Recommendation for the eIDAS toolbox - Version 2

Eurosmart, the Voice of the Digital Security Industry, started working on digital identity topics in 1999 – long before the eIDAS Regulation was even enacted. The association has developed strong expertise in the field, including standardisation aspects.

In this new document, Eurosmart would like to focus on specific points that deserve attention in the context of the eIDAS toolbox. This document builds on the set of technical guidelines that Eurosmart prepared at the beginning of the year.

Eurosmart's recommendation concerns six topics:

- Security and data protection
- Specific functionalities of the Wallet that need to be considered in the design phase or for which there is a lack of standardisation
- The level of trust that relying parties can place in the attestations of attributes
- Gatekeepers' ecosystems
- Governance aspects
- The format of attestations of attributes

In addition, readers will find an Annexe that compiles standards per Wallet functionality.

For the eIDAS toolbox, the most relevant European standardisation working groups are CEN/TC 224/ WG 17 and WG 20) and ETSI TC ESI. Their past and ongoing work is particularly useful for the eIDAS toolbox and often mentioned in this paper.

I. Data protection and security

Privacy Warning: Identity portrait

Eurosmart recommends adopting a specific approach of ISO/IEC 18013-5 when it comes to portrait use. Overall, Eurosmart warns against the general use of the portrait, which would not be in line with European privacy values. The use of ISO/IEC 18013-5 with portrait disclosure may only be appropriate for offline transactions (in person) in the context of the driving licence. In such a context, law enforcement authorities would need to control the identity of a driver and hence could compare the portrait from the Wallet with the driver in front of their eyes. This use is in line with ongoing international implementations.

However, other user binding methods are highly advisable for online and offline transactions in other contexts, with no portrait disclosure. These other binding methods are more in line with GDPR principles. Therefore, having the portrait in the authentic sources is not necessary or desirable. Eurosmart recommends considering the **solution proposed in ISO/IEC 23220-4 for holder authentication, which is itself compatible with ISO/IEC 18013-5 but without a generalised use of the portrait.**

Requirements for storage and processing of data

The eIDAS toolbox should contain measures to ensure that the users' data are protected from misuse and foreign interference. First, Eurosmart identified two missing standards for compliance with GDPR:

- A missing code of conduct for Wallet issuers
- A missing standard proposing guidance for the fulfilment of GDPR obligations by providers of attestations

Secondly, Eurosmart identified the need to put data territoriality requirements in place to limit the risk of foreign access to Wallet users' data as much as possible. The eIDAS toolbox should require Wallet issuers and attestation providers to store and process data in the EU territory only. They should also put in place technical means to prevent non-EU entities or persons from accessing these data. In that regard, the eIDAS toolbox should incorporate requirements similar to those of SecNumCloud defined by ANSSI for cloud-based applications and integrate data protection requirements.

ENISA is preparing a cybersecurity certification scheme for cloud services (EUCS scheme). This scheme (level "high") could also be used for cloud services used by Wallet issuers and attestation providers.

Risk analysis of the Wallet

Eurosmart would see fit to include a complete risk analysis of the Wallet in the toolbox. This risk analysis should:

- identify the assets related to the Wallet, including the identity of the instance of the Wallet, the Wallet itself, the biometrics, the assets/credentials for the citizen’s identity, the documents, the attestations (the ones received, and the ones produced);
- identify the level of protection needed per asset in terms of integrity, confidentiality, authenticity and resilience, and the corresponding level of security;

- address the authorised or mandated locations for the assets: secure element, memory of the mobile device, SIM, software, cloud (and which cloud owned by governments or third parties) etc.

Security certification of the Wallet

The Wallet will likely involve several technologies, amongst which (non-exhaustive list):

- Secure hardware (to support authentication and signature etc.);
- Secure software (on mobile for the Wallet parts on the mobile of the user, or the part running on the server);
- Cloud (for the server part of the Wallet);
- Biometry for authentication (e.g., identity proofing and possibly other operations).

Each of these key technologies shall be security certified, ideally using a European cybersecurity certification scheme -to have a harmonised level of trust. Article 6c states that if a Wallet is certified under a cybersecurity scheme pursuant to Regulation 2019/881 (Cybersecurity Act), it will benefit from a presumption of compliance with the eIDAS requirements on cybersecurity. The level of assurance "high" should be required in order to cater to the high level of expectation regarding Wallet security. Therefore, the following should be available for each of the technologies listed above:

- Security certification methodologies covering security certification level "high";
- Security certification schemes pursuant to Regulation 2019/881 covering security certification level "high".

Unfortunately, there are no security certification schemes for biometry and secure software under Regulation 2019/881. The European Commission should issue as soon as possible dedicated mandates to ENISA to have security certification schemes covering these technologies up to level "high".

Regarding security certification methodologies, a standard is under preparation within CEN-CLC JTC 13/WG 3 that could be used for the security certification of secure software (EN 17640). This document[1] covers any security certification level from "basic" to 'high" and will soon be available. It should also support the security certification scheme covering secure software under Regulation 2019/881 up to level "high".

For biometric technologies, some standards are available that could support security certification under Regulation 2019/881 up to level "high":

- for the detection of presentation attacks (e.g., using a mask), ISO/IEC 30107 - Biometric presentation attack detection should be used. Unfortunately, standards describing attacks catalogue – necessary to support these security assessments - are missing;
- for the detection of video injection when capturing biometric data (e.g., when using a mobile phone to capture the face of a user), the pre NWI "Digital Presentation Attack in biometric systems" being prepared by the CEN/TC 224/WG 18 addresses the patterns of attacks through video injection when capturing biometric data.

Regarding secure hardware or HSM that may be involved in the Wallet design, they should be certified at level EAL4+AVA_VAN.5 according to the Common Criteria pursuant to the EUCC, the SOG-IS or other

[1] CEN/CLC/JTC 13, Fixed-time cybersecurity evaluation methodology for ICT products, EN 17640:2022.

adequate schemes providing a level of trust “high” as defined in Article 52 of the Cybersecurity Act. Besides, secure hardware included in user devices should be certified according to one (or several) of the following Protection Profiles:

- BSI-CC-PP-0084
- BSI-CC-PP-0117

In addition, the upcoming European cybersecurity certification scheme on 5G is relevant for the Wallet, as well as the EUCS scheme on the cloud (already mentioned above).

2. Focus on specific functionalities of the Wallet

Functionalities that need to be considered in the design phase

Offline mode & storage of PID/attestations

Some functionalities seem crucial and would deserve to be considered in the design phase. The first one is the offline mode, which the European Commission introduced in the proposal. The user shall be able to "securely request and obtain, store, select, combine and share [...] the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline to use online public and private services" (Article 6a(3)a/Article 6a(4)a(3)).

First, the legal text (Article 3) would deserve a clear definition of what offline means. A clear definition could be the following:

> *"Offline service" refers to the capability for a user to carry out an operation with a third party with close proximity technologies, irrespective of whether the device is connected to the internet or not, in order to access a wide range of public and private services.*

The offline feature is instrumental for some use cases, for instance, granting access to premises without an internet connection. The online mode only is quite restrictive and does not allow identity control in real timing in all circumstances. There are plenty of cases where a mobile device will not be able to connect and will only have contactless interfaces (e.g., NFC) available, such as in remote areas with weak coverage, where natural disasters occur, if a mobile phone is in low power mode. Therefore, the Wallet needs to be able to support the following operations in offline mode:

- presentation of attestation (which implies that the attestation should be locally available to the Wallet and not stored in a central server);
- electronic identification/presentation of person identification data - PID (which implies that the person identification data should be locally available to the Wallet and not stored in a central server);
- authentication.

The eIDAS toolbox needs to address the definition of offline and the above-mentioned functionalities. In this respect, special care should be taken when selecting reference standards for the Wallet so that all these usages are effectively possible. Among others, ETSI TC ESI Work Item "Electronic Signatures and Infrastructures (ESI); Wallet interfaces for trust services and signing" (TS 119 462) and CEN/TC 224/WG 20's activities can be considered if it is confirmed that they address the offline mode as well. Please refer to Eurosmart's full list of standards in Annexe for the offline mode.

In particular, Eurosmart notes that **authentication in offline mode is a crucial feature and should mandatorily be supported by the Wallet.**

Likewise, the toolbox needs to mandate local storage of person identification data and some (if not all) attestations so that they can be presented offline. **As a general rule, person identification data should always be hosted onboard the device (at least for the purpose of offline and online authentication).** Storage of attestations in the local device should be considered to support retrieval of attestations in offline mode. Storage of attestations in the local device allows for a full offline mode, i.e., both the user and the relying party do not need internet connection.

Remote storage of attestations (excluding person identification data) could also be considered. In that case, the Wallet would return a token or a pointer that could be used by the relying party to obtain the attestation. For this option, the full offline mode is excluded, as the relying party would need an internet connection. Nevertheless, in case of remote storage of attestations, the Wallet shall still support offline authentication to ensure strong binding between the holder and the attestation.

Digital Travel Credentials and mobile driving licence

The Wallet should also comply with the Digital Travel Credential technical reports, as defined by ICAO. It entails the Wallet should (1) support the corresponding applicative, cryptographic and transport protocols but also (2) store and disclose the necessary data (probably under the shape of an attestation) to relying parties. Digital Travel Credential technical reports (at least DTC type 2 and 3) directly impact the Wallet's design. In that regard, the Wallet shall comply with the ICAO technical reports defining the Digital Travel Credential when delivering (qualified) attestations representing a digital travel document (named Digital Travel Credential Virtual component – DTC-VC).

Likewise, the mobile driving license is likely to fall within the category of (qualified) attestations. Therefore, the Wallet shall comply with ISO/IEC 18013-5 for driving licences and could be a source of inspiration for other use cases. The abstraction level provided by ISO/IEC 18013-5 allows for a variety of formats for storage, including travel credentials, mobile driving licences, vehicle registration documents, mobile identity, etc. It should be analysed how the mechanisms specified in ISO/IEC 18013-5 and ISO/IEC 23220 can be re-used for the ICAO DTC specification in case ICAO specifications do not meet all market expectations.

Functionalities for which there is a lack of standardisation

Exchange of identification data with parties other than trust services

Pursuant to the proposed Regulation, it shall be possible to exchange data with relying parties that are not necessarily trust services. Article 6a(4)a(2) of the proposal for eIDAS 2 states the following:

> *Digital Identity Wallets shall, in particular: (a) provide a common interface: [...]* ***(2) for relying parties to request and validate person identification data and electronic attestations of attributes****.*

ETSI TC ESI is currently working on a New Work Item named "Wallet interfaces for trust services and signing". The goal of this Work Item is to specify interfaces enabling interaction of Wallet and trust services, including signing. Therefore, it seems that **a standard covering the Wallet interface to relying parties other than trust services is missing. Other instances, such as CEN/TC 224, also work on this aspect to elaborate on general purpose interface. Cooperation with ETSI TC ESI may be necessary.**

Synchronisation of a Wallet on different devices

Synchronisation of a Wallet on different devices seems **highly challenging** as a qualified attestation is likely to be bound to a Wallet's key and hence could not be transferred. At this point in time, there is no guarantee of feasibility. Trust relationship models would need to be defined. In that regard, **Eurosmart does not recommend this feature for the Wallet**.

However, several approaches could be considered to allow for **portability and recovery** of the Wallet:

- One solution would be to keep a copy of the attestations and the Wallet's key on the server. However, this approach raises security issues as it could put at risk the Wallet's key (exposed during the transfer from the Wallet to/from the server), and thus the link with the user;
- Another solution could be to directly have the Wallet's key on the server (without any duplication), meaning the server is also part of the Wallet. This approach seems interesting but raises serious concerns. First, it would deprive the user of the benefits of its Wallet when the user does not have any connection. Secondly, where the user has a connection, it would expose him to asynchronous processing of its requests: as the server has a limited maximal processing capacity, it will have to smooth requests over time. This is likely to end up in several minutes of waiting time (or more) during the peak period before the user's request to use its Wallet is executed.

The best approach would be not to bind the attestation to the Wallet's key but to bind it to the user's person identification data or a pseudonym. This would allow for complete portability and recovery without putting the Wallet's key at risk or creating shortcomings in the user experience.

Withdrawal of the Wallet following a security breach

Article 10 of the proposal for eIDAS 2 stipulates that if the Wallet is breached or compromised, and if this cannot be remedied within three months, the Member State concerned shall withdraw the European Digital Identity Wallet. The Wallet shall be withdrawn without delay if this is a severe breach. Therefore, **standards are needed to organise the termination of a Wallet**.

Decommissioning is part of the withdrawal of the Wallet. This is a technical means to ensure that the storage cannot offer access to the data of the withdrawn Wallet. Guidance is needed for decommissioning as well.

3. Level of trust that relying parties can place in the presented attestations of attributes

Enrolment and onboarding

User enrolment and user onboarding are important first steps to foster trust in the person identification data and attributes presented via the Wallet. A reliable user enrolment and user onboarding guarantee, first and foremost, that the Wallet belongs to its legitimate holder and that the holder is who he/she claims to be.

For the eIDAS toolbox, **Eurosmart recommends clearly differentiating identity proofing, enrolment and onboarding**. **Enrolment** consists in verifying and confirming the identity of someone and creating and populating the corresponding record with all the necessary information. Once enrolled, the application is ready to be processed by the issuing authority so that digital identity credentials can be issued to that person (adjudication). **Identity proofing** is part of the enrolment and only provides confidence in the link between a claimed identity and an applicant. Digital identity credentials are issued to a citizen by national authorities. However, enrolment does not give any guarantee on the device that will be used to store the credentials. How to ensure that the issued credentials will be stored and used in a device that belongs to the legitimate holder?

The **onboarding** encompasses the enrolment but also addresses the measures to guarantee that the issued credentials are transferred and stored in **a device and Wallet compliant with the issuing authority requirements (technical, security etc.) and under the sole control of the rightful holder**. For instance, it may take the shape of a link sent to the user through an SMS where the user would be prompted to enter a code to ensure that the device belongs to the legitimate holder of the credentials.

ISO/IEC 23220 part 5 distinguishes the two concepts. For the eIDAS toolbox, Eurosmart recommends considering ISO/IEC 23220-5 (part of the ISO/IEC 23220 series), which defines the level of confidence in identity proofing.

There is currently a lack of standards for the onboarding process on a wallet, but CEN/TC 224/WG 20 is working on this issue. A proposal of new work item[2] should be adopted soon.

ETSI has recently issued TS 119 461 on identity proofing in the context of trust services. This document may be useful, but it shall be noted that:

- It has a narrow scope compared to the needs: identity proofing compared to onboarding on a wallet.
- It (only) addresses the case of identity proofing for the issuance of qualified certificates and attestations. It does not apply to digital identity and thus does not consider its specific requirements.

Reaching level "high" for authentication

Article 6a(4)d states that the Wallet shall "(d) provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes".

A few standards should be part of the toolbox:

- ISO/IEC 23220-1 describes various modalities to perform holder authentication. This standard should be considered.
- ISO/IEC 23220-4 provides mechanisms for the relying party to request multi-factor holder authentication to the Wallet. This standard should be considered to spare the need for portrait divulgation to the relying party.
- ISO/IEC 23220-5 defines the level of confidence in the holder authentication. This could be useful for the relying party to assess the quality of holder authentication to the Wallet. This standard should be considered.

The full set of standards for holder authentication is in the process of being complemented by ISO/IEC.

[2] “Guidelines for the on boarding of user personal identification data within European Digital Identity Wallets”.

Secure hardware must be used for a Wallet to reach the requirements of assurance level "high" for authentication. Local secure hardware may be used by the Wallet to meet this requirement:

- secure hardware present in the mobile device, such as secure element or eUICC;
- secure hardware in the hand of the user, such as an identity card.

While the communication layer with the secure hardware is standardised, access by the Wallet application from the OS layer is not standardised and depends on the OS provider. In this respect, standardisation is needed. This paper further develops this point in the following section.

The SAM specification prepared by the GSMA is promising and will allow managing two areas in the eUICC. One area would be under the control of the mobile operator and linked to the user's mobile subscription, while the other area would be independent of the mobile operator and managed by a third party. The latter area could host secure applications (such as a secure Wallet application) managed by another entity different from the mobile operator. Thus, this secure area could remain even if the user's mobile subscription changes.

Nevertheless, this GSMA specification needs improvements to better address market needs, in particular regarding the trust model. The current version of SAM requirements contains technical limitations which do not allow risk owners (represented by the Application Service Provider Security Domain – ASP SD) to install freely any secure application in their area (e.g., it is hardly possible for a risk owner managing its Application Service Provider Security Domain to install an eMRTD or payment applications). Therefore, the GSMA SAM specification should be very cautiously considered at this stage.

It is also worth noting that ETSI TS 102 221 is in the process of being amended to achieve the support of several logical secure elements. ETSI TC SET prepares this technical specification. This specification could help emulate the existing physical secure hardware in mobile devices into two logical secure hardware. One is the traditional eUICC/SIM – bound to the user's mobile subscription - and the other one is managed independently and could host secure applications (such as a secure Wallet application) under the control of a third party.

Other secure hardware combinations, such as eUICC, eSIM, eSE and secure elements, are also possible. GSMA and GlobalPlatform prepare the technical standards for these supports.

How to ensure the right level of trust the relying party can place in the attributes?

This point can be particularly useful for non-qualified attestations.

Amongst the useful information that may fall into the category "scope of those attributes" (as defined in Annex V of the proposed Regulation), the level of trust a relying party can put in the attribute and the attestation may be very useful. There are nowadays several relevant standards for this purpose. The ISO/IEC 23220-5 (part of the ISO/IEC 23220 series) defines a methodology for assessing the trust to put in attribute and attestation (quality of the binding etc.). Pursuant to ISO/IEC 23220-5: "This technical specification provides a definition of confidence level, covers trust models and its assessment which allows an Issuer to deliver trust information to the mobile eID-document and a verifier to consume that trust information to make informed risk decision during a transaction." This assessment should apply to both qualified and non-qualified attestations of attributes.

4. Standardisation to avoid vendor lock-in ecosystems

The Wallet application will need to access the physical components of the user device to meet the requirements enacted in the proposed Regulation:

- **Access to local hardware components** (keyboard, biometric sensor, camera, flash etc.) necessary to authenticate the user. Besides, when biometric technics are used, it is of the utmost importance that the Wallet application could have access to the biometric score - which is usually not the case - to gauge the confidence to put in the authentication as well as to manage its own risks;
- **Access to the secure hardware** to meet the requirement of LoA "high" with regards to authentication;
- **Access to the interfaces to meet the requirement of offline mode support** (NFC, WiFi Aware, BLE, camera, screen, etc.);
- **Access to identity cards compliant with Regulation 2019/1157 to perform the holder binding (camera, NFC etc.)**.

It shall be possible for the Wallet application to get access to these features through the OS layer in an easy and interoperable manner to avoid (1) fragmentation across devices, (2) vendor lock-in situations, or (3) even worse, abuse of power from devices vendors on the European digital identity ecosystem that is being shaped.

For all these reasons, standardisation of API -so that Wallet application could access these features through the OS layer- is absolutely needed. In addition, browsers should not be set up by default to avoid problems in application communication.

Such standardisation will also serve the purpose of the Digital Markets Act (DMA), which aims to ensure that business users and providers can interoperate with hardware and software features of the platforms offered by the gatekeepers (i.e. biometric sensors, keyboards etc.).

Furthermore, the Wallet should rely on Qualified Website Authentication Certificates (QWACs), as defined in Article 45 of eIDAS 2. QWACs from relying parties would strengthen security and transparency. The users would then have a guarantee regarding the identity of whom they are connecting to.

5. Governance

Administration of relying parties

Standardisation is needed for the following Wallet features:

- management of the trust anchors in the Wallet used for relying parties/trust service providers authentication
- management of trust list of relying parties/ trust service providers in the Wallet
- management of security policies to be applied for relying parties/trust service providers

Governance of legal persons

The toolbox should include mechanisms that enable assigning the roles and rights to the Wallets relating to legal persons. For instance, **a legal person can be represented by a natural person that possesses a qualified electronic attestation of attribute**. This could be an attestation originating from a national trade registry (in general, electronic attestation of attributes must be proved against authentic sources) and endorsed by a qualified trust service provider. **The qualified attestation binds this natural person to the legal person and can give rights to act as a legal person**.

Governance of ledgers

The Wallet might rely on ledgers for some of its use cases. If this is the case, clear standards are needed and implementing act should reference them. DLT and blockchain systems aim for decentralised decision rights and the technical enactment of accountability (cf. ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance). It might be overlooked that the blockchain paradigm can only be met if all stakeholders agree on a clear consensus on the ground of a common charter determining the rules and the incentives. Rules are fundamental to clear potential technical issues that are likely to happen while the blockchain is growing, and incentives are necessary to achieve consensus. If incentives are not aligned to balance between blockchain nodes, these nodes will not contribute to the consensus. The algorithmic part of such consensus endows it with a standalone capability that is only effective if all blockchain users (notably validators) abide by the rules.

Additionally, if smart contracts are used to implement autonomous transaction enforcement, they shall be subject to careful test methods in order to prevent risks of attacks and offset logical breaches that smart contract programming languages might expose. **These aspects impacting blockchain application are fundamental and seem not enough considered as part of ledger/blockchain inherent concern.**

6. Format of attestation of attribute

Useful standards

The eIDAS toolbox should not tamper with existing encoding but should support all existing encoding with metadata.

The following standards should be considered for the format of attestation of attribute:

- W3C Verifiable Credential
- AFNOR XP Z42-105 - Spécifications relatives à la mise en œuvre 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 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

- 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

There are also standards for generic presentation format based on all or part:

- RFC 8259 - The JavaScript Object Notation (JSON) Data Interchange Format
- 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 8825-1 - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

Eurosmart recommends that a universal format of attestation of attribute be introduced with metadata to identify the format (e.g., unique identifier referring to the format). This should be considered in the work being carried out by ETSI on TS 119 472 "Electronic Signatures and Infrastructures (ESI); Profiles for Attribute Attestations".

Resolving the semantic problem of attributes

Eurosmart invites national representatives to **agree on a common semantic for attributes**. **This common semantic is needed to achieve interoperability across the EU**. For instance, different languages, alphabets, data structures and purposes should be understandable cross-border. In addition to localisation, there is a need for semantic specification. This need could be fulfilled through **meta-data heading the attributes**. 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.

National representatives can draw inspiration from the example of the international standard mDL/mID data model (ISO/IEC 18013-5, section 7.1 & 7.2). This model solved the semantic problem of cross-border recognition of data elements by adopting « namespaces ». 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. 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 extensible and can be used to define other doctypes. And the namespace for mDL data was fixed as "org.iso.18013.5.1", where the number "1" in the namespace might be increased in future versions of the standard. Only data elements defined explicitly in the standard may be used within this namespace. This simple concept can be reemployed for credentials and other attributes ported on the Wallet. It suffices in practice to:

- define doctypes (compartments standing for application containers) and their namespaces (set of attributes), and
- allocate labels and assign value to each attribute (or data element) within a namespace, and
- register (e.g. in a decentralised registry or a ledger) the attributes' label and respective description and coding type.

Additionally, the ISA (Interoperability solutions for public administrations, businesses and citizens) programme has already defined several data models that should be considered. Several core vocabularies have been defined, which are simplified, reusable, and extensible data models that capture the fundamental characteristics of an entity, such as a person or a public organisation, in a context-neutral manner. In particular, a core vocabulary defines the semantics and the identification of each attribute, as well as their relations, in a technology-neutral manner. The following core vocabularies are available:

- Core Person Vocabulary
- Core Business Vocabulary
- Core Location Vocabulary
- Core Criterion and Core Evidence Vocabulary
- Core Public Organisation Vocabulary

Besides, the W3C Data Model for Verifiable Credentials provides an alternative worth being considered as well. It nests attributes that employ a property called '@context'[3], allowing for two software systems to exchange data with terminology that both systems understand. It is well known that the '@context' concept allows mapping attributes short-form aliases to the URIs required by application-specific verifiable credentials and verifiable presentations. The '@context' property can as well be used to communicate other details, such as datatype information, language information, transformation rules, etc.

The value of the '@context' property is an ordered set where the first item is a URI, and subsequent items express context information and are composed of any combination of URIs or objects, where each URI in the '@context' is one that if dereferenced, results in a document containing machine-readable information about the '@context'. Verifiable credentials created in this way provide a mechanism to prevent namespace conflicts and semantic ambiguity. Accordingly, the verifier or relying party can check the context to determine unambiguously the meaning of attributes or claims presented by the Wallet.

The associated human-readable vocabulary document for the Verifiable Credentials Data Model is available at https://www.w3.org/2018/credentials/ and can be expanded according to W3C extensibility rules. Verifiable credentials and verifiable presentations are being envisioned in eIDAS 2 deployment with decentralised/distributed systems (see 'ledger' mentioned in the Regulation, see EBSI project); their implementation shall include a '@context' if the W3C data model is adopted.

Last but not least, the work achieved for eIDAS 1 for the semantic of person identification data in the context of SAML requests shall be considered, such as eIDAS SAML Attribute Profile v1.2 for the semantic of person identification data in the context of SAML requests.

[3] https://www.w3.org/TR/vc-data-model/#contexts

7. Gap analysis

The CEN/TC 224/WG 20 was created in 2021 to identify the existing standards that could be used to support the different provisions of the eIDAS 2 Regulation. Besides, where gaps are identified, this working group will work on preparing standards to fill these gaps.

The first deliverable of this working group is the Technical Report "Gap Analysis European Digital Identity Wallets", which should be published soon.

8. Annexe

Existing and upcoming standards (per functionality) to be used

Functionality of the Wallet	Standard(s)
Signature	-CEN/EN 419 212-1 -CEN/EN 419 212-2 -CEN/EN 419 211-2 - Protection profiles for secure signature creation device - Part 2: Device with key generation -CEN/EN 419 211-3 - Protection profiles for secure signature creation device - Part 3: Device with key import -CEN/EN 419 211-4 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application -CEN/EN 419 211-5 - Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application -CEN/EN 419 211-6 - Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application -CEN/EN 419 241-1 Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements -CEN/EN 419 241-2 Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing -CEN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services -ETSI TS 119 431-1 Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev use of other openly available specifications
Installation, issuance of the Wallet and provisioning of data in the Wallet	-ISO/IEC IS 23220-1 -ISO/IEC TS 23220-3
Secure **online** provisioning/storage of identity data, credentials, attributes, and electronic attestations	-ISO/IEC IS 23220-1 -ISO/IEC TS 23220-2 -ISO/IEC TS 23220-3

Reading data (of any kind) from the Wallet in **online mode**	-ISO/IEC IS 23220-1 -ISO/IEC TS 23220-2 -ISO/IEC TS 23220-4 -SAML (Oasis) -Supporting documents for implementation of eIDAS 1 based on SAML (eIDAS eID Profile (europa.eu)) - for person identification data only eIDAS Message Format v1.2 eIDAS Interoperability Architecture v.1.2 eIDAS Cryptographic Requirement v.1.2 eIDAS SAML Attribute Profile v1.2 eIDAS Message Format v1.2 Errata 01 -OpenID Connect OpenID Connect Self-Issued OpenID Provider v2 - OIDC-SIOP (Implementer's Drafts public review) (Self-Issued OpenID Provider v2) OpenID Connect for Verifiable Presentations (Implementer's Drafts public review) (OpenID Connect for Verifiable Presentations) Note: These widespread specifications pose limitations in terms of privacy (identity providers know to whom you are delivering your attestation). OpenID Foundation (OIDF) is currently amending its specifications to resolve this issue. -W3C Verifiable Credential (published) Data Model (https://www.w3.org/TR/vc-data-model/) Implementation guide (https://www.w3.org/TR/vc-imp-guide/) Decentralized Identifiers (DIDs) (published) (https://www.w3.org/TR/did-core/) -Identity Foundation DIDComm Messaging (editor's draft) (https://identity.foundation/didcomm-messaging/spec/)

	Presentation Exchange 2.0.0 (working group draft) (https://identity.foundation/presentation-exchange/) Presentation Exchange v1.0.0 (Published) (https://identity.foundation/presentation-exchange/spec/v1.0.0/) -ITU-T/X509:2019 "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks " -ICAO TR DTC PC (to support the use case of mobile travel document) Note: Possible mismatch between DTC and mdoc (18013-5) data format encoding. **Relevant standards and initiatives for SSI implementation** The standards being investigated by CEN/CENELEC/JTC19 can be considered. Outcomes of EBSI/ESSIF initiative should be considered.
Reading data (of any kind) from the Wallet in **offline mode**	-ISO/IEC IS 23220-1 -ISO/IEC TS 23220-2 -ISO/IEC IS 18013-5 -Open ID Connect Open ID Connect Self-Issued OpenID Provider v2 - OIDC-SIOP (Implementer's Drafts public review) (Self-Issued OpenID Provider v2) OpenID Connect for Verifiable Presentations (Implementer's Drafts public review) (OpenID Connect for Verifiable Presentations) Note: These widespread specifications pose limitations in terms of privacy (identity providers know to whom you are delivering your attestation). OpenID Foundation (OIDF) is currently amending its specifications to resolve this issue. -ICAO TR DTC PC (to support the use case of mobile travel document) Note: Possible mismatch between DTC and mdoc (18013-5) data format encoding. **Relevant standards under preparation** -DIDComm Messaging (editor's draft) (https://identity.foundation/didcomm-messaging/spec/)

	from identity foundation as offline use case is in the scope of this work.
Authentication	-FIDO (FIDO 2.0, FIDO WebAuthn, FIDO UAF, FIDO U2F https://fidoalliance.org/specifications/) which focuses on authentication -Open ID Connect Self-Issued OpenID Provider v2 - OIDC-SIOP (Implementer's Drafts public review) (Self-Issued OpenID Provider v2) -Supporting documents for implementation of eIDAS 1 based on SAML (eIDAS eID Profile (europa.eu)) eIDAS Message Format v1.2 eIDAS Interoperability Architecture v.1.2 eIDAS Cryptographic Requirement v.1.2 eIDAS SAML Attribute Profile v1.2 eIDAS Message Format v1.2 Errata 01 -ICAO TR DTC PC (to support the use case of mobile travel document)
Holder authentication (binding to the data)	-ISO/IEC IS 23220-1 (holder authentication modalities) -ISO/IEC TS 23220-4 (holder authentication request) -ISO/IEC TS 23220-5 (holder authentication assessment)
Transport protocols for **offline mode** Local communication with the Wallet (storage/provision of data)	-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 - JAB Code polychrome bar code symbology specification -ISO/IEC 14443 - Identification cards -Contactless integrated circuit cards - Proximity cards -ISO/IEC IS 18092 – Near Field Communication -ETSI/EN 302190 - Near Field Communication -Bluetooth SIG, Bluetooth Core Specification, Version 5.2, December 2019 -Bluetooth SIG, Supplement to the Bluetooth Core Specification, Revision v9, December 2019 -NFC Forum, Bluetooth Secure Simple Pairing Using NFC, Version 1.2, May 2019

	-NFC Forum, Data Exchange Format (NDEF) Technical Specification, Version 1.0 -NFC Forum, Type 4 Tag Version 1.1 -ISO/IEC IS 18013-5 (for provision of data) -ICAO TR DTC PC (to support the use case of mobile travel document)
Identity proofing and verification	-ISO/IEC IS 23220-1 -ISO/IEC TS 23220-5 -ETSI TS 119 461, only for issuance of qualified certificates or attestations
Security certification of software embedded on secure hardware	EUCC Scheme *(https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1)* BSI-CC-PP-0084 BSI-CC-PP-0117
Security certification of secure software	EN 17640
Security certification of biometry for authentication	ISO/IEC IS 30107
Security certification of cloud-based application	EUCS scheme (under preparation)
Harmonised compliance requirements with the GDPR	ISO/IEC IS 27701

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at the EU level, like CEN-CENELEC, ECIL, ETSI, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com