SLOVENSKI STANDARD
SIST-TS CEN/TS 18098:2026

01-oktober-2026

Smernice za vnašanje osebnih identifikacijskih podatkov uporabnikov v evropske denarnice za digitalno identiteto

Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets

Leitlinien für das Onboarding von persönlichen Identifikationsdaten der Nutzer in europäischen digitalen Identity Wallets

Lignes directrices pour l'intégration des données d'identification personnelle des utilisateurs dans les portefeuilles d'identité numérique européens

Ta slovenski standard je istoveten z: **CEN/TS 18098:2026**

ICS:

35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST-TS CEN/TS 18098:2026 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 18098

June 2026

ICS 35.240.15

English Version

Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets

Lignes directrices pour l'intégration des données d'identification personnelle des utilisateurs dans les portefeuilles d'identité numérique européens

Leitlinien für das Onboarding von persönlichen Identifikationsdaten der Nutzer in europäischen digitalen Identity Wallets

This Technical Specification (CEN/TS) was approved by CEN on 17 March 2026 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 18098:2026 E

Contents

Page

European foreword

This document (CEN/TS 18098:2026) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

The amended eIDAS [1] regulation introduces the concept of on-boarding of person identification data of natural or legal persons within a Wallet. In addition, the amended eIDAS [1] clarifies that on-boarding is also subject to conformity with the Level of Assurance “High”.

This entails first to define (1) the concept of on-boarding and (2) how to implement it.

In addition, despite the requirements for the Level of Assurance “High” pursuant to eIDAS [1] are defined in the annex of implementing act 2015/1502 [2] (legally binding) and further refined in a supporting guidance prepared by the eIDAS cooperation group [3] (non-binding), they remain difficult to interpret as they are fuzzy, which leads to diverging interpretations between Member States.

This document aims at solving these two shortcomings by providing harmonized definition, procedures and technical framework for the on-boarding of person identification data of natural or legal person within a Wallet, in line with the requirements of *Level of Assurance* “High” pursuant to eIDAS [1].

This document will sustain:

a) a shared understanding of trust, security and quality of person identification data obtained from Wallet by third parties;

b) harmonized procedures and technical framework applied for the on-boarding within the Wallet, taking into account all the best practices;

c) convergence of existing procedures and technical framework supporting the on-boarding within the Wallet;

NOTE 1 While eIDAS [1] talks of "on-boarding of users", this document talks of “on-boarding of person identification data” as it is more accurate to describe the process at stake.

NOTE 2 Many of the concepts and principles introduced by the first version of eIDAS are not modified by the amended version of eIDAS [1] and thus remain valid, e.g. Level of Assurance.

This document identifies:

— the data to be sent and stored in the wallet as part of the on-boarding as well as their format;

— the main scenarios for the on-boarding of person identification data within European Digital Identity Wallets;

— the requirements to achieve on-boarding reaching the *Level of Assurance* “High” pursuant to the annex of CIR 2015/1502 [2];

— for each of the scenario aforementioned the additional requirements to be met to achieve on-boarding reaching the *Level of Assurance* “High” pursuant to the annex of CIR 2015/1502 [2];

— the qualifications, expertise, skills and potentially accreditations needed for the conformity assessment by a Conformity Assessment Body (CAB) of the on-boarding of person identification data within a Wallet;

— the services and resources that could be used – if available – for the successful on-boarding which can only be provided by Member States;

In addition, this document defines the metadata, scenarios, and particular requirements which are relevant during the on-boarding phase such that the Wallet can support after the on-boarding the specific privacy requirements explicitly envisioned in eIDAS [1], i.e.

— “[…] enable the user in a manner that is user-friendly, transparent, and traceable by the user […]” in eIDAS [1] article 5a(4);

— "Users shall have full control of the use of and of the data in their European Digital Identity Wallet" in eIDAS [1] article 5a(14);

— "[…] Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet […]" in eIDAS[1] article 5a(14);

— transparency of digital transactions, by making available to the User the descriptions of past transactions as well as data that were exchanged.

This document covers the various ways to carry out on-boarding of person identification data:

— in the course of a face to face interaction;

— remotely, including the use of either electronic identification means conforming to *Level of Assurance* "High" or electronic identification means conforming to *Level of Assurance* "Substantial" in conjunction with additional remote on-boarding procedures that together meet the requirements of Level of Assurance "High" as envisioned by eIDAS [1] article 5a(5) (a)(v) and article 5a(24).

This document is neutral with regard to the location of the storage of person identification data: they can be stored locally and/or remotely, and this document covers both cases. Local and remote storage are defined in the Architecture and Reference Framework [4]. Local storage of person identification data means storage of person identification data in the client side of the Wallet and/or in an External Token controlled by the User of the Wallet (e.g. electronic identity document, electronic identification means,…) and remote storage of person identification data means storage of person identification data in the server side of the Wallet (a cloud or remote server) endowed with Hardware Security Module(s) (HSM).

This document is neutral with regard to the Wallet architecture. It applies to (1) Wallets comprising only a client application (e.g. application on a mobile device), (2) Wallets entirely based on a server without a client application (e.g. server Wallet accessed through a web browser), or (3) combination thereof.

NOTE 3 This document will be further improved and refined in subsequent versions.

1 Scope

This document defines and describes the concept of on-boarding of person identification data (PID) within a Wallet. The scope of this document includes cases where a natural person is the User in control of a Wallet. This includes a natural person who is in control of their own information, as well as natural persons who control information to represent another natural person or a legal person. This document considers a single set of PID attributes linked to a single Wallet Unit. This does not exclude the issuance of multiple PIDs representing the same set of PID attributes, e.g. batch issuance.

It also provides the general workflow, the roles and responsibilities at stake, and links the on-boarding with the *Level of Assurance* concept underpinning eIDAS [1];

The scope of this document includes cases where a natural person is the User in control of a wallet. This includes a natural person who is in control of their own data as well as natural persons who control data to represent another natural person or legal person.

EXAMPLE If a natural person represents a legal person, the PID provider can issue a "representation PID" in an own Wallet Unit for representation purposes controlled by the natural person Wallet User. The "representation PID" is a kind of attestation which contains PID about the natural person (representative) and about the legal person (representee).

This document is limited to the on-boarding of an unique set of person identification data, complying with the legal provisions of eIDAS [1], in particular (1) issued in accordance with Union or National laws, and (2) conformant with the relevant implementing act [5].

The following aspects are out of scope of this document:

- the on-boarding of person identification data within a Wallet where the User is a legal person;
- other types of on-boarding, such as:
  - provisioning of person identification data after revocation, expiration or deletion;
  - addition of other Attributes (under the shape of attestations) in accordance with the requirement of *Level of Assurance* “High” which are not part of the set of person identification data but are part of the legal identity under National’s laws;
  - management of person identification data (deletion, update, etc.);
  - provisioning of person identification data which is not compliant with the relevant implementing act [5];
  - provisioning of a partial set of person identification data;
  - provisioning of supplemental set(s) of person identification data (multiple PIDs);

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18013-5:2021, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*

ISO/IEC 19989-3, *Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection*

CEN/TS 18099, *Biometric data injection attack detection*

Common Methodology for Information Technology Security Evaluation - Evaluation methodology - November 2022 - Revision 1 (https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf)

ETSI TS 119 461, *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects v2.1.1*

RFC 7905, *ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)*

RFC 8422, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
action key
key used by an mdoc App to endorse one of its actions, such as credential holder verification

[SOURCE: ISO/IEC TS 23220-4:2026 [6], 7.2.5.5 and A.1.5]

3.2
Attribute
characteristic, quality, right or permission of a natural or legal person or of an object

Note 1 to entry: A Credential is an evidence supporting a claim of Attribute of any type (including identity Attribute). Credential may contain none, one or several Attributes. The following items are Credentials:

— PID;

— Electronic attestation of Attributes (EAA);

— Electronic attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source;

— Qualified Electronic Attestation of Attributes (QEAA);

— Wallet Unit trust attestation;

— Wallet Unit Validity Attestation.

Note 2 to entry: This definition is drawn from eIDAS [1] article 2.

3.3
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.

3.4
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.

Note 1 to entry: The document is an identity document compliant with ICAO doc 9303 Ed8 [7] which may be a passport, a travel document or an identity card.

[SOURCE: ICAO doc 9303 Ed8 [7] part 1]

3.5
conformity assessment
demonstration that specified requirements are fulfilled

[SOURCE: EN ISO/IEC 17000:2020 [8]]

3.6
conformity assessment body
CAB
body that performs conformity assessment activities including calibration, testing, certification and inspection

Note 1 to entry: This definition is drawn from [9]

3.7
Credential
evidence or testimonials that support a claim of identity or assertion of an Attribute and usually are intended to be used more than once

Note 1 to entry: A Credential is an evidence supporting a claim of Attribute of any type (including identity Attribute). A Credential may take various encoding formats. For instance a Credential may contain or not the Attribute, or may be signed by an authority or not. The following items are Credentials:

— PID;

— Electronic attestation of Attributes (EAA);

— Electronic attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source;

— Qualified Electronic Attestation of Attributes (QEAA);

— Wallet Unit Trust Attestation;

— Wallet Unit Validity Attestation.

Note 2 to entry: This meaning of Credentials is much larger than the one considered in the recital of eIDAS [1].

[SOURCE: *Committee on National Security Systems (CNSS) Glossary* [10]]

3.8
cryptographic binding
association of two or more related elements of information using cryptographic techniques

[SOURCE: NIST [11]]

3.9
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

Note 1 to entry: ISO/IEC TS 23220-3:2026 [12] defines a framework for mobile capability descriptor which corresponds to device attestation.

Note 2 to entry: Examples of device attestation are (1) key attestation, (2) WSCD/WSCA attestation, or (3) evidence of proprietary App integrity check provided by the platform/OEM.

3.10
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.

[SOURCE: Architecture and Reference Framework [4]]

3.11
device key
mdoc authentication key

[SOURCE: ISO/IEC 18013-5:2021 [13]]

3.12
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.

3.13
authentication factor
possession-based authentication factor, knowledge-based authentication factor or inherent authentication factor

Note 1 to entry: This definition is based on [2] (annex).

3.14
possession-based authentication factor
factor confirmed as being bound to a person where the subject is required to demonstrate possession of it

Note 1 to entry: This definition is based on [2] (annex).

3.15
knowledge-based authentication factor
factor confirmed as being bound to a person where the subject is required to demonstrate knowledge of it

Note 1 to entry: This definition is based on [2] (annex).

3.16
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

Note 1 to entry: This definition is based on [2] (annex).

3.17
account authentication factor
authentication factor allowing Wallet Users to authenticate to the Wallet Providers and get access to their User Account

3.18
Wallet Unit authentication factor
authentication factor allowing the Wallet User to authenticate to the Wallet Unit and get access to the features of the Wallet Unit.

Note 1 to entry: This authentication factor allows the Wallet User to access the features of the Wallet Unit, but not to use the PID keys.

3.19
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.

3.20
electronic attestation of Attributes
EAA
attestation in electronic form that allows the authentication of Attributes

Note 1 to entry: An electronic attestation of Attributes (EAA) is a Credential.

[SOURCE: Regulation (EU) No 2024/1183 [14], article 3.]

3.21
electronic attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source
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

Note 1 to entry: An electronic attestation of Attributes issued by or on behalf of a public sector body responsible for an authentic source is a Credential meeting the requirements laid down in eIDAS [1] Annex VII. In particular, it is a Credential containing the Attribute(s) at stake and signed by an authority.

[SOURCE: Regulation (EU) No 2024/1183 [14], article 3.]

3.22
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 [1] article 3.