EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

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

NL-SYS-02

NL EUDI Wallet Certification System

Vocabulary

RC1.0

2026.10.20

Document reference	NL-SYS-02
Version	*RC1.0*
Status	Release Candidate
Date	*20/10/206*
Document type	*Vocabulary*
Parent framework	*none*
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	European Digital Identity Wallets and the electronic identification scheme under which they are provided
Primary audience	*System/Scheme Owner, CABs, EUDI Wallet providers, PID Provider*
Secondary audience	*EUDI Wallet ecosystem stakeholders*
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Subsidiary Documents	*NL Certification System Documents*

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

History of changes			
Version	Change	State	Date
RC1.0	First Consolidated Version following European Collaboration and Refinement Discussion with BZK-Policy Department and Legal.	Release Candidate	2026-10-20

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

Table of Contents

Acronyms and Abbreviations 5
Terms by Category 6
Alphabetical Glossary 9

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

Acronyms and Abbreviations

Acronym	Full Term
CA	Certificate Authority
CAB	Conformity Assessment Body
CAB-CB	Conformity Assessment Body – Certification Body
CAB-ITSEF	Conformity Assessment Body – Testing Laboratory (ITSEF)
CP	Certificate Policy
EAA	Electronic attestation of attributes
FAR	False accept rate
FRR	False reject rate
HSM	Hardware security module
IDVP	Identity verification provider
LoA	Level of Assurance
LoA "High"	Level of Assurance "High"
LoA "Substantial"	Level of Assurance "Substantial"
LoIP	Level of identity proofing
Acronym	**Full Term**
MCD	mdoc App capability descriptor
MSO	Mobile security object
NAB	National Accreditation Bodies
PID	Person Identification Data
PKI	Public Key Infrastructure
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualified Electronic Signature
QSCD	Qualified Electronic Signature Creation Device
QTSP	Qualified Trust Service Provider
SAAO	Secure area attestation object
SA-Application	Secure area application
TOE	Target of Evaluation
WSCA	Wallet Secure Cryptographic Application
WSCD	Wallet Secure Cryptographic Device
WUA	Wallet Unit Attestation
WUTA	Wallet Unit Trust Attestation
WUVA	Wallet Unit Validity Attestation
eID means	Electronic identification means

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

Terms by Category

Actor

Entities that participate in the EUDI Wallet ecosystem

- Attestation Provider
- Authentic Source
- Conformity Assessment Body (CAB)
- Conformity Assessment Body – Certification Body (CAB-CB)
- Conformity Assessment Body – Testing Laboratory (ITSEF) (CAB-ITSEF)
- Device manufacturer
- Holder
- Identity verification provider (IDVP)
- Intermediary
- National Accreditation Bodies (NAB)
- Provider of registration certificates
- Provider of wallet-relying party access certificates
- Public Sector Body
- Qualified Electronic Signature Remote Creation Provider
- Qualified Trust Service Provider (QTSP)
- Registrar
- Relying Party
- User
- Verifier
- Wallet Provider
- Wallet User

Component

Technical components of the EUDI Wallet architecture

- Composite TOE
- Hardware security module (HSM)
- Holder Wallet Unit Keystore mdoc App
- Qualified signature creation device (QSCD)
- Relying Party Instance
- Target of Evaluation (TOE)
- Verifier Wallet Unit
- Wallet Instance
- Wallet Secure Cryptographic Application (WSCA)
- Wallet Secure Cryptographic Device (WSCD)
- Wallet Solution
- Wallet Unit

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

Credential

Types of credentials and attestations

- Account authentication factor
- Action key
- Attestation
- Attribute
- Authentication factor
- Electronic attestation of attributes (EAA)
- Electronic attestation of attributes issued by or on behalf of a public sector body
- Electronic identification means (eID means)
- External token
- Inherent authentication factor
- Knowledge-based authentication factor mdoc
- Person Identification Data (PID)
- PID key
- PID key authentication factor
- Possession-based authentication factor
- Qualified Electronic Attestation of Attributes (QEAA) user account
- Wallet Unit Attestation (WUA)
- Wallet Unit Trust Attestation (WUTA)
- Wallet Unit Validity Attestation (WUVA)

Data

- Biographical data
- False accept rate (FAR) False reject rate (FRR) mdoc App capability descriptor (MCD)
- Namespace Pseudonym
- Secure area attestation object (SAAO) Subject

Other

- Administrative validity period
- Specified requirement
- Supervised
- Technical validity period
- Unsupervised

Process

Processes and operations in the wallet lifecycle

- Authentication
- Binding
- Conformity assessment
- Cryptographic binding
- Device attestation

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

- Device binding
- Electronic identification scheme
- Issuance
- Notification
- On-boarding Pairing
- PID issuance
- Provisioning Selective Disclosure strong User authentication user binding

Security

Security-related concepts and mechanisms

- Asymmetric cryptography
- Certificate Policy (CP) critical assets
- Device key
- Embedded disclosure policy
- Qualified Electronic Signature (QES)
- Qualified Electronic Signature Creation Device (QSCD) risk register seal
- Secure area
- Secure area application (SA-Application) signature
- Wallet Key

Trust

Trust framework and infrastructure concepts

- access certificate assurance (evaluation) assurance (identity proofing) Attestation Revocation List Attestation Rulebook
- Attestation Status List
- Attestation type
- Certificate Authority (CA)
- Level of Assurance "High" (LoA "High")
- Level of Assurance "Substantial" (LoA "Substantial")
- Level of Assurance (LoA)
- Level of identity proofing (LoIP) Public Key Infrastructure (PKI) registration certificate SUA attestation
- Top-level certificate
- Trust Anchor
- Trust Framework Trusted List wallet

Alphabetical Glossary

A

access certificate

A certificate for electronic seals or signatures authenticating and validating the (Wallet-) Relying

Party, issued by a provider of wallet-relying party access certificates

Category: Trust

Source: CIR 2024/2977 (CIR), Article 2(12)

Account authentication factor

Authentication factor allowing Wallet Users to authenticate to the Wallet Providers and get access to their User Account.

Category: Credential

Source: CEN TS 18098, Section 3.17

Action key

Key used by an mdoc App to endorse one of its actions, such as credential holder verification.

Category: Credential

Source: CEN TS 18098, Section 3.1

Administrative validity period

The date(s) from and/or up to which the attributes in the attestation are valid, which are represented as attribute(s) in the attestation. Note: Some attestations, for instance diplomas, do not have an administrative validity period.

Category: Other

Source: Architecture Reference Framework (ARF), Section 2.3

assurance (evaluation)

grounds for confidence that a target of evaluation (TOE) meets the security functional requirements

Category: Trust

Source: EN ISO/IEC 15408-1, 3.6

assurance (identity proofing)

degree of confidence in the claimed or asserted identity of a person

Note 1 to entry: The definition is derived from EU Regulation 2014/910, art. 8.

Category: Trust

Source: EU Regulation 2014/910, art. 8

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

Asymmetric cryptography

A cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

Category: Security

Source: ISO/IEC 18013-5, Section 4.1

Attestation

When not further qualified, a collective term for a QEAA, PuB-EAA, or (non-qualified) EAA.

Category: Credential

Source: Architecture Reference Framework (ARF)

Attestation Provider

When not further qualified, a collective term for QEAA Provider, PuB-EAA Provider, or (non qualified) EAA Provider.

Category: Actor

Source: Architecture Reference Framework (ARF), Section 3.6-3.8

Attestation Revocation List

A mechanism provided by a PID Provider or an Attestation Provider (or a trusted party acting on its behalf) for communicating the revocation status of PIDs and attestations, by publishing a list of identifiers of revoked PIDs or attestations.

Category: Trust

Source: Architecture Reference Framework (ARF)

Attestation Rulebook

A document describing the attestation type, namespace(s), and other features for a specific attestation type.

Category: Trust

Source: Architecture Reference Framework (ARF)

Attestation Status List

A mechanism provided by a PID Provider or an Attestation Provider (or a trusted party acting on its behalf) for communicating the revocation status of PIDs and attestations, by publishing status information (Valid or Invalid) for all relevant PIDs or attestations.

Category: Trust

Source: Architecture Reference Framework (ARF)

Attestation type

An identifier for a type of attestation, unique within the context of the EUDI Wallet ecosystem.

Category: Trust

Source: Architecture Reference Framework (ARF)

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

Attribute

A characteristic, quality, right or permission of a natural or legal person or of an object.

Category: Credential

Source: European Digital Identity Regulation (eIDAS 2.0)

Authentic Source

A repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union law or national law, including administrative practice.

Category: Actor

Source: European Digital Identity Regulation (eIDAS 2.0)

Authentication

An electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form.

Category: Process

Source: European Digital Identity Regulation (eIDAS 2.0)

Authentication factor

Possession-based authentication factor, knowledge-based authentication factor or inherent authentication factor.

Category: Credential

Source: CEN TS 18098, Section 3.13

B

Binding

Act or process of securing, attaching, or tying something together.

Note 1 to entry: It can also describe as a state of being committed or obligated.

Note 2 to entry: Binding is the logical link established between two or more items. These items may be data, person or entity. This binding can be for instance between data and issuer, data and person, data and device or person and device.

Category: Process

Source: CEN TS 18098, Section 3.3

Biographical data

Personalized details of the bearer of the document appearing as text in the visual and machine readable zones on the MRTD, or on the chip if present.

Category: Data

Source: CEN TS 18098, Section 3.4

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

C

Certificate Authority (CA)

An entity which is trusted by one or more parties in the EUDI Wallet ecosystem to create and seal certificates.

Category: Trust

Source: European Digital Identity Regulation (eIDAS 2.0), Section 3.18

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Category: Security

Source: Architecture Reference Framework (ARF), Section 6

Composite TOE

part of a composite product being subject to composite TOE evaluation

Note 1 to entry: A composite TOE can contain parts that are independent from the base component or base TOE respectively. For simplification, such parts are considered as belonging to the dependent component.

Note 2 to entry: The composite TOE evaluation can be applied as many times as necessary to a multi-component product, in an incremental approach.

Category: Component

Source: EN 17640:2022+ A1:2026, 3.22

Conformity assessment

Demonstration that specified requirements are fulfilled.

Category: Process

Source: CEN TS 18098, Section 3.5

Conformity Assessment Body (CAB)

A conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment.

Category: Actor

Source: European Digital Identity Regulation (eIDAS 2.0), Article 2, point 13

Legal References: Article 2, Regulation (EU) 765/2008

Conformity Assessment Body – Certification Body (CAB-CB)

third-party conformity assessment body that issues and manages certificates

Category: Actor

Source: EN ISO/IEC 17065, 3.12

Conformity Assessment Body – Testing Laboratory (ITSEF) (CAB-ITSEF)

conformity assessment body that performs testing or evaluation activities

Category: Actor

Source: Adopted from PN-EN 17025, 3.6

critical assets

Assets within or in relation to a Wallet Unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, this would have a very serious, debilitating effect on the ability to rely on the Wallet Unit

Category: Security

Source: CIR 2024/2977 (CIR), Article 2(10)

Cryptographic binding

Association of two or more related elements of information using cryptographic techniques.

Category: Process

Source: CEN TS 18098, Section 3.8

D

Device attestation

Evidence demonstrating that the device manufacturer vouches for the security and trustworthiness of the device and providing technical details about the features it supports.

Category: Process

Source: CEN TS 18098, Section 3.9

Device binding

Property that an attestation is bound to a specific device (e.g. a WSCD) and cannot be used independent from that device.

Note 1 to entry: Device binding protects the attestation against copying or cloning, which enhances its security. A PID provider or an Attestation Provider implements device binding by including a cryptographic public key in the attestation and signing it. The corresponding private key is protected by the certified WSCD used by the Wallet Unit.

Note 2 to entry: Device binding is a kind of cryptographic binding, where the secret key is securely stored in the device.

Category: Process

Source: CEN TS 18098, Section 3.10

Device key *mdoc authentication key*

Category: Security

Source: CEN TS 18098, Section 3.11

Device manufacturer

Manufacturer of the device on which the Wallet Solution is installed.

Note 1 to entry: It may be the mobile manufacturer, the operating system (OS) or equipment manufacturer (OEM), or computer manufacturer.

Category: Actor

Source: CEN TS 18098, Section 3.12

E

Electronic attestation of attributes (EAA)

An attestation in electronic form that allows attributes to be authenticated.

Category: Credential

Source: European Digital Identity Regulation (eIDAS 2.0)

Electronic attestation of attributes issued by or on behalf of a public sector body

An electronic attestation of attributes issued by a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII.

Category: Credential

Source: European Digital Identity Regulation (eIDAS 2.0), Annex VII, Article 45f

Also known as: PuB-EAA

Electronic identification means (eID means)

Material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service.

Note 1 to entry: This definition is drawn from eIDAS article 3.

Category: Credential

Source: CEN TS 18098, Section 3.22

Electronic identification scheme

A system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons.

Category: Process

Source: European Digital Identity Regulation (eIDAS 2.0)

Embedded disclosure policy

A set of rules, embedded in an electronic attestation of attributes by its provider, that indicates the conditions that a wallet-relying party has to meet to access the electronic attestation of attributes

Category: Security

Source: CIR 2024/2979 (CIR), Article 2(9)

External token

Container of a person identification data (PID) and/or cryptographic keys, that allows the onboarding process in some scenarios, assuring a Level of Assurance "High" or equivalent.

Note 1 to entry: "Equivalent" stands for those cases where the solution is provided at an eIDAS Level of Assurance "High" plus other means that increases it to an equivalent of eIDAS Level of Assurance "High".

Note 2 to entry: According to the definition given in the Architecture and Reference Framework, an external token is a local external Wallet Secure Cryptographic Device (Local External WSCD).

Category: Credential

Source: CEN TS 18098, Section 3.23

F

False accept rate (FAR)

Proportion of verification transactions with false biometric claims erroneously accepted.

Category: Data

Source: CEN TS 18098, Section 3.24

False reject rate (FRR)

Proportion of verification transactions with true biometric claims erroneously rejected.

Category: Data

Source: CEN TS 18098, Section 3.25

H

Hardware security module (HSM)

Physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital keys and other secrets, as well as crypto-processing.

Category: Component

Source: CEN TS 18098, Section 3.26

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

Holder

A User wishing to use their Wallet Unit to present attributes from a PID or attestation to the User of another Wallet Unit. Notes: See also Verifier.

Category: Actor

Source: Architecture Reference Framework (ARF)

Holder Wallet Unit

A Wallet Unit used by a Holder.

Category: Component

Source: Architecture Reference Framework (ARF), Section 3.2

I

Identity verification provider (IDVP)

Entity carrying out identity verification (or part of) of an individual using an identity document.

Category: Actor

Source: CEN TS 18098, Section 3.27

Inherent authentication factor

Factor confirmed as being bound to a person that is based on a physical Attribute of a natural person, and of which the subject is required to demonstrate that they have that physical Attribute.

Category: Credential

Source: CEN TS 18098, Section 3.16

Intermediary

A Relying Party that offers services to other (intermediated) Relying Parties to, on their behalf, connect to Wallet Units and request the User attributes that these intermediated Relying Parties need.

Category: Actor

Source: Architecture Reference Framework (ARF)

Issuance

Process of issuing and possibly provisioning.

Note 1 to entry: This term relates to a credential, and designates its creation by an authority, and possibly its provisioning. It encompasses the formating of the data and its signature using a cryptographic algorithm to obtain a credential.

Category: Process

Source: CEN TS 18098, Section 3.28

K

Keystore

A hardware-backed repository and service in which non-critical cryptographic assets are generated, stored, and used exclusively inside a dedicated hardware security boundary. Notes: Examples include a Secure Element, a TPM, TEE, or secure enclave, or a remote HSM. - Critical cryptographic assets are generated, stored, and used in a WSCA/WSCD.

Category: Component

Source: Architecture Reference Framework (ARF), Section 4.3.2

Knowledge-based authentication factor

Factor confirmed as being bound to a person where the subject is required to demonstrate knowledge of it.

Category: Credential

Source: CEN TS 18098, Section 3.15

L

Level of Assurance "High" (LoA "High")

Assurance level which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, the purpose of which is to prevent misuse or alteration of the identity.

Note 1 to entry: This definition is inspired from eIDAS article 8(2)c

Category: Trust

Source: CEN TS 18098, Section 3.30

Level of Assurance "Substantial" (LoA "Substantial")

Assurance level which provides a substantial degree of confidence in the claimed or asserted identity of a person, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity.

Note 1 to entry: This definition is inspired from eIDAS article 8(2)b

Category: Trust

Source: CEN TS 18098, Section 3.31

Level of Assurance (LoA)

Assurance level of the reliability and quality of the (1) enrolment, (2) electronic identification means management, (3) authentication, (4) management and organization of an electronic identification means.

Note 1 to entry: This definition is drawn from eIDAS article 8.

Category: Trust

Source: CEN TS 18098, Section 3.29

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

Level of identity proofing (LoIP)

Confidence achieved in the identity proofing.

Category: Trust

Source: CEN TS 18098, Section 3.32

M

mdoc

Credential formatted in accordance with ISO/IEC 18013-5:2021.

Category: Credential

Source: CEN TS 18098, Section 3.33

mdoc App

Application on a mobile device that manages user Attributes and credentials for electronic identification purposes and controls access to the user Attributes and credentials whether the user Attributes and credentials are stored on the mobile device, on a server or on an external device.

Note 1 to entry: In the context of this document, the mdoc App corresponds to the Wallet Instance (and not the Wallet Unit).

Category: Component

Source: CEN TS 18098, Section 3.34

mdoc App capability descriptor (MCD)

Set of data describing capabilities of mdoc App including one or more secure area attestation objects.

Category: Data

Source: CEN TS 18098, Section 3.35

Mobile security object (MSO)

Mobile Security Object as defined in ISO/IEC 18013-5:2021 §9.1.2.3.

Source: CEN TS 18098, Section 3.36

N

Namespace

A specification of the attribute identifier, syntax and semantics of attributes that can be used in an attestation, having an identifier that is unique within the context of the EUDI Wallet ecosystem.

Category: Data

Source: Architecture Reference Framework (ARF)

National Accreditation Bodies (NAB)

A body that performs accreditation with authority derived from a Member State under Regulation (EC) No 765/2008.

Category: Actor

Source: Architecture Reference Framework (ARF), Section 3.16

Legal References: Regulation (EU) 765/2008

Notification

The act of transferring information to the European Commission.

Category: Process

Source: Architecture Reference Framework (ARF)

O

On-boarding

Process whereby the complete set of person identification data (PID) issued in accordance with Union or national laws - are issued to a Wallet Unit which either does not contain PID or contains invalid PID (revoked and/or expired), in a manner ensuring it is bound (1) to the User of that Wallet Unit, and (2) to the device in which the Wallet Unit was installed.

Note 1 to entry: On-boarding includes the processes described in 7.2.1. In particular on-boarding includes installation of client appliction(s) and software(s) on the User's device (depending on the architecture; those may be the entire Wallet Instance), and (2) wallet activation.

Note 2 to entry: Person identification data (PID) are defined by eIDAS article 3(3) and further refined by the implementing act.

Category: Process

Source: CEN TS 18098, Section 3.37

P

Pairing

Process whereby an initial linkage is establish between devices or a device and a natural person, to allow interactions between them.

Category: Process

Source: CEN TS 18098, Section 3.38

Person Identification Data (PID)

A set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.

Category: Credential

Source: European Digital Identity Regulation (eIDAS 2.0)

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

PID issuance

Process of issuing a person identification data (PID) to the User of a Wallet Unit and storing the person identification data (PID) in the Wallet Unit.

Note 1 to entry: The set of person identification data as defined by eIDAS article 3(3) and further refined by the implementing act is not issued, as those are immutable data assigned to a legal or natural person in accordance with national laws. What is issued is(are) ephemeral representation(s) of the person identification data as defined by eIDAS article 3(3) and further refined by the implementing act , under the shape of one or several credentials, which is(are) subsequently stored in the Wallet Unit. This(these) ephemeral representation(s) (credentials) is(are) also issued and stored in accordance with national laws.

Category: Process

Source: CEN TS 18098, Section 3.40

PID key

Cryptographic key allowing the Wallet to perform security operations and endorsed by the PID Provider.

Category: Credential

Source: CEN TS 18098, Section 3.41

PID key authentication factor

Authentication factor allowing the Wallet User to authenticate to the Wallet Unit and get access to the PID key.

Note 1 to entry: This authentication factor allows the Wallet User to use the PID keys.

Note 2 to entry: PID key authentication factor may be different for each PID key (if there are several) or the same.

Category: Credential

Source: CEN TS 18098, Section 3.19

Possession-based authentication factor

Factor confirmed as being bound to a person where the subject is required to demonstrate possession of it.

Category: Credential

Source: CEN TS 18098, Section 3.14

Provider of registration certificates

a natural or legal person mandated by a Member State to issue (wallet-relying party) registration certificates to (wallet-)relying parties registered in that Member State

Category: Actor

Source: CIR 2024/2982 (CIR), Article 2(15)

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

Provider of wallet-relying party access certificates

A natural or legal person mandated by a Member State to issue Relying Party access certificates to (Wallet-) Relying Parties registered in that Member State.

Category: Actor

Source: CIR 2024/2982 (CIR)

Also known as: Access CA, Access Certificate Authority

Provisioning

Loading and storage.

Note 1 to entry: This term relates to a credential, and designates its loading and storage.

Note 2 to entry: The provisioning of a credential does not include its issuance.

Category: Process

Source: CEN TS 18098, Section 3.43

Pseudonym

Data uniquely representing a User which in itself does not allow to infer the User's attributes or person identification data, without the use of additional information that is kept separately by the issuer of the data uniquely representing the user.

Category: Data

Source: Architecture Reference Framework (ARF)

Public Key Infrastructure (PKI)

Systems, software, and communication protocols that are used by EUDI Wallet ecosystem components to distribute, manage, and control public keys. A PKI publishes public keys and establishes trust within an environment by validating and verifying the public keys mapping to an entity.

Category: Trust

Source: Architecture Reference Framework (ARF), Section 6

Public Sector Body

A state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.

Category: Actor

Source: European Digital Identity Regulation (eIDAS 2.0)

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

Q

Qualified Electronic Attestation of Attributes (QEAA)

An electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V.

Category: Credential

Source: European Digital Identity Regulation (eIDAS 2.0), Annex V

Qualified Electronic Signature (QES)

An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Category: Security

Source: European Digital Identity Regulation (eIDAS 2.0)

Qualified Electronic Signature Creation Device (QSCD)

Configured software or hardware used to create an electronic signature that meets the requirements laid down in Annex II of the [European Digital Identity Regulation].

Category: Security

Source: European Digital Identity Regulation (eIDAS 2.0), Annex II

Related Terms: Qualified Electronic Signature

Qualified Electronic Signature Remote Creation Provider

A natural or a legal person that offers services related to the remote creation, validation, and management of qualified electronic signatures that meet legal requirements and standards in the [European Digital Identity Regulation] to be considered as legally equivalent to handwritten signatures.

Category: Actor

Source: Architecture Reference Framework (ARF), Section 3.9

Qualified signature creation device (QSCD)

Electronic signature creation device which creates qualified signature.

Note 1 to entry: The applicable requirements are laid down in eIDAS Annex II

Note 2 to entry: This definition is drawn from eIDAS article 3

Category: Component

Source: CEN TS 18098, Section 3.45

Qualified Trust Service Provider (QTSP)

Qualified Trust Service Provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.

Category: Actor

Source: European Digital Identity Regulation (eIDAS 2.0)

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

R

Registrar

The body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory who has been designated by a Member State

Category: Actor

Source: CIR 2024/2982 (CIR), Article 2(16)

registration certificate

A data object that indicates the attributes the Relying Party has registered to intend to request from Users

Category: Trust

Source: CIR 2024/2982 (CIR), Article 2(14)

Relying Party

A Relying Party that intends to rely upon Wallet Units for the provision of public or private services by means of digital interaction

Category: Actor

Source: CIR 2024/2977 (CIR), Article 2(11)

Relying Party Instance

A software and/or hardware module with the capability to interact with a Wallet Unit and to perform Relying Party authentication, that is controlled by a Relying Party.

Category: Component

Source: Architecture Reference Framework (ARF), Section 3.11.2

risk register *record of information relevant to the certification process about identified risks*

Category: Security

Source: Commission Implementing Regulation 2024/2981, art. 2(7)

S

seal

Data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity

Category: Security

Source: European Digital Identity Regulation (eIDAS 2.0)

Secure area

Isolated internal or attached area of a mobile device that ensures secure processing and storing of data even when the primary operating system (OS) is compromised.

Category: Security

Source: CEN TS 18098, Section 3.47

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

Secure area application (SA-Application)

Application of the secure area that manages credentials and that may manage user attributes for user identification purposes and can control access to the user attributes.

Category: Security

Source: CEN TS 18098, Section 3.48

Secure area attestation object (SAAO)

Set of data describing capabilities of SA-Application.

Category: Data

Source: CEN TS 18098, Section 3.49

Selective Disclosure

The capability enabling the User to present a subset of the attributes included in a PID or attestation.

Category: Process

Source: Architecture Reference Framework (ARF), Section 2.3

signature

Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Category: Security

Source: European Digital Identity Regulation (eIDAS 2.0)

Specified requirement

need or expectation that is stated

Category: Other

Source: CEN TS 18098, Section 3.51

strong User authentication

An authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

Category: Process

Source: European Digital Identity Regulation (eIDAS 2.0)

SUA attestation

An attestation used for strong user authentication in the context of electronic payments, such that, when a Relying Party sends a presentation request for the attestation to a Wallet Unit, it includes transactional data in the request.

Category: Trust

Source: Architecture Reference Framework (ARF)

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

Subject

Entity to whom the person identification data (PID) are associated.

Note 1 to entry: Subject includes natural person, legal person, or natural person representing a natural or legal person in accordance with eIDAS. For example, a parent (the "User") might hold the PID of his child (the "Subject").

Category: Data

Source: CEN TS 18098, Section 3.52

Supervised

Observed and/or directed by a human, which is skilled and has been trained to eliminate the risks of frauds.

Category: Other

Source: CEN TS 18098, Section 3.53

T

Target of Evaluation (TOE)

set of software, firmware, hardware, or a combination of these, possibly accompanied by guidance, which is the subject of an evaluation

Category: Component

Source: EN ISO/IEC 15408-1, 3.93

Technical validity period

The dates (and possibly times) from and up to which the attestation is valid, which are represented as metadata of the attestation. Note: All PIDs and attestations have a technical validity period, which is typically much shorter than its administrative validity period (if existent).

The technical validity period is chosen based on a risk analysis, e.g. with regard to User privacy.

Category: Other

Source: Architecture Reference Framework (ARF), Section 2.3

Top-level certificate

statement of conformity to European Commission and EDICG in accordance with EU 2024/1183 Article 5d.1. based on the set of certificates, resulted from implementation of all respective certification schemes within PL EUDI Wallet Certification system

Category: Trust

Source: EU 2024/1183, Article 5d.1

Trust Anchor

An authoritative entity represented by a public key and associated data. Note: based on RFC 5914.

Category: Trust

Source: Architecture Reference Framework (ARF), Section 6

Trust Framework

set of rules, standards, and legal requirements that define how digital identities can be securely created, verified, and shared across different stakeholders of EUDI Wallet ecosystem.

Category: Trust

Source: Architecture Reference Framework (ARF)

Trusted List

Repository of information about authoritative entities in a particular legal or contractual context which provides information about their current and historical status.

Category: Trust

Source: Architecture Reference Framework (ARF), Section 3.5

U

Unsupervised

not supervised

Category: Other

Source: CEN TS 18098, Section 3.54

User

A natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with the [European Digital Identity Regulation].

Category: Actor

Source: Architecture Reference Framework (ARF)

user account

account at the Wallet Provider allowing the Wallet User to request management operations of his Wallet Unit to the Wallet Provider on his behalf, after successful authentication with his account authentication factor(s)

Category: Credential

Source: CEN TS 18098, Section 3.55

user binding

property that the PID or attestation, meaning the data of the natural or legal person described in the PID or attestation, is under the control of the person that presents the PID or attestation to the Relying Party

Category: Process

Source: CEN TS 18098, Section 3.56

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

V

Verifier

A User wishing to use their Wallet Unit to request attributes from a PID or attestation from the User of another Wallet Unit.

Category: Actor

Source: Architecture Reference Framework (ARF)

Verifier Wallet Unit

A Wallet Unit used by a Verifier.

Category: Component

Source: Architecture Reference Framework (ARF), Section 3.2

W

wallet

electronic identification means which allows the User to securely store, manage and validate person identification data and electronic attestations of Attributes

Category: Trust

Source: CEN TS 18098, Section 3.57

Also known as: EUDI wallet

Wallet Instance

The application installed and configured on a Wallet User's device or environment, which is part of a Wallet Unit, and that the Wallet User uses to interact with the Wallet Unit

Category: Component

Source: CIR 2024/2977 (CIR), Article 2(6)

Wallet Key

cryptographic key allowing the Wallet Unit to carry out security operations and endorsed by the Wallet Provider

Category: Security

Source: CEN TS 18098, Section 3.59

Wallet Provider

A natural or legal person kto provides Wallet Solutions

Category: Actor

Source: CIR 2024/2979 (CIR), Article 2(9)

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

Wallet Secure Cryptographic Application (WSCA)

An application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the Wallet Secure Cryptographic Device

Category: Component

Source: CIR 2024/2977 (CIR), Article 2(7)

Wallet Secure Cryptographic Device (WSCD)

A tamper-resistant device that provides an environment that is linked to and used by the Wallet Secure Cryptographic Application to protect critical assets and provide cryptographic functions for the secure execution of critical operations

Category: Component

Source: CIR 2024/2977 (CIR), Article 2(8)

Wallet Solution

A combination of software, hardware, services, settings, and configurations, including Wallet Instances, one or more Wallet Secure Cryptographic Applications and one or more Wallet Secure

Cryptographic Devices **Category:** Component

Source: CIR 2024/2977 (CIR)

Wallet Unit

A unique configuration of a Wallet Solution that includes Wallet instances, Wallet Secure

Cryptographic Applications and Wallet Secure Cryptographic Devices provided by a Wallet

Provider to an individual Wallet User **Category:** Component

Source: CIR 2024/2977 (CIR), Article 2(2)

Wallet Unit Attestation (WUA)

A data object that describes the components of the Wallet Unit or allows authentication and validation of those components;

Category: Credential

Source: CIR 2024/2977 (CIR), Article 2(5)

Wallet Unit Trust Attestation (WUTA)

credential describing the properties of the Wallet Solution, the Wallet Instance, the device on which it is installed and the WSCD

Category: Credential

Source: CEN TS 18098, Section 3.66

Wallet Unit Validity Attestation (WUVA)

credential identifying a Wallet Instance, demonstrating that the Wallet Provider vouches for the security

Category: Credential

Source: CEN TS 18098, Section 3.67

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

Wallet User

natural person who is in control of the Wallet Unit

Category: Actor

Source: CEN TS 18098, Section 3.68

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