

STN P	Usmernenie pre zavádzanie osobných údajov používateľov v európskych peňaženkách digitálnych identít	STN P CEN/TS 18098 97 4239
------------------	--	--

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

Táto norma obsahuje anglickú verziu európskej normy.

This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 08/26

Táto predbežná slovenská technická norma je určená na overenie. Prípadné pripomienky pošlite do júna 2028 Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.

Obsahuje: CEN/TS 18098:2026

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

CEN/TS 18098:2026 (E)

Contents	Page
European foreword	6
Introduction	7
1 Scope	9
2 Normative references	9
3 Terms and definitions	10
4 Abbreviated terms	21
5 Conformance claim	23
6 Data storage location & on-boarding	23
6.1 Architecture of the Wallet	24
6.2 Storage of PID(s) and Electronic Attestation(s) of Attribute	25
6.3 Storage of cryptographic keys	25
7 Guidelines for on-boarding workflow	26
7.1 General	26
7.2 On-boarding	26
7.2.1 Overview	26
7.2.2 User vs Subject	29
7.2.3 Wallet installation and activation	29
7.2.4 Identity proofing & Wallet Unit credentials binding	36
7.2.5 PID issuance	38
7.3 Possible on-boarding workflows	40
7.3.1 Regular workflow	40
7.3.2 Alternative workflow	40
7.4 Mapping of on-boarding with ISO/IEC 23220 series	41
7.4.1 Mapping with ISO/IEC 23220-1:2023 [18]	41
7.4.2 Mapping with ISO/IEC TS WD7 23220-5:2025 [25]	43
7.5 Data to be provisioned during on-boarding	44
7.5.1 Overview	44
7.5.2 Wallet Unit Validity Attestation	44
7.5.3 Wallet Unit Trust Attestation	45
7.5.4 Cryptographic keys	46
7.5.5 Other Wallet data	52
7.5.6 PID	53
7.5.7 PID metadata	55
7.5.8 Impact of delegation of representation	56
7.6 Considerations regarding the Wallet Provider	58
7.6.1 Responsibilities of the Wallet Provider	58
7.6.2 Wallet Provider vs supplier and subcontractor	58
7.6.3 Privacy and data protection aspects	58
7.7 Cryptographic binding of credentials to a Wallet Unit	59
7.7.1 Overview	59
7.7.2 Process to cryptographically bind a credential to the Wallet Unit	59
7.7.3 Proof of Association (PoA)	59
7.7.4 Proof of Possession (PoP)	60
8 Requirements to meet the Level of Assurance 'High'	61
8.1 General	61
8.2 Wallet installation and activation	62
8.2.1 User eligibility checks and User Account creation	62
8.2.2 Client application loading and installation	62
8.2.3 Binding between the User, the User's device and the Wallet Unit	62
8.2.4 Configuration of the Wallet Unit	65
8.2.5 Initialisation of the Wallet Unit	66

8.2.6	Finalisation	67
8.3	Identity proofing & Wallet Unit credentials binding	67
8.3.1	Requirements applicable to the whole process	67
8.3.2	Identification of the Subject	67
8.3.3	Identity verification of the User	68
8.3.4	Identification and authentication of the Wallet Unit	80
8.3.5	Verification of binding between the identified User and the Wallet Unit	80
8.3.6	Verification of the relationship between the identified User and the Subject	80
8.3.7	Collection of information needed to issue credentials	80
8.4	PID issuance	82
8.4.1	Requirements applicable to the whole process	82
8.4.2	Eligibility checks of the Wallet and issuance of PID	82
8.4.3	Identification and authentication of the Wallet Unit	82
8.4.4	Provisioning of credentials	82
8.4.5	Finalisation of PID issuance	83
8.5	Case of alternative workflows for on-boarding	83
8.5.1	C-REQ	83
8.6	Requirements common to all processes	83
8.6.1	REQ	83
8.6.2	C-REQ	84
8.6.3	C-REQ	84
8.6.4	REQ	84
8.7	Requirements regarding the Wallet Unit	85
8.7.1	REQ	85
8.7.2	REQ	85
8.7.3	REQ	85
8.7.4	REQ	85
8.7.5	RECO	86
8.7.6	C-REQ	86
8.7.7	REQ	86
8.7.8	RECO	86
8.7.9	REQ	86
8.7.10	REQ	86
8.7.11	C-REQ	87
8.7.12	REQ	87
8.7.13	POS	87
8.8	Requirements regarding authentication factors	87
8.8.1	REQ	87
8.8.2	REQ	87
8.8.3	REQ	87
8.8.4	REQ	88
8.8.5	C-REQ	88
8.8.6	C-REQ	88
8.8.7	C-REQ	89
8.8.8	C-REQ	89
8.8.9	C-REQ	89
8.8.10	C-REQ	89
8.8.11	C-REQ	90
8.8.12	C-RECO	90
8.8.13	C-REQ	90
8.8.14	C-REQ	91
Annex A	(informative) Use cases for on-boarding	92
A.1	General	92
A.2	On-boarding using an External Token as a local proxy of the PID Provider	92
A.2.1	Overview	92
A.2.2	Detailed description	92
A.2.3	Coverage of the on-boarding processes	94

CEN/TS 18098:2026 (E)

A.2.4	Example of implementation	95
A.2.5	Pros and cons	96
A.3	On-boarding using a Qualified Signature Creation Device (QSCD)	97
A.3.1	Overview	97
A.3.2	Detailed description	97
A.3.3	Coverage of the on-boarding processes	98
A.3.4	Pros and Cons	99
A.4	On-boarding with a Wallet Unit using an External Token as WSCD/WSCA	100
A.4.1	Overview	100
A.4.2	Detailed description	100
A.4.3	Coverage of the on-boarding	107
A.4.4	Examples of implementation	108
A.4.5	Risk assessment and mitigation measures	110
A.4.6	Pros and cons	111
A.5	On-boarding using OID4VCI	111
A.5.1	Overview	111
A.5.2	Detailed description (OID4CVCI protocol supplemented by the work of POTENTIAL Large Scale Pilot [52])	111
A.5.3	Detailed description (OID4CVCI protocol supplemented by HAIP [53])	117
A.5.4	Coverage of the on-boarding (OID4CVCI protocol supplemented by the work of POTENTIAL Large Scale Pilot [52])	117
A.5.5	Example of implementation (OID4CVCI protocol supplemented by the work of POTENTIAL Large Scale Pilot [52])	118
A.5.6	Pros and cons	123
A.6	On-boarding using REST API (based on HPKE SA protocol)	123
A.6.1	Overview	123
A.6.2	Detailed description	123
A.6.3	Coverage of the on-boarding	124
A.6.4	Pros and cons	125
Annex B (informative)	Requirements to meet the Level of Assurance 'High' in the context of the use cases for on-boarding	126
B.1	General	126
B.2	On-boarding using OID4VCI	126
B.2.1	REQ-OIDVCI	126
B.2.2	REQ-OIDVCI	126
B.2.3	REQ-OIDVCI	127
B.2.4	REQ-OIDVCI	127
B.2.5	REQ-OIDVCI	127
B.3	On-boarding using REST API (based on HPKE SA protocol)	127
B.3.1	REQ-RESTAPI	127
B.3.2	REQ-RESTAPI	128
B.3.3	REQ-RESTAPI	128
B.3.4	REQ-RESTAPI	128
B.3.5	REQ-RESTAPI	128
B.3.6	REQ-RESTAPI	129
Annex C (informative)	Example of use cases of Electronic Attestation of Attribute(s) from the PID set	130
C.1	General	130
C.2	Support of data minimization and control of the level of trust	130
C.2.1	Overview	130
C.2.2	Benefits of Electronic Attestation of Attribute(s) from the PID set	131
C.2.3	Mapping of Electronic Attestation of Attribute(s) from the PID set and PID to the various contexts	132
C.3	Creation of a single bundle combining one or several Attribute(s) and the Attribute(s) of the PID set to which they relate	133
C.3.1	Overview	133

C.3.2 Benefits of Electronic Attestation of Attribute(s)	133
C.4 Comparison with PID	134
Annex D (informative) Overview of the ephemeral keys a Wallet Unit can use	135
Annex E (informative) On-boarding and Electronic Attestations of Attributes	137
E.1 Overview	137
E.2 Format of credentials	137
E.3 Electronic Attestation of Attribute(s) from the PID set	138
Annex F (informative) Other possible credential formats	139
Annex G (informative) Eligibility checks	142
G.1 Overview	142
G.2 Eligibility checks of the User	142
G.3 Eligibility checks of the User's device	142
G.4 Eligibility checks of the Wallet Provider and Wallet Unit	143
Annex H (informative) On-boarding policies	144
Annex I (informative) Mapping of the criteria for LoA "High" with the requirements for on-boarding	145
Annex J (informative) Mapping of on-boarding with the criteria for Level of Assurance	156
J.1 Overview	156
J.2 Enrolment	156
J.3 Electronic identification means management	156
J.4 Management and organisation	158
J.5 Coverage of the LoA criteria	159
Annex K (informative) Coverage of the provisions of eIDAS [1] by this document	162
Bibliography	164

CEN/TS 18098:2026 (E)**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);

CEN/TS 18098:2026 (E)

- “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*

CEN/TS 18098:2026 (E)

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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN