



SLOVENSKI STANDARD

kSIST-TS FprCEN/TS 18098:2025

01-september-2025

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: FprCEN/TS 18098

[kSIST-TS FprCEN/TS 18098:2025](https://standards.sist.si/catalog/standards/sist/856cd015-7f1b-4b66-9c39-59f1bd386c3d/kSIST-TS-FprCEN-TS-18098-2025)

ICS:

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

kSIST-TS FprCEN/TS 18098:2025

en,fr,de

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/TS 18098

July 2025

ICS

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 draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 224.

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

<https://standards.iteh.ai/catalog/standards/sist/856ed6f5-7f4b-4b60-9c59-59f4bd586c5d/ksist-ts-fprcen-ts-18098-2025>

<https://standards.iteh.ai/catalog/standards/sist/856ed6f5-7f4b-4b60-9c59-59f4bd586c5d/ksist-ts-fprcen-ts-18098-2025>



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

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

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[14]	41
7.4.2 Mapping with ISO/IEC TS WD7 23220-5:2025[21]	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

FprCEN/TS 18098 (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 [55])	111
A.5.3	Detailed description (OID4CVCI protocol supplemented by HAIP [56])	117
A.5.4	Coverage of the on-boarding (OID4CVCI protocol supplemented by the work of POTENTIAL Large Scale Pilot [55])	117
A.5.5	Example of implementation (OID4CVCI protocol supplemented by the work of POTENTIAL Large Scale Pilot [55])	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