SLOVENSKI STANDARD
SIST-TP CEN/TR 17982:2024

01-februar-2024

Analiza vrzeli v standardih evropskih denarnic za digitalno identiteto

European Digital Identity Wallets standards Gap Analysis

Analyse von europäischen Normungsbedarfen für digitale Identitätsbrieftaschen

Analyse des écarts entre les standards existants et les exigences du portefeuille européen d’identité numérique

Ta slovenski standard je istoveten z: CEN/TR 17982:2023

ICS:

35.030	Informacijska varnost	IT Security
35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST-TP CEN/TR 17982:2024 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER REPORT

CEN/TR 17982

September 2023

ICS 35.240.15; 35.030

English Version

European Digital Identity Wallets standards Gap Analysis

Analyse des écarts entre les standards existants et les exigences du portefeuille européen d'identité numérique

Analyse von europäischen Normungsbedarfen für digitale Identitätsbrieftaschen

This Technical Report was approved by CEN on 14 August 2023. 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.

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

This document (CEN/TR 17982:2023) has been prepared by Technical Committee CEN/TC 224 “Personal identification, electronic signature and cards and their related systems and operations”, 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.

Introduction

The proposal of revision of the eIDAS regulation [1] introduces the concept of European Digital Identity Wallet.

Throughout the proposal of regulation, numerous requirements are set forth regarding the Wallet, its functionalities, the services it shall provide to user, as well as its interactions with other entities it shall support.

Interoperability and user experience of the Wallet are key factors for its uptake but also for its large use and reach amongst European population. So much that the proposal of regulation also vests the European Commission with the responsibility to define the technical specifications the Wallet shall meet through implementing acts, which are legally binding. In that regards, standards are crucial.

This technical report aims at supporting the implementation of the Wallet as defined in the proposal of regulation by:

- Identifying the articles and clauses in the proposal of regulation defining requirements that are applicable to the Wallet;

- Identifying for each requirement listed above (1) the available standards or standards under preparation that could be used or considered, as well as their scope of application, and (2) the missing standards (named “Missing Standard” in the document) which may require to start standardization activities;

- Proposing suggestions for standards under preparation so that they fully meet the requirements listed above (named “Recommendation” in the document);

In that regards, this technical report may be useful to several stakeholders:

- European Commission that could use this technical report as a guide when preparing implementing act for the implementation of the Wallet;

- Authorities willing to issue a Wallet or entities willing to provide Wallet that could use it to easily identify available standards on which they could leverage to implement, use or interact with the Wallet;

- Standardization Organisations that could use it to easily identify normalization gaps where they could contribute by preparing standards in accordance with their mandate and core competencies;

- Entity tasked by the European Commission in charge of preparing the European Digital identity Wallet reference implementation;

- Pilot projects launched by the European Commission to build and realize use cases based on the European Digital Identity Wallet;

The purpose of this document that started before the Architecture Reference Framework (ARF) release is to map the legal text (here the proposal of revision of the eIDAS regulation [1]) to available standards and identify possible gaps. Note that the proposal of revision of the eIDAS regulation [1] is likely to be updated as the legislative process is still ongoing at the time of preparation of this document.

1 Scope

This document identifies relevant existing standards and standards work in progress which could support implementation of the European Digital Identity Wallets. It also identifies missing work items and overlaps in standards and is supposed to serve as a roadmap for future standardization projects in the area. This document takes into account the gap analysis produced by TC224/WG17.

This document is based on the proposal of revision of the eIDAS regulation [1] which was the only available text at the time this document was initiated

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

3.1
wallet
product and service that allows the user to store identity data and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline; and to create qualified electronic signatures and seals

Note 1 to entry Adapted from article 3(42) of [1]

4 Gap Analysis

Item	Article	Topic	Possible standards – for specific requirements
1	3(42) 6a(3)b	"'European Digital Identity Wallet' is a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and **to create qualified electronic signatures and seals**"; "European Digital Identity Wallets shall enable the user to: (b) **sign by means of qualified electronic signatures**." This requirement may be achieved in several ways: either (1) the Wallet has the capacity to sign/seal by means of qualified electronic signature/seal – and thus is a QSCD, or (2) relies on an external but local qualified signature/seal creation device with which it interacts locally to create a	**<u>The following standards have been identified</u>** *If the Wallet has the capacity to sign/seal by means of qualified electronic signature/seal:* -CEN/EN 419 212-1 - Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions -CEN/EN 419 212-2 - Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services *If the Wallet relies on an external but local qualified signature/seal creation device:* *1/For applicative layer*

Item	Article	Topic	Possible standards – for specific requirements
		qualified signature/seal or (3) relies on a remote qualified signature/seal creation device with which it interacts to create a qualified signature/seal. *Case 1: If the Wallet has the capacity to sign/seal by means of qualified electronic signature/seal:* The creation of qualified signature/seal is supported by a local secure hardware part of the Wallet, such as a SE, an eUICC, a TPM,…. The standard CEN/EN 419 212 prepared by the CEN/TC224 to support qualified signature/seal is relevant and should be considered with the following reservations: • The device authentication protocols described in part 3 may not be applicable depending on the form factor (SE/eUICC...); • The privacy protocols described in part 4 may not be relevant; • The trust eServices described in part 5 may not be relevant; Part 1 and part 2 seem to be the most relevant parts of this series. *Case 2: If the Wallet relies on an external but local qualified signature/seal creation device:* The creation of qualified signature/seal is supported by a local but external secure hardware such as an external token or an electronic identification document (e.g. national identity card). The standard CEN/EN 419 212 prepared by the CEN/TC224 to support qualified signature/seal is relevant and should be considered with the following reservations: • The device authentication protocols described in part 3 may not be applicable depending on the form factor; • The privacy protocols described in part 4 may not be relevant;	-CEN/EN 419 212-1 - Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions -CEN/EN 419 212-2 - Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services -ISO/IEC IS 7816-15 - Identification cards — Integrated circuit cards - Cryptographic information application *2/For the transport protocols to be used for the local communication between the Wallet and the QSCD:* -ISO/IEC IS 7816-3 - Identification cards — Integrated circuit cards - Cards with contacts — Electrical interface and transmission protocols -ISO/IEC IS 18004 - QR Code bar code symbology specification -ISO/IEC IS 24778 - Aztec Code bar code symbology specification -ISO/IEC IS 16022 - Data Matrix bar code symbology specification -ISO/IEC IS 23634 (DIS) - JAB Code polychrome bar code symbology specification -ISO/IEC IS 18092 – Near Field communication -ETSI/EN 302190 - Near Field Communication -USB specifications as defined by the USB forum Note: This list is not exhaustive. Additional standards and protocols may exist, or change in the future. *If the Wallet relies on a remote qualified signature/seal creation device:* -CEN/EN 419 241-1 - Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Item	Article	Topic	Possible standards – for specific requirements
		• The trust eServices described in part 5 may not be relevant; Part 1 and part 2 seem to be the most relevant parts of this series. The following standards are available for the transport layer: ISO/IEC IS 7816-3, barcode capture, BLE, Wifi aware… These standards should be considered. While the transport layer is standardized, the access to these services by the wallet application from the OS layer is not standardized and depends on the OS provider. Standardization is needed. ISO/IEC IS 7816-15 allows the Wallet to use the QSCD by providing a harmonized description of its capacity, and thus allowing the discovery of the QSCD capacity by the Wallet. *Case 3: If the Wallet relies on a remote qualified signature/seal creation device:* The following standards are relevant: • “Architectures and protocols for remote signature” by Cloud Signature Consortium (CSC) defining the architecture and protocols for interfacing each components needed for remote signing; • ETSI TS 119 432 which defines interfaces and protocols between a server signing application service component (managing the signature key) and a signature creation application service component (requesting the signature/seal). This standard relies on the “Architectures and protocols for remote signature” v1.0.3 by Cloud Signature Consortium (CSC); CEN/EN 419 241-1 which defines security requirements and recommendations for Trustworthy Systems Supporting Server Signing that generate digital signatures/seals	-ETSI TS 119 462 - Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation (relying on -“Architectures and protocols for remote signature” v1.0.3 by Cloud Signature Consortium); -“Architectures and protocols for remote signature” v1.0.4 by Cloud Signature Consortium (CSC) (https://cloudsignatureconsortium.org/wp-content/uploads/2020/01/CSC_API_V1_1.0.4.0.pdf); *For the provisioning of signature/seal qualified certificate:* -WI “Electronic Signatures and Infrastructures (ESI); Wallet interfaces for trust services and signing “ (DTS/ESI-0019462 (TS) https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63566)

Item	**Article**	**Topic**	**Possible standards – for specific requirements**
		(entity managing the signature/seal key); Moreover, ETSI/TC ESI has launched the WI "Electronic Signatures and Infrastructures (ESI); Wallet interfaces for trust services and signing " (DTS/ESI-0019462 (TS) https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63566) covering the wallet interface with provider of qualified signature/seal certificate.	
2	3(44) 45c	Format of the electronic attestation of attribute. Several technical standards are already used to authenticate attribute relating to a person within various domain. These standards should all be considered, in particular to support qualified attestation of attributes	**The following standards have been identified** *For the format of attestation of attribute:* -W3C Verifiable Credential -AFNOR XP Z42-105 - Spécifications relatives à la mise en oeuvre du Cachet Électronique Visible (CEV) Otentik aux fins d'authentification, de vérification et de saisie automatique des données véhiculées par un document ou un objet -ISO/IEC IS 22385 (CD) - Guidelines for establishing a framework for trust and interoperability -ISO/IEC TS 7367 (AWI) - ISO-compliant vehicle mobile registration certificate -ISO/IEC IS 18013-5 - Mobile driving licence (mDL) application -ICAO TR Digital Travel Credentials -ISO/IEC IS 22376 (WD) - Security and resilience — Authenticity, integrity and trust for products and documents — Electronic Storage Specifications for use of Visible Digital Seal (VDS) for the authentication, verification and acquisition of data carried by a document or object -Generic presentation format based on all or part: • RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format

Item	Article	Topic	Possible standards – for specific requirements
			• RFC 7519 - JSON Web Token (JWT) • RFC 7165 - Use Cases and Requirements for JSON Object Signing and Encryption (JOSE) • RFC 4648 - The Base16, Base32, and Base64 Data Encodings • RFC 8610 - Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures • RFC 8949 - Concise Binary Object Representation (CBOR) • RFC 8152 - CBOR Object Signing and Encryption (COSE) • RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile • ISO/IEC IS 8825-1 - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) -WI in progress “Electronic Signatures and Infrastructures (ESI); Profiles for Attribute Attestations” by ETSI/TC ESI (DTS/ESI-0019472 (TS) https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=63560) **Recommendations to ETSI/TC ESI** All the standards listed above should be taken into consideration. It is recommended to ETSI/TC ESI: • that the overall structure of attestations will be dealt with by ETSI/TC ESI. However it’s fundamental that such structure be able to accommodate a wide range of externally defined specific attribute semantics, syntaxes and encodings; • to consider ISO/IEC TS 23220-2;

Item	Article	Topic	Possible standards – for specific requirements
3	3(43)	A common semantic for attributes is needed in order to achieve interoperability between all the MS. The proposed regulation envisions cross-border recognition of qualified electronic attestation of attributes, where appropriate i.e. without prejudice to Union or national law defining additional sector specific requirements as regards form with underlying legal effects. Such attestations of attributes can only be interoperable if there semantic is determined and shared by qualified eAA TSPs. For instance, different languages/alphabets and data structures and purposes for these attributes should be understandable cross-border. In addition to usual localization, there is a need for a semantic specification. This can as example be achieved by meta-data heading the attributes to make it interoperable. Those metadata may be defined in binary coding with a definition language as ASN.1, or with markup language as XML or with JavaScript notation as JSON, or else. As an example, the international standard mDL/mID data model (ISO/IEC IS 18013-5, section 7.1 and 7.2) the semantic problem of cross-border recognition of data elements by adopting "namespaces" concept. Accordingly, abstract containers are used to host the attributes; they are called DocType and NameSpace and are used to encapsulate the document type and the space in which the attributes are defined. Accordingly, the document type field follows the following general format: [Reverse Domain].[Domain Specific Extension]. The document type for an mDL document was fixed as "org.iso.18013.5.1.mDL" in which the reverse domain (org.iso) was selected to avoid collisions. This approach is	<u>**The following standards have been identified**</u> *For the data model:* -ISA deliverables (https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/our-resources) • Core Person Vocabulary • Core Business Vocabulary • Core Location Vocabulary • Core Criterion and Core Evidence Vocabulary • Core Public Organization Vocabulary *Data model defined for eIDAS 1:* -eIDAS SAML Attribute Profile v1.2 (https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/467109280/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=1&modificationDate=1639417533653&api=v2) <u>**Missing standard**</u> A standard ensuring any attribute could be "resolved". This standard should make attribute "resolvable" (attribute should resolve to semantic so that it could be understood). This standard shall be independent of the formatting of attestation of attributes, as portability of standalone attribute in Wallet in envisioned by the proposed regulation (article 3(42)). It should include i.e. management of metadata, translation, purposes, term of usage. This could be handled in the ISO/IEC TS 23220-2 (AWI). <u>**Recommendations to ETSI/TC ESI**</u> TC224 kindly requests ETSI/TC ESI to allow for an open format/any format of attestation in the WI "Electronic Signatures and Infrastructures (ESI); Profiles for Attribute Attestations"