decision and certificate of conformity; manages surveillance and recertification activities.	ISO/IEC 17065; NL-SYS-05
Applicant / Certificate Holder	Submits the eID scheme for certification; provides evaluation evidence; complies with post-certification obligations including surveillance cooperation and change notification.	NL-P-P
National Accreditation Body (NAB)	Accredits CABs in accordance with ISO/IEC 17065 for the relevant scope under this scheme.	Regulation (EC) No 765/2008
Market Surveillance Authorities	Oversight of certified services in the market. This role will be performed by the NL-TL Scheme Owner.	ISO/IEC 17067; NL-TL

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

6.2.2 Accreditation of CABs

30 CABs operating under this scheme shall be accredited by the National Accreditation Body in accordance with ISO/IEC 17065 with a scope covering the NL-P-P and subsidiary documents. The required competences and other accreditation requirements are specified in NL-SYS-05.

31 General provisions on CAB accreditation, including requirements for accreditation scope and recognition of accreditation granted by other national accreditation bodies within the EU, are set out in NL-SYS-01 and NL-SYS-05.

6.3 Mechanisms to ensure impartiality

32 The CAB is obliged to implement mechanisms to ensure impartiality in accordance with ISO/IEC 17065. General provisions on impartiality requirements are set out in NL-SYS-05.

6.4 Relationship to NL-P-W

33 NL-P-P is one of the Certification Schemes within the NL-SYS-01 EUDI Wallet Certification System. The NL-P-W (EUDI Wallet Provider Certification Scheme) addresses the certification of Wallet Providers that co-exist in the same National eID Scheme ("stelsel") as per art 5c (1) of REGULATION (EU) 2024/1183 and which rely on the PID provider to provide a PID to their certified and admitted wallets.

6.5 Relationship to NL-P-01/02/03/04 Subsidiary Documents

34 The subsidiary documents of NL-P-P (NL-P-01/02/03 and NL-P-P04/W04b) — constitute the normative substance of the eID Certification Scheme. They specify, respectively:

- NL-P-01 Org. and Techn. requirements for Wallet & PID providers, which describes the management and operational requirements for this essential trust anchors of the NL National eID Scheme.
- NL-P-02 Essential Entity Requirements, which describes --in the spirit of NIS2-- the cyber resilience requirements that Wallet and PID Providers need to meet.
- NL-P-03 Development & Vulnerability Mngt Requirements, which describes --in the spirit of the CRA-- which development and vulnerability management practice need to be met.
- NL-P-P04 PID Issuance & Lifecycle Mngt Requirements, which elaborates requirements that need to be met during the PID Issuance process as well as during lifecycle events as to ensure PIDs are issued and remain under control of the correct citizen and his/her walle..
- NL-P-P04b Fraud Mngt Requirements, which elaborates requirements that should additionally be met to ensure the service and the overall NL national eID scheme ("stelsel") has resistance against fraud modus operandi.

35 ***NOTE —*** *Annex A of this document provides the normative allocation of legal requirements to subsidiary documents. This allocation confirms which subsidiary*

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

document implements each legal requirement derived from the relevant EU instruments.

6.6 Scheme Type

36 This certification scheme follows the Type 6 model as defined in EN ISO/IEC 17067, which includes initial testing and evaluation, surveillance of the service delivery, and periodic re-evaluation. The scheme specifies the elements listed in Section 6.5 of ISO/IEC 17067, in accordance with Article 4(3), point (a) of Commission Implementing Regulation (EU) 2024/2981.

6.7 Use of certification and marks of conformity

37 The PID provider will not carry any mark of conformity. But any suspension or revocation will have an immediate effect on the top-level certificates of all Wallet Providers in the NL national eID scheme ("stelsel").

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

7 Evaluation Framework

7.1 General

38 This section specifies a general evaluation methodology for CABs to apply when evaluating the conformity of the electronic identification system and services related to this system with the requirements specified in the NL-P-01/02/03 and NL-P-P04/P04b.

39 The evaluation activities shall follow the process requirements set out in NL-SYS-05 (Section 7), and shall be planned, performed and documented in accordance with the procedures established by the CAB.

40 The evaluation activities shall consider the minimum requirements for evaluating the electronic identification scheme set out in Annex VI of Commission Implementing Regulation (EU) 2024/2981, including the assessment of the risk register.

7.2 Scope of Evaluation

41 The scope of the evaluation shall encompass services related to provision and operation of PID Issuance and Lifecycle Management in context of the NL national eID scheme ("stelsel"). As a minimum, the evaluation shall cover:

- Org. and Techn. requirements for Wallet & PID providers, which describes the management and operational requirements for this essential trust anchors of the NL National eID Scheme as specified in NL-P-01.
- Essential Entity Requirements, which describes --in the spirit of NIS2-- the cyber resilience requirements that Wallet and PID Providers need to meet as specified in NL-P-02.
- Development & Vulnerability Mngt Requirements, which describes --in the spirit of the CRA-- which development and vulnerability management practice need to be met as specified in NL-P-03.
- PID Issuance & Lifecycle Mngt Requirements, which elaborates requirements that need to be met during the PID issuance process as well as during lifecycle events as to ensure the PID stays under control of the correct citizen, as specified in NL-P-P04
- Fraud Mngt Requirements, which elaborates requirements that should additionally be met to ensure the PID-issuance service has resistance against fraud modus operandi, as-well-as transversal services that support the trust in the overall eID national scheme (like user dashboard and notification in order to combat fraud). as specified in NL-P-P04b

42 Where the scheme relies on services provided by third parties (outsourced or subcontracted services), the scope of the evaluation shall extend to those services to the extent that they are material to the fulfilment of the certification requirements.

43 Where external assurance evidence is available and evaluated as acceptable in accordance with Section 7.6, the CAB may reduce the extent of its own evaluation activities for the requirements covered by that assurance evidence. The scope of the certification shall not be reduced based on external assurance evidence.

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

7.3 Evaluation Methods

44 The CAB shall use one or more of the following evaluation methods, as appropriate to the nature of the requirement being evaluated.

- Document review — examination of policies, procedures, records, contracts, risk assessments, and other documented information.
- Interview — structured discussions with relevant personnel of the Provider or Scheme Owner to verify understanding, implementation, and operational effectiveness of the requirements;
- Observation — direct observation of processes, systems, facilities, and operational practices at Provider and any other relevant sites;
- Technical testing — testing of technical controls, including vulnerability assessments, configuration reviews, and security testing, as appropriate to the nature and risk level of the systems under evaluation;
- Sampling — where the complete evaluation of all instances of a recurring process is impracticable, the CAB may employ sampling in accordance with the trust justification requirements. The sampling methodology shall be documented in the evaluation plan.

45 The CAB shall determine the appropriate combination of evaluation methods for each evaluation activity, considering the nature of the requirement, the level of risk, the maturity of the Provider's management systems.

7.4 Types of evidence

46 The CAB shall obtain sufficient and appropriate evidence to support its evaluation conclusions. Evidence may include, but is not limited to documented policies, procedures and records maintained by the Provider;

- system configurations and technical documentation regarding the services provided by the PID Provider as-well-as regarding fraud limiting services supporting the NL national eID System ("stelsel") it operates;
- results of technical testing and security assessments;
- audit trails and log records from the server-side infrastructure operated by the PID Provider in the live operational environment — that is, systems serving real users in authentic transactions, as distinct from test, pilot, or reference environments — including back-end systems for PID (and attestation) issuance and revocation, event logging, and interfaces with other EUDI Wallet ecosystem components;
- valid certificates for the (Qualified) eSealing services it uses and/or QeSCDs it operates.
- external assurance evidence evaluated in accordance with Section 7.6;
- statements, explanations, and demonstrations provided by PID Provider, PID Provider and Scheme Owner personnel;
- results of sampling activities;
- reports from previous evaluations or certifications, including any regulatory or supervisory assessments.

47 The CAB shall document the evidence obtained and shall retain it in accordance with the record-keeping requirements set out in NL-SYS-01, section 5.10.

7.5 Proportionality

48 In the application of the requirements, the following principles of proportionality shall apply:

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

- All requirements derived from Commission Implementing Regulation (EU) 2015/1502, Section 2.4, shall be understood as commensurate to the risks at assurance <identity proofing> level High, in accordance with the introductory provision of that section.
- All requirements derived from Commission Implementing Regulation (EU) 2024/2690 shall be applied taking due account of the degree of PID Provider exposure to risks due to the functionalities it supports, accesses/exchanges it enables, attack surface it is exposed to and the likelihood of occurrence of incidents and their severity, in accordance with Article 2(2) of that regulation.
- Where Commission Implementing Regulation (EU) 2024/2690 provides that a technical or methodological requirement shall be applied "where appropriate", "where applicable" or "to the extent feasible", and PID Provider considers it not appropriate, not applicable or not feasible, the PID Provider shall document its rationale in a comprehensive manner. The CAB shall evaluate the adequacy and substantiation of such rationale.

49 The CAB shall consider the risk register content (meeting the minimum content requirements specified in NL-SYS-04) when determining the depth and focus of the evaluation activities, giving particular attention to risks arising from the integration of their Wallet(s) with the NL PID-provider.

7.6 Acceptability and re-use of assurance evidence

50 NOTE 1: The rules for acknowledging evidence from external sources are specified in NL-SYS-01, section 5.3.

51 In accordance with Article 13(1), point (f) of Commission Implementing Regulation (EU) 2024/2981 and Annex VI thereof, the CAB shall, as part of the evaluation, evaluate the acceptability of assurance evidence provided by the PID Provider.

52 The CAB decision on acceptability and further re-use of assurance evidence shall be made in compliance with general rules specified in NL-SYS-01, section 5.3 and detailed rules presented below.

53 Assurance evidence, if applicable, may be presented to the CAB as evidence of conformity with the requirements of the subsidiary documents, subject to the evaluation criteria below:

- Certificates of conformity issued under ISO/IEC 27001 by a certification body accredited by a Dutch Accreditation Body, in accordance with ISO/IEC 17021-1.
- Certificates of conformity issued under ETSI EN 319 411-1 or EN 319 411-2 for qualified trust service providers, by a conformity assessment body accredited in accordance with ISO/IEC 17065 by a relevant National Accreditation Body.
- Certificates of conformity or evaluation reports issued under European or national cybersecurity certification schemes (such as EUCC).
- Other assurance reports or certificates issued under recognised standards or frameworks, provided they meet the evaluation criteria set out in section 7.7

7.7 Evaluation criteria

54 The CAB shall evaluate the acceptability of assurance evidence in accordance with the methodology set out in Annex VI of Commission Implementing Regulation (EU) 2024/2981 and the criteria in Annex II thereof. The evaluation shall address at a minimum the following dimensions:

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

- **Issuer competence and impartiality**. The CAB shall verify the professional competence and impartiality of the body or person that issued the assurance report or certificate, according to Section 7.6. For certification bodies, accreditation under the relevant standard (ISO/IEC 17021-1, ISO/IEC 17065, or equivalent) by a national accreditation body appointed pursuant to Regulation (EC) No 765/2008 shall be verified.
- **Scope adequacy**. The CAB shall verify that the scope of the assurance documentation covers the services, processes, controls, and systems that are relevant to the requirements being evaluated under this certification scheme.

  EXAMPLE 1: ISO/IEC 27001 certification attests to the conformity of the information security management system itself (the processes of establishing, implementing, maintaining and continually improving the ISMS); it does not, on its own, provide sufficient assurance that the individual controls selected in the statement of applicability are designed and operating at the level of rigour required by this scheme. The CAB shall therefore perform its own evaluation of the design and operating effectiveness of the specific controls required by the NL-P-P subsidiary documents, even where an ISO/IEC 27001 certificate is in place.

- **Timeliness.** The assurance evidence shall be up to date at the time of evaluation. Certificates shall be within their validity period. Assurance reports shall cover a reporting period that is sufficiently recent to provide confidence that the controls described remain in operation. Where a gap exists between the end of the reporting period and the date of the evaluation, the CAB shall perform its own supplementary evaluation of the period not covered.
- **Rigor and depth of evaluation**. The degree of confidence provided by the assurance documentation shall be commensurate with the criticality of the requirements it covers. The CAB shall consider the rigor of the evaluation methodology applied, the depth of testing performed, and the nature of the assurance opinion or conclusion expressed.
- **Findings and exceptions**. The CAB shall review any findings, qualifications, exceptions, or caveats noted in the assurance evidence. Where material findings exist, the CAB shall determine whether they are relevant to the requirements of this scheme and, if so, whether they have been adequately addressed.

55 *NOTE 1: For the cases specified in Clauses II and III, the CAB shall document the scope and results of any supplementary or alternative testing performed and shall ensure that these are included in the certification records.*

56 *EXAMPLE 2: See the outcome from Example 1. In case of ISO/IEC 27001, the CAB performs its own evaluation of the design and operating effectiveness of the specific controls required by the NL-P-P subsidiary documents, even where an ISO/IEC 27001 certificate is in place.*

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

8 Certification Process

8.1 General

57 The NL-P-P certification process is divided into three main phases: a preparation and application phase, an evaluation phase, and a certification phase. Each phase is described in the subsections below.

58 The evaluation methodology applicable to each phase is set out in Section 7 of this document. The certification process shall be conducted in accordance with the procedures established by the CAB under NL-SYS-01 and NL-SYS-05.

8.2 Preparation and application phase

59 NOTE: this phase reflects ISO/IEC 17065, 7.2 and 7.3.

60 The following documents and information are required from the Applicant prior to commencement of the evaluation:

- a description of the PID Provider's environment and systems, including the governance structure, the scope of services, and the organisational arrangements and if appropriate;
- documentation demonstrating compliance with NL-P-P subsidiary requirement documents, including policies, procedures, risk assessments, and records relevant to the evaluation scope;
- valid certificates with regard to any (Qualified) eSealing services it has and/or QeSCDs it operates in order to be able to e-seal PIDs.
- any available external assurance evidence (e.g. ISO/IEC 27001 certificates, audit reports) that the Applicant intends to present for reliance under Section 7.6;
- the completed application form as distributed by the CAB in accordance with its internal procedures.

61 The Applicant may submit the application form under NL-P-P separately, or as a combined application covering multiple certification schemes within the NL EUDI Wallet Certification System, in accordance with NL-SYS-01.

8.3 Evaluation phase

62 NOTE: this phase reflects ISO/IEC 17065, 7.4.

8.3.1 Kick-off meeting

63 A kick-off meeting shall be held no later than 10 working days after receipt of a complete application and all required documentation. All parties involved in the evaluation — the Applicant, representatives of the Scheme Owner and the CAB — shall attend the kick-off meeting.

64 At the kick-off meeting, the CAB shall agree with the Applicant the evaluation plan, including the scope and schedule of evaluation activities, the reliance determination approach for any external assurance evidence, and the arrangements for on-site visits and interviews.

8.3.2 Evaluation

65 The evaluation shall be conducted in accordance with the evaluation methodology specified in Section 7. The CAB shall document all evaluation activities, evidence obtained, and findings in an Evaluation Report.

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

66 Where substantial findings arise during the evaluation that may prevent a positive certification decision, the CAB shall notify the Applicant without undue delay. The Applicant may provide additional information or clarification in response to such findings within the timeframe agreed at the kick-off meeting.

67 The Evaluation Report shall contain an overall assessment of conformity with each requirement stemming from the subsidiary documents, the reliance determination for any external assurance evidence used, and a recommendation for the certification decision.

8.4 Certification phase

68 NOTE: This phase reflects ISO/IEC 17065, 7.5 -7.7 and 7.13.

69 After reviewing of the evaluation results, the CAB shall complete the certification decision and inform the Applicant of the outcome within 5 working days. If the certification decision is positive, the certificate of conformity shall be issued no later than 14 working days after the decision.

70 Appeals and complaints shall be dealt with in accordance with the general provisions contained in NL-SYS-01.

71 If the certification decision is negative, the Applicant has 14 working days to lodge a written complaint with the CAB. The CAB shall process the complaint and issue a final decision within 14 working days of receipt of the objection.

72 In case of no objection by the applicant, the publication procedure, if applicable, commences immediately after the declaration.

8.5 Evaluation and certification efforts

73 The indicative workload for carrying out the evaluation and certification under NL-P-P is presented in Table 3. These estimates cover the initial certification. Surveillance and recertification activities are specified in Sections 8.8 and 8.9 of this document.

74 The values listed in Table 3 are maximum and planned values, and they may be subject to change upon agreement with the Scheme Owner.

Table 3 Planned evaluation and certification efforts

Phase	Planned CAB effort
Evaluation	30 working days
Certification	15 working days

8.6 Additional provisions

75 The certificate of conformity is valid for four years from the date of issuance.

76 The CAB shall archive all evidence relevant to the certification, in accordance to and for a period specified in NL-SYS-01, section 5.10.

77 Exchange of information between the CAB and the Applicant shall be secured using state-of-the-art cryptographic mechanisms approved by the Scheme Owner. The requirements for maintaining and disseminating the list of applicable mechanisms are specified in NL-SYS-03, Section 9.2.2.

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

8.7 Certificate of conformity

78 Upon successful completion of the evaluation, the CAB shall issue a certificate of conformity specifying:

- the object of certification
- the scope of the certification, with explicit reference to each of the NL-P-P subsidary documents;
- name of the PID Provider;
- the version(s) of the wallet solutions in scope;
- the validity period of the certificate (not to exceed four years);
- any conditions, limitations or exceptions attached to the certificate.

79 The CAB shall notify the Scheme Owner of the issued certificate within five working days of issuance, in accordance with the procedure established in NL-SYS-03.

8.8 Surveillance

80 NOTE 1: The rules for conducting surveillance activities are specified in NL-SYS-01, section 5.4.

81 Throughout the period of validity of the certificate, the CAB shall conduct annual surveillance activities to verify that the certification holder continues to meet the certification requirements. Surveillance shall include, at a minimum:

- review of material changes to the PID issuance & Lifecycle mngt services and/or NL national eID scheme fraud detection measures, its components, or the organizational arrangements as duly notified towards the CAB.
- review of any incidents or security breaches as duly notified towards the CAB;
- review of any updates to NL-P-P and subsidiary documents and their implications;
- review of the impact of any updates to NL-P-P and subsidiary documents and their implications
- targeted evaluation activities as determined by the CAB, based on the risk register (meeting the minimum content requirements specified in NL-SYS-04) and any intelligence gathered during the surveillance period;
- follow-up on any non-conformities, observations or conditions previously identified by the CAB-CB, to verify that corrective actions have been implemented effectively.

82 CAB-CB shall conduct surveillance activities throughout the life cycle of certification, including at least the following:

- perform a full evaluation of the object of conformity assessment in the initial evaluation and each recertification evaluation, including any updates to its components;
- conduct a vulnerability assessment during the initial evaluation, each recertification, and at least every two years during surveillance activities. The assessment shall, at a minimum, address changes to the object of certification and the threat environment since the previous assessment;
- perform additional activities such as penetration testing, where the risk level increases or the new threats emerge;

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

Table 4 4-year certificate life cycle in NL-P-P

Year	Type of activity	Mandatory activities
0	Initial certification	• Full evaluation of the provisioning of the PID Issuance& Lifecycle Management services and National eID schems fraud prevention services, including vulnerability assessment • Evaluation of the maintenance processes, excluding their operating effectiveness • Granting of certification and start of the 4-year cycle
1	Surveillance	• Evaluation of the operating effectiveness of the maintenance processes • At least version check, update, vulnerability management • Evaluation of changes impacting the security of the solution(s)
2	Surveillance	• Vulnerability assessment of the full solution • Evaluation of the operating effectiveness of the maintenance processes— At least version control, update, vulnerability management • Evaluation of changes impacting on the security of the solution(s)
3	Re-certification	• Full re-evaluation. • Full evaluation of the object of certification, including vulnerability assessment • Simplified evaluation for features/processes that have not changed including a feature to perform updates on each software component • Evaluation of the maintenance processes, including their operating effectiveness • Granting a new certification

83 Each surveillance activity shall be conducted within 12 months of the issuance of certificate and thereafter within 12 months of the previous surveillance activity. Recertification shall be conducted within 12 months after the last surveillance activity.

8.9 Recertification

84 Recertification shall be initiated before the expiry of the current certificate and shall follow the process for initial certification set out in Section 8. Recertification can rely on assurance evidence from the surveillance activities conducted during the validity period, and the CAB may reduce the scope of its evaluation activities accordingly, in accordance with Section 7.6.

85 Recertification is also required where a major change occurs to the electronic identification scheme, including a change of wallet solution version where the new version is not covered by the existing certificate; a change to the organisational structure of Provider or a material change to the Trust Framework established under NL-SYS-03.

86 All relevant activities related to recertification shall be undertaken by the PID Provider and the relevant CABs in a timely manner. The Applicant shall notify the CAB of the need for recertification no later than six months before the expiry of the current certificate.

8.10 Suspension, Termination or Withdrawal of certificate

87 General provisions included in NL-SYS-01 sections 5.7 and 5.8 apply.

88 The CAB shall suspend a NL-P-P certificate in the following circumstances:

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

- The PID Provider fails to implement corrective actions within the agreed time following a non-conformity identified during surveillance;
- A significant incident or security breach is notified that can impact conformity, pending the outcome of an impact assessment;
- The PID Provider fails to cooperate with or provide access for surveillance activities.

89 *NOTE — The timeframe for implementing corrective actions referred to in the first suspension ground shall be agreed in writing between the CAB and PID Provider at the time the non-conformity is notified. The CAB shall determine an appropriate timeframe considering the nature and severity of the non-conformity, in accordance with the provisions of NL-SYS-05. The CAB shall document the agreed timeframe in the Surveillance Report.*

90 The suspension period shall not exceed 45 days. Any extension shall be subject to the Scheme Owner decision but in any case, may not exceed one 90 days. The suspension period does not affect the validity period of the certificate.

91 The CAB shall withdraw a NL-P-P certificate in the following circumstances:
- The PID Provider fails to remedy the conditions leading to suspension within the time specified by the CAB;
- A confirmed non-conformity is established that cannot be remedied within a reasonable time;

92 CAB-CB shall terminate the certificate on request of PID Provider.

93 In all cases of suspension, termination or withdrawal, the CAB shall notify the Scheme Owner without undue delay. The Scheme Owner shall update the Certificate Register in accordance with the obligations specified in NL-SYS-03.

8.11 Implications of NL-P-P Certificate Changes

94 Any suspension or revocation of the NL-P-P will have an immediate effect on the top-level certificate of active wallet providers in the NL eID scheme, as per consequence of the composition of certificates in the NL Certification System.

8.12 National legislation

95 The NL-P-P Certification Scheme is established pursuant to national legislation implementing the eIDAS Regulation in The Netherlands, in accordance with the legal instruments listed in Section 3 of this document.

8.13 Certification contracts

96 The CAB shall conclude a certification contract with the Applicant based on the provisions of NL-P-P. Contractual arrangements may be imposed by the Scheme Owner.

97 The certification contract shall not contain provisions that would obstruct the correct conduct of the certification or the transfer of information relevant to the certification decision between the Applicant and the CAB.

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

8.14 Costs

98 All costs shall be based on actual certification efforts.

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

9 Final provisions

9.1 National legislation

99 The NL-P-P Certification Scheme is established pursuant to national legislation implementing the eIDAS Regulation in The Netherlands, in accordance with the legal instruments listed in Section 3 of this document.

9.2 Certification contracts

100 The CAB shall conclude a certification contract with the Applicant based on the provisions of NL-P-P. Contractual arrangements may be imposed by the Scheme Owner.

101 The certification contract shall not contain provisions that would obstruct the correct conduct of the certification or the transfer of information relevant to the certification decision between the Applicant and the CAB.

9.3 Costs

102 All costs shall be based on actual certification efforts.

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

Annex A (Normative) — Allocation of Requirements to Subsidiary Documents

103 *NOTE: This Annex provides the normative allocation of legal requirements — derived from the instruments listed in Section 3 — to the subsidiary documents of NL-P-P. This allocation is the basis for the evaluation scope defined in Section 7.2 of this document. Requirements applicable specifically to PID Provider are located in the subsidiary documents and are not separately listed in this Annex; they are derived from the same legal instruments referenced below.*

A.1 Requirements from Regulation (EU) 2024/1183

Identifier	Requirement
REQ-910-01	EUDIW shall enable users to securely manage PID and EAAs under sole user control. [Art. 5a(4)(a)] → NS-FS and NL-CS as-well-as NL-P-P04 / NL-P-P04B
REQ-910-02	EUDIW shall enable users to download their data and configurations. [Art. 5a(4)(f)] → NS-FS and NL-CS
REQ-910-03	EUDIW shall meet assurance level High. [Art. 5a(5)(d)] → NS-FS and NL-CS as-well-as NL-P-01 AND NL-P-02 AND NL-P-03 as-well-as NL-P-P04 / NL-P-P04B and NL-P-P04 / NL-P-P04B
REQ-910-04	PID shall uniquely represent the natural person. [Art. 5a(5)(f)] → NL-P-P04 / NL-W-P04B
REQ-910-05	Personal data of EUDIW provision kept logically separate. [Art. 5a(14)] → NS-FS and NL-CS as-well-as NL-P-01 AND NL-P-02 AND NL-P-03 as-well-as NL-P-P04 / NL-P-P04B and NL-P-P04 / NL-P-P04B
REQ-910-06	Users onboarded using assurance level High eID means. [Art. 5a(24)] → NL-P-P04 / NL-P-P04B

A.2 Requirements from CIR (EU) 2015/1502

Identifier	Requirement
REQ-1502-2.1	Enrolment requirements at assurance level High. [Annex 2.1] → NL-P-P04 / NL-P-P04B
REQ-1502-2.2	eID means management at assurance level High. [Annex 2.2] → NL-P-P04 / NL-P-P04B as-well-as NL-P-P04 / NL-P-P04B
REQ-1502-2.4.1	Legal status, financial capacity, outsourcing. [Annex 2.4.1] → NL-P-01 AND NL-P-02 AND NL-P-03 as-well-as admission criteria
REQ-1502-2.4.2	Published notices and user information. [Annex 2.4.2] → NL-P-01 and NL-P-03
REQ-1502-2.4.3	Information security management system. [Annex 2.4.3] → NL-P-01 AND NL-P-02 AND NL-P-03
REQ-1502-2.4.4	Record keeping. [Annex 2.4.4] → NL-P-01 AND NL-P-02 AND NL-P-03
REQ-1502-2.4.5	Facilities and staff. [Annex 2.4.5] → NL-P-01 AND NL-P-02

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

Identifier	Requirement
REQ-1502-2.4.6	Technical controls. [Annex 2.4.6] → NL-P-01 AND NL-P-02
REQ-1502-2.4.7	Compliance and audit. [Annex 2.4.7] → NL-P-01 AND NL-P-02 AND NL-P-03

A.3 Requirements from CIR (EU) 2024/2977

Identifier	Requirement
REQ-2977-3	PID issuance technical requirements. [Art. 3] → NL-P-P04 / NL-P-P04B
REQ-2977-5	PID validity status management and revocation. [Art. 5] → NL-P-P04 / NL-P-P04B

A.4 Requirements from CIR (EU) 2024/2979

Identifier	Requirement
REQ-2979-3,4	Wallet unit attestation issuance. [Art. 3, 4] → NL-FS and NL-CS as-well-as NL-P-P04 / NL-P-P04B
REQ-2979-6,7	PID Provider obligations — user information, revocation. [Art. 6, 7] → NL-P-P04 / NL-P-P04B
REQ-2979-9,13	Logging and data portability. [Art. 9, 13] → NL-P-P04 / NL-P-P04B

A.5 Requirements from CIR (EU) 2024/2981

Identifier	Requirement
REQ-2981-4	Risk assessment and security criteria. [Art. 4, 8] → NL-CS, NL-P-01 AND NL-P-02 AND NL-P-03
REQ-2981-5	Incident and vulnerability management. [Art. 5] → NL-P-01 AND NL-P-02 AND NL-P-03
REQ-2981-8(3)(g)	Use of currently certified wallet solution version. [Art. 8(3)(g)] → NL-CS and NL-P-P04 / NL-P-P04B
REQ-2981-19	Record retention. [Art. 19] → NL-P-01 AND NL-P-02 AND NL-P-03

A.6 Requirements from CIR (EU) 2024/2690

Identifier	Requirement
REQ-2690-Annex	Technical and methodological cybersecurity requirements. [Annex, Sections 1–13] → NL-CS as-well-as NL-P-01 AND NL-P-02 AND NL-P-03

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

Annex B (Normative) Audit framework

B.1 Purpose

104 This annex sets out common framework for planning, conducting and documenting cybersecurity audits performed by a Conformity Assessment Body under the NL-P-P eID Certification Scheme thus creating evaluation methodology for the scheme

105 The annex maps the audit-related approach of ETSI EN 319 403-1 into the structure of the NL EUDI Wallet Certification System and provides a consistent basis for CAB elaborated audit frameworks

106 The document specifies universal audit principles, methods, sampling, competence, evidence gathering, reporting and corrective action follow-up. It does not define how individual requirements from technical specifications, including ETSI EN 319 401, implementing acts or other criteria are to be tested.

B.2 Scope

107 This framework applies to cybersecurity audits conducted within the NL-P-P evaluation phase. The object of certification is the electronic identification system, elated services and processes.

108 The framework is applicable to :

- initial evaluation audits;
- annual surveillance audits;
- re-evaluation audits;
- special audits triggered by significant changes, incidents, complaints or other substantiated information; or by audits of outsourced services, subcontracted processes or separately evaluated components to the extent material to the certification requirements.

109 The framework shall be applied to the extent appropriate to the nature, risk and scope of the evaluation activity.

110 The scope of evaluation shall not be reduced solely because external assurance evidence is available. External evidence may reduce the extent of the CAB's own audit activities only after a documented determination of reliance.

B.3 References, terms and roles

B.3.1 References

111 ISO/IEC 17065 - Conformity assessment - Requirements for bodies certifying products, processes and services;

112 ETSI EN 319 403-1 - Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;

113 NL-SYS-01 NL EUDI Wallet Certification System;

114 NL-SYS-05 Accreditation requirements for CABs;

115 NL-P-P Certification Scheme;

116 NL-P-P applicable subsidiary requirement documents

B.3.2 Roles and responsibilities

117 Relevant roles and responsibilities are presented in Table 1 in this annex.

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

Table 1 Roles and responsibilities in the cybersecurity audit framework

Role	Responsibilities
CAB	The certification body accredited and authorised to perform NL-P-P conformity assessment and certification activities.
Applicant / Certificate Holder	The entity that applies for or holds NL-P-P certification.
Provider	PID Provider
Object of certification	The electronic identification system and related services defined by NL-P-P.
Audit Team	One or more auditors appointed by the CAB or its subcontractor, supported by technical experts, if necessary.
Audit Team Leader	The auditor responsible for managing the audit and reporting findings to the CAB.
Technical Expert	A person providing specialist knowledge to the Audit Team who does not act independently as an auditor.

B.3.3 Terms specific to cybersecurity audit framework

118 The terms and their definitions presented in Table 2 apply.

Table 2 Terms and definitions

Term	Definition
Audit criteria	The applicable requirements from NL-SYS-*, NL-P-*, legal acts, standards and specifications.
Objective evidence	Verifiable information supporting the fulfilment or non-fulfilment of an audit criterion.
External assurance evidence	A certificate, report, evaluation result or other evidence produced outside the current NL-P-P evaluation and submitted for possible reliance.

B.4 General audit principles

119 Audits shall be planned and conducted in a way that ensures impartiality and consistency and protects confidential information.

120 Audit conclusions shall be based on sufficient and appropriate objective evidence.

121 The depth and scope of audit activities shall be proportionate to risk, the criticality of the requirement, the maturity of the relevant controls and the results of previous audits.

122 Audit Team shall not prescribe a particular implementation or documentation format unless explicitly required by the audit criteria.

123 Statements and explanations shall be corroborated by records, observations, interviews, testing results or other objective evidence where necessary.

124 Audit Team shall assess the design and operational effectiveness of controls where the applicable requirement concerns both their existence and their functioning.

125 The audit shall consider the risk register maintained by the PID Provider or by the Scheme Owner and other risk information relevant to the object of certification when

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

selecting audit trails, samples, sites and technical focus areas.

B.5 Audit objectives, scope and time

B.5.1 Audit objectives

126 For each audit, the CAB shall define objectives appropriate to the evaluation activity.

127 NOTE: Objectives may include:

- *Assess conformity with the requirements applicable to the approved scope;*
- *check whether controls are implemented, and operate effectively;*
- *confirming continued conformity during surveillance;*
- *evaluating the impact of a significant change or incident;*
- *tracking resolutions of previously detected nonconformities;*
- *obtaining evidence required for re-assessment, extension, reduction or another scheme decision.*

B.5.2 Audit scope

128 The audit scope shall include, as applicable:

- the part of the electronic identification system and related services to be evaluated;
- the Applicant organisations and organisational units included in the audit;
- the NL-P-P subsidiary requirements and versions included in the audit criteria;
- processes, systems, components, interfaces, data flows and operational environments;
- physical and logical sites;
- outsourced and subcontracted activities;
- the period from which records and samples are to be selected;
- any accepted limitations or exclusions and their justification.

129 The scope and boundaries shall be clear enough to avoid ambiguity regarding the organisations, services, processes, systems and sites subject to audit.

130 Where outsourced or subcontracted services are material to fulfilment of the certification requirements, the audit scope shall extend to those services or shall obtain sufficient equivalent assurance concerning them.

B.5.3 Audit time

131 The CAB shall allocate sufficient time for preparation, evidence review, audit activities, reporting and follow-up. To specify audit time the CAB shall consider at least:

- the number and complexity of applicable requirements;
- the size and complexity of the object of certification and the participating Provider organisations;
- the number of sites, systems, interfaces and outsourced services;
- the diversity and volume of transactions or recurring processes;
- the use of automation, cryptography, biometrics, remote onboarding or other specialist technologies;
- results of previous evaluations, incidents and changes;
- the availability and acceptability of external assurance evidence;
- the need for specialist technical expertise;
- the use of on-site and remote techniques.

132 The CAB shall document specification and justification of audit time.

133 NOTE: Guidelines for determining audit time for management system audits are provided in the standard ISO/IEC 27006-1 "Requirements for bodies providing audit

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

and certification of information security management systems – Part 1: General", Annex D.

134 Commercial or scheduling constraints shall not reduce audit time below the level necessary to obtain sufficient and appropriate evidence.

B.6 Audit planning and kick-off

135 The CAB shall prepare an audit plan based on the objectives, scope, risk, available evidence and competence requirements.

136 The audit plan shall specify at least:

- audit objectives, scope and criteria;
- Audit Team members and roles;
- dates, locations, timetable and mode of audit activities;
- planned audit trails and principal samples;
- interviews, observations and technical activities;
- use of remote techniques and security arrangements;
- arrangements for opening, progress and closing meetings;
- reporting and communication arrangements.

137 The audit plan shall be agreed with the Applicant or Certificate Holder without transferring responsibility for audit design to the audited parties.

138 A kick-off or opening meeting shall confirm the scope, timetable, responsibilities, communication channels, access arrangements, reliance approach and handling of substantial findings.

139 Changes to the plan during the audit shall be documented and communicated to the relevant parties.

B.7 Audit methods and techniques

140 The CAB shall select an appropriate combination of methods for each evaluation activity. Criteria-specific

B.7.1 Documentation review

141 NOTE: Documentation review may cover policies, procedures, practice statements, contracts, risk assessments, architectural descriptions, technical specifications, configurations, records, logs, internal audit reports, management reviews, test reports and prior evaluation evidence.

142 Documentation review shall be used to understand the design of the audited arrangements and to prepare subsequent audit trails.

B.7.2 Interviews

143 Interviews shall be conducted with personnel whose roles and responsibilities are relevant to the audit scope. Questions shall seek to establish actual practice, responsibility, competence and awareness and shall be corroborated where appropriate.

B.7.3 Observation and inspection

144 NOTE: Observation can include processes, facilities, security controls, system operation, administrative activities and technical demonstrations. Inspection can be performed on-site or through controlled remote access.

145 The Audit Team shall agree access, recording, screenshot, copying and confidentiality arrangements before inspection activities begin.

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

146 Audit activities shall avoid unnecessary disruption and not introduce unacceptable risk to production services or personal data.

B.7.4 Analysis of records, logs and transactions

147 NOTE: The Audit Team may analyse logs, audit trails, transaction records, change records, incident records and other operational evidence to confirm execution, authorisation, traceability, integrity and effectiveness of the relevant processes.

B.7.5 Testing and technical verification

148 NOTE: Technical verification can include controlled demonstrations, configuration review, test-case execution, re-performance, interface verification or review of specialist security testing.

149 Intrusive testing shall be separately authorised and performed by competent personnel under controlled conditions.

B.7.6 Remote audit techniques

150 NOTE: Remote techniques may be used where they provide evidence of sufficient reliability and completeness and are permitted by the applicable scheme and criteria.

151 The plan shall define the tools, authentication, transmission security, recording rules and contingency arrangements used for remote audit activities.

152 Where remote techniques do not provide sufficient evidence, the Audit Team shall perform additional on-site or alternative activities.

B.8 Audit evidence and sampling

B.8.1 Sufficiency and appropriateness

153 The Audit Team shall obtain sufficient and appropriate evidence to support each audit conclusion.

154 Evidence shall be relevant to the requirement, reliable in origin and method, sufficiently current and traceable to the audited scope.

155 The absence of a particular document shall not in itself establish nonconformity unless the criterion requires that document. Conversely, the existence of documentation alone shall not establish operational effectiveness.

B.8.2 Sampling

156 Sampling may be used where examination of every instance is impracticable. Sampling shall be risk-based, documented and appropriate to the objective of the audit.

157 NOTE: Sample selection should consider:

- *high-risk and critical processes;*
- *different process variants and technologies;*
- *successful, failed, rejected, exceptional and escalated cases;*
- *incidents, complaints, anomalies and fraud indicators;*
- *different periods, sites, systems, providers and operational teams;*
- *recent changes and software or configuration versions;*
- *both selective and non-selective elements.*

158 The CAB shall document the population, selection method, sample size, items selected and limitations of the sample.

B.8.3 Multiple sites

159 A sample-based multi-site approach may be used only where the relevant sites operate under common control and a common management and review framework.

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

160 Site selection shall consider differences in size, activity, technology, risk, legal requirements, working practices, subcontracting and interaction with critical or sensitive systems.

161 Sites presenting significant risk or material differences shall be included in the audit programme.

162 A finding at one site shall be assessed for possible systemic impact on other sites.

B.9 External assurance evidence

163 External assurance evidence may be used to reduce duplicate evaluation activity, but only after a documented assessment in accordance with NL-P-P. The CAB remains fully responsible for its evaluation conclusions and certification decision.

B.9.1 Acceptability assessment

164 For each item of external assurance evidence, the Audit Team shall assess at least:

- issuer competence, independence and accreditation where applicable;
- scope adequacy and correspondence with the current object of certification;
- timeliness and continued validity;
- rigour and depth of the method applied;
- findings, qualifications, exceptions and limitations;
- the period, versions, sites, systems and controls covered;
- the need for supplementary audit activity.

B.9.2 Use of external assurance evidence in audit planning and execution

165 The Audit Team shall assess the extent to which external assurance evidence supports the applicable audit criteria and shall identify any requirements, aspects or periods not sufficiently covered by that evidence.

166 Based on this assessment, the Audit Team shall identify the supplementary audit activities necessary to obtain sufficient and appropriate evidence.

167 The Audit Team shall document its assessment of the external assurance evidence, identified limitations and proposed supplementary activities in the audit records and Audit Report.

168 The formal determination of full reliance, partial reliance or no reliance shall be made by the CAB in accordance with NL-SYS-01, Section 5.3, and Sections 7.6 and 7.7 of NL-P-P and is not determined by the Audit Team under provisions specified in this document.

B.10 Audit Team competence, independence and outsourcing

B.10.1 Collective competence

169 The Audit Team shall collectively possess competence appropriate to the scope, including as applicable:

- the NL Wallet Certification System and NL-P-P;
- applicable legal, regulatory, normative and scheme requirements;
- information security management, cybersecurity and network security;
- risk assessment and risk management;
- electronic identification, PID, EUDI Wallet and authentication processes;
- cryptography, PKI, secure components and protocols;
- identity proofing, remote onboarding, biometrics and fraud prevention;
- audit principles, methods, sampling, evidence evaluation and reporting;

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

— the technologies and operational processes included in the audit scope.

170 Criteria-specific WM-03-0x documents shall identify any additional specialist competence required for their application.

B.10.2 Audit Team Leader and technical experts

171 The Audit Team Leader shall have sufficient audit experience and knowledge of the applicable criteria to manage the audit and consolidate the findings.

172 Technical experts may advise auditors on specialist matters but shall not act as the sole evaluator of conformity or take the certification decision.

B.10.3 Outsourcing of audit activities

173 Audit activities may be outsourced only where permitted by NL-SYS-01, NL-SYS-05, NL-P-P and the applicable normative framework.

174 The CAB shall define the scope of outsourcing, competence requirements, confidentiality, reporting obligations and access to records.

175 The CAB shall retain responsibility for the audit, evaluation conclusions and certification decision.

176 The CAB shall review and accept outsourced outputs before using them as evaluation evidence.

B.11 Audit process

177 NOTE: The audit forms part of the NL-P-P evaluation phase. The process below does not replace the preparation and application or certification phases defined in NL-P-P.

B.11.1 Initial and re-assessment audits

178 NOTE: Initial and re-assessment audits should normally comprise Stage 1 and Stage 2. The sequence may be adapted where justified and permitted by NL-SYS-05 and the audit plan.

B.11.2 Stage 1 - documentation and readiness review

179 NOTE: Stage 1 is intended to understand the object of certification, confirm audit readiness and plan Stage 2. It should cover, as applicable:

- *scope, governance and organisational responsibilities;*
- *architecture, systems, services, processes, interfaces and outsourced activities;*
- *applicable policies, procedures and practice statements;*
- *risk assessment, risk treatment and the relevant risk register;*
- *internal audits, management reviews, previous findings and external assurance evidence;*
- *availability of records, samples, systems, sites and personnel;*
- *areas of concern and additional competence or time required for Stage 2.*

180 Stage 1 results shall be documented and used to finalise the Stage 2 plan.

181 Potential nonconformities identified during Stage 1 shall be treated as areas of concern until supported by sufficient evidence.

B.11.3 Stage 2 - implementation and operational effectiveness

182 Stage 2 shall collect objective evidence that applicable requirements are implemented and operate effectively.

183 NOTE: Stage 2 can include documentation review, interviews, observation, inspection, sampling, transaction review, log analysis and technical verification.

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

184 Stage 2 shall include relevant sites and operational environments unless sufficient equivalent evidence is obtained and the use of remote or external assurance evidence is justified.

B.11.4 Surveillance and special audits

185 Surveillance and special audits can use a targeted, risk-based sequence rather than the full Stage 1 and Stage 2 model. The CAB shall nevertheless define scope, criteria, methods, samples, evidence and reporting sufficient for the audit objective.

B.11.5 Meetings and communication

186 The Audit Team shall conduct an opening or kick-off meeting appropriate to the audit.
187 Substantial findings that influence a certification decision shall be communicated without undue delay in accordance with NL-P-P.
188 A closing meeting shall present the audit scope, methods, limitations, findings and next steps and shall provide the audited parties with an opportunity to clarify factual
189 matters.

B.12 Evaluation of findings and pass/fail principles

B.12.1 Applicability

190 For each requirement included in the assessment matrix, the Audit Team shall determine its applicability to the approved audit scope.
191 The applicability status shall be one of the following:
192 Applicable - the requirement applies to the approved audit scope;
193 Not applicable - the requirement does not apply to the approved audit scope and the rationale for exclusion has been documented and accepted.
194 A requirement classified as not applicable shall not be assigned a conformity assessment result.

B.12.2 Requirement-level assessment results

195 For each applicable requirement, the Audit Team shall assign one of the results presented in Table 3.

Table 3 Audit results

Result	Meaning
Conforming	Sufficient and appropriate objective evidence demonstrates fulfilment of the specified requirement.
Major nonconformity	A non-fulfilment of a specified requirement that has a substantial security impact and/or a substantial impact on the ability of the object of certification to achieve the intended service or process outcome.
Minor nonconformity	A non-fulfilment of a specified requirement that does not have any substantial security impact and does not have any substantial impact on the ability of the object of certification to achieve the intended service or process outcome.
Not concluded - insufficient evidence	Sufficient and appropriate evidence was not available to determine conformity. This result shall not be treated as conformity and shall be resolved before a positive audit recommendation is issued in relation to the applicable scope.

B.12.3 Observations

196 The Audit Team may record positive or negative observations in addition to requirement-level assessment results.

197 NOTE: An observation is an informative audit finding identifying a risk, weakness, positive practice or emerging issue where the available evidence does not demonstrate non-fulfilment of a specified requirement.

198 An observation may not replace a conformity assessment result and shall not, by itself, constitute a failure to meet a requirement.

B.12.4 Relationship with the certification decision

199 The assessment results and audit findings shall constitute input to the review and certification decision conducted in accordance with NL-P-P and NL-SYS-05.

200 The Audit Team shall not issue the certification decision. The formal certification decision shall be made by the CAB in accordance with the applicable certification scheme.

B.13 Audit reporting and interface with the Evaluation Report

B.13.1 Audit report

201 The Audit Team Leader shall provide the CAB with an Audit Report with content in accordance with NL-SYS-01, section 6.3.

202 The Audit Report shall contain sufficient detail to allow independent review of the audit and its conclusions.

B.13.2 Evaluation Report

203 NL-P-P requires an Evaluation Report covering the overall evaluation. The CAB may use the Audit Report as an input or may issue a combined Audit and Evaluation Report where the audit constitutes the complete evaluation activity.

204 The Evaluation Report shall contain an overall assessment of conformity with each applicable NL-P-P subsidiary requirements, the reliance determination for external assurance evidence and a recommendation for the certification decision.

205 Where several audits, evaluations or external reports contribute to the Evaluation Report, the CAB shall ensure traceability from each requirement to the evidence and conclusion used.

B.14 Corrective actions and follow-up

206 For each nonconformity, the Applicant or Certificate Holder shall provide information appropriate to its significance, including correction, root-cause analysis, corrective action, responsible owner, target date and evidence of completion.

207 The CAB shall evaluate the adequacy of proposed corrective actions and determine the verification activities required for closure.

208 Major nonconformities shall be corrected, and their closure verified before a positive certification recommendation or decision.

209 Timeframes for minor nonconformities shall be agreed in accordance with NL-P-P, G-SYS-05 and the applicable CAB procedure. This framework does not establish an independent fixed deadline.

210 Where a nonconformity can affect multiple sites, systems, processes or Providers, corrective action shall address the full systemic extent and underlying cause.

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

211 NOTE: Verification can be performed by document review, interview, sampling, observation, testing, additional audit or another justified method.

B.15 Surveillance, re-assessment and special audits

212 Audit frequency and scope shall follow NL-P-P, including annual surveillance and re-assessment before certificate expiry.

213 Surveillance audit planning shall consider material changes, incidents, updated scheme documents, risk-register information, intelligence, compliance-monitoring results, external certificates and previous findings.

214 NOTE: Re-assessment may make documented use of acceptable evidence from surveillance activities and may reduce duplicate audit work in accordance with the determination of reliance.

215 Special audits shall be initiated by the CAB in case of one or more events occurring:

- significant changes,
- security incidents,
- complaints,
- failure to implement corrective actions or other information relevant to continued conformity.

216 NOTE: This framework does not independently define certificate suspension, withdrawal or recertification decisions; those matters are governed by NL-P-P, NL-SYS-01 and NL-SYS-05.

B.16 Records, confidentiality and quality control

217 The CAB shall retain audit plans, competence records, evidence records, notes, samples, reliance assessments, reports, corrective-action records and review records in accordance with NL-SYS-01 and NL-SYS-05.

218 Access to sensitive evidence, including personal data, security architecture, cryptographic information, vulnerabilities and incident information, shall be restricted to authorised persons in accordance to 'need to know' principle

219 Audit evidence shall be transferred, stored and disposed of using controls appropriate to its sensitivity.

220 The CAB shall apply review and quality-control arrangements sufficient to ensure consistency of findings, classification and reporting across Audit Teams and subsidiary NL-P-P-documents.

221 Interpretation questions that cannot be resolved by the CAB's shall be escalated in accordance with the governance arrangements of the certification scheme.

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

Annex C (Normative) Minimum contents of an audit plan

222 The audit plan shall contain at least the following elements:

- audit identification and type;
- objectives, scope, boundaries and criteria;
- Audit Team and roles;
- dates, duration, sites and activity timetable;
- Stage 1 and Stage 2 arrangements, where applicable;
- methods, principal audit trails and planned samples;
- external assurance evidence and intended reliance approach;
- remote techniques, access and information-security arrangements;
- meetings, communication and reporting arrangements;
- known limitations, assumptions and contingency arrangements.

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

Annex D (Normative)- Minimum contents of an audit evidence record

223 The audit evidence record shall contain or reference to at least the following:

- requirement or audit criterion;
- audit method and audit trail;
- documents and records reviewed;
- persons interviewed and processes observed;
- systems, sites and technical components examined;
- sample population, selection method and sampled items;
- external assurance evidence and reliance outcome;
- objective evidence obtained;
- factual conclusion and any limitation;
- cross-reference to findings and report sections.

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

Annex E (Normative) Evaluation results matrix

Requirement	Applicability	Method	Evidence / sample	Reliance	Result	Finding reference
[ID]	Applicable / N/A	Document / interview / observation / sampling / test	[evidence and sample]	Full / Partial / None	C / Major NC / Minor NC / N/E / OBS	[reference]

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