EUROPEAN UNION AGENCY
FOR CYBERSECURITY

DIGITAL IDENTITY STANDARDS

Analysis of standardisation requirements in support of cybersecurity policy

JULY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use standardisation@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Ignacio Alamillo
Stefane Mouille
Andrea Röck
Nikolaos Soumelidis
Michal Tabor

Slawomir Gorniak

ACKNOWLEDGEMENTS

ENISA would like to thank all the experts who contributed to the study, by providing input, advising on the content and reviewing the study at various stages. Special thanks to the members of the ETSI TC ESI for their valuable support.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-617-0, DOI 10.2824/28598

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital services and electronic transactions are becoming more and more important. This trend has been accelerated by the COVID-19 restrictions limiting in-person contact, which increased digital interactions between people around the world. However, electronic transactions in which the identities of parties cannot be trusted give rise to fraud. Digital identity – that is, the identification of a legal or natural person or an entity within an electronic service – is more important than ever.

'Digital identity' is defined, for the purpose of this document, as a unique representation of a subject engaged in an online transaction. This contains two elements constituting the role of digital identity: to represent a subject and to support an online transaction. 'Identity' itself can be defined as a set of attributes related to an entity.

There is a multitude of standards in the area of digital identity. The goal of this document is to give an overview of the most important standards and standardisation organisations in this area. This information is useful for the novice, to find out what is available, but also for more experienced readers who might not be aware of some (parts of) existing standards. It also provides an analysis of standards related to different means supporting digital identity. This covers means created and managed by trust services, electronic identification means and the EU Digital Identity Wallet.

Digital identity standards cover several areas. They can describe policies; services issuing or managing digital identity means; formats and protocols to be used; ways of auditing related services; requirements for secure devices; or recommended processes and algorithms.

Digital identity standards have been developed due to the increasing demand for secure, reliable and cross-recognised digital transactions, fuelled by several governmental digital transformation programmes and the COVID-19 restrictions. The standardisation efforts involve several layers of digital identities, extending from the policy and governance level down to the operational and technical specifications level. They also address several elements and technologies supporting digital identities, such as electronic certificates, person identification, signature devices and cybersecurity aspects.

The following criteria are considered in the analysis of available standards:

- coverage of the identity management life cycle,
- maturity of the standards,
- authentication capabilities (in person versus remote, online versus offline),
- user sole control and dependencies, for example whether 'call home' is needed,
- data-protection-enhancing technologies, for example selective disclosure,
- trust model.

Based on this analysis, we propose a series of recommendations on the digital identity standardisation requirements in support of cybersecurity policy standards for various groups of stakeholders: EU policymakers, European Standardisation Organisations (ESOs) and ENISA.

1. INTRODUCTION

1.1. PURPOSE OF THIS DOCUMENT

Digital services and electronic transactions are becoming more and more important. This trend has been accelerated by the COVID-19 restrictions limiting in-person contact, which increased digital interactions between people around the world. However, electronic transactions in which the identities of parties cannot be trusted give rise to fraud ([1]). Digital identity – that is, the identification of a legal or natural person or an entity within an electronic service – is more important than ever.

There is a multitude of standards in the area of digital identity. The goal of this document is to give an overview of the most important standards and standardisation organisations in this area. This information is useful for the novice, to find out what is available, but also for more experienced readers who might not be aware of some (parts of) existing standards.

1.2. DIGITAL IDENTITY STANDARDS

Digital identity standards cover several areas. They can describe policies; services issuing or managing digital identity means; formats and protocols to be used; ways of auditing related services; requirements for secure devices; or recommended processes and algorithms.

A wide range of bodies and organisations are working on digital identity standards, among them:

- European standardisation organisations (European Telecommunications Standards Institute (ETSI), European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC)),
- international standardisation organisations (International Organization for Standardization (ISO), International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers, International Electrotechnical Commission (IEC), Common Criteria for Information Technology Security Evaluation (hereinafter 'Common Criteria'), International Civil Aviation Organization (ICAO)),
- commercial forums and consortia (Internet Engineering Task Force (IETF), Certification Authority Browser Forum, Cloud Signature Consortium (CSC), Organization for the Advancement of Structured Information Standards (OASIS), OpenID Foundation (hereinafter 'OpenID'), FIDO Alliance (hereinafter 'FIDO'), etc.),
- national organisations (Agence nationale de la sécurité des systèmes d'information (ANSSI) (the French national cybersecurity agency), Bundesamt für Sicherheit in der Informationstechnik (BSI) (the German national cybersecurity authority), British Standards Institution, National Institute of Standards and Technology (NIST) (United States)).

Historically, the first standards were linked to interoperability (i.e. protocols and formats), since agreeing on a common way of doing things is particularly important. Security-related standards were later created for the certification of devices but also for policy requirements for service providers, to enable best practices to be described and to establish a comparable level of security. A more detailed description of the different standards and standardisation bodies can be found in Chapter 3.

[1] https://www.merchantsavvy.co.uk/payment-fraud-statistics/

1.3. RELATED EUROPEAN UNION LEGISLATION

In 1999, the European Union published Directive 1999/93/EC [2], which provided the first framework for electronic signatures. However, the scope of the directive was limited, and the fact that it was only a directive allowed different transpositions into the national law of each EU Member State. A huge boost for the EU digital market was the publication of Regulation (EU) No 910/2014 [3], hereinafter 'the electronic identification, authentication and trust services (eIDAS) regulation'. First of all, this regulation is directly applicable in all Member States. Second, it covers not only electronic signatures, but a much broader area of digital identity. The eIDAS regulation has two parts. Part 1 discusses electronic identification means to be provided by the different Member States. These means would enable the identification of anyone with an electronic ID from one Member State involved in a process of another Member State that allows the use of electronic identification at the same level or a lower level of assurance. In Part 2, the eIDAS regulation specifies various (qualified) trust services that can be used to support electronic transactions. The idea is that qualified trust services are supervised, in terms of their compliance with the requirements of the regulation, by the Member State in which they are based. Such a qualified trust service will then be recognised in all Member States. After a few years of experience with the eIDAS regulation, a review was conducted [4], which led in June 2021 to a proposal for an update of the regulation, which is commonly known as the eIDAS 2.0 regulation [5]. This proposal is still a draft, but it introduces some interesting new elements. The most important is the EU Digital Identity Wallet (hereinafter 'EUDI Wallet'). This would allow each EU citizen to be digitally identifiable, with the owner of the EUDI Wallet being able to choose which information they want to share. The wallet also enables the collection and sharing of attestations of attributes, which might be used, for example, to prove possession of a driving licence or some university degrees in a format that can be understood all over Europe. The proposed update of the eIDAS regulation also includes new qualified trust services for qualified attestations of attributes: management of remote electronic qualified signature and seal creation devices, the electronic archiving of electronic documents and recording of electronic data in an electronic ledger.

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093).

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG).

[4] *Revision of the eIDAS Regulation: Findings on its implementation and application* (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf).

[5] Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European digital identity, COM(2021) 281 final (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN).

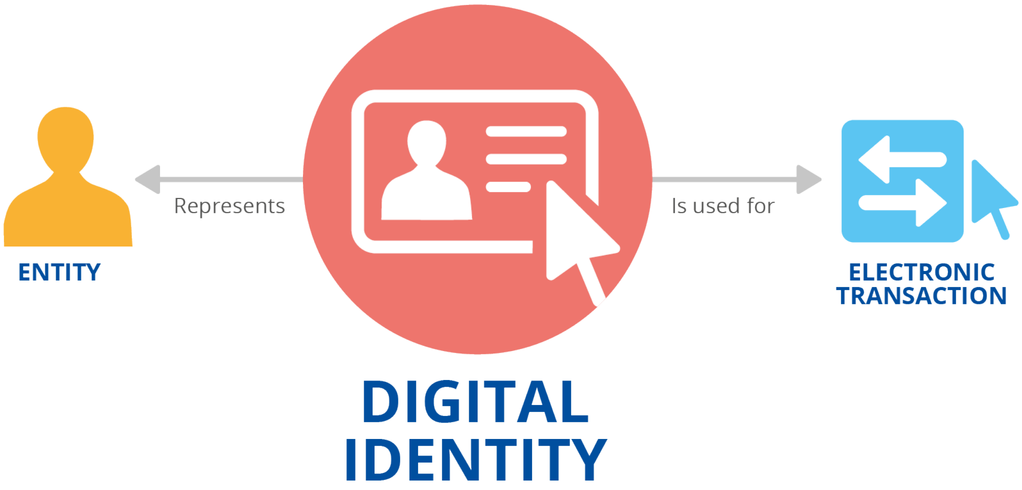
2. SCOPE

2.1. BASIC MODEL

2.1.1. Digital identity

'**Digital identity**' is defined, for the purpose of this document, as a '**unique representation of a subject engaged in an online transaction**' ([6]). This contains two elements constituting the role of digital identity: to represent a subject and to support an online transaction. '**Identity**' itself can be defined as a '**set of attributes ... related to an entity**' ([7]). Figure 1 provides an overview of digital identity.

Figure 1: Digital identity



A digital identity represents (attributes related to) an entity and is used in electronic transactions. Note that a digital identity is unique to the context of a digital service. A digital identity does not need to uniquely identify the entity in all contexts.

The eIDAS regulation specifies the rules for electronic identification and trust services for electronic transactions in the internal market. It recognises again the importance of identifying an entity in the context of electronic transactions. Its proposed update, the eIDAS 2.0 regulation, goes even further by proposing the EUDI Wallet, which would enable the identification of a user within different electronic transactions.

2.1.2. Means to support digital identity

There are different means enabling the representation of an entity in an electronic transaction. They can be separated into two categories: means created and managed by trust services, and means created and issued by identification schemes. These means support the digital identity and allow the relying parties to have trust in the identity. This landscape is depicted in Figure 2.

2.1.2.1. Means created and managed by trust services

[6] Grassi, P. A., Garcia, M. E. and Fenton, J. L. (2017), *Digital Identity Guidelines*, National Institute of Standards and Technology (NIST) Special Publication 800-63-3, NIST, Gaithersburg, MD.

[7] ISO/IEC 24760-1:2019: IT security and privacy – A framework for identity management – Part 1: Terminology and concepts.

- Electronic attestations of attributes (EAAs). These are attestations in electronic form that enable the authentication of a feature, characteristic or quality of an entity.
- Certificates. These enable the identification of the owner of a key pair.
- Signatures/seals. A signature can be used to identify the signer of a document. A seal can be used to prove the integrity and origin of a document.
- Electronic registered delivery service (ERDS) evidence. This is data generated within the ERDS, which aims to prove that a certain event has occurred at a certain time (8). The ERDS evidence can identify actors in the delivery process, for example the sender or recipient of a message.

Those means are created and managed by the following trust services:

- certificate authorities, which verify the identity represented in a certificate, link this identity to a key and provide information to relying parties if the certificate is allowed to be used;
- EAA services, which enable the attestation of specific identity attributes of an entity;
- ERDSs, which create and manage ERDS evidence;
- services for remote management of a private key, where the key of an entity is managed by another entity, in a secure environment.

2.1.2.2. Means created and managed by identification schemes

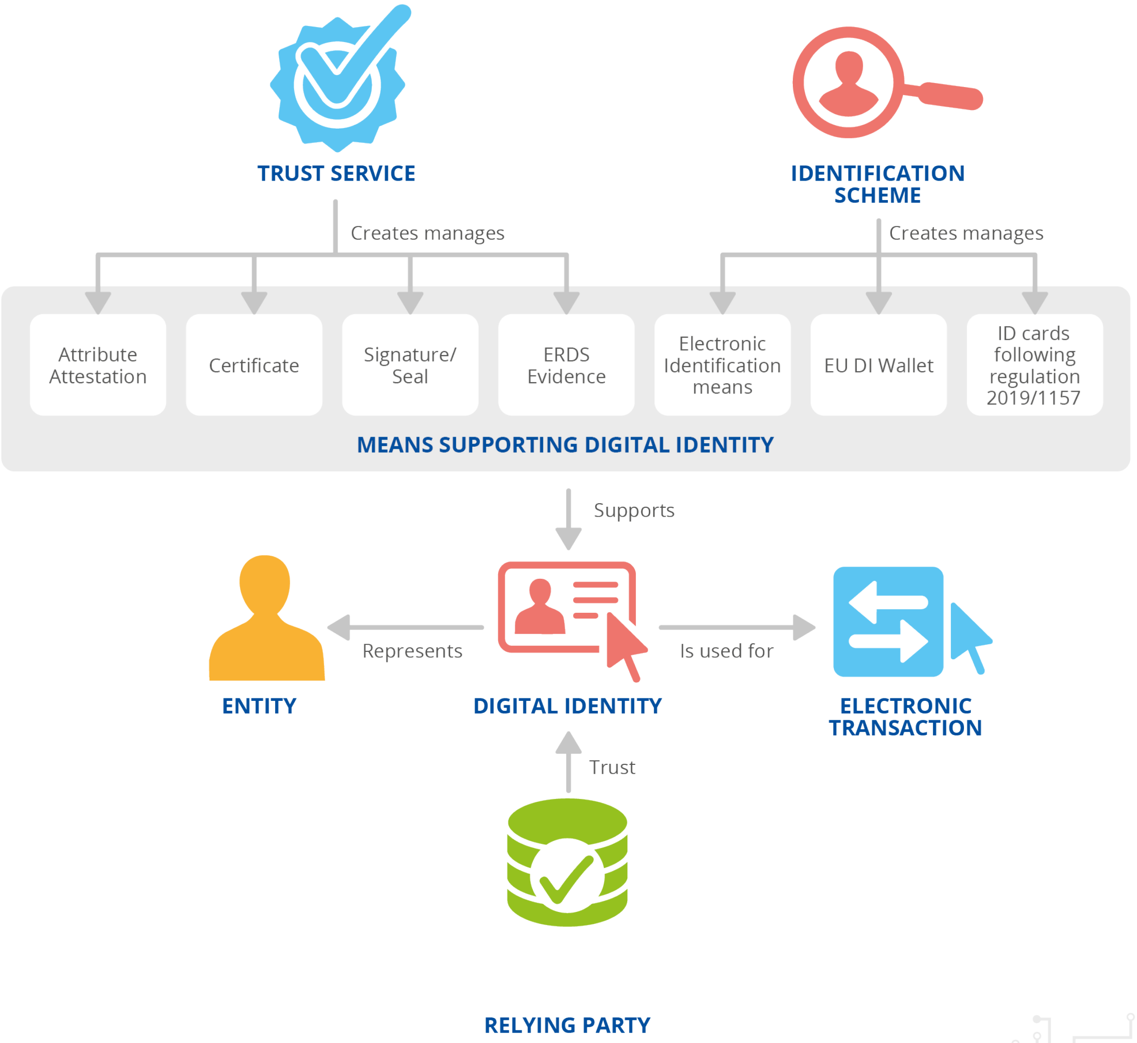
- Electronic identification means (9). These enable the identification of a user. The identification can be context specific; for example, it can be linked to a private/consumer context or provided by the state to its citizens. These means include but are not limited to electronic identification means notified by EU Member States.
- The EUDI Wallet, as defined in the proposed eIDAS 2.0 regulation. This enables the authentication of a user, but also provides specific attributes of a user.
- ID cards in line with Regulation 2019/1157 (10). Note that these ID cards are defined in the proposed eIDAS 2.0 regulation as electronic identification means.

[8] ETSI EN 319 521: Electronic Signatures and Infrastructures (ESI); policy and security requirements for electronic registered delivery service providers.

[9] The eIDAS regulation defines 'electronic identification means' as 'a material and/or immaterial unit containing person identification data and which is used for authentication for an online service'.

[10] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1157).

Figure 2: Digital identity landscape



2.1.3. Supporting services

For digital identities to be usable, several supporting services may be used. These services do not create or manage any means supporting digital identities but are helpful when using these means. The following are examples of supporting services.

- **Timestamping authority.** A timestamp provides proof that something (evidence, signature, etc.) was created before a specific time.
- **Signature validation service.** This enables validation of a specific signature.
- **Preservation service.** This enables the extension of the validity of a signature.
- **Signature creation service.** The presentation of the document prior to a signature and the formatting of the signature (not the cryptographic signature) may be carried out by a specific service.

2.2. SCOPE OF THE ANALYSIS

This document provides an analysis of standards related to different means supporting digital identity. It covers means created and managed by trust services, electronic identification means and the EUDI Wallet.

It also focuses on standards related to digital identity (Section 2.1.1) and related identity means (Section 2.1.2).

3. SETTING THE SCENE

3.1. ROLE OF DIGITAL IDENTITY STANDARDS

Standards are developed and defined through a process of sharing knowledge and building consensus among technical experts nominated by interested parties and other stakeholders. When it comes to developing and establishing standards, a large variety of players exist. Naturally, there is competition between these players, but they also cooperate in many instances, in particular when there is a common interest.

Standards are voluntary, which means that there is no automatic legal obligation to apply them. However, laws and regulations may refer to standards and even make compliance with them compulsory.

Digital identity standards have been developed due to the increasing demand for secure, reliable and cross-recognised digital transactions, fuelled by several governmental digital transformation programmes and the COVID-19 restrictions. The standardisation efforts involve several layers of digital identities, extending from the policy and governance level down to the operational and technical specifications level. They also address several elements and technologies supporting digital identities, such as electronic certificates, person identification, signature devices and cybersecurity aspects.

Standards in the area of digital identity have significantly evolved over time. A chronological review reveals that the initial focus was on addressing fundamental technical aspects, such as encodings and formats, card specifications, interfaces, profiles, algorithms and protocols. In this first era, almost all standards were published by the European and international standardisation organisations CEN, ISO and IETF. The second era, starting around 2007, saw the publication of important standards to address information security evaluation aspects (e.g. Common Criteria), cryptographic issues, signatures and, later, secure signature creation devices and biometrics. The eIDAS regulation triggered the involvement of ETSI and the publication of standards for trust services. These include policy and security requirements for operators and auditors, requirements for trustworthy systems, etc. At the same time, there were several other publications by standardisation organisations and industrial bodies on the use of, inter alia, signing technology means, identity management means and interconnected authentication means. Currently, the focus of standardisation is on newer challenges driven by market needs and by market-shaping initiatives such as the proposed eIDAS 2.0 regulation. These challenges include the EUDI Wallet, attestations of attributes, distributed ledgers, online user identification, self-sovereign identities and verifiable credentials.

3.2. STANDARDISATION ORGANISATIONS

The following sections present standardisation organisations and industrial bodies active in the area of digital identities. The huge demand for standards to ensure interoperable and secure services in the rapidly evolving digital identities arena is reflected in the large number of contributing organisations.

3.2.1. European Standardisation Organisations (ESOs) and standards

European standards (with the prefix 'EN') are documents that have been ratified by one of the three European Standardisation Organisations recognised as competent in the area of voluntary technical standardisation as set out by Regulation (EU) No 1025/2012 ([11]):

- CEN, the European Committee for Standardization, reflects the economic and social interests of its 34 member countries, channelled through their national standardisation organisations, and provides a platform for the development of European standards and other technical documents in relation to a wide range of fields and sectors including air and space, consumer products, defence and security, energy, health and safety, ICT, machinery, services, smart living and transport;
- CENELEC is the European Committee for Electrotechnical Standardization and is responsible for standardisation in the electrotechnical engineering field;
- ETSI addresses the ICT domain, with a particular focus on communications aspects regarding connected devices and the networks that connect them.

A European standard 'carries with it the obligation to be implemented at national level by being given the status of a national standard and by withdrawal of any conflicting national standard'. Therefore, a European standard automatically becomes a national standard in each of the 34 CEN/CENELEC member countries.

An important aspect is that industry can be directly involved in the process of standards development in the case of ETSI. However, industry can access CEN and CENELEC only through the national standardisation bodies.

- European standardisation organisation deliverables include the following.
- CEN/CENELEC Workshop Agreements (CWAs). A CWA is a CEN/CENELEC agreement, developed through a workshop, which reflects the agreement of identified individuals and organisations responsible for its contents. A CWA does not have the status of a European standard, and CEN/CENELEC national members are not obliged to withdraw national standards in conflict with a CWA.
- ETSI Standards (ETSI ES) and ETSI Guides (ETSI EG). These are ETSI deliverables adopted after voting weighted according to ETSI membership.
- ETSI Technical Specifications (ETSI TSs) and ETSI Technical Reports (ETSI TRs). These are ETSI deliverables adopted by the responsible technical body.

Within the three European standardisation organisations, ETSI has published several standards to support the eIDAS regulation and the general requirements of the international community to provide trust and confidence in electronic transactions. The ETSI Electronic Signatures and Infrastructures Technical Committee has published several standards on policy, security and technical requirements for trust service providers. The work of this technical committee also addresses the format of digital signatures, procedures and policies for creation and validation, and trusted lists as a trust anchor.

CEN Technical Committee 224, 'Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment', has published several standards to strengthen the interoperability and security of personal identification and related personal devices (see the annex to this document). This is the work of several working groups within CEN Technical Committee 224, including:

[11] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R1025).

- Working Group 17, ‘Protection Profiles in the Context of SSCD’,
- Working Group 18, ‘Biometrics’,
- Working Group 19, ‘Breeder Documents’.

More recently, an ad hoc group (Working Group 20) has been formed to develop EUDI Wallet standards (none had been produced or publicly announced at the time of writing).

CEN/CENELEC Joint Technical Committee 19, ‘Blockchain and Distributed Ledger Technologies’, in particular Working Group 1, ‘Decentralised Identity Management’, works in close contact with its ISO counterpart ISO Technical Committee 307 (see next section).

3.2.2. International Standardisation Organisations (SDOs) and standards

An international standard (IS) is a document that has been developed with the consensus of experts from many countries and is approved and published by one of the globally recognised international standardisation organisations:

- ISO. The International Organization for Standardization (ISO, which is an independent international organisation with a membership of 165 national standards bodies and develops voluntary, consensus-based international standards;
- IEC. The International Electrotechnical Commission (IEC, which develops international standards for all electrical, electronic and related technologies;
- ITU. International Telecommunications Union (ITU) is the United Nations specialized agency for information and communication technologies.

Deliverables include:

- technical specifications developed by international standardisation organisations address work under technical development or work expected to eventually be transformed and republished as an international standard;
- technical reports, which are more informal than an international standard or technical specification and do not contain any requirements; they may, for example, include data from an informative report, or information on the perceived ‘state of the art’.

Most international digital-identity-related activities happen within ISO/IEC Joint Technical Committee 1, ‘Information Security’, and in particular:

- Subcommittee 6, ‘Telecommunications and information exchange between systems’,
- Subcommittee 17, ‘Cards and security devices for personal identification’,
- Subcommittee 27, ‘Information security, cybersecurity and privacy protection’,
- Subcommittee 31, ‘Automatic identification and data capture techniques’.

In addition, within the scope of this study, ISO Technical Committee 307 provides a family of standards in the area of blockchain technologies and distributed ledger technologies, several of which have already been prepared.

3.2.3. National standardisation bodies and specialised agencies

National standardisation bodies and specialised agencies in the EU are also directly represented in the European standardisation organisations and, in many instances, their national publications eventually become European norms or international standards. However, the inventory provided in the annex to this document includes several digital identity standards available solely from national standardisation bodies and specialised agencies. Examples of such bodies include the following.

- **ANSSI** (Agence nationale de la sécurité des systèmes d'information), the French national cybersecurity agency, has been involved in the standardisation process for trust services and digital identities. ANSSI has issued standards on:
  - trust services based on the relevant ETSI standards,
  - remote identity proofing ('Prestataires de vérification d'identité à distance, Référentiel d'exigences'),
  - electronic identification means ('Moyens d'identification électronique – Référentiel d'exigences de sécurité'; not yet published).
- **BSI**, the German national cybersecurity authority, promotes cybersecurity in Germany and develops cybersecurity standards and guidelines. BSI standards and technical reports are available at no cost from www.bsi.bund.de. These include:
  - TR-03110 – technical guideline on advanced security mechanisms for machine-readable travel documents (MRTDs),
  - TR-03147 – technical guideline on assurance-level assessment of procedures for identity verification of natural persons (i.e. remote identity proofing).
- The **British Standards Institute**, the national standards body of the United Kingdom, produces technical standards on a wide range of products and services, and supplies certification and standards-related services to businesses:
  - BS 8626, 'Design and operation of online user identification systems – Code of practice', gives recommendations and supporting guidance for the design and operation of an online user identification system and the corresponding user digital identity management systems.
- **NIST** is part of the US Department of Commerce. Its Information Technology Laboratory is one of six research laboratories within NIST. The laboratory has seven divisions, including the Applied Cybersecurity Division and the Computer Security Division, both of which develop cybersecurity standards and guidelines. NIST standards and guidelines are available at no cost from its website (http://www.nist.gov). Information Technology Laboratory publications include:
  - the SP 800-63 Digital Identity Guidelines suite of documents, including volumes SP 800-63A 'Enrollment and identity proofing', SP 800-63B 'Authentication and lifecycle management' and SP 800-63C 'Federation and assertions',
  - FIPS PUB 140-3, 'Security requirements for cryptographic modules', which specifies security requirements for a cryptographic module utilised within a security system protecting sensitive information.

3.2.4. Industrial bodies

Industrial bodies and forums are not formally considered standardisation organisations; however, they offer de facto standards in certain areas, including the area of digital identities. In several cases, these bodies may submit the specifications they produce to other standards bodies (e.g. ISO/IEC, ITU Telecommunication Standardization Sector (ITU-T), ETSI) for additional ratification. Where applicable, the output of industrial bodies is included in the inventory provided in the annex to this document.

Such bodies include the following.

- The **Certification Authority Browser Forum**, a voluntary group of certification authorities, vendors of internet browser software, operating systems and other public key infrastructure (PKI)-enabled applications that promulgates industry guidelines governing the issuance and management of X.509 version 3 digital certificates that chain to a trust anchor embedded in such applications (Secure Socket Layers / Transport Layer Security (TLS), code signing and Secure/Multipurpose Internet Mail Extensions (S/MIME)). The standards/guidelines most relevant to this study are:
  - 'Baseline requirements certificate policy for the issuance and management of publicly-trusted certificates';
  - 'Guidelines for the issuance and management of extended validation certificates'.

- The **Cloud Signature Consortium (CSC)**, a global group of industry, government and academic organisations committed to driving standardisation of highly secure and compliant digital signatures in the cloud.
    - CSC has developed a protocol ('Architectures and protocols for remote signature applications') that enables the generation of remote signatures using the representational state transfer (REST) / JavaScript Object Notation (JSON) application programming interface (API).
- The **Financial Action Task Force (FATF)**, an intergovernmental organisation founded in 1989 on the initiative of the G7 to develop policies to combat money laundering. Relevant to this study is:
    - 'Guidance on digital ID', a publication intended to assist governments, regulated entities (e.g. financial institutions) and other relevant stakeholders in determining how digital ID systems can be used to conduct certain elements of customer due diligence under FATF Recommendation 10.
- **FIDO**, an open industry association launched in February 2013 whose stated mission is to develop and promote authentication standards that 'help reduce the world's over-reliance on passwords'. Relevant work includes:
    - the Client to Authenticator Protocol (CTAP), which describes an application layer protocol for communication between a roaming authenticator and another client/platform;
    - bindings of this application protocol to a variety of transport protocols using different physical media.
- The Internet Engineering Task Force (IETF), an open standards organisation that develops and promotes voluntary internet standards, in particular the technical standards that comprise the internet protocol suite.
    - A substantial number of requests for comments (RFCs) issued by the IETF cover data exchanges and formats and are considered the building blocks in the area of electronic signatures, PKI and trust services.
- The **Organization for the Advancement of Structured Information Standards (OASIS)**, which began as a consortium of vendors and users and today is a large non-profit standards organisation advancing projects for, for example, cybersecurity, blockchain, the internet of things, emergency management and cloud computing.
    - OASIS has developed technical specifications (protocols, profiles) related to digital signatures, such as the 'Digital signature service core protocols, elements, and bindings'.
- **OpenID**, a non-profit international standardisation organisation of individuals and companies committed to enabling, promoting and protecting OpenID (an open standard and decentralised authentication protocol).
    - 'OpenID Connect Core' defines the core OpenID functionality: authentication built on top of OAuth 2.0 and the use of claims to communicate information about the end user. Additional technical specification documents have been created to extend to issuance of verifiable credentials and verifiable presentations.
- **SOG-IS**, an agreement between government organisations or government agencies from EU or EFTA countries, produced in response to Council Decision 92/242/EEC ([12]) and the subsequent Council Recommendation 95/144/EC ([13]).
    - 'SOG-IS Crypto Evaluation Scheme – Agreed cryptographic mechanisms' specifies which cryptographic mechanisms are recognised as agreed (i.e. ready to be accepted by all SOG-IS participants). It is useful for both evaluators and developers.
- The **World Wide Web Consortium (W3C)**, the main international standards organisation for the World Wide Web. Founded in 1994 and currently led by Tim Berners-Lee, it is focused on

([12]) Council Decision of 31 March 1992 in the field of security of information systems (92/242/EEC) (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31992D0242).

([13]) Council Recommendation of 7 April 1995 on common information technology security evaluation criteria (95/144/EC) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995H0144).

the development of open standards to ensure the long-term growth of the World Wide Web. Technical specifications within the scope of this study include:

- the 'Verifiable credentials data model', a mechanism to express credentials on the web in a way that is cryptographically secure, privacy respecting and machine verifiable,
- 'Web authentication: An API for accessing public key credentials level 2', an API enabling the creation and use of strong, attested, scoped, public key-based credentials by web applications, for the purpose of strong authentication,
- the upcoming decentralised identifiers (DIDs) technical specification, which will specify data formats and protocols related to DIDs.

3.3. TOPICS

The multitude of standards developed by the above organisations can be examined in many different ways, and lead to different conclusions, that may be useful to the interested user. For example, apart from the main identifying information (name, code, reference link, version, year, etc.), standards can be read by:

- document source, for example a national standard, a European standard, an international standard, a forum or a consortium,
- document type, for example a standard, a technical specification or a technical report,
- document scope, for example policy, format/protocol or algorithm/process.

A more sophisticated grouping of standards related to digital identity is based on layers. For the purposes of this document, we introduce a four-layer approach, inspired by the Trust over IP approach, which we extend and adapt to any system managing digital identities. Each layer refers to technical and governance standards:

- Layer 1 includes standards for the infrastructures and public utilities deployed to support digital identities;
- Layer 2 includes standards for personal devices and software, and communication protocols, that enable digital-identity-related processes, and for end-user cryptographic key management;
- Layer 3 includes standards for representing means supporting digital identities, such as certificates, credentials and protocols supporting the digital identity life cycle;
- Layer 4 includes sector-specific standards related to digital identity.

On the other hand, standards may be grouped according to the technical approach used to represent digital identity, especially when using credentials. In this case, we can differentiate at least the following approaches:

- ICAO electronic MRTD (e-MRTD),
- ISO/IEC mobile driving licence (mDL) and mobile document (mdoc),
- X.509 certificate,
- Security Assertion Markup Language (SAML),
- OpenID Connect,
- self-sovereign identity.

In the following chapter, the categories (layers and technical approach) are combined to present the different standards and perform the analysis.

4. ANALYSIS

4.1. EACH GROUP OF STANDARDS

The following criteria are considered in the analysis:

- coverage of the identity management life cycle,
- maturity of the standards,
- authentication capabilities (in person versus remote, online versus offline),
- user sole control and dependencies, for example whether 'call home' is needed,
- data-protection-enhancing technologies, for example selective disclosure,
- trust model.

4.2. GENERAL GROUPS OF STANDARDS

4.2.1. General standards used in identity management

The ISO/IEC 24760 series specifies a general framework for identity management, including a life cycle for identity information. Moreover, it specifies fundamental concepts and operational structures of identity management with the purpose of realising information system management that enables information systems to meet business, contractual, regulatory and legal obligations.

- Part 1 of the standard specifies the terminology and concepts of identity management, to promote a common understanding in the field of identity management.
- Part 2 of the standard defines a reference architecture for an identity management system, including key architectural elements and their interrelationships. These architectural elements are described in respect of identity management deployment models. This part also specifies requirements for the design and implementation of an identity management system so that it can meet the objectives of stakeholders involved in the deployment and operation of that system.
- Part 3 of the standard introduces practices of identity management. They cover assurance in controlling identity information use, controlling access to identity information and other resources based on identity information, and controlling objectives that should be implemented when establishing and maintaining an identity management system.

ISO/IEC 29115 provides a framework for entity authentication assurance, which refers to the confidence placed in all the processes, management activities and technologies used to establish and manage the identity of an entity for use in an authentication transaction.

In particular, ISO/IEC 29115 (1) specifies four levels of entity authentication assurance; (2) specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance; (3) provides guidance for mapping other authentication assurance schemes to the four levels of assurance; (4) provides guidance for exchanging the results of authentication that are based on the four levels of assurance; and (5) provides guidance concerning controls that should be used to mitigate authentication threats.

4.2.1.1. Identity proofing

Identity proofing is defined by ISO/IEC 24760-1 as the verification based on identity evidence aiming to achieve a specific level of assurance (in line with ISO/IEC 29115). Under ISO/IEC 24760-1, verification is the process of establishing that identity information associated with a particular entity is correct.

ISO/IEC TS 29003 gives guidelines for the identity proofing of a person, and specifies levels of identity proofing and requirements to achieve these levels. This technical specification is intended to be used by any entity that performs identity proofing, as described in ISO/IEC 29115 and/or the ISO/IEC 24760 series.

BSI TR-03147 examines threats and requirements regarding identity proofing and verification procedures based on the use of ID documents (e.g. ID cards or passports), taking into account that the (minimum) required level of assurance varies depending on the kind of e-government or business process.

Other reference documents include ANSSI's 'Prestataires de vérification d'identité à distance – Référentiel d'exigences or CCN-STIC-140 Anexo F.11'.

4.2.1.2. Biometrics

Biometrics play an important role in identity proofing and verification. The presentation of a biometric spoof (e.g. a facial image or video of a person shown on a tablet or a fake silicone or gelatin fingerprint) to a biometric sensor can be detected by methods broadly referred to as presentation attack detection. ISO/IEC 30107-1 provides a foundation for presentation attack detection by defining terms and establishing a framework through which presentation attack events can be specified and detected so that they can be categorised, detailed and communicated for subsequent decision-making and performance assessment activities. ISO/IEC 30107-2 defines data formats for conveying the mechanism used in biometric presentation attack detection and for conveying the results of presentation attack detection methods.

4.2.2. General standards used in trust services

4.2.2.1. Layer 1: trust anchor distribution

A trust anchor is defined as an authoritative entity represented by a public key and associated data (IETF RFC 5914). The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative.

Trust anchors can be managed in different ways, including by using hierarchical, centralised or decentralised models. In the case of a decentralised model, Layer 1 utilities are needed.

ETSI TS 119 612 establishes a common template and a harmonised way for a trusted list scheme operator to provide information about the status and status history of the trust services provided by trust service providers regarding compliance with the relevant provisions of the applicable legislation on digital signatures and trust services for electronic transactions.

Trusted lists enable a decentralised system for distributing trust anchors' information, as happens in the eIDAS regulation, in which each supervisory body publishes its own trusted list containing the trust anchors for the trust services offered by the trust service providers established in its territory.

ETSI TS 119 614-1 defines specifications for testing conformity of Extensible Markup Language (XML) representation of trusted lists – that is, the set of checks to be performed for testing conformity of trusted lists as specified in ETSI TS 119 612.

ETSI TS 119 615 determines procedures for using and interpreting EU Member States' national trusted lists. This includes (1) authenticating the European-Commission-compiled list of trusted lists, (2) authenticating an EU Member State trusted list, (3) obtaining listed services matching a certificate, (4) EU qualified certificate determination, (5) qualified signature/seal creation device determination, (6) EU qualified timestamp determination, (7) EU qualified validation service determination, (8) EU qualified preservation service determination and (9) EU qualified ERDS determination.

Once the proposed eIDAS 2.0 regulation is approved, the three technical specifications – the electronic archiving of electronic documents, the management of remote electronic signature and seal creation devices, and the recording of electronic data in an electronic ledger – should be modified to include the proposed new trust services.

The current trusted list model is closely aligned to public key X.509 certificates, which are to be included mandatorily. To support other public key trust anchor approaches, such as decentralised PKI, the three technical specifications should be updated.

4.2.2.2. Layer 2: cryptographic standards

ETSI TS 119 312 provides guidance on the selection of cryptographic suites used in trust services, with particular emphasis on interoperability, based on the specified agreed cryptographic mechanisms of the SOG-IS crypto evaluation scheme.

4.2.2.3. Layer 3: governance frameworks

ETSI EN 319 401 is the base standard establishing general policy requirements on the operation and management practices of trust service providers. This is to be complemented and extended by other policy and security requirements for each trust service or for their service components (see Sections 4.3.3.3, 4.4.1.3 and 4.4.2.3). ETSI EN 319 401 is aligned with ISO/IEC 27002 and ISO/IEC 27701.

ETSI TS 119 461 defines policy and security requirements for trust service components providing identity proofing of trust service subjects. Because identification and authentication services are not trust services themselves (according to the eIDAS regulation), the scope of this technical specification is identity proofing of applicants to be enrolled as subjects or subscribers of a trust service provider.

Nevertheless, identity proofing can be carried out by the trust service provider as an integral part of the trust service provisioning, but it can also be the task of a specialised identity-proofing service provider acting as a subcontractor for the trust service provider; such a separate identity-proofing service provider can provide services to several trust service providers. In both cases, ETSI TS 119 461 would cover the trust service identity-proofing service component (part of the trust service), which may be (1) the issuance of (qualified) certificates for electronic signatures/seals or for website authentication; (2) the remote managing of (qualified) signature/seal creation devices and (3) the provision of (qualified) ERDSs.

ETSI TS 119 461 poses policy and security requirements specific to identity proofing, covering applicable technologies and use cases, resulting in a baseline level of identity proofing considered applicable to all relevant ETSI trust service standards.

This technical specification will probably need to be updated in respect of the proposed new trust services when the proposed eIDAS 2.0 regulation is approved.

Regarding conformity assessment of trust service providers, ETSI maintains a set of standards.

- ETSI EN 319 403-1 contains requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing and certifying conformity of trust service providers and the trust services they provide with defined criteria against which they claim conformity. This standard is not dependent on the eIDAS regulation.
- ETSI EN 319 403 applies the general requirements of ISO/IEC 17065 to the specific requirements of conformity assessment of trust service providers. ISO/IEC 17065 is the

international standard that establishes the requirements for bodies certifying products, processes and services.

- ETSI TS 119 403-2 determines additional requirements for conformity assessment bodies auditing trust service providers that issue publicly trusted certificates. These include specific requirements supplementary to those defined in ETSI EN 319 403-1 for conformity assessment bodies performing audits based on ETSI EN 319 411-1 and those from the Certification Authority Browser Forum, and requirements for audit attestations, including their content.
- ETSI TS 119 403-3 defines the additional requirements for conformity assessment bodies assessing qualified trust service providers and qualified trust services against the requirements of the eIDAS regulation.

4.2.2.4. Layer 4

Not applicable.

4.3. SPECIFIC GROUPS OF STANDARDS PROVIDING AUTHENTICATION CAPABILITIES

4.3.1. International Civil Aviation Organization electronic machine-readable travel documents and the eIDAS token

ICAO develops and maintains international standards in its Annex 9 (facilitation of the Chicago Convention for implementation by Member States). In the development of such standards, a fundamental precept is that, if public authorities are to facilitate inspection formalities for the vast majority of air travellers, those authorities must have a satisfactory level of confidence in the reliability of travel documents and in the effectiveness of inspection procedures. The production of standardised specifications for travel documents and the data contained therein aims to build that confidence.

An MRTD is an official document, conforming with the specifications contained in ICAO Document 9303, issued by a state or organisation, that is used by the holder for international travel (e.g. a machine-readable passport, a machine-readable visa, a machine-readable official travel document) and contains mandatory visual (eye-readable) data and a separate mandatory data summary in a format capable of being read by a machine.

The basic MRTD, with its optical character recognition readability, is designed for both visual and mechanical reading. ICAO member states have recognised that standardisation is a necessity and that the benefits of adopting the Document 9303 standard formats for passports and other travel documents extend beyond the obvious advantages for states that have machine readers and databases for use in automated clearance systems. In fact, the physical characteristics and data security features of the documents themselves offer a strong defence against alteration, forgery or counterfeit. Moreover, adoption of the standardised format for the visual zone of an MRTD facilitates inspection by airline and government officials, with the result that clearance of low-risk traffic is expedited, problem cases are more readily identified and enforcement is improved.

The optional introduction of biometric identification using data stored on a contactless integrated circuit (IC) provides greater security and resistance to fraud and thus makes it easier for the legitimate document holder to obtain visas for travel and to be processed through border inspection systems.

Building on ICAO Document 9303, the BSI and ANSSI have developed the eIDAS token set of technical specifications, published in TR-03110, as a contribution to the interoperability framework for electronic identification. It enables the development of token-based and customised solutions for electronic identification, authentication and signatures that are directly interoperable, without the need for translation using proxies. Thus, it supports the eIDAS middleware approach.

Key features of TR-03110 include user consent, two-factor authentication, strong authentication procedures, data minimisation procedures and an interoperable electronic logical data structure (LDS) covering all data fields in use in deployed European electronic identification infrastructures that can be easily extended by new attributes.

4.3.1.1. Layer 1

In the electronic machine-readable travel document (e-MRTD) PKI (see Section 4.3.1.3), there are several mechanisms to distribute PKI objects, such as country signing certification authorities (CSCAs). In this case, bilateral distribution is the primary mechanism, but master lists can also be used.

Master lists are a supporting technology for the bilateral distribution scheme. Given this, distribution of CSCA certificates through master lists is part of the bilateral distribution scheme. A master list is a digitally signed list of the CSCA certificates that are ‘trusted’ by the receiving state or organisation that issued the master list. CSCA self-signed root certificates and CSCA link certificates may be included in a master list.

The structure and format of a master list is defined in ICAO Document 9303, Part 12, Section 8. Publication of a master list enables other receiving states or organisations to obtain a set of CSCA certificates from a single source (the master list issuer) rather than having to establish a direct bilateral exchange agreement with each of the issuing authorities or organisations represented on that list.

Use of a master list does enable more efficient distribution of CSCA certificates for some receiving states. However, a receiving state making use of master lists must still determine its own policies for establishing trust in the certificates contained in that list.

4.3.1.2. Layer 2

Agents and devices

An e-MRTD is an MRTD (passport, visa or card) that has a contactless IC embedded in it and the capability of being used for biometric identification of the MRTD holder in accordance with the standards specified in the relevant part of ICAO Document 9303. This includes electronic machine-readable official travel documents – TD1- or TD2-sized machine-readable official travel documents conforming to the specifications of Document 9303, Part 5 or 6, respectively, that additionally incorporate a contactless IC and have the capability of biometric identification of the holder – and electronic machine-readable passports. The eIDAS token is an e-MRTD with extended capabilities.

Authentication capabilities

Part 11 of ICAO Document 9303 provides specifications to enable states and suppliers to implement cryptographic security features for e-MRTDs offering contactless IC access. Cryptographic protocols are specified to:

- prevent skimming of data from the contactless IC;
- prevent eavesdropping on the communication between the contactless IC and the reader;
- provide authentication of the data stored on the contactless IC based on the PKI described in Part 12 of Document 9303;
- provide authentication of the contactless IC itself.

An inspection system – that is, a system used for the inspection of MRTDs by any public or private entity that needs to validate the MRTD, and the use of this document for identity verification (e.g. border control authorities, airlines and other transport operators, financial institutions), involving the document signer public key of each state, or having read the document signer certificate from the e-MRTD – will be able to verify the document security object. In this way, through the contents of the document security object, the contents of the LDS are authenticated (see Section 4.3.1.3).

This verification mechanism does not require processing capabilities of the contactless IC in the e-MRTD. This is called passive authentication of the contactless IC's contents. Passive authentication proves that the contents of the document security object and LDS are authentic and have not changed. It does not prevent exact copying of the contactless IC's content or chip substitution. Validation of the document security object is described in ICAO Document 9303, Part 11, Sections 5.1.1 and 8.3.

An issuing state or organisation **may** choose to protect its e-MRTDs against chip substitution. There are different mechanisms to verify the authenticity of the chip:

- active authentication, which authenticates the contactless IC by signing a challenge sent by the IFD (inspection system) with a private key known only to the IC;
- chip authentication, which uses an ephemeral–static Diffie–Hellman key agreement protocol that provides secure communication and unilateral authentication of the e-MRTD chip;
- PACE with Chip Authentication Mapping.

Terminal authentication is also supported. It is a two-step challenge-response protocol that provides explicit unilateral authentication of the terminal. The protocol is based on extended access control as specified in TR-03110-1. If this protocol is supported by the IC, it must support Chip Authentication or PACE with Chip Authentication Mapping.

e-MRTDs do not support online user authentication. They are limited to offline, in-person authentication procedures based in biometric verification.

The eIDAS token TR-03110-2 specification defines a general authentication procedure for authentication terminals, among others. It requires password verification based in PACE and Extended Access Control version 2, which includes Terminal Authentication version 2, passive authentication and Chip Authentication version 2 or 3.

In addition, TR-03110-2 defines enhanced role authentication, which enables the use of attribute terminals to write attribute requests to the eIDAS token. Each attribute request may be read by an authenticated attribute provider, which will then write attributes to the eIDAS token. The eIDAS token restricts read access for stored specific attributes to the authentication terminal authenticated during the preceding general authentication procedure, and for generic attributes to authentication terminals with the required authorisation.

Both processes can be performed in person or online. Where they are performed online, the authentication terminal is composed of the following.

- An eID Server: The eID server is the remote part of the authentication terminal. It is authorised to access eIDAS token data and contains the interfaces with the user device and with the PKI. The electronic identification server provides the user device with a chain of terminal authentication certificates and a digital signature created on the eIDAS token's challenge with the corresponding private key.
- User Device: The user device is the local part of the authentication terminal and interacts with the user, the eIDAS token and the electronic identification server but is not authorised to access eIDAS token data. In particular, the user device contains an electronic identification

client software, a token reader, a display and an interface for user credential input. The chain of terminal authentication certificates received from the electronic identification server are displayed to the user and, only if the user accepts, the user device forwards the received certificates to the eIDAS token.

4.3.1.3. Layer 3

Technical format: the logical data structure electronic machine-readable travel document structure

The LDS e-MRTD structure provides space to store and digitally sign mandatory and optional data elements that can be used to link the holder to the document. The information stored in the LDS1 e-MRTD portion of the e-MRTD becomes static at the time of issuance and cannot be modified in any way. This feature is necessary to ensure that personal information is protected, and that document tampering can be more easily detected.

This is implemented as a document security object and as a Cryptographic Message Syntax (CMS) SignedData object containing and encoded with LDSSecurityObject, as defined in ICAO 9303, Part 10, Section 4.6.2. This object is digitally signed by the issuing state or organisation and contains hash representations of the LDS contents.

The LDS1 content includes the identity data, including the biometric data. Advanced authentication mechanisms use an LDS2. The eIDAS token supports specific and generic attributes.

- Specific attributes are attributes that are stored in data containers, which can be files or self-controlled data objects.
- Generic attributes are attributes that are not linked to the terminal sector of the requesting terminal. Each generic attribute is stored in a file, identified by a file identifier.

Governance frameworks

Parts 1 and 10–12 of ICAO 9303 constitute the governance framework for e-MRTDs and the supporting PKI.

The e-MRTD PKI enables the creation and subsequent verification of digital signatures on e-MRTD objects, including the Document Security Object to ensure the signed data is authentic and has not been modified. Revocation of a certificate, failure of the certification path validation procedure or failure of digital signature verification does not, on its own, cause an e-MRTD to be considered invalid. Such a failure means that the electronic verification of the integrity and authenticity of the LDS data has failed and other non-electronic mechanisms could then be used to make the determination as part of the overall inspection of the e-MRTD.

The e-MRTD PKI is much simpler than more generic multi-application PKIs such as the internet PKI defined in RFC 5280. In the e-MRTD PKI, each issuing State/Authority establishes a single Certification Authority (CA) that issues all certificates directly to end-entities, including Document Signers. These CAs are referred to as Country Signing Certification Authorities (CSCAs). There are no other CAs in the infrastructure. Receiving states establish trust directly in the keys/certificates of each issuing state's or organisation's CSCA.

A profile of X.509 and IETF RFC 5280 standards, tailored to the e-MRTD application, is specified in Part 12 of ICAO Document 9303. Unique aspects of the e-MRTD application include the following:

- there is precisely one CSCA per issuing State;

- certification paths include precisely one certificate (e.g. Document Signer).
- signature verification must be possible 5–10 years after creation;
- CSCA name change is supported;
- CSCA link certificates are not processed as intermediate certificates in a certification path.

The e-MRTD PKI consists of the following entities:

- a Country Signing CA (CSCA).
- Document Signer Certificates (DSC) which are used to sign the Document Security Objects (SOD).
- LDS2 Signer Certificates, which consists of the following:
    - LDS2-TS Signer – signs LDS2 Travel Stamps.
    - LDS2-V Signer – signs LDS2 Electronic Visas.
    - LDS2-B Signer – signs LDS2 Additional Biometrics.
- Bar Code Signer Certificates (BCSC), of which the following two specific types are defined:
    - Visa Signer Certificates (VSC).
    - Emergency Travel Document Signer Certificates (ESC).
- Master List Signer Certificates (MSC) used to sign Master Lists.
- Deviation List Signer Certificates (DLSC) used to sign Deviation Lists.
- Certificate Revocation List (CRL).

All the different certificate types are signed by the same CSCA. The CSCA also signs the certificate revocation list (CRL), which contains any revoked certificate irrespective of the type of certificate. All the certificates issued under the CSCA are collectively referred to as Signer Certificates.

For LDS2 applications, a separate Authorisation PKI is defined. The Authorisation PKI enables the e-MRTD-issuing state or organisation to control and manage the foreign states that are given authorisation to write LDS2 data objects to their e-MRTDs and to read those data objects. A foreign state intending to read or write LDS2 data must obtain an authorisation certificate directly from the e-MRTD-issuing state or organisation.

The authorisation PKI uses a different certificate structure (as per ISO 7816 on card-verifiable certificates) and therefore requires additional infrastructure components. LDS2 requires the terminal to prove to the e-MRTD contactless IC that it is entitled to write LDS2 data objects to the contactless IC or that it is entitled to read LDS2 data objects. Such a terminal is equipped with at least one private key and the corresponding terminal certificate, encoding the terminal's public key and access rights. Once the terminal has proven knowledge of this private key, the MRTD chip grants the terminal access to read/write LDS2 data as indicated on the Terminal Certificate.

The LDS2 authorisation PKI consists of the following entities:

- Country Verifying CAs (CVCAs).
- Document Verifiers (DVs).
- Terminals.
- Single Point of Contact (SPOC).

Distribution and management of the authorisation certificates between CVCAs in one State and DVs in other States is handled through a Single Point of Contact (SPOC) in each State.

TR-03110-3 describes the rules applicable to the PKI supporting EAC certification.

ICAO has published a guide on evidence of identity ([14]). This provides a framework and tools that enable states to methodically consider how best to uniquely identify individuals for the purpose of traveller identification.

The guide focuses on particular core principles to be considered when establishing and validating identity, to gain confidence that:

- the claimed identity is genuine (i.e. the identity is valid and not fictitious, and the identity is still living);
- the presenter links to the identity (i.e. the person can be linked to the claimed identity, the identity is unique within the authority’s system and the presenter is the sole claimant);
- the presenter uses the claimed identity (i.e. the person is operating under this identity in the community).

The guide does not set standards for how confidence in a person’s identity will be established. Practices will vary from state to state, depending on the processes and systems in place, the technologies obtainable, and the foundational documents and information available.

4.3.1.4. Layer 4

Not applicable.

4.3.1.5. Analysis

ICAO e-MRTDs and the eIDAS token	
Coverage of the identity management life cycle	Enrolment, verification, issuance, authentication, revocation
Maturity of the standards	High
Authentication capabilities	Data origin authentication, with different levels of security Offline user authentication based in biometric verification The eIDAS token supports online user authentication
User sole control and dependencies	The user has sole control over the document once it has been issued The digital identity is not portable, but uniquely bound to the device
Data-protection-enhancing technologies	The eIDAS token supports selective disclosure
Trust model	Federated

[14] https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf

4.3.2. Mobile Driving Licence (mDL/mdoc) and Mobile eID

ISO/IEC 18013-5 is an international standard that describes interface and related requirements to facilitate ISO-compliant driving licence functionality on a mobile device. It establishes interface specifications for the implementation of a driving licence in association with a mobile device.

To this end, it defines an mDL as a driving licence that fulfils at least the same function as an ISO-compliant driving licence but, instead of being paper or plastic based, is an mdoc. An mdoc is defined as a document or application that resides on a mobile device or requires a mobile device as part of the process of gaining access to the document or application.

The standard specifies the interface between the mDL and the mDL reader, and the interface between the mDL reader and the issuing authority infrastructure. The standard also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to (1) use a machine to obtain the mDL data, (2) tie the mDL to the mDL holder, (3) authenticate the origin of the mDL data and (4) verify the integrity of the mDL data.

ISO/IEC 18013-5 does not define how mDL-holder consent to share data is obtained; requirements on storage of mDL data and mDL private keys; or the interface between the mDL and the issuing authority.

Concise Data Definition Language (CDDL), specified in IETF RFC 8610, is used to express mdoc and other data structures related to mDLs. These data structures may be encoded using Concise Binary Object Representation (CBOR), as specified in IETF RFC 7049 (see also IETF RFC 8949), or the JavaScript Object Notation (JSON) Data Interchange Format, as specified in IETF RFC 8259.

As an evolution of this mDL standard, the ISO/IEC 23220 series of standards, which is under development, defines the building blocks of identity management through mobile devices. It considers generic system architectures of mobile eID-Systems (Part 1), data objects and encoding rules for generic eID systems (Part 2), protocols and services for the issuing phase (Part 3), protocols and services for the operational phase (Part 4), trust models and confidence level assessment (Part 5) and mechanisms for use in the certification on trustworthiness of secure areas (Part 6).

4.3.2.1. Layer 1

mDLs and other mdoc readers (see Sections 4.3.2.2 and 4.3.2.3) need access to the certificate authorities' root certificates issued by issuing authorities to verify issuer data authentication and for other security mechanisms.

Annex C of ISO/IEC 18013-5 defines a mechanism for distributing and disseminating the set of certification authorities' certificates issued by issuing authorities, namely a verified issuer certificate authority list (VICAL), and its policy, security and compliance requirements.

It does not make having a unique VICAL provider a requirement, nor does it preclude other mechanisms or models, including bilateral and/or regional agreements.

A VICAL is defined using a CDDL structure and encapsulated and signed using elliptic curve digital signature and CBOR Object Signing and Encryption (COSE), as defined in IETF RFC 8152. The standard also defines the VICAL signer certificate profile.

4.3.2.2. Layer 2

Agents and devices

An mDL works jointly with a mobile device, which is defined as a portable computing device that, at least, (1) has a small form factor such that it can be easily carried by a single individual, (2) is designed to operate, transmit and receive information without a wired connection, (3) possesses local, non-removable or removable data storage, (4) includes a self-contained power source, (5) includes a display and (6) includes a means for the holder of the portable computing device to interact with the device.

An mDL reader is a specific type of mdoc reader, which is a device that can retrieve mdoc data for verification purposes.

Authentication capabilities

According to the standard, an mDL must support at least the following functional requirements: (1) an mDL verifier, together with an mDL reader shall be able to request, receive and verify the integrity and authenticity of an mDL, whether online connectivity is present or not, for either the mDL or the mDL reader; (2) an mDL verifier not associated with the issuing authority shall be able to verify the integrity and authenticity of an mDL; (3) an mDL verifier shall be enabled to confirm the binding between the person presenting the mDL and the mDL holder; and (4) the interface between the mDL and the mDL reader shall support the selective release of mDL data to an mDL reader.

There are two mDL data retrieval methods.

- Device retrieval exclusively uses the interface between the mdoc and the mdoc reader. Data exchange is possible without the requirement of any device being connected to the internet. Bluetooth Low Energy BLE), near-field communication (NFC) or Wi-Fi Aware can be used to retrieve the information.
- Server retrieval uses the interface between the mdoc reader and the issuing authority infrastructure. OIDC or WebAPI can be used to retrieve the information. The issuing authority is involved in each transaction and therefore knows when an mdoc is used and what data is shared.

When using device retrieval, the mDL and the mDL reader communicate using mdoc request and mdoc response messages encoded with CBOR, which are transported using a data retrieval method. When using server retrieval, WebAPI or OpenID Connect may be used.

The device retrieval mdoc request allows the mDL reader to specify the requested documents, which includes the data elements requested and, optionally, the mdoc reader authentication information. In addition, for each requested data element, the requester may indicate the intention to retain the requested data. The device request may include a request for server retrieval information.

The device retrieval response includes the mdoc and other relevant information (see Section 4.3.2.3).

An mDL supports mdoc reader authentication, based in ECDSA/EdDSA digital signatures, in device retrieval. In server retrieval, this is based in TLS with client authentication.

ISO/IEC 23200-4 adds device retrieval based in OpenID Connect with SIOP, enhancing privacy.

4.3.2.3. Layer 3

Technical formats: mdoc CBOR and mdoc signed JWT

An mDL is, as introduced before, an ISO-compliant driving licence represented as an mdoc, the data model of which is based on elements with unique identifiers within a namespace. An mdoc representing an mDL follows the mDL data model described in the standard, including mandatory and optional data elements. This mdoc is identified using the document type element set to ‘org.iso.18013.5.1.mDL’.

Mandatory data includes family name, given names, date of birth, dates of issue and expiry, issuing country and authority, licence number, portrait of mDL holder and driving privileges. In this set of mandatory data, the portrait of the mDL holder is the only data item that can be used to verify that the person presenting the mDL is the mDL holder.

Optional data includes, among many other things, biometric templates. These data elements are associated with the mDL namespace, which is identified as ‘org.iso.18013.5.1’.

In the device retrieval method, an mdoc response contains an array of all returned documents, containing the document type, the returned data elements signed by the issuer and the returned data types signed by the device.

Issuer-signed data contains the mobile security object for issuer data authentication and data elements protected by issuer data authentication, while device-signed data contains the mdoc authentication structure and the data elements protected by mdoc authentication.

Issuer data authentication confirms that the mdoc data is issued by the issuing authority and that is has not changed since issuance, and mdoc authentication prevents cloning of the mdoc and mitigates man-in-the-middle attacks. The mdoc authentication mechanism is also available for the server retrieval token.

Issuer data authentication is implemented by way of a digital signature using COSE. The issuing authority calculates a message digest for each data element present in the mdoc and includes all digests in the mobile security object (MSO). The MSO also contains the public key of the mdoc device, which is used in mdoc authentication. This MSO is signed, and the signature is added to the mdoc.

The public key used for signing the MSO is provided as part of an X.509 public key certificate. When the mdoc is provided to an mdoc reader, the mdoc reader retrieves the certificate and executes the issuer data inspection procedure, which includes the following steps: (1) validating the X.509 public key certificate, (2) validating the digital signature of the issuer authentication structure and (3) calculating the digest value for every issuer-signed item received in the device response and verifying that they are equal to the corresponding digest values in the MSO.

Two mechanisms exist for mdoc authentication: ECDH-agreed MAC or ECDSA/EdDSA digital signature. Both mechanisms are based in a device private key, whose public key is included in the MSO, as stated above.

In server retrieval, the mdoc request and response structures are JSON encoded. Thus, a JSON Web Token (JWT) (conformant to IETF RFC 7519, updated by IETF RFCs 7797 and 8725) is returned for each document. This JWT is protected using a JSON Web Signature (JWS), conformant to IETF 7515. There is a JWT inspection procedure, similar to the case of MSOs as described above. WebAPI and OpenID Connect may be used for requesting and delivering the mdoc.

In ISO/IEC 23220-2, the JSON data model supports two types of data format: the issuer-signed model, for the server retrieval method, and the holder-signed model, for the presentation of issuer-signed data over the web. The issuer-signed model may support the verifiable credential model, as defined by W3C, or the ID token model. The holder-signed model may support the verifiable presentation model, as defined by W3C, or the ID token model. Both the issuer-signed model and the holder-signed model can support DID (Decentralised Identifiers) methods.

Governance frameworks

ISO/IEC 18013-5 does not define a complete governance framework because it does not cover the full life cycle (i.e. it does not cover enrolment, issuance, activation or revocation).

It only provides normative content for the certificate and certificate revocation list profiles.

4.3.2.4. Layer 4

Other mdoc-based document types may be defined to support mobile credentials, such as mobile identities, so that they can use the engagement and retrieval protocols defined in the ISO/IEC standard.

4.3.2.5. Analysis

mDLs/mdocs and mobile electronic identification	
Coverage of the identity management life cycle	Authentication Enrolment, issuance and activation are not defined. Suspension and/or revocation are not covered
Maturity of the standards	Medium (mDL) Low (mID)
Authentication capabilities	Data origin authentication Device authentication Reader authentication Offline user authentication based in portrait comparison or biometric verification, with optional reader authentication
User sole control and dependencies	The user has sole control over the mDL (or any other mdoc) once it has been issued, because the user possesses the device. This may not be effective if reader authentication is not used or when using authenticated readers in mDLs with no explicit user consent mechanism. mDL reader authentication cannot be required as a precondition for the release of mandatory mDL data. It could be required for the release of other mdoc types No user consent mechanism is defined in the mDL standard The digital identity may be portable, depending on the use of secure elements to protect device keys

Data-protection-enhancing technologies	Supports selective disclosure In server retrieval, user tracking is possible. This is corrected for mobile IDs in ISO/IEC 23220
Trust model	Federated. The standard defines an optional mechanism to convey trust information, in the form of a Verified issuer certificate authority list (VICAL).

4.3.3. X.509 certificates (PKI-PMI)

The frameworks for public key infrastructure (PKI) and privilege management infrastructure (PMI) are defined by the Recommendation ITU-T X.509 | ISO/IEC 9594-8 standard.

Issuers of X.509 public key certificates are technically known as Certification Authorities (CA), and they usually operate Registration Authorities (RA) and offer certificate status information to subjects and relying parties, eventually implementing Validation Authorities (VA), such as Online Certificate Status Protocol servers, or they issue Certificate Revocation Lists (CRLs). Issuers of X.509 attribute certificates are technically known as Attribute Authorities (AA), and they issue Attribute Revocation Lists (ARL). Entities that request and receive X.509 certificates are known as subscribers and/or subjects. Third parties needing to rely on certificates are known as relying parties.

Public key certificates can be used for user authentication before a relying party (direct authentication), such as in the Transport Layer Security (TLS) protocol, or before an IdP to which the authentication process is delegated by the relying party, usually as part of an identity federation system. Certificates issued under an electronic identification scheme are recognised as electronic identification means.

Public key certificates are also used for server authentication, for example in TLS, and they can also be used for creating advanced electronic signatures or seals. Public key certificates for electronic signatures, for electronic seals and for website authentication issued in the EU are regulated by the eIDAS Regulation and are issued by trust service providers. When used with an authentication mechanism, they can also be recognised by Member States as electronic identification means.

Attribute certificates can also be used to assert identity attributes of users, both in authentication protocols and in advanced electronic signatures or seals. Once approved, the eIDAS 2.0 regulation will regulate them as a trust service consisting in the issuance of electronic attestations of attributes.

4.3.3.1. Layer 1

Trusted lists conformant to ETSI TS 119 612 are used by supervisory bodies to publish the trust anchors for X.509 public key certificates (see Section 4.2.2.1).

ETSI TS 119 612, and the accompanying ETSI TS 119 614-1 and ETSI TS 119 615, would need to be updated if X.509 attribute certificates were to be used for representing (qualified) electronic attestations of attributes.

4.3.3.2. Layer 2

Agents and devices

X.509 public key certificates may be used for different types of agents and devices, including software-based or hardware-based devices.

Software agents typically used for managing X.509 certificates and the corresponding private keys typically include internet browsers, operating system repositories or files such as PKCS#12 files. Hardware-based devices include smart cards, secure elements and trusted platforms.

The eIDAS token specification (BSI TR-03110, Parts 1–4) is a contribution from BSI, the German cybersecurity agency, and ANSSI, the French cybersecurity agency, supported by European industry partners, to the interoperability framework for electronic identification. It enables the development of token-based and customised solutions for electronic identification, authentication and signatures that are directly interoperable, without the need for translation through proxies. The specification provides a modular and homogeneous secure element API to protect the authenticity, integrity, originality, confidentiality and privacy of the data stored on tokens for electronic identification, authentication and signatures (e.g. the eIDAS token).

CEN EN 419 212 is a multipart standard establishing an application interface for secure elements for electronic identification, authentication and trusted services. Some eIDAS token specifications are incorporated. Part 5 describes its use for client/server authentication.

Issuers of X.509 certificates must use trustworthy systems and proper key management techniques and modules when issuing certificates. The relevant standards include the following.

- **ISO/IEC 19790 and FIPS PUB 140-3** define security requirements for cryptographic modules. As stated in ETSI EN 319 411-1, with regard to the general availability of devices that meet the Common Criteria, it is expected that ISO/IEC 19790 or FIPS 140-2 Level 3 will no longer be acceptable.
- **CEN/TS 419 221, Parts 1–4, and CEN EN 419221-5** define protection profiles according to the Common Criteria for cryptographic modules for TSP signing operations with backup (Part 2), for TSP key generation services (Part 3), for TSP signing operations without backup (Part 4) and for trust services (CEN EN 419221-5).

Authentication capabilities

In respect of end entity authentication, several authentication protocols may be used, among which possibly the most widely used is the Transport Layer Security (TLS), currently defined in IETF RFC 8446, corresponding to version 1.3.

The main goal of TLS is to provide a secure channel between two communicating peers. It enables client/server applications to communicate over the internet in a way that is designed to prevent eavesdropping, tampering and message forgery. This secure channel should provide several security properties, including authentication. While the server side of the channel is always authenticated, the client side is optionally authenticated.

Authentication can happen through asymmetric cryptography (e.g., RSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), or the Edwards-Curve Digital Signature Algorithm (EdDSA) or a symmetric pre-shared key (PSK). TLS supports server authentication and client authentication, except in the PSK handshake flows.

To this end, there are two primary components: (1) a handshake protocol that authenticates the communicating parties, negotiates cryptographic modes and parameters, and establishes shared keying material; and (2) a record protocol that uses the parameters established by the handshake protocol to protect traffic between the communicating peers.

X.509 certificates do not support selective disclosure, because of the digital signature mechanism used to protect them. Thus, to implement selective disclosure, it may be necessary to limit the subject's information contained in their public key certificate and to issue different attribute certificates. Nevertheless, attribute certificates have scarcely been deployed to date and they are not supported in widely deployed protocols such as TLS.

4.3.3.3. Layer 3

Technical formats: X.509 public key certificates and X.509 attribute certificates

The Recommendation ITU-T X.509 | ISO/IEC 9594-8 standard offers an Abstract Syntax Notation One (ASN.1) syntax-based for representing digital identities. This standard specifies the information objects and data types for a public key infrastructure (PKI), including public key certificates, certificate revocation lists (CRLs), trust brokers, and authorisation and validation lists (AVLs). The attribute certificate framework specifies the information objects and data types for a privilege management infrastructure (PMI), including attribute certificates and attribute certificate revocation lists (ACRLs).

Attributes used to describe digital identity, where contained in public key certificates or attribute certificates, are defined in the Recommendation ITU-T X.520 | ISO/IEC 9594-6 standard, using ASN.1 syntax.

IETF RFC 5280 contains a profile of X.509 version 3 public key certificates, for their use on the internet, that will foster interoperability and a reusable PKI. To this end, the X.509 version 3 certificate format is described in detail, with additional information regarding the format and semantics of internet name forms; standard certificate extensions are described, and two internet-specific extensions are defined; and a set of required certificate extensions is specified. Currently, IETF RFC 5912, updated by IETF RFC 6069, contains the ASN.1 modules for X.509 version 3 certificates.

IETF RFC 3739 defines specific conventions for certificates that are qualified within a defined legal framework, namely Qualified Certificates, including an extension (QCStatements) that can contain any statement by the certificate issuer that can be useful to the relying party in determining the applicability of the certificate for an intended usage.

The eIDAS Regulation regulates the use of different types of public key certificates for electronic signatures, for electronic seals and for website authentication. The proposed eIDAS 2.0 regulation will regulate electronic attestations of attributes, which could be based in X.509 attribute certificates, among other possibilities.

ETSI has defined specific profiles of IETF RFC 5280 public key certificates, for both qualified and non-qualified certificates, according to the eIDAS regulation:

- ETSI EN 319 412-1 defines common data structures, including the use of semantics identifiers and of validity-assured certificates;
- ETSI EN 319 412-2 specifies the requirements regarding certificate content for TSPs issuing certificates to natural persons; providing a certificate profile, which facilitates interoperability of certificates issued to natural persons for the purpose of supporting digital signatures; peer entity authentication; data authentication; and data confidentiality;
- ETSI EN 319 412-3 specifies the requirements regarding certificate content for TSPs issuing certificates to legal persons; providing a certificate profile, which facilitates interoperability of certificates issued to legal persons for the purpose of supporting digital signatures; peer entity authentication; data authentication; and data confidentiality;
- ETSI EN 319 412-4 specifies the requirements regarding certificate content for TSPs issuing website certificates for sites that are accessed through the TLS protocol as specified in

IETF RFC 5246 and regarding providing a certificate profile, which enables interoperability of website certificates issued to legal or natural persons;

- ETSI EN 319 412-5 specifies the requirements regarding the QCStatements as required for qualified certificates as specified in Parts 2–4 of ETSI EN 319 412.

IETF RFC 5755 defines an internet attribute certificate profile for authorisation, based on X.509 attribute certificates. These attributes are bound to a subject, called a ‘holder’, through (1) reference to a public key certificate issued to the holder, (2) the holder’s name, in which case, if the authentication mechanism is based on a public key certificate, the holder’s name will need to coincide with the subject’s name contained in that public key certificate, or (3) an object digest produced from the holder’s public key or the holder’s public key certificate. The third possibility may provide some additional privacy.

Public key certificates and attribute certificates are associated with, and support, credentials – that is, representations of identities to be used in authentication processes, based in digital signatures and other cryptographic techniques – as previously seen when describing Layer 2.

Governance frameworks

Several general governance frameworks define how X.509 public key certificates must be issued and managed.

- ISO/IEC 27099:2022 sets out a framework of requirements to manage information security for PKI trust service providers through certificate policies, certificate practice statements and, where applicable, their internal underpinning by an information security management system. The framework of requirements includes the assessment and treatment of information security risks, tailored to meet the agreed service requirements of its users as specified through the certificate policy, and addresses the life cycle of public key certificates that are used for digital signatures, authentication or key establishment for data encryption. This general framework has been derived from ISO 21188, which defines a practices and policy framework for PKI for financial services.
- ETSI EN 319 411-1 specifies general policy and security requirements for trust service providers issuing certificates for electronic signature, certificates for electronic seals and certificates for website authentication. This standard builds on ETSI EN 319 401, which defines general policy requirements common to all trust services, including controls from ISO/IEC 27002, and incorporates requirements from other governance frameworks, for example the Certification Authority Browser Forum requirements for certificates for website authentication.
- ETSI EN 319 411-2 specifies additional policy and security requirements for trust service providers issuing EU qualified certificates. Thus, it extends ETSI EN 319 411-1 to ensure regulatory compliance.
- The Certification Authority Browser Forum (CA/B Forum), a voluntary gathering of certificate issuers and vendors of internet browser software and other applications that use certificates, publishes and maintains the ‘Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates’, which describes a subset of the requirements that a certification authority must meet in order to issue digital certificates for SSL/TLS servers to be publicly trusted by browsers.
    - This is augmented by the extended validation certificate requirements. These aim to identify the legal entity that controls a website by providing reasonable assurance to the user of an internet browser that the website the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name; address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information. They also aim to enable encrypted communications with a website by facilitating the exchange of encryption keys in order to enable the

encrypted communication of information over the internet between the user of an internet browser and a website.

There are no updated governance frameworks for X.509 attribute certificates. ETSI TS 102 158, which specified policy requirements for Certification Service Providers issuing attribute certificates usable with qualified certificates, was published in 2003 and has not been updated. For electronic attestations of attributes to be represented using X.509 attribute certificates, standardisation work would be required.

4.3.3.4. Layer 4

Sector-specific X.509 certificates

ETSI TS 119 495 defines certificate profiles for Open Banking. Open Banking enables third parties to provide additional payment services through an open interface to financial institutions, such as banks, as regulated, for example, in the EU revised payment services directive (PSD2). These certificate profiles extend the qualified certificate profile for electronic seals and for website authentication.

Governance frameworks

ISO 21188 defines a practices and policy framework for public key infrastructure for financial services.

4.3.3.5. Analysis

eIDAS X.509 certificates (PKI/PMI)	
Coverage of the identity management life cycle	Enrolment, verification, issuance, authentication, suspension, revocation
Maturity of the standards	High
Authentication capabilities	Data origin authentication Device authentication, in some cases Reader authentication Online user authentication
User sole control and dependencies	The user has sole control over the certificate once it has been issued An X.509 public key certificate is portable attending to the device used for generating and/or storing the private key
Data-protection-enhancing technologies	It could support selective disclosure, when combining public key certificates with attribute certificates, but there is no support for attribute

	certificates in standard end entity authentication protocols
Trust model	Federated, based in the eIDAS regulation trusted list

4.3.4. Security Assertion Markup Language and the eIDAS regulation

Security Assertion Markup Language (SAML) defines the syntax and processing semantics of assertions made about a subject by a system entity. When making or relying upon such assertions, SAML system entities may use other protocols to communicate regarding either an assertion itself or the subject of an assertion. The SAML core specification defines both the structure of SAML assertions and an associated set of protocols, in addition to the processing rules involved in managing an SAML system.

SAML assertions and protocol messages are encoded in XML and use XML namespaces. They are typically embedded in other structures for transport, such as HTTP POST requests or XML-encoded SOAP messages. The SAML bindings specification provides frameworks for the embedding and transport of SAML protocol messages. The SAML profiles specification provides a baseline set of profiles for the use of SAML assertions and protocols to accomplish specific use cases or achieve interoperability when using SAML features.

The current eIDAS Regulation provides that an interoperability framework should be established for the purposes of interoperability of the national electronic identification schemes notified by Member States. Commission Implementing Regulation (EU) 2015/1501 ([15]) established the possibility of adopting technical specifications necessary for the interoperability and security of notified electronic identification schemes and means. The eIDAS Cooperation Network has published a favourable opinion regarding version 1.2 of the eIDAS technical specifications, the domains of which are:

- eIDAS Attribute Profile version 1.2,
- eIDAS Message Format version 1.2,
- eIDAS Cryptographic Requirements for the Interoperability Framework – TLS and SAML version 1.2,
- eIDAS Interoperability Architecture version 1.2.

Interoperability between different eID schemes is achieved by defining the technical interfaces between eIDAS Connectors and eIDAS Services, collectively eIDAS Nodes. The interfaces between the eIDAS Connectors and the relying parties and between the eIDAS Services and the eID scheme are part of the national system of the Receiving MS and the Sending MS, respectively, and therefore out of the scope of the eIDAS interoperability framework specifications.

4.3.4.1. Layer 1

The Trust anchors for all eIDAS nodes are provided by the Member States (i.e. no central trust anchor is provided). Trust anchors are exchanged bilaterally between Member States, in the form of certificates, each certifying a signing key held by the Member State (a 'Root"). Such a signing key can be used either (1) to directly sign SAML metadata objects or (2) as a root certificate of a PKI used to sign SAML metadata objects.

([15]) Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1501).

A bilaterally exchanged Trust Anchor can be used to sign an optional MetadataServiceList, which may contain information about national metadata resources and how to validate them. Its purpose is to provide a consolidated list of the different metadata locations across Member States covering one or more end points.

This list may be cryptographically signed, but the integrity of the metadata is ensured through a signature on each metadata document that can be retrieved at any specified location. This format is inspired by trusted lists used in trust services.

The following cases have been considered:

- Member States with one connector and one proxy (the 'classic' eIDAS – Node case),
- Member States with no proxy (the middleware case; middleware services do not need publicly available metadata),
- Member States with some or many connectors (the decentralised case).

4.3.4.2. Layer 2

Agents and devices

Usually, the agent used for SAML-supported authentication is a web browser.

In some cases, a hardware device is used, such as in the eIDAS middleware approach using an eIDAS token. When this is the case, higher levels of assurance are achievable.
CEN EN 419 212, Part 4, describes a protocol flow, based on BSI TR-03110, for e-services with a trusted third party (an Attribute Provider), which can be used in SAML flows (in the middleware approach).

Authentication capabilities

The protocols defined by SAML achieve, among other things, the performance of authentication on request, the returning of the corresponding assertion and the performance of a near-simultaneous logout of a collection of related sessions ('single logout') on request.

The SAML bindings specification describes specific means of transporting protocol messages using existing widely deployed transport protocols. The SAML profiles specification describes several applications of the SAML protocols together with additional processing rules, restrictions and requirements that facilitate interoperability.

In the scenario supported by the web browser SSO profile, a web user either accesses a resource at a service provider or accesses an identity provider such that the service provider and desired resource are understood or implicit.

The web user authenticates (or has already authenticated) to the identity provider, which then produces an authentication assertion (possibly with input from the service provider), and the service provider consumes the assertion to establish a security context for the web user. During this process, a name identifier might also be established between the providers for the principal, subject to the parameters of the interaction and the consent of the parties.

To implement this scenario, a profile of the SAML Authentication Request protocol is used, in conjunction with the HTTP Redirect, HTTP POST and HTTP Artifact bindings.

eIDAS Message format version 1.2 specifies the message format of exchanged metadata or SAML AuthnRequest and SAML Response messages to be exchanged between eIDAS nodes.

It considers sign-on use cases only, neglecting logout use cases, and it refers to the SAML web browser SSO profile.

4.3.4.3. Layer 3

Technical format: SAML assertion

An SAML assertion is a package of information that supplies zero-or-more statements made by an SAML authority, usually about a subject. Typically, service providers can make use of assertions about a subject in order to control access and provide customised service. Accordingly, they become the relying parties of an asserting party (an identity provider).

There are three different kinds of assertion statements that can be created by an SAML authority.

- **Authentication**. The assertion subject was authenticated by a particular means at a particular time.
- **Attribute.** The assertion subject is associated with the supplied attributes.
- Authorisation Decision. A request to allow the assertion subject to access the specified resource has been granted or denied or is indeterminate. This statement type has been abandoned in favour of eXtensible Access Control Markup Language (XACML).

The outer structure of an assertion is generic, providing information that is common to all the statements within it. Within an assertion, a series of inner elements describe the authentication, attribute, authorisation decision or user-defined statements containing the specifics. Furthermore, extensions are permitted by the SAML assertion schema, allowing user-defined extensions to assertions and statements, and allowing the definition of new kinds of assertions and statements.

The generic assertion contains a set of mandatory elements: version, id, issue instant and issuer. It may also contain optional elements: subject of the statement(s) in the assertion, conditions that must be evaluated when assessing the validity of and/or when using the assertion, additional information related to the assertion that assists processing in certain situations but that may be ignored by applications that do not understand the advice or do not wish to make use of it, zero-or-more statements and an XML Signature that protects the integrity of and authenticates the issuer of the assertion.

An entity or principal that is the subject of all the (zero-or-more) statements in the assertion may be included using the subject element, which contains an identifier, a series of one or more subject confirmations or both. The subject confirmation element is used to describe information that enables the subject to be confirmed (i.e. provides the means for a relying party to verify the correspondence of the subject of the assertion with the party with whom the relying party is communicating, for example using a cryptographic key).

Conditions to be considered may include the earliest time instant at which the assertion is valid or has expired, whether the assertion is addressed to a particular audience, that the assertion should be used immediately and must not be retained for future use, or limitations that the asserting party imposes on relying parties that wish to subsequently act as asserting parties themselves and issue assertions of their own on the basis of the information contained in the original assertion.

The authentication statement element describes a statement by the SAML authority asserting that the assertion subject was authenticated by a particular means at a particular time. It is mandatory to specify the time at which the authentication took place and the context used by the authenticating authority up to and including the authentication event that yielded this statement.

The attribute statement element describes a statement by the SAML authority asserting that the assertion subject is associated with the specified attributes. Each attribute element contains an attribute name and the corresponding value(s).

eIDAS SAML Attribute Profile version 1.2 provides a list of attributes included in the eIDAS minimum data sets, conforming to the annex to the interoperability framework implementing act. All attributes for the eIDAS minimum data sets can be derived from the ISA Core Vocabulary, including the Core Person Vocabulary and the Core Business Vocabulary. The technical specification provides rules for unique identifiers and natural and legal person representatives.

Governance framework

The eIDAS SAML-based identity federation is governed by the eIDAS Rregulation and Commission Implementing Regulation (EU) 2015/1501.

4.3.4.4. Layer 4

Not applicable.

4.3.4.5. Analysis

SAML and the eIDAS regulation	
Coverage of the identity management life cycle	Authentication Attribute sharing
Maturity of the standards	High
Authentication capabilities	Online user authentication
User sole control and dependencies	It depends on the underlying authentication agent/device and the policies of the SAML authority / identity provider
Data-protection-enhancing technologies	Supports selective disclosure User tracking by the SAML authority / identity provider and, depending on the configuration, by other parties, such as proxy SAML nodes, is possible. User tracking may be limited in the middleware-to-middleware approach
Trust model	Enterprise/federated The eIDAS interoperability framework adopts a federated identity management approach with a decentralised trust model at EU level. Each Member State may decide whether to adopt a centralised or decentralised approach both for issuing and for consuming identity assertions

4.3.5. OpenID Connect

The OAuth 2.0 Authorisation Framework (IETF RFC 6749) and OAuth 2.0 Bearer Token Usage (IETF RFC 6750) specifications provide a general framework for third-party applications to obtain and use limited access to HTTP resources. They define mechanisms to obtain and use Access Tokens to access resources but do not define standard methods to provide identity information. Without profiling, OAuth 2.0 is incapable of providing information about the authentication of an end user.

OpenID Connect 1.0 is a simple identity layer on top of the Oauth 2.0 protocol. It enables clients to verify the identity of the end user based on the authentication performed by an Authorisation Server, and to obtain basic profile information about the end user in an interoperable and REST-like manner. The specification suite is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID Providers and session management, when relevant.

The OpenID Connect Core 1.0 technical specification defines the main functionality (i.e. authentication built on top of OAuth 2.0) and the use of Claims to communicate information about the end user. It also describes the security and privacy considerations for using OpenID Connect.

4.3.5.1. Layer 1

Not applicable.

4.3.5.2. Layer 2

Agents and devices

OpenID Connect enables clients of all types, including web-based, mobile and JavaScript clients, to request and receive information about authenticated sessions and end users. In some cases, a hardware device is used. When this is the case, higher levels of assurance are achievable.

CEN EN 419 212, Part 4, describes a protocol flow, based on BSI TR-03110, for e-Services with a trusted third party (an Attribute Provider), which can be used in OpenID Connect flows.

Authentication capabilities

The OpenID Connect protocol, in summary, involves the following steps: (1) the relying party (the ‘client’) sends a request to the OpenID Provider (OP); (2) the OP authenticates the end user and obtains authorisation, (3) the OP responds with an ID Token and usually an Access Token; (4) the relying party can send a request with the Access Token to the UserInfo Endpoint and (5) the UserInfo Endpoint returns Claims about the End-User.

OpenID Connect performs authentication to log in the end user or to determine that the end user is already logged in. OpenID Connect returns the result of the authentication performed by the server to the client in a secure manner so that the client can rely on it. The authentication result is returned in an ID Token (see Section 4.3.5.3).

Authentication can follow one of three paths: (1) the Authorisation Code Flow, (2) the Implicit Flow, or (3) the Hybrid Flow. The flows determine how the ID Token and Access Token are returned to the client. The Authorisation Code Flow returns an Authorisation Code to the Client, which can then directly exchange it for an ID Token and an Access Token. In the Implicit Flow, all tokens are returned from the Authorisation Endpoint and the Token Endpoint is not used.

OpenID Connect also supports Self-Issued OpenID Providers (OIDC with SIOP) (i.e. personal, self-hosted OPs that issue self-signed ID Tokens. The Self-Issued OP does not itself assert identity information about this End-user. Instead, the End-user becomes the issuer of identity information. Using Self-Issued OPs, End-Users can authenticate themselves with self-issued ID Tokens signed with keys under the End-user's control and present self-attested claims directly to the RPs.

Self-issued OPs can also present cryptographically verifiable claims issued by the third parties trusted by the RPs, allowing End-Users to interact with RPs, without RPs interacting directly with claims issuers. Self-Issued OpenID Provider v2 supports DIDs.

OIDC with SIOP is being extended to cover verifiable credentials (of different formats) and verifiable presentations, supporting decentralised and user-centric identity trust models.

4.3.5.3. Layer 3

Technical format: ID Token

An OpenID Connect ID Token is a security token that contains claims about the authentication of an end user by an Authorisation Server when using a Client, and potentially other requested claims. The ID Token is represented as a JSON Web Token (JWT). ID Tokens must be signed using JWS and optionally both signed and then encrypted using JWS and JWE, respectively, thereby providing authentication, integrity, non-repudiation and, optionally, confidentiality. Self-issued ID Tokens do not require an X.509 public key certificate.

A claim is defined as a piece of information asserted about an entity (such as an end user), which is something that has a separate and distinct existence and can be identified in a particular context.

All ID Tokens contain the following required claims: the issuer identifier for the issuer of the response, the subject identifier, the audience(s) that this ID Token is intended for, the expiration time at or after which the ID Token must not be accepted for processing and the time at which the JWT was issued. OpenID Connect Core defines a standard set of claims to be used in ID Tokens, with commonly used identity attributes of end users (natural persons).

Human-readable claim values, and claim values that reference human-readable values, may be represented in multiple languages and scripts. To specify the languages and scripts, BCP 47 (IETF RFC 5646) language tags are added to member names, delimited by a '#' character.

Governance framework

Not applicable.

4.3.5.4. Layer 4

OpenID Foundation working groups develop sector-specific activities. These activities include the Health Relationship Trust (HEART), a set of profiles that enables patients to control how, when and with whom their clinical data is shared; the Financial-grade API (FAPI); Mobile Operator Discovery, Registration and authentication profiles (MODRNA); or eKYC and Identity Assurance (eKYC & IDA), for the communication of assured identity information – that is, verified claims and information about how the verification was carried out and how the claims in question are maintained.

4.3.5.5. Analysis

OpenID Connect / OpenID Connect with SIOP	
Coverage of the identity management life cycle	Authentication Attribute sharing
Maturity of the standards	High, except for some emerging specifications such as OpenID for Verifiable Credentials and OpenID for Verifiable Presentations
Authentication capabilities	Online user authentication (delegated/self)
User sole control and dependencies	It depends on the underlying authentication agent/device and on the policies of the OpenID Connect authority / identity provider OIDC with SIOP provides a higher degree of user autonomy
Data-protection-enhancing technologies	Supports selective disclosure User tracking by the OpenID Connect authority / identity provider is possible. User tracking may be limited in the OIDC with SIOP approach
Trust model	Enterprise, federated, decentralised

4.3.6. FIDO2

FIDO comprises three sets of specifications oriented to passwordless strong user authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) and the Client to Authenticator Protocols (CTAP). Recommendation ITU-T X.1277 describes the FIDO universal authentication framework (UAF), and Recommendation ITU-T X.1278 contains the Client to authenticator protocol/Universal 2-factor framework.

FIDO UAF is composed of the following:

UAF protocol specification (message formats and processing rules for all UAF protocol messages);

- the FIDO UAF application API and transport binding specification (APIs and interoperability profile for client applications utilising FIDO UAF);
- FIDO UAF authenticator commands (a low-level functionality that FIDO UAF authenticators should implement to support the FIDO UAF protocol);
- the FIDO UAF authenticator-specific module API (authenticator-specific module API provided by an authenticator-specific module ASM to the FIDO client);
- the FIDO UAF registry of predefined values, which defines all the strings and constants reserved by UAF protocols;

- FIDO UAF APDU, which provides a mapping of FIDO UAF authenticator commands to application protocol data units (APDUs)).

WebAuthn specification defines an API enabling the creation and use of strong, attested, scoped, public-key-based credentials by web applications, for the purpose of strong authentication of users. A public key credential is created and stored by a WebAuthn authenticator at the command of a WebAuthn Relying Party, subject to user consent. Subsequently, the public key credential can only be accessed by origins belonging to that Relying Party. This scoping is enforced jointly by conforming User Agents and authenticators. In addition, privacy across Relying Parties is maintained: Relying Parties are not able to detect any properties, or even the existence, of credentials scoped to other Relying Parties.

The CTAP is intended to be used in scenarios in which a user interacts with a relying party (a website or native app) on a platform (e.g. a personal computer) that prompts the user to interact with an external authenticator (e.g. a smartphone). In order to provide evidence of user interaction, an external authenticator implementing this protocol is expected to have a mechanism to obtain a user gesture. Possible examples of user gestures include a consent button, a password, a personal identification number (PIN), biometrics or a combination of these. Prior to executing this protocol, the client/platform and external authenticator must establish a confidential and mutually authenticated data transport channel.

The CTAP and the W3C's Web Authentication (WebAuthn) specification are known as FIDO2, which supports passwordless, second-factor and multifactor user experiences with embedded (or bound) authenticators (such as biometrics or PINs) or external (or roaming) authenticators (such as FIDO Security Keys, mobile devices and wearables).

FIDO protocols complement federated identity management (FIM) frameworks, such as OpenID and SAML, and web authorisation protocols, such as OAuth. FIM relying parties can leverage an initial authentication event at an identity provider (IdP). However, OpenID and SAML do not define specific mechanisms for direct user authentication at the IdP. When an IdP is integrated with a FIDO-enabled authentication service, it can subsequently leverage the attributes of the strong authentication with its relying parties.

4.3.6.1. Layer 1

FIDO Servers must have access to a trust anchor for verifying attestation public keys (i.e. an Attestation Certificate trust store) because the Relying Party must be able to verify the FIDO Authenticator model/type (in order to calculate the associated risk). To this end, an authenticator must provide its attestation signature during the registration process for the same reason.

Metadata statements contain the trust anchor required to verify the attestation object (i.e. the KeyRegistrationData object, referred to in X.509 PKI certificates). They also describe several other important characteristics of the authenticator, including supported authentication and registration assertion schemes, and key protection flags.

The attestation trust anchor is shared with FIDO Servers out of band, as part of the FIDO Metadata Service. The authentication vendor provides metadata as part of the FIDO Certification process. The FIDO Server downloads the metadata file from a well-known FIDO URL, caches it locally and verifies the integrity and authenticity of this metadata file using the digital signature. It then iterates through the individual entries and parses the metadata statements related to authenticator models relevant to the relying party.

Optionally, a FIDO Server may cross-reference the attested authenticator model with other metadata databases published by third parties, allowing some degree of decentralisation of the trust model. Such third-party metadata might, for example, inform the FIDO Server if an authenticator has achieved certifications relevant to certain markets or industry verticals, or whether it meets application-specific regulatory requirements.

4.3.6.2. Layer 2

Agents and devices

An authenticator is a cryptographic entity, existing in hardware or software, that can register a user with a given Relying Party and later assert possession of the registered public key credential, and optionally verify the user, when requested by the Relying Party. Authenticators can report information regarding their type and security characteristics through attestation during registration.

Attestation is how authenticators make claims to a relying party that the keys they generate and/or certain measurements they report originate from genuine devices with certified characteristics. To ensure the public key credential has been created in a specific device, that device uses its own private key to produce an attestation. To support unlinkability, the same private attestation key is used by several authenticators. Thus, a form of device binding is provided, with no user traceability.

Compliant authenticators protect public key credentials and interact with user agents to implement the Web Authentication API and, eventually, the FIDO CTAP2 protocol. Implementing compliant authenticators is possible in software executing (1) on a general-purpose computing device, (2) on an on-device Secure Execution Environment, Trusted Platform Module (TPM), or a Secure Element (SE), or (c) off device. Authenticators being implemented on device are called platform authenticators'. Authenticators being implemented off device (roaming authenticators) can be accessed over transport such as a Universal Serial Bus (USB), Bluetooth Low Energy (BLE), or Near Field Communications (NFC).

Authentication capabilities

Relying Parties employ the Web Authentication API during two distinct, but related, ceremonies involving a user. The first is Registration, when a public key credential is created on an authenticator and scoped to a Relying Party with the present user's account (the account will either already exist or be created at this time). The second is Authentication, when the Relying Party is presented with an Authentication Assertion proving the presence and consent of the user who registered the public key credential.

4.3.6.3. Layer 3

Technical formats: Public credential source, authentication assertion

FIDO is not oriented to define technical formats for representing or sharing identity information; rather, it supports passwordless, strong authentication processes based in public key cryptographic mechanisms.

At the time of registration, the authenticator creates an asymmetric key pair, and stores its private key portion and information from the Relying Party in a public key credential source. The public key portion is returned to the Relying Party, which then stores it in conjunction with the present user's account. Subsequently, only that Relying Party can employ the public key credential in authentication ceremonies. The Relying Party uses its stored copy of the credential public key to verify the resultant authentication assertion.

An authentication ceremony is defined as the ceremony in which a user and the user's client (containing at least one authenticator) work in concert to cryptographically prove to a Relying Party that the user controls the credential private key of a previously registered public key credential. This includes a test of user presence or a user verification process.

- A test of user presence is a simple form of authorisation gesture and a technical process in which a user interacts with an authenticator by (typically) simply touching it (other modalities may also exist), yielding a Boolean result. An authorisation gesture is a physical interaction between a user and an authenticator as part of a ceremony, such as registration or authentication. By making such an authorisation gesture, a user provides consent for (i.e. authorises) a ceremony to proceed. A test of user presence does not constitute user verification because a user presence test, by definition, is not capable of biometric recognition, nor does it involve the presentation of a shared secret such as a password or PIN.
- User verification is the technical process by which an authenticator locally authorises the invocation of the creation of credentials and the production of authentication assertions. User verification may be instigated through various authorisation gesture modalities, for example touch plus pin code, password entry or biometric recognition (e.g. presenting a fingerprint). While the intent is to distinguish individual users, user verification does not provide the Relying Party with concrete identification of the user. However, when two or more ceremonies with user verification have been carried out with that credential, user verification expresses that it was the same user that performed all of them. The same user might not always be the same natural person, however, if multiple natural persons share access to the same authenticator.

A public key credential source contains the credential type, the ID, the private key and the Relying Party identifier (RP ID) the public key credential source is scoped to, among other data. The authentication assertion is a cryptographically signed AuthenticatorAssertionResponse object, which contains a SHA-256 hash of the RP ID the credential is scoped to; flags signalling the results of the user presence and user verification tests, among other things; a signature counter; and, optionally, attested credential data and extension-defined authenticator data. For example, CTAP2 has defined five extensions supporting different features.

Governance frameworks

Not applicable.

4.3.6.4. Layer 4

Not applicable.

4.3.6.5. Analysis

FIDO2	
Coverage of the identity management life cycle	Authentication
Maturity of the standards	High
Authentication capabilities	Online/offline user authentication
User sole control and dependencies	Depends on the authenticator type
Data-protection-enhancing technologies	Implements unlinkability techniques at authenticator level

Trust model	Centralised or, optionally, decentralised, but limited to the authenticator

4.3.7. Self-Sovereign Identity

Self-Sovereign Identity is an emerging concept associated with how identity is managed in the digital world. According to the Self-Sovereign Identity approach, users should be able to create and control their own identities without relying on any centralised authority. The concept of SSI accounts for a narrow concept of 'identity' as a specific identifier that enables self-management, in the sense of being able to authenticate the person, self-assert claims, and receive, control and share third-party-asserted claims, without any essential dependence on a third party (i.e. a public or private identity provider). The ideological approach does not preclude the possibility that other parties may issue identity assertions not central to the identity itself.

SSI approaches relay on Decentralised Identifiers and Verifiable Credentials/Presentations, which use different syntaxes and cryptographic proofs, and verifiable data registries.

DIDs are a new type of identifier that enables verifiable, decentralised digital identity. They may refer to any subject (person, organisation, thing, data model, abstract entity, etc.) as determined by its controller. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers and certificate authorities, thus supporting decentralised identity management and user autonomy. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are Uniform Resource Identifiers (s) that associate a DID subject with a DID document, enabling trustable interactions associated with that subject.

Each DID document can express cryptographic material, verification methods or services, which provide a set of mechanisms enabling a DID controller to prove it has control of the DID. Services enable trusted interactions associated with the DID subject. A DID might provide the means to return the DID subject itself, if the DID subject is an information resource such as a data model.

A DID is formally defined as a globally unique persistent identifier that does not require a centralised registration authority and is often generated and/or registered cryptographically. Identity management based on the use of decentralised identifiers is known as 'decentralised identity management', and extends authority for identifier generation, registration and assignment beyond traditional roots of trust.

4.3.7.1. Layer 1

Because of the desirable properties of an SSI approach, DIDs and Verifiable Credentials/Presentations are usually designed to use verifiable data registries to store information supporting identity processes instead of centralised storage. A verifiable data registry is defined as a system that facilitates the creation, verification, updating and/or deactivation of decentralised identifiers and DID documents or other cryptographically verifiable data structures such as verifiable credentials. It can be, for example, a Distributed Ledger or a Blockchain or a distributed database.

In the European self-sovereign identity framework (ESSIF) approach, this layer, which is based in the European Blockchain Services Infrastructure (EBSI), supports a series of trusted registries in support of decentralised identity management, including a DID registry for issuers, a trusted issuer's registry and a trusted data schema registry. A DID registry can be seen as a self-controlled cryptographic trust anchor, and a trusted issuer's registry is a data trust anchor, similar to a trust list, but with a higher level of redundancy and immutability.

Depending on the type of cryptographic proof used for verifiable credentials, this layer contains additional cryptographic data, as in the Hyperledger Indy approach, which is based in Camenisch–Lysyanskaya signatures for ZKP anonymous credentials.

4.3.7.2. Layer 2

Agents and devices

The SSI approach is typically based in a user agent or identity wallet – that is, a program, such as a browser, mobile app or other web client, that mediates the communication between holders, issuers and verifiers. It can work jointly with hardware devices such as secure elements in mobile phones.

Authentication capabilities

There are different protocols supporting authentication, normally based on the cryptographic mechanisms associated with the corresponding DIDs. These include OpenID Connect with SIOP and other novel protocols such as DIDCOMM, a secure, private communication methodology built on top of the decentralised design of DIDs.

4.3.7.3. Layer 3

Technical formats: Verifiable Credentials/Presentations

Because a DID is just an identifier, it does not provide information about the subject itself. In practice, DIDs are used in combination with Verifiable Credentials (VC) to support digital interactions in which information about the subject must be shared with third parties, by proving to those third parties that the DID subject has ownership of certain attestations or attributes. This proof is based on the cryptographic link between the VC, the DID subject the VC are about and the issuer of the VC, which can be the DID subject (self-asserted claims) or a trusted entity. Trust in the issuer is established either by trusting the issuer's DID (e.g. out-of-band, bilateral relationship, trusted lists) or by any other means. The third party can then use the presented cryptographically protected proof to verify the ownership and trustworthiness of the claims about the subject.

A credential is a set of one or more claims made by the same entity. Credentials might also include an identifier and metadata to describe properties of the credential, such as the issuer, the expiry date and time, a representative image, a public key for verification purposes and the revocation mechanism. A verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it.

A verifiable presentation expresses data from one or more verifiable credentials and is packaged in such a way that the authorship of the data is verifiable. If verifiable credentials are presented directly, they become verifiable presentations. Data formats derived from verifiable credentials that are cryptographically verifiable, but do not of themselves contain verifiable credentials, might also be verifiable presentations. The data in a presentation is often about the same subject but might have been issued by multiple issuers. The aggregation of this information typically expresses an aspect of a person, organisation or entity.

Verifiable Credentials/Presentations can be expressed using different syntaxes and proofs, including JSON, JSON-LD), XML, CBOR or others. While the data model is the canonical representation of a credential or presentation, the proofing mechanisms for these are often tied to the syntax used in the transmission of the document between parties. Proof syntaxes include JWT, Linked Data Proofs, ZKP CL, or JSON-LD with BBS+, which support selective disclosure. Some of these cryptographic mechanisms are relatively new and cannot be subject to formal certification.

Governance frameworks

An SSI approach should be aligned with a set of principles that affect the governance framework. Trust over IP currently considers the following principles: (1) representation, (2) interoperability, (3) decentralisation, (4) control and agency, (5) participation, (6) equity and inclusion, (7) usability, accessibility and consistency, (8) portability, (9) security, (10) verifiability and authenticity, (11) privacy and minimal disclosure and (12) transparency. Many of these are present in other approaches, including those based in identity federations.

4.3.7.4. Layer 4

The EBSI Diploma use case builds upon ESSIF to establish a sector-specific SSI approach for educational and professional verifiable credentials.

4.3.7.5. Analysis

Self-Sovereing Identity	
Coverage of the identity management life cycle	Authentication
Maturity of the standards	Medium
Authentication capabilities	Online user authentication (self)
User sole control and dependencies	It is designed to be under the sole control of the user
Data-protection-enhancing technologies	It supports selective disclosure, by design of the VC or because of the proof User tracking is limited
Trust model	Decentralised

4.4. SPECIFIC GROUPS OF STANDARDS NOT PROVIDING AUTHENTICATION CAPABILITIES

4.4.1. Advanced electronic signature/seals (AdES)

Advanced electronic signatures/seals can be seen as specific means supporting the digital identity of a natural person signing a document or a legal person sealing a document, because they are a form of data origin authentication. Moreover, according to Article 26(b) of the eIDAS Regulation, an advanced electronic signature is capable of identifying the signatory (a natural person), while, under Article 36(b) of the same regulation, an advanced electronic seal is capable of identifying the creator of the seal (a legal person).

This identification requirement is typically fulfilled using X.509 v3 public key certificates representing the identity of the signatory or of the creator of the seal, as described in Section 4.4.1.3, and providing entity authentication, although this is connected to the legal effect of an electronic signature (data in an electronic form attached to or logically associated with other data in an electronic form and used by the signatory to sign) or seal (data in an electronic form that is attached to or logically associated with other data in an electronic form to ensure the latter's origin and integrity).

Advanced electronic signatures or seals based in qualified certificates inherit the level of assurance of the corresponding certificate, which is moderate because of the possibility of using any type of agent or device for managing keys.

Qualified electronic signatures or seals offer a higher level of assurance, because they are created using devices fulfilling security requirements, especially from the perspective of key management and usage.

4.4.1.1. Layer 1

Because advanced signatures or seals are based in X.509 public key certificates, the description contained in Section 4.3.3.1 is applicable.

Trusted lists conformant to ETSI TS 119 612 could be used by supervisory bodies to publish the trust anchors for the new proposed trust service consisting in the management of remote electronic signature and seal creation devices (see Section 4.2.2.1). This would require updating the corresponding implementing act.

4.4.1.2. Layer 2

Agents and devices

Advanced electronic signatures or seals are created using different types of software agents and devices.

- CEN EN 419211 is a six-part European standard dedicated to secure signature/seal creation devices (they are called 'qualified [electronic] signature creation devices' and 'qualified electronic seal creation devices' in the eIDAS regulation), in support of qualified electronic signatures or seals. The standard specifies terms used in specifying protection profiles, according to Common Criteria, for secure signature creation devices. It also specifies functional and operational requirements for secure signature creation devices and describes the targets of evaluation for the protection profiles.
- Protection profiles cover devices with key generation (CEN EN 419211-2), devices with key import (CEN EN 419211-3), devices with key generation and trusted channel to certificate generation application (CEN EN 419211-4), devices with key generation and trusted channel to signature creation application (CEN EN 419211-5) and devices with key import and trusted channel to signature creation application (CEN EN 419211-6).
- CEN/TS 419221-6 is a Technical Specification that establishes the conditions for use of CEN EN 419221-5 as a qualified electronic signature/seal creation device, where the signatory or seal creator has direct local control of the cryptographic module.
- Parts 1 and 2 of CEN EN 419 241 are dedicated to trustworthy systems supporting remote signature/seal creation in accordance with security requirements and recommendations, and with a Common Criteria protection profile, under the responsibility of a qualified trust service provider. CEN EN 419 241 presupposes the use of a cryptographic module conforming to EN 419 221-5.
- The Cloud Signature Consortium defines an API specification for Remote Electronic Signatures and Remote Electronic Seals (CSC API), focused on the interface between a signature application and a remote signature service provider, using JSON/Rest.
- OASIS Open defines different technical specifications related to digital signature services, including the Digital Signature Service Core Protocols, Elements and Bindings; the Advanced Electronic Signature Profiles of the OASIS Digital Signature Services; and the Asynchronous

Processing Abstract Profile of the OASIS Digital Signature Services. These support the implementation of local or remote signature creation services.

- ETSI TS 119 432 defines a protocol to request the creation of remote signatures, including the general functionalities of such a protocol, and a JSON/Rest implementation based on the Cloud Signature Consortium CSC API and an XML version based on the OASIS DSS protocol.

Authentication capabilities

Advanced electronic signatures or seals provide data origin authentication in respect of the signed or sealed data, and of its unique association with a signatory or a creator of a seal.

These means supporting digital identity do not implement end entity authentication – that is, they cannot be used in authentication protocols to prove the identity of a natural or legal person.

4.4.1.3. Layer 3

Technical formats: CadES, XadES, PadES, AsIC, JadES

ETSI has produced several standards describing formats of advanced electronic signatures or seals using digital signature schemes based in X.509 certificates. In all cases, the formats are built upon previous formats, through the incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long-term validity of digital signatures) in a number of use cases, being functionally equivalent.

- Parts 1 and 2 of ETSI EN 319 122 define the CadES digital signature format, built upon CMS signatures. CMS signatures are defined in IETF RFC 5652 – Cryptographic Message Syntax, updated by IETF RFC 8933, using ASN.1 syntax (currently according to IETF RFC 5911, updated by IETF RFC 6268). IETF RFC 2634 and RFC 5035 define a specific attribute to cryptographically bind a public key X.509 version 3 certificate with a CMS signature.
  IETF RFC 5940 describes how to add revocation information into CMS signatures. IETF 6211 defines a specific attribute to prevent algorithm substitution attacks. ETSI TS 119 122-3 extends CadES through the incorporation of Evidence Record Syntax (ERS) mechanisms, according to IETF RFC 4998.
  - Part 1 of ETSI EN 319 122 specifies four baseline profiles, which are intended to facilitate interoperability and to encompass the life cycle of an electronic signature, namely B-B, B-T, B-LT and B-LTA. ETSI EN 319 122-1 should be the successor of ETSI TS 103 173.
- ISO 14533-1 specifies the elements, among those defined in CadES digital signatures, that enable verification of a digital signature over a long period.
  - Parts 1 and 2 of ETSI EN 319 132 define the XadES digital signature format, which is built upon XML Signatures. XML Signatures are defined in the W3C recommendation of 11 April 2013, ‘XML Signature Syntax and Processing Version 1.1’.
    ETSI TS 119 132-3 extends XadES through the incorporation of Evidence Record Syntax (ERS) mechanisms, in accordance with IETF RFC 4998 and RFC 6283, which implement ERS in XML format.
  - Part 1 of ETSI EN 319 132 specifies four baseline profiles, which are intended to facilitate interoperability and to encompass the life cycle of an electronic signature, namely B-B, B-T, B-LT and B-LTA. ETSI EN 319 132-1 should be the successor of ETSI TS 103 171.
- ISO 14533-2 specifies the elements, among those defined in XadES digital signatures, that enable verification of a digital signature over a long period.
  - Parts 1 and 2 of ETSI EN 319 142 define the PadES digital signature format, building upon PDF signatures specified in ISO 32000-1 with an alternative signature encoding to support digital signature formats equivalent to the signature format CadES as specified in ETSI EN 319 122-1. ETSI TS 119 142-3 extends XadES through the

incorporation of Evidence Record Syntax (ERS) mechanisms, in accordance with IETF RFC 4998 and RFC 6283, which implements ERS in XML format.

- Part 1 of ETSI EN 319 142 specifies four baseline profiles, which are intended to facilitate interoperability and to encompass the life cycle of the electronic signature, namely B-B, B-T, B-LT and B-LTA. ETSI EN 319 142-1 should be the successor of ETSI TS 103 172.

- ISO 14533-3 specifies the elements, among those defined in PDF Advanced Electronic Signatures (PadES), that enable verification of a digital signature over a long period.
  - Parts 1 and 2 of ETSI EN 319 162 define a standardised use of container types to establish a common way of associating files containing data objects with files containing digital signatures and/or time assertions, with the aim of facilitating data interchange and interoperability among various signing and validation services.
  - Part 1 of ETSI EN 319 162 specifies four baseline profiles, which are intended to facilitate interoperability and to encompass the life cycle of an electronic signature, namely B-B, B-T, B-LT and B-LTA. ETSI EN 319 142-1 should be the successor of ETSI TS 103 174.
  - ETSI TS 119 182-1 defines a JSON format for AdeS signatures (JadES signatures) built on JSON Web Signatures (JWS) as specified in IETF RFC 7515. It specifies four baseline profiles, which are intended to facilitate interoperability and to encompass the life cycle of an electronic signature, namely B-B, B-T, B-LT and B-LTA.

The four baseline levels are as follows.

- B-B provides requirements for the incorporation of signed and some unsigned attributes when the signature is actually generated. The X.509 version 3 public key certificate of the signatory or the creator of the seal must be mandatorily included using a secure reference in the advanced signature or seal. From this perspective, these formats are not technically neutral (i.e. it would not be possible to represent the identity of the signatory or the creator of the seal using a different syntax; only X.509 v3 certificates are supported).
- B-T provides requirements for the generation and inclusion, for an existing signature, of a trusted token proving that the signature itself actually existed at a certain date and time.
- B-LT provides requirements for the incorporation of all the material required for validating the signature in the signature document. This level aims to address the long-term availability of the validation material.
- B-LTA provides requirements for the incorporation of timestamp tokens that enable validation of the signature a long time after its generation. This level aims to address the long-term availability and integrity of the validation material.

Because they enable the incorporation of additional information required for the validation over time of advanced electronic signatures or seals, the three additional baseline profiles (B-T, B-LT and B-LTA) contribute to the validity of such signatures and seals and their effectiveness when used as means supporting digital identity.

In addition, these formats support the inclusion of attributes claimed by the signer or creator of the seal, of attributes certified in X.509 attribute certificates issued by an attribute authority (see Section 4.3.3.3) and/or of assertions signed by a third party. For claimed or signed assertions, any format can be used, and the use of claimed and signed SAML assertions is explicitly defined (see Section 4.3.4.3).

It may be helpful to include specific rules for other formats for assertions, including those based in Verifiable Credentials, as already noted in ETSI TS 119 182-1.

Governance frameworks

ETSI has defined a governance framework for the creation of advanced electronic signatures/seals.

- ETSI EN 319 102-1 specifies procedures for the creation of AdES digital signatures (specified in CadES, XadES and PadES), and for establishing whether an AdES digital signature is technically valid whenever the AdES digital signature is based on public key cryptography and supported by X.509 public key certificates.
- ETSI TS 119 101 specifies general security and policy requirements for applications for signature creation, validation and augmentation.
- Parts 1–4 of ETSI TS 119 172 set out rules for signature policies. The purpose of a signature policy is to describe the requirements imposed on or committing the involved actors (signers, verifiers, relying parties and/or potentially one or more trust service providers) in respect of the application of signatures to documents and data that will be signed in a particular context, transaction, process, business or application domain, in order for these signatures to be considered valid or conformant signatures under this signature policy.
    - Part 1 describes the main building blocks and sets out the table of contents for human-readable signature policy documents (i.e. how a signature is created and what specific elements are used in its validation). Parts 2 and 3 provide XML and ASN.1 formats to represent signature policies. Finally, Part 4 specifies a set of rules that aims to define the technical requirements for determining whether a digital signature is fit for meeting the requirements of EU qualified electronic signatures/seals, taking into account EU Member States' trusted lists (see Section 4.4.1.1).
- ETSI TS 119 431-1 specifies policy and security requirements for service components operating a digital signature creation device, including a QSCD (Qualified Signature/Seal Creation Device) to create a digital signature value on behalf of a remote user. These requirements are based on the general policy requirements specified in ETSI EN 319 401, take into account related requirements for certificate issuance in ETSI EN 319 411-1 and are aligned with the requirements specified in EN 419 241-1.
- ETSI TS 119 431-2 specifies policy and security requirements for TSP service components creating AdES digital signatures, based on the general policy requirements specified in ETSI EN 319 401 and taking into account related requirements from ETSI TS 119 101. The TSP service component relies either on remote server signing or on a signature creation device in the user's environment to create the digital signature.
- Trust service providers offering remote signature/seal creation may use ETSI TS 119 461, which defines policy and security requirements for trust service components providing identity proofing of trust service subjects.

4.4.1.4. Layer 4

Not applicable.

4.4.1.5. Analysis

Advanced electronic signature/seals (AdES)	
Coverage of the identity management life cycle	Authentication
Maturity of the standards	High
Authentication capabilities	Data origin authentication, with binding to an X.509 public key certificate

	It does not provide any user authentication per se but needs to ensure the identity of the user
User sole control and dependencies	The user has sole control over the signature/seal creation data
Data-protection-enhancing technologies	None
Trust model	Decentralised, based in the eIDAS regulation trusted list

4.4.2. ERDS evidence

An Electronic Registered Delivery Service (ERDS) is a trust service defined in Article 3(36) of the eIDAS regulation as a service that makes it possible to transmit data between third parties by electronic means, that provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations. Registered Electronic Mail (REM) is a specific type of ERDS.

Qualified ERDSs must fulfil a series of requirements, including (1) ensuring, with a high level of confidence, the identification of the sender and (2) ensuring the identification of the addressee before the delivery of the data. These include collecting and storing identity information as part of the ERDS and QERDS evidence set.

Thus, the ERDS and QERDS evidence set can be considered specific means supporting the digital identity of the sender and of the recipient of transmitted data. A (Q)ERDS provider may act as a relying party in respect of the identification of a party carried out by another (Q)ERDS provider.

4.4.2.1. Layer 1

Trusted lists conformant to ETSI TS 119 612 are used by supervisory bodies to publish the trust anchors for (qualified) electronic registered delivery services (see Section 4.2.2.1).

4.4.2.2. Layer 2

Depending on the service, any internet browser may be used (ERDS general model), or an email agent implementing S/MIME may be required.

4.4.2.3. Layer 3

Technical formats: ERDS evidence set

ETSI EN 319 522-1 describes in detail the ERDS events that may happen within an electronic delivery process and that may be relevant from a probative perspective. In this sense, ERDS evidence is data generated by the electronic registered delivery service that aims to prove that a certain event has occurred at a certain time, including identification and authentication events.

On the occurrence of an ERDS event, an ERDS may produce ERDS evidence, which will contain a reference to the event as detailed in ETSI EN 319 522-2. ERDS evidence is different from a non-repudiation token, as defined in ISO/IEC 13888 (i.e. a special type of security token, consisting of evidence and, optionally, of additional data).

According to ETSI TS 319 522-2, an ERDS needs to generate, exchange and validate attributes to support the identification and authentication of end entities such as senders, recipients or delegates. To this end, identifiers and identity attributes are defined. All attributes related to identification and authentication are derived from the EU Vocabulary:

- For natural persons, the attributes defined by the Core Person Vocabulary version 2.0 (https://joinup.ec.europa.eu/solution/core-person-vocabulary) are to be used.
- For legal persons, the attributes defined by the Registered Organization Vocabulary version 2.0 (https://joinup.ec.europa.eu/solution/registered-organization-vocabulary) are to be used. The Registered Organization Vocabulary defines the core vocabulary for legal persons registered through a formal process, typically in a national or regional register.

Supported attributes are limited to those defined in the eIDAS attribute profile specification, based in SAML, which are also derived from the ISA vocabulary. Information related to the level of assurance may also be included.

ETSI EN 319 522-3 defines, among other formats used in (qualified) ERDS, evidence and identification formats using XML conformant to a XSD vocabulary defined in the standard. Sending or receiving party evidence of identity is described using the UserDetailsType, which may contain an identity element, an identifier element and an assurance level details element.

The Identity element enables inclusion of SAML:Attribute elements. X.509 public key certificates can also be used, but there is no support for other types of identity assertions, for example those using JSON or Verifiable Credentials.

The ERDS evidence set and components defined in ETSI EN 319 522-2 also apply to REM services.

Governance frameworks

ETSI EN 319 521 defines a general governance framework regarding policy and security requirements for (qualified) registered electronic delivery services, which builds upon ETSI EN 319 401. More specifically, ETSI EN 319 521 contains specific requirements for users' identification and authentication in (Q)ERDS, which may be fulfilled, for natural persons, by applying ETSI TS 119 461.

This standard lists the following mechanisms for the identification of the sending and receiving parties by the service provider or a third party, under the responsibility of the service provider, aligned with the eIDAS regulation requirements for issuing qualified certificates.

- By the physical presence of the natural person or of an authorised representative of the legal person.
- Remotely, using electronic identification means, for which the physical presence of the natural person or of an authorised representative of the legal person is ensured, meeting the requirements set out in Article 8 of the eIDAS regulation with regard to the assurance level 'substantial' or 'high'.
- By means of a certificate issued to the natural person or to an authorised representative of the legal person under NCP policy as defined in ETSI EN 319 411-1, verifying a digital signature.
- Using other identification methods recognised at national level that provide assurance in terms of reliability equivalent to that of physical presence. The equivalence of the assurance level shall be confirmed by a conformity assessment body.

ETSI EN 319 521 considers that a (Q)ERDSP can issue a means of authentication for the sender, the recipient or both to be used in the authentication process. In this case, one of the following mechanisms should be used:

- multifactor authentication mechanisms, at a level of assurance compatible with Substantial 150216/2015, or LoA3 ISO 29115, or AAL2 NIST SP 800-63B or an equivalent level in a different assurance framework;
- mutual TLS authentication, which includes the certificate issued to the sender or recipient under NCP policy as defined in ETSI EN 319 411-1;
- a digital signature supported by a certificate issued under NCP policy as defined in ETSI EN 319 411-1;
- an authentication means with a security level equivalent to the above.

ETSI EN 319 531 defines a specific governance framework regarding policy and security requirements for (qualified) Registered Electronic Mail Service Providers, i.e., (Q)ERDS providers offering their services using secure email). Identification and authentication requirements defined in ETSI EN 319 521 do apply to (Q)REM service providers.

4.4.2.4. Layer 4

Not applicable.

4.4.2.5. Analysis

ERDS evidence	
Coverage of the identity management life cycle	Authentication
Maturity of the standards	High
Authentication capabilities	Data origin authentication, with binding to an SAML attribute set or an X.509 public key certificate It does not provide any user authentication per se but needs to ensure the identity of the user
User sole control and dependencies	It depends on the identification and authentication mechanisms
Data-protection-enhancing technologies	None
Trust model	Decentralised, based in the eIDAS regulation trusted list

4.5. SUMMARY

This chapter has described the main general and specific groups of standards related to means supporting digital identity, which either provide or do not provide authentication capabilities.

- [16] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32015R1502).

The following matrix provides a summary of the different digital identity approaches providing authentication capabilities, using a set of criteria especially meaningful in the context of the proposed eIDAS 2.0 regulation.

	eMRTD (ISO 7501 – ICAO 9303)	**eIDAS Token (TR-03110-2)**	**mDL (ISO/IEC 18013-5)**	**mID (ISO/IEC 23220)**	**X509 PKI certificates (ISO/IEC 9594-8)**	**SAML eIDAS (ITU-T**	**OpenID Connect**	**OpenID Connect with SIOP**	**FIDO2 (ITU-T X.1277 and X.1278)**	**SSI**
Formal standard	Yes, international	Yes, EU level	Yes, international	In progress	Yes	Yes	No	No	Yes	No
Personal Identification Data (PID) format	LDS1 eMTRD	LDS2 eMRTD/Specific ASN.1 definition	mdoc mDL CBOR/mdoc mDL signed JWT	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LD, Anoncreds …
(Qualified) Electronic Attestation of Attributes format	N/A	LDS2 eMRTD/Specific ASN.1 definition	N/A	mdoc CBOR, mdoc signed JWT (planned support for VC)	X.509 and X520 ASN.1 definitions	SAML assertion in XML format, according to an XSD definition	ID Token signed JWT	ID Token signed JWT (planned support for VC)	N/A	VC according to JWT, JSON-LD, Anoncreds …
Subject's offline authentication	Yes	Yes	Yes	Yes	No	No	No	No	Yes	No
Subject's online authentication (LoA)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Relying party's offline authentication	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Relying party's online authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Device binding (e.g. smart phone)	No	Optional	No	Optional	Optional	N/A	N/A	N/A	Yes	Optional
Use of secure element (level of confidence)	No	Yes	No	No	Optional	N/A	N/A	N/A	Optional	Optional

User sole control	No	Yes	No	Yes	Optional	No	No	No	Yes	Yes
Initially designed for law enforcement	Yes	No	Yes	No	No	No	No	No	No	No
Need of centralised identity provider	No	Yes, for additional attributes	Yes, but only for server retrieval	Yes, but only for server retrieval	No	Yes	Yes	Yes	N/A	No
Selective disclosure	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Non traceability/unlinkability	No	Yes	No	No	No	No	No	No	Yes	Yes
Support for the identity management lifecycle	Issuance/Authentication/Revocation	Issuance/Authentication/Attribute sharing/Revocation	Issuance/Authentication/Attribute sharing/Revocation	Issuance/Authentication/Attribute sharing/Revocation	Issuance/Suspension/Revocation/Renewal	Authentication/Attribute sharing	Authentication/Attribute sharing	Authentication/Attribute sharing	Authentication	Issuance/Authentication/Suspension/Revocation/Renewal
Trust model	Federated	Federated	Federated	Federated	Enterprise/Federated	Enterprise/Federated	Enterprise/Federated	Federated/Decentralised	Centralised , and optionally decentralised, but limited to authenticators	Decentralised
Maturity of the standards	High	High	Medium	Low	High	High	High	Medium/Low	High	Medium/Low

5. RECOMMENDATIONS

Based on the analysis provided in Chapter 4, we propose the following recommendations on Digital Identity standardisation requirements in support of cybersecurity policy standards for various groups of stakeholders.

5.1. EUROPEAN UNION POLICYMAKERS

Recommendation 1

EU policymakers should provide a clear legal definition of the term Digital Identity. The revised eIDAS regulation may be the right vehicle through which to define it. This definition should be inspired by the current ISO/IEC 24760-1:2019 standard, which provides a definition of Identity (not Digital Identity)

Recommendation 2

In the context of the EU Digital Identity Wallet, EU policymakers should make use of the new Digital Markets Act to provide direct access from the Mobile Application to the security anchor provided by EU CC certified secure elements available on smartphones. This direct assessment will help create a Trusted Mobile EU Digital Identity. This recommendation should be complemented by a new standardisation request to the European Standardisation Organisations, to develop a unique API from the mobile application to the security anchor provided by the secure element certified by the EU cybersecurity certification scheme. This is crucial for the provision of full interoperability by various smartphone manufacturers.

Recommendation 3

EU policy should consider the need of the EU Mobile Application security and privacy evaluation methodology as a strategic issue and not only as a technical issue. CEN/CENELEC JTC13 should be empowered to define it in fast-track mode.

Recommendation 4

EU policymakers should create a new mandate requiring European standardisation organisations to standardise the EUDI Wallet interfaces with QTSP, Relying Parties, Device, existing national eID documents (eID, E-pass, e-resident permit card, eDL) and existing eIDAS Nodes infrastructures. This mandate should cover methods for recognition and authentication by relying parties through the EUDI Wallet.

Recommendation 5

EU policymakers should create a new mandate requiring European standardisation organisations to standardise a privacy evaluation methodology for general Digital Identity and more precisely for the EU Digital Identity Wallet.

5.2. EUROPEAN STANDARDISATION ORGANISATIONS

Recommendation 6

Strong coordination and a clear division of responsibility between the European standardisation organisations should be defined, in terms of the standardisation activities, to avoid duplication of activities. The European standardisation organisations should also make use of the work on the toolbox process that was used to produce the *European Digital Identity Architecture and Reference Framework Outline* (ARF outline).

Recommendation 7

No existing European standard for Mobile Application assessment methodology is available at European level, making it difficult to reference applicable standards in EU legislation.

Efforts should be made to address this gap.

Recommendation 8

European standardisation organisations should adopt ISO/IEC 18013-5 and the ISO/IEC DIS 23220 series as European norms.

Benefits of such regional adoption in the case of European norms include:

- harmonisation within Europe makes it easier to comply with European rules and regulations (avoiding standstills in national work in this area);
- documents can be targeted to European needs;
- consensus building within Europe is easier than in the global context.

The potential adoption of ISO/IEC 18013-5 and/or the ISO/IEC DIS 23220 series as European standards will help to harmonise European approaches towards Digital Identity.

Recommendation 9

European standardisation organisations should define a harmonised mutual authentication protocol between the EUDI Wallet and the Relying Parties. This should be in line with the QWAC approach.

Recommendation 10

European standardisation organisations should prepare a generic code-of-conduct methodology to be applied to the (Q)TSP and the EUDI Wallet. This methodology should reference current CEN/CENELEC Joint Technical Committee 13 cybersecurity and evaluation standards and the incorporation of the ISO/IEC 27005 standard on cybersecurity risk management into national law.

5.3. EUROPEAN UNION AGENCY FOR CYBERSECURITY

Recommendation 11

ENISA should publish, on a regular basis, an overview of endorsed Digital Identity **standards** concerning different domains and sectors.

Recommendation 12

ENISA should publish an overview of existing Digital Identity Models in Europe and beyond and identify their impact in terms of cybersecurity standards.

Recommendation 13

ENISA should encourage and support the creation of an ad hoc group to address potential vulnerabilities related to digital identity systems and the EUDI Wallet.

Recommendation 14

ENISA should work closely with European standardisation organisations in fulfilling potential EU standardisation requests.

Recommendation 15

ENISA should establish a mechanism for assisting EU institutions, bodies and agencies, EU Member States and private organisations regarding various aspects of Digital Identity management.

A. ANNEX: ANALYSIS – DIGITAL IDENTITY WALLETS

A.1. INTRODUCTION TO DIGITAL IDENTITY WALLETS

Wallet terminology has been introduced into the blockchain ecosystem. Blockchain has been preliminarily used to manage cryptoassets such as bitcoin. As the technology has become more widely used, some new use cases – such as digital identity wallet solutions supporting the concept of self-sovereign identity – have emerged, which are presented in detail in ENISA's *Digital Identity: Leveraging the SSI concept to build trust* ([17]).

This annex focuses mainly on the EUDI Wallet, which is defined by the proposed revision of the eIDAS regulation (eIDAS 2.0) and in the *European Digital Identity Architecture and Reference Framework Outline*, which was released on 22 February 2022. The main objective/goal is to analyse which international and European standards can be used to fulfil the EUDI Wallet functional requirements.

The proposed eIDAS 2.0 regulation defines the EUDI Wallet as a product and service that enables the user to store identity data, credentials and attributes linked to their identity, to provide them to relying parties on request and to use them for strong authentication, and that enables qualified electronic signatures and seals. This definition may evolve, as the co-decision process was ongoing at the time of writing.

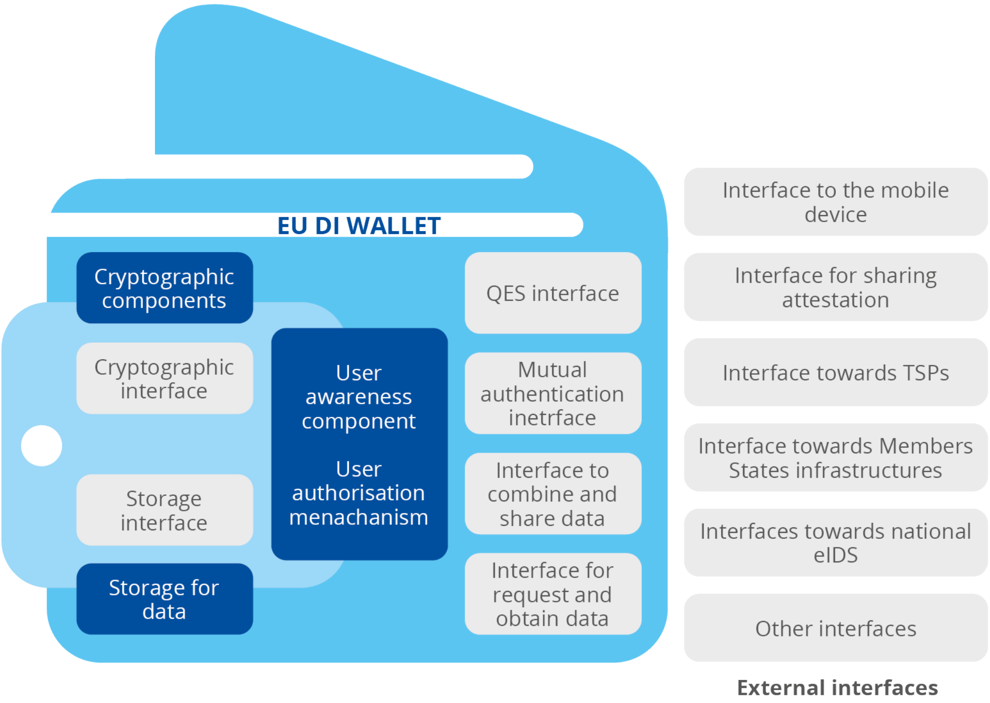
The *European Digital Identity Architecture and Reference Framework Outline* defines the following functional requirements of the EUDI Wallet:

1. performing electronic identification, storing and remotely or locally managing qualified EAAs (QEAAs) and EAAs;
2. requesting and obtaining attestations from providers, qualified electronic attestation of attributes (QEAAs and electronic attestation of attributes (EAAs);
3. providing or accessing cryptographic functions;
4. ensuring mutual authentication between the EUDI Wallet and external entities;
5. selecting, combining and sharing Personal Identification Data (PID), QEAAs and EAAs with relying parties;
6. having a user interface supporting user awareness and an explicit authorisation mechanism;
7. enabling the signing data by means of qualified electronic signatures/seals;
8. providing interfaces with external parties.

Figure 3 shows the internal and external interfaces of the EUDI Wallet specified in the *European Digital Identity Architecture and Reference Framework Outline*.

[17] https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

Figure 3: European Digital Identity Wallet interfaces


EU DI WALLET
Cryptographic components
Cryptographic interface
Storage interface
Storage for data
User awareness component
User authorisation menachanism
QES interface
Mutual authentication inetrface
Interface to combine and share data
Interface for request and obtain data
Interface to the mobile device
Interface for sharing attestation
Interface towards TSPs
Interface towards Members States infrastructures
Interfaces towards national eIDS
Other interfaces
External interfaces

Internal interfaces enable communication with the components of the EUDI Wallet. These internal interfaces are:

- cryptographic interfaces,
- storage interfaces,
- qualified electronic signature (QES) interfaces,
- mutual authentication interfaces,
- interfaces to combine and share data,
- interfaces to request and obtain data.

External interfaces enable interaction with EUDI Wallet stakeholders (users, wallet issuers, issuers of personal identification data, trust service providers and relying parties). These external interfaces are:

- interfaces for mobile devices,
- interfaces for Member States' infrastructures,
- interfaces regarding official national eIDs documents (electronic eID cards, ePassports, eResident Permit cards, eDriving licences, etc.),
- interfaces for sharing attestations,
- interfaces for (Qualified Trusted Service Providers – (Q)TSPs,
- other interfaces.

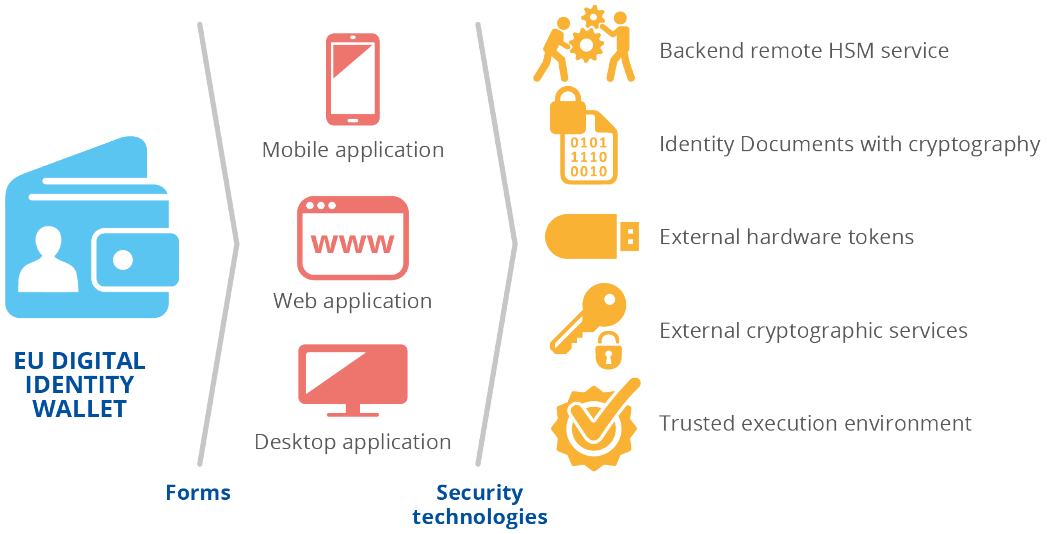
European Digital Identity Wallets might be available in one of the following forms or a combination of them:

- on mobile devices (e.g. smartphones, tablets) (mobile application),
- in the cloud, where the keys and (Q)EAA can be stored (web application)
- on personal computers, both laptops and desktops (desktop application).

Each form of the EUDI Wallet uses various security technologies, as described below.

- A back-end remote hardware security module (HSM) service may be used. This is a service operated by a wallet issuer that supports the wallet's security by storing, managing and using keys linked to the wallet.
- Member States issue electronic documents compliant with Regulation 2019/1157, which have integrated cryptographic components. Depending on their functionalities, those solutions can support the security of the wallet, for example through an electronic identification component, mutual authentication, electronic identification and digital signatures.
- External tokens such as eID cards,ePassports, smart cards, sim-cards or other cryptographic tokens may be used. They support authentication and authorisation.
- External cryptographic services (e.g. remote SSCD or QSCD) supporting the wallet in some transactions may be used. Those services are not provided by the wallet issuer.
- Hardware-backed security modules (eSE, SIM cards, universal integrated circuit cards, etc.) and software for trusted execution environments on user devices (e.g. mobile phones, laptops or desktops), which support the security of transactions and of the cryptographic keys for the wallet, may be used.

Figure 4: European Digital Identity Wallet forma and security technologies


EU DIGITAL IDENTITY WALLET
Mobile application
WWW
Web application
Desktop application
0101
1110
0010
Backend remote HSM service
Identity Documents with cryptography
External hardware tokens
External cryptographic services
Trusted execution environment
Forms
Security technologies

NB: HSM, hardware security module.

The harmonised interfaces that allow direct access to the internal and external mobile device cryptographic security that the EUDI Wallet can use to perform cryptographic security functions are an essential and instrumental function.

The internal and external cryptographic components of the mobile device need to have a standardised security profile. This solution must be certified, and the certification process usually lasts at least several months.

In a short-term approach, the cryptographic security component of the EUDI Wallet may be based on external devices that have already been certified under robust certification schemes (e.g.: Common Criteria EAL 4+ or equivalent). Components include eID cards, ePassports, smart cards, SIM cards or other cryptographic tokens.

In addition, there are remote cryptographic security components that have already been used for qualified signatures and that can operate the cryptographic security functions needed by the

EUDI Wallet. The EUDI Wallet may also make use of hybrid solutions using internal, connected and remote cryptographic components for different cryptographic functions.

The following table presents the main features of each solution.

Solution	Advantage	Disadvantage
Internal trusted execution environment (T.E.E.)	Available offline, Easy to integrate into the EUDI Wallet	Certification of T.E.E is limited to EU CSA Substantial (EAL2+ AVAN 2) No direct access, we should relying on the smart phone manufacturer trust model – which may not be compatible with the certification process
External cryptographic device	Available offline Solutions available on the market NFC interface is widely deployed and interoperable and available on all smart phone device types (some may need some contractual activities before to be able to use it)	EUDI Wallet Users needs to have their external cryptographic device in hand in addition of their EUDI Wallet. Some older versions of smart phones are not compatible (esp. on iOS).
Remote cryptographic component	Already certified at equivalent level of EU CSA High level (under the SOGIS) and well-known solutions	Available online only Still need some local cryptographic components to manage the mutual authentication and the encryption of data which are exchanged during the transaction.
Hybrid	Available offline for the function that need a certain level of confidence Security level and Assurance level can be set up depending on the targeted function	Remote cryptographic is not available in offline The EUDI Wallet is becoming an asset to be protected as it is managing the Hybrid mode.

A.2. STANDARDS RELATING TO THE EUROPEAN DIGITAL IDENTITY WALLET

The objective of this annex is **not to define the EUDI Wallet standards**, but to provide an overview of the available standards that can be used to define the 'what' of the EUDI Wallet.

None of the standards presented in the table below fulfils the EUDI Wallet needs. All of them have been designed for pure online or offline use cases.

We note that only one of them has been designed to target digital identity wallets: the ISO/IEC 23220 series. It is still a working draft but fits most of the requirements. This series defines the ‘what’ and not the ‘how’. **Defining the ‘how’ would require specific work to set out a concrete interoperable implementation of the EUDI Wallet.**

We also note that the EUDI Wallet shall support some existing and well-known offline use cases, such as EU Mobile Driving Licence and EU Digital Travel Credentials. These two offline use cases are supported by ISO/IEC 18013-5 and ICAO 9303-5, the latter of which is in the development phase. The integration of these specific use cases into the EUDI Wallet would need specific analysis or to be considered as distinct applications running in parallel with the EUDI Wallet core functions.

As previously mentioned, and based on the Chapter 4 analysis, the EUDI Wallet will be based on European and international standards that are expected to be published and validated in the coming years. However, many wallet components are based on standards that have already been published or drafted by European and international standardisation organisations.

This section describes standards with potential usability for the EUDI Wallet. It is worth mentioning that CEN/CENELEC, through Technical Committee 224 / Working Group 20, has started work to convert the ISO/IEC 23 2220 series and the ISO/IEC 18013-5 standards into European norms.

The ETSI Electronic Signatures and Infrastructures Technical Committee has started to prepare updates to the current ETSI standards used in the eIDAS ecosystems to enable them to support new use cases and trusted services such as those regarding (Q)EAAs.

ISO/IEC FDIS 18013-5 (‘Personal Identification – ISO-compliant driving licence’), designed to support mobile devices, has already been published. This standard describes the application, data format and communication protocol for sharing trusted digital copies of an official document (the user’s driving licence) in a face-to-face law enforcement situation. This standard is structured to support the storage of personal information data and its presentation in the EUDI Wallet.

ISO is drafting a set of standards (ISO/IEC DIS 23220) for building blocks for identity management through mobile devices. Those standards are supporting the general architecture of the EUDI Wallet as an application on mobile devices and all wallet life cycle processes. These standards also inherit from ISO/IEC FDIS 18013-5, thereby allowing the use of the structures that are defined for mDLs. In addition, they are capable of containing more advanced structures.

Currently, there are no ISO standards directly supporting Verifiable Credentials and Self Sovereign Identity.

The table below lists the standards relating to the EUDI Wallet.

Name	Document reference	Standard supports wallet	Current version / publication year
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 1: Generic system architectures of mobile eID systems	ISO/IEC DIS 23220-1	Multiple components of the wallet (architecture)	D
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 3: Protocols and services for installation and issuing phase	ISO/IEC DIS 23220-3	Multiple components of the wallet (architecture)	Draft
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 4: Protocols and services for operational phase	ISO/IEC DIS 23220-4	Multiple components of the wallet (architecture)	Draft
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 2: Data objects and encoding rules for generic eID-System	ISO/IEC DIS 23220-2	Data formats and interfaces	Draft
QR Code bar code symbology specification	ISO/IEC 18004	Data formats and interfaces	2017
Aztec Code bar code symbology specification	ISO/IEC 24778	Data formats and interfaces	2008
Data Matrix bar code symbology specification	ISO/IEC IS 16022	Data formats and interfaces	2006
Information technology – Automatic identification and data capture techniques – JAB	ISO/IEC PRF 23634	Data formats and interfaces	Draft

Code polychrome bar code symbology specification			
Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures	RFC 8610	Data formats and interfaces	2019
Concise Binary Object Representation (CBOR)	RFC 8949	Data formats and interfaces	2020
CBOR Object Signing and Encryption (COSE)	RFC 8152	Data formats and interfaces	2017
Client to Authenticator Protocol (CTAP)	N/A	Data formats and interfaces	2019

Currently, there are no standards for technical devices containing wallets, but there are some standards for devices capable of contact with wallets through an NFC interface.

Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)	**ISO/IEC 18092:2013**	**Devices supporting the wallet**	**2013**
Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) – Technical Corrigendum 1	ISO/IEC 18092:2013 / COR 1:2015	Devices supporting the wallet	2015
Near Field Communication; Interface and Protocol (NFCIP-1)	EN 302 190	Devices supporting the wallet	1.1.1 (2005)
Cards and security devices for personal identification – Building blocks for identity management via mobile devices – Part 5: Trust models and confidence level assessment	ISO/IEC DIS 23220-5	Other requirements	Draft

A.3. ANALYSIS

Based on the Chapter 4 analysis and the *European Digital Identity Architecture and Reference Framework Outline* requirements, we can see that some standards are directly applicable to the EUDI Wallet; some of them are published and some are working drafts.

We have also identified some **major gaps**:

1) there are no European or international standards for the Cryptographic Device Interface, which is mainly the direct interface of the cryptographic component of the Mobile Device;
2) The Functional Testing Requirements are missing for all the elements of the EUDI Wallet except:

- PID/(Q)EAA mutual authentication protocols,
- Qualified Electronic Signatures.

It is interesting to note that two standardised PID/(Q)EAA mutual authentication protocols (EAC2 and FIDO2) are available, and more than six are available for the user authentication.

The EUDI Wallet standards presented in the following section can be used to define the ‘what’ of the EUDI Wallet. None of the standards fulfils the EUDI Wallet needs. All of them have been designed for pure online or offline use cases.

We note that only one of them has been designed to target Digital Identity Wallets: the ISO/IEC 23220 series. It is still a working draft but fits most of the requirements. This series defines the ‘What” and not the ‘How’. Defining the ‘How’ would require specific work to set out a concrete interoperable implementation of the EUDI Wallet. This is to be set out in a dedicated functional requirement specification (FRS).

This functional requirement specification (FRS) must reference the relevant chapters of European and international standards when possible.

We also note that the EUDI Wallet is to support some existing and well-known offline use cases, such as EU Mobile Driving License and EU Digital Travel Credentials. These two offline use cases are supported by ISO/IEC 18013-5 and ICAO 9303-5, the latter of which is in the development phase. The integration of these specific use cases into the EUDI Wallet would need specific analysis or to be considered as distinct applications running in parallel with the EUDI Wallet core functions.

A.3.1. Functional requirements

This section identifies standards that may define functional requirements for the EUDI Wallet.

Data format

Area	Standard	Applicability	Status
Functional Requirements	W3C Verifiable Credentials Data Model	(Q)EAA data format	Published

	ETSI TS 119 472	(Q)EAA data format	Draft
	ISO/IEC 18013-5	PID data format	Published
	ISO/IEC DIS 23220-2	PID data format	Voting
Functional Testing Requirements	Not available		
Functional certification scheme	Not available		

Storage

Area	Standard	Applicability	Status
Requirements	ISO/IEC DIS 23220-1	Storage interface architecture	Draft
Functional Testing Requirements	Not available		
Functional certification scheme	Not available		

Communication protocols

Area	Standard	Applicability	Status
Requirements	OpenID Connect Core	General authentication model	Published
	Self-Issued OpenID Provider v2	Potential communication protocol for wallet authentication to relying party	Unspecified
	OpenID Connect for Verifiable Credential Issuance	(Q)EAA issuance	Unspecified

	OpenID Connect for Verifiable Presentations	(Q)EAA presentation	Unspecified
	DIDComm	Potential communication protocol for mutual authentication to relying party	Unspecified
	RFC 8446TLS 1.3	Potential communication protocol for mutual authentication to relying party	Published
	ISO/IEC FDIS 18013-5	Communication protocol for PID presentation	Published
	ISO/IEC DIS 23220-3	Communication protocol for PID/(Q)EAA issuance	Draft
	ISO/IEC DIS 23220-4	Communication protocol for PID/(Q)EAA presentation	Draft
	ETSI TS 119 462	Communication protocol for TSPs, (Q)EAA issuance, (Q)EAA presentation, creation of electronic signatures and seals	Draft
Functional Testing Requirements	Not available		
Functional certification scheme	Not available		

PID/(Q)EAA mutual authentication protocols

Area	Standard	Applicability	Status
Requirements	eIDAS Token Specifications TR-03110-2	Yes: EAC2 protocol + RI + ERA	Published in 2012
	ITU-T X.1277 and ITU-T X.1278	Only for mutual authentication (not for identification)	Published in 2018

Functional Testing Requirements	BSI TR-03105	Yes	Published in 2012
Functional certification scheme	FIDO functional certification scheme		

User authentication

Area	Standard	Applicability	Status
Requirements	ISO/IEC 29115:2013	Levels of assurance for authentication	Published
	Self-Issued OpenID Provider v2	**Potential communication protocol for mutual authentication to relying party**	**Unspecified**
	DIDComm	Potential communication protocol for mutual authentication to relying party	Unspecified
	RFC 8446 TLS 1.3	**Potential communication protocol for mutual authentication to relying party**	**Published**
	ETSI TS 119 461	Identity proofing requirements	Published
	TR-03147	**Identity proofing requirements**	**Published**
Functional Testing Requirements	Not available		
Functional certification scheme	**Not available**		

Verification mechanisms

Area	Standard	Applicability	Status
Requirements	ETSI TS 119 441	Signature validation requirements	Published

	ETSI TS 119 442	Profiles for signature validation	Published
	ETSI EN 319 102-1	Signature validation process	Published
Functional testing requirements	Not available		
Functional certification scheme	Not available		

Qualified electronic signatures

Area	Standard	Applicability	Status
Requirements	ETSI TS 119 432	Remote signature protocols	Published
	CSC API 1.0.4.0	Remote signature protocols	Published
	ETSI EN 319 102-1	Signature creation process	Published
	ETSI TS 119 101	Signature application requirements	Published
	ETSI EN 319 122-1	Signature creation format	Published
	ETSI EN 319 132-1	Signature creation format	Published
	ETSI EN 319 142-1	Signature creation format	Published
	ETSI EN 319 162-1	Signature creation format	Published
	ETSI TS 119 462	Protocol for signature creation	Draft
Functional testing requirements	ETSI EN 319 124 series	CAdES test suites	Published
	ETSI EN 319 134 series	XAdES test suites	Published

	ETSI EN 319 142 series	PAdES test suites	Published
	ETSI TS 319 164 series	Associated signature container test suites	Published
Functional certification scheme	Not available		

Cryptographic algorithms

Area	Standard	Applicability	Status
Requirements	ETSI TS 119 312	Cryptographic Suites	Published
	SOG-IS (note it is the only one accepted within the eIDAS framework)	Agreed Cryptographic Mechanisms	Published
	ISO/IEC 19790	Security requirements for cryptographic modules	Published
	CEN EN 419211-1	Policy requirements for cryptographic modules	Published
	CEN EN 419211-2	Policy requirements for cryptographic modules	Published
	CEN EN 419211-3	Policy requirements for cryptographic modules	Published
	CEN EN 419211-4	Policy requirements for cryptographic modules	Published
	CEN EN 419211-5	Policy requirements for cryptographic modules	Published
	CEN EN 419211-6	Policy requirements for cryptographic modules	Published

	CEN/TS 419221-1	Policy requirements for cryptographic modules	Published
	CEN/TS 419221-2	Policy requirements for cryptographic modules	Published
	CEN/TS 419221-3	Policy requirements for cryptographic modules	Published
	CEN/TS 419221-4	Policy requirements for cryptographic modules	Published
	CEN EN 419221-5	Policy requirements for cryptographic modules	Published
	CEN/TS 419221-6	Policy requirements for cryptographic modules	Published
Functional testing requirements	Not available		
Functional certification scheme	Not available		

A.3.2. Interface requirements

This section identifies standards that may define requirements for EUDI Wallet interfaces with external entities.

Interfaces with Member States' infrastructures

Area	Standard	Applicability	Status
Functional requirements	ISO/IEC DIS 23220-3	Communication protocol for PID/(Q)EAA issuance	Draft
	ISO/IEC FDIS 18013-5	PID-obtaining interface	Published
Functional testing requirements	Not available		
Functional audit requirements	Not available		

Interfaces with national electronic identification documents

Area	Standard	Applicability	Status
Requirements	ISO/IEC DIS 23220-3	Yes	Draft
Functional testing requirements	Not available		
Functional audit requirements	Not available		

Interfaces with (qualified) trust service providers

Area	Standard	Applicability	Status
Requirements	ETSI TS 119 462	Interface for obtaining (Q)EAA Interface for signature	Draft
Functional testing requirements	Not available		
Functional audit requirements	Not available		

Interfaces for sharing (Q)EAA with relying parties, brokers and proxies, including eIDAS nodes and others

Area	Standard	Applicability	Status
Requirements	ETSI TS 119 462	Usable when a (Qualified) Trust Service Provider acts as a Relying Party	Draft
	ISO/IEC DIS 23220-4	Yes	Draft
Functional testing requirements	Not available		

Functional audit requirements	Not available		

Device (smartphone) interfaces with cryptographic components

Area	Standard	Applicability	Status
Requirements	Not available		
Functional testing requirements	Not available		
Functional audit requirements	Not available		

Other interfaces

Area	Standard	Applicability	Status
Requirements	Not available		
Functional testing requirements	Not available		
Functional audit requirements	Not available		

TP-04-23-010-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-617-0
doi: 10.2824/28598