FIDO Alliance White Paper: Using FIDO for the EUDI Wallet

April 2023

Author:
Sebastian Elfors, IDnow

Abstract

This white paper describes the eIDAS2 ecosystem and how to use the FIDO standard with the EU Digital Identity (EUDI) Wallet.

In the Czech Republic and Norway, FIDO is already approved under eIDAS as an authentication standard for eID schemes at “Level of Assurance High” or “Substantial.“ Under eIDAS2, such eID schemes can be used for onboarding identification of Person Identification Data (PID) to the EUDI Wallet, or enrollment of Qualified Electronic Attribute Attestations (QEAAs) or Qualified Certificates (QCs). This means that FIDO can play an important role in identification for PID Providers or (Qualified) Trust Service Providers (qTSPs) that issue PIDs, QEAAs, or QCs. FIDO can also be used for authentication to multiple qTSPs in order to issue short-lived, atomic qEAAs, which can be combined into verifiable presentations that cater for selective disclosure.

An additional important use case for FIDO is authentication to a hosted wallet, which is operated in a cloud-based environment. In this scenario, a standard web browser can be used with FIDO for accessing the users’ qEAAs that are hosted in a cloud-based wallet. Interoperability between EUDI Wallets and relying parties could be based on the delegated authorization protocols OAuth2 and OpenID Connect (OIDC), and FIDO can be used for user authentication to these authorization servers.

Furthermore, FIDO can be used for authentication to remote Qualified Signature Creation Devices (QSCDs), which are operated centrally by QTSPs. In this scenario, the user will use FIDO for authenticating to its QCs that are protected in the remote QSCD, and thereby create Qualified Electronic Signatures (QES) remotely under sole control. FIDO can be used for direct access to the remote QSCD or used for OAuth2 delegated authorization in a Cloud Signature Consortium solution.

The ISO 18013-5 Mobile Driving License (ISO mDL) is a prioritized use case for the EUDI Wallet large scale pilots. FIDO can be used for authentication from the EUDI Wallet to the mDL issuer during the online ISO mDL checks that are based on OIDC. In order to enhance the users’ privacy, the new ISO 18013-7 draft standard will rely upon Self-Issued OpenID Provider (SIOP) with OpenID Connect for Verifiable Presentations (OIDC4VP); in such scenarios, FIDO can be used for access from the device to hosted wallets.

Payments are also an important use case for the EUDI Wallet. The EU PSD2 directive requires that the user explicitly approve online web payments by dynamic linking, i.e., an authentication code that is linked to a particular transaction. FIDO can be used in compliance with the PSD2 requirement on dynamic linking in conjunction with Strong Customer Authentication.

Hence, FIDO is already compliant under the existing eIDAS regulation and has the potential to continue to expand its use cases under eIDAS2.

Audience

This white paper is aimed at governmental agencies that are interested in using FIDO for the EUDI Wallet according to the eIDAS2 regulation. The intended readers are project managers, technical experts, and developers.

Contents

1. Introduction 6
1.1 The Evolution of eIDAS 6
1.1.1 National Signature Acts and the EU Signature Directive 6
1.1.2 The eIDAS Regulation 6
1.1.3 Deploying FIDO in compliance with the eIDAS regulation 7
1.2 Introducing eIDAS2 and the EUDI Wallet 8
1.2.1 Review of the eIDAS Regulation 8
1.2.2 Enter eIDAS2 and the EUDI Wallet 8
2. The EUDI Wallet Architecture 9
2.1 EUDI Wallet Architecture Reference Framework (ARF) 9
2.2 Roles in the EUDI Wallet ecosystem 9
2.3 EUDI Wallet Form Factors and Security 10
2.3.1 Legal Definition 10
2.3.2 Technical Solutions and Standards 11
2.4 Issuance of the EUDI Wallet and the PID 11
2.4.1 Legal Definition 11
2.4.2 Technical Solutions and Standards 12
2.5 Issuance of Qualified Certificates 12
2.5.1 Legal Definition 12
2.5.2 Technical Solutions and Standards 12
2.6 Issuance of qEAAs 13
2.6.1 Legal Definition 13
2.6.2 Technical Solutions and Standards 13
2.7 Credential Formats 14
2.7.1 Legal Definition 14
2.7.2 Technical Solutions and Standards 14
2.8 Access to Relying Parties 15
2.8.1 Legal Definition 15
2.8.2 Technical Solutions and Standards 15
2.9 Interoperability 15

2.9.1 Legal Definition 15
2.9.2 Technical Solutions and Standards 15
2.10 Authentication 16
2.10.1 Legal Definition 16
2.10.2 Technical Solutions and Standards 17
2.11 Selective Disclosure 17
2.11.1 Legal Definition 17
2.11.2 Technical Solutions and Standards 17
2.12 Privacy Aspects 18
2.12.1 Legal Definition 18
2.12.2 Technical solutions and standards 18
2.13 Remote Qualified Signature Creation Device (QSCD) 19
2.13.1 Legal Definition 19
2.13.2 Technical Solutions and Standards 19
3. EUDI Pilot Projects 20
3.1 EUDI Wallet Reference Implementation 20
3.2 Large Scale Pilots 21
3.3 Timeline 22
4. How FIDO Can be Used with the EUDI Wallet 22
4.1 Scope of FIDO for eIDAS2 22
4.2 Integrating FIDO with the EUDI Wallet 23
4.3 Deployment of FIDO in the eIDAS2 Ecosystem 24
4.4 eID Scheme for Onboarding of PID 25
4.5 eID Scheme for Issuance of QC or QEAA 26
4.6 Issuance of Short-Lived EAA for Selective Disclosure 26
4.7 Access to Hosted Wallets 27
4.8 Interoperability 29
4.9 Access to Remote QSCD 30
4.10 ISO Mobile Driving License 31
4.11 Compliance with PSD2 for Online Payments 33
5. Why Use FIDO for the EUDI Wallet? 35
5.1 The FIDO Alliance 35
5.2 FIDO is a Global Standard Supported by Every Major Platform 36

6. Conclusions **37**
7. Acknowledgments **39**
8. Glossary of Terms **40**
9. References **42**
9.1 Legal references 42
9.2 Technical standards 42
9.3 Other references 45

Figures

Figure 1 – The history of eIDAS **6**
Figure 2 – The EUDI Wallet ecosystem **9**
Figure 3 – Oauth2 and OpenID Connect (OIDC) illustrated **16**
Figure 4 – Interaction with external cryptographic tokens **21**
Figure 5 – Timeline for the eIDAS2 project **22**
Figure 6 – eIDAS2 ecosystem with FIDO deployments **24**
Figure 7 – PID onboarding with FIDO to the EUDI Wallet **25**
Figure 8 – qC or qEAA enrollment with FIDO to the EUDI Wallet **26**
Figure 9 – Enrollment with FIDO of short-lived EAAs for selective disclosure **27**
Figure 10 – Access to hosted wallet with FIDO **28**
Figure 11 – Authentication with FIDO for OIDC/OAuth2 ..... **29**
Figure 12 – Using FIDO for access to remote QSCD **30**
Figure 13 – Using FIDO with the CSC API **31**
Figure 14 – Using FIDO with the ISO 18013-5 (mDL) online flow **32**
Figure 15 – Using FIDO with the ISO 23220-4 flow **33**
Figure 16 – Using FIDO with PSD2 Strong Customer Authentication **34**
Figure 17 – FIDO use cases for the EUDI Wallet **37**

1. Introduction

1.1 The Evolution of eIDAS

1.1.1 National Signature Acts and the EU Signature Directive

The history of eIDAS goes back to the 1990s, when there were a wide range of national signature acts that set forth different legal requirements. Germany and Italy stipulated the strictest rules in their signature legislations, while Scandinavian countries had very relaxed requirements. This formed the basis for a disperse set of technical solutions across the EU, which resulted in poor interoperability of electronic signatures between the EU member states.

In an attempt to harmonize the electronic signatures in the EU, the European Commission created the Electronic Signatures Directive 1999/93/EC [1] in 1999. The concepts of Advanced Electronic Signature (AES), Qualified Electronic Signature (QES) and SSCD (Secure Signature Creation Device) were introduced with the Signature Directive. However, when the Signature Directive was implemented in national acts across the EU, the interpretation differed between EU member states, so there was still a lack of interoperability between the countries' different electronic signature types.

1.1.2 The eIDAS Regulation

In 2014 the European Commission ratified the "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" [11], better known as the eIDAS regulation.

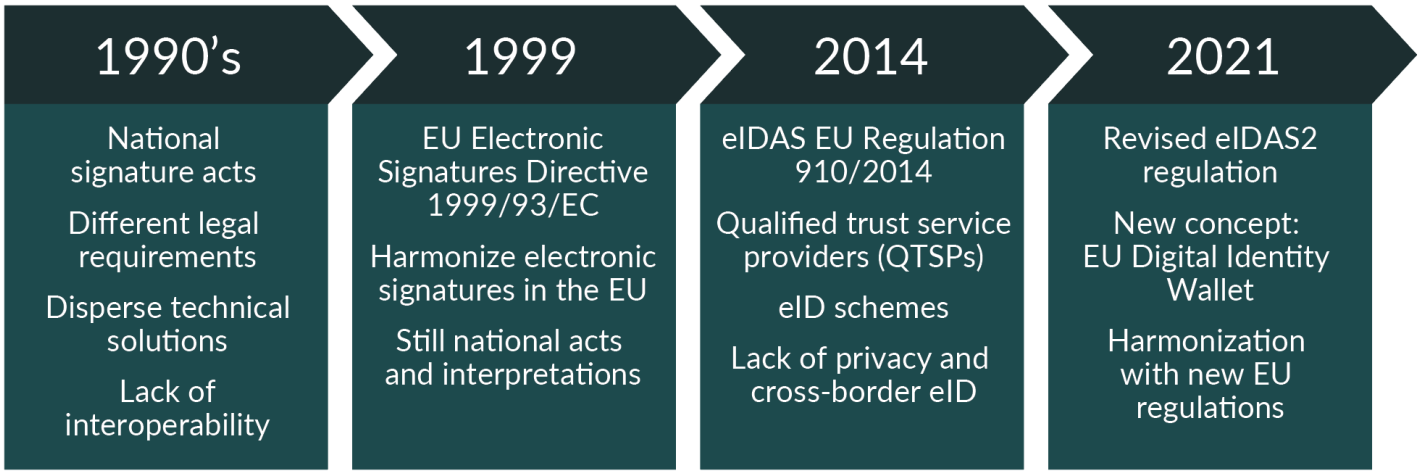

Figure 1 – The history of eIDAS

In addition to the EU regulation, eIDAS is legally constituted by a set of Commission Implementing Regulations and Decisions that regulate the interoperability framework [1], assurance levels for electronic identification schemes [2], formats of trusted lists [3], formats of advanced electronic signatures and advanced seals [4], and security assessment of qualified signature and seal creation devices [5].

The eIDAS regulation introduced the concepts of Trust Service Providers (TSPs) and Qualified Trust Service Providers (QTSPs), which are supervised service providers that are accredited to perform the trusted services: issuing signature/seal certificates, signature validation, timestamping, registered delivery, preservation, and signature/seal creation.

The eIDAS regulation also specified a common electronic identification framework [1] that will recognize electronic identity (eID) schemes from other EU Member States and ensure its authenticity and security. The goal of this interoperable identification and authentication framework is to allow EU citizens to access online services across borders within the EU by simply using their domestic eID scheme. Technically, the cross-border interoperability of eID schemes is based on the EU member states' eIDAS-Nodes that are federated with the authorization protocol SAML v2 [13].

The eIDAS regulation also introduced three Levels of Assurance (LoA) for electronic identification: low, substantial, and high; those assurance levels are defined in the eIDAS regulation [11] and the implementing act with assurance levels for electronic identification schemes [2]:

- The low assurance level requires the electronic identification scheme to use at least one authentication factor, for example, username and password.
- The substantial assurance level requires the electronic identification scheme to use at least two authentication factors from different categories (possession, knowledge, or biometric) for dynamic authentication.
- The high assurance level requires the substantial level plus additional means to protect the electronic identification scheme against duplication and tampering. High assurance level states the following requirements: multi-factor authentication, private data/keys stored on tamper-resistant hardware tokens, and cryptographic protection of personally identifying information.

1.1.3 Deploying FIDO in compliance with the eIDAS regulation

In April 2020, the FIDO Alliance published the white paper "Using FIDO with eIDAS Services" [68] that describes how FIDO can be deployed in compliance with the eIDAS regulation. The white paper contains detailed information on how FIDO can fulfill the authentication requirements on LoA Substantial and High for notified eID schemes.

One year later, the FIDO white paper was quoted by EU Cybersecurity Agency (ENISA) in the report Remote ID Proofing [76], which describes the current regulatory landscape and supporting standards for the European countries' remote identity proofing laws, regulations, and practices. ENISA's report was in turn based on the ETSI TR 119 460 report [26], which also refers to FIDO as an authentication standard that can be deployed for eIDAS eID schemes.
FIDO has also been deployed as part of an eID scheme by the Czech domain register CZ.NIC's identity provider MojeID, and FIDO's eID scheme was recognized as LoA Substantial and High by Czech ministry of interior under the following conditions:

- The FIDO2 authenticator is FIDO certified at Level 2 (or higher).
- The FIDO2 authenticator is based on a secure element that is certified at NIST FIPS 140-2 Level 3 or Common Criteria (CC) EAL4 + AVA_VAN.5.
- The FIDO2 authenticator has a PIN set, and the PIN is required for all transactions at level of assurance High.
- Username and password are used in conjunction with FIDO2.

The user needs to register at the MojeID identity provider by following the procedure in this form. Once the user is registered, it is possible to enroll FIDO2 credentials to a roaming FIDO authenticator ("security key") according to this description.

Furthermore, the Norwegian trust service provider Buypass has deployed FIDO2 as an authentication standard for an eIDAS eID scheme of LoA Substantial and High. The user is onboarded to the Buypass FIDO2 service by remote identity proofing, which matches the user's scanned passport with the user's face image. The solution has been accredited by the Norwegian digitalization agency and is rolled out in the Norwegian healthcare sector.

For more information on how to use FIDO for eIDAS, see the FIDO Alliance white paper "Using FIDO with eIDAS Services" [68] and the blog post "FIDO Recognition for European Digital Identity Systems and eIDAS Grows."

1.2 Introducing eIDAS2 and the EUDI Wallet

1.2.1 Review of the eIDAS Regulation

In June 2021, the EU Commission announced its major revision of the eIDAS regulation. The previous two years, the EU Commission had been working on preparations, public surveys, expert committees, and legal enhancements.

The EU report of the eIDAS revision made several conclusions about the existing eID schemes. Only 19 EU member states have notified their national eID schemes on EU level, so the notified eID schemes cover approximately 59% of the EU population. Furthermore, the eID certification requirements differ between the EU member states, and the SAML v2 [54] federation protocol does not scale, so the adoption and cross-border interoperability of eIDs across the EU is rather low. There are also privacy concerns with the existing eID schemes. The electronic identities, which are often X.509 certificates [35], contain a set of attributes about its users. Hence, the citizens cannot limit what eID attributes they want to present during authentication when it is sometimes desirable to present only a specific or derived attribute (such as age).

1.2.2 Enter eIDAS2 and the EUDI Wallet

The EU Commission published their proposal for amending the eIDAS regulation [10], commonly known as "eIDAS2," in June 2021. After the EU Commission's eIDAS2 proposal was published, the EU Council responded with their eIDAS2 compromise proposal in December 2022, and the EU Parliament followed with their amended eIDAS2 proposal in February 2023. As of February 2023, there are three eIDAS2 proposals, which differ on a few specific topics, but in general, the eIDAS2 proposals share the main objectives. The EU Commission, EU Council, and EU Parliament will continue their negotiations in a "trialogue" with the aim at finalizing the eIDAS2 regulation and implementation during the second half of 2023.

The most significant improvement in the proposed eIDAS2 regulation [10] is the EU Digital Identity Wallet (EUDI Wallet), which will be made available to all EU citizens. The use cases for the EUDI Wallets are for example, mobile driving licenses, electronic passports, electronic national ID-cards, vaccination certificates, and payments.

The EUDI Wallet will contain Person Identification Data (PID) and several (Qualified) Electronic Attribute Attestations (qEAAs), which will be provided by (qualified) trust service providers that can issue PID and/or qEAAs.

It will be mandatory for each EU member state to provide EUDI Wallets to all citizens free of charge, as opposed to the current situation when eID schemes are voluntary. Private actors can also be accredited to provision EUDI wallets and credentials, in contrast to the first eIDAS regulation where national certification authorities dominated the issuance of eIDs.

Privacy for the EU citizens will also be an important topic for eIDAS2 regulation; technically, this will be achieved by selective disclosure of the EUDI Wallet attributes.

The next section will describe the EUDI Wallet in more detail with respect to its architecture reference framework, large-scale pilot projects, and timeline.

2. The EUDI Wallet Architecture

2.1 EUDI Wallet Architecture Reference Framework (ARF)

The EU Commission, DG-CONNECT, and the EU Member States are cooperating within the assembled eIDAS Expert Group to establish a common EUDI Wallet Toolbox. This Toolbox will be based on the European Digital Identity Architecture and Reference Framework (ARF), which will specify the technical architecture, standards, and guidelines for EUDI Wallets.

The outline of the EUDI Wallet ARF [8] (denoted as "ARF outline") was published in February 2022. The ARF outline essentially clarified the roles in the EUDI Wallet ecosystem and described the technical interfaces on a high level.

The ARF v1.0.0 (denoted as "ARF") was published in February 2023 [9] and contained technical details about the credential formats, protocols, and APIs.

2.2 Roles in the EUDI Wallet ecosystem

In the EUDI Wallet ARF v1 [8], the different roles in the EUDI Wallet ecosystem are described in section "3 Roles in the ecosystem." An overview of the EUDI Wallet ecosystem with a selection of the roles is illustrated below:

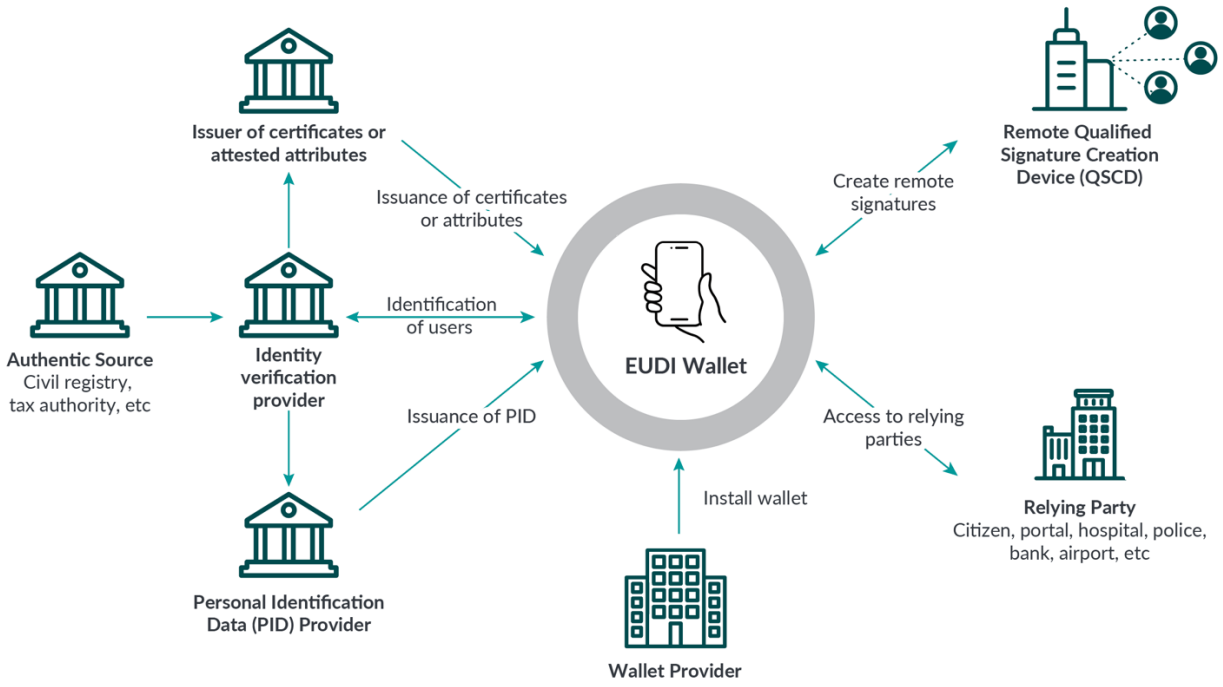

Figure 2 – The EUDI Wallet ecosystem

The illustrated EUDI Wallet roles are summarized below:

- Authentic sources are the public or private repositories or systems recognized or required by law to provide official identification documents about a natural or legal person.
- Identity verification providers would verify the identity of the EUDI Wallet user based on the user's official identification documents or by electronic means. For issuance of qualified certificates, eIDAS2 Article 24.1 will apply, which specifies the following identification options: eID scheme, Qualified Electronic Signature, physical identification, or remote identity proofing.

- PID providers will issue the PID to the user's EUDI Wallet, based on the identity verification provider (see section 2.4).
- Issuer of certificates is a qTSP that operates a certification authority for issuance of qualified or non-qualified certificates (see section 2.5).
- Issuer of Electronic Attribute Attestations is a new qTSP under eIDAS2 that issues qualified or non-qualified Electronic Attribute Attestations (see section 2.6).
- Wallet providers, formally denoted as EUDI Wallet Issuers, are EU Member States or organizations that have been either mandated or recognized by the EU Member States to provide the EUDI Wallet to the end users.
- Relying Parties are services that rely upon an electronic identification or a trust service. In the context of EUDI Wallets, they would request and validate the necessary attributes contained within the PID dataset, qEAA, or certificates from EUDI Wallet users. In practice, Relying Parties are government portals, hospitals, banks, customs, police authorities, airports, etc.
- Remote QSCD is operated by a QTSP with the purpose of signing electronic documents remotely on behalf of a user (see section 0).

2.3 EUDI Wallet Form Factors and Security

2.3.1 Legal Definition

Security of the EUDI Wallet is of essence, and the eIDAS2 regulation [10] states in recital 10:

"In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States."

According to the ARF outline [8], the EUDI Wallet will be provided in three form factors:
"The different functions of the EUDI Wallet can be implemented using existing technologies such as:

- *Form factor 1: Mobile application.*
- *Form factor 2: Web application.*
- *Form factor 3: Secure Application on PC."*

Furthermore, the ARF has specified the following Cryptographic Keys Management Systems:

"EUDI Wallet Solution [...] rely on one of the following components to store and manage cryptographic keys:

- *Embedded Secure Element or Trusted Execution Environment (for mobile devices),*
- *reliance on an external device (Secure Elements / Smart Cards), and*
- *a backend (remote Hardware Security Module)."*

Hence, technical standards are necessary to specify the security and certification schemes of the EUDI Wallets.

2.3.2 Technical Solutions and Standards

The form factors mentioned in the ARF outline can be implemented in the following ways:

- Form factor 1: This is an app that will run on a mobile device, where the keys for the credentials and certificates will be protected in the mobile device's Trusted Execution Environment (TEE).
- Form factor 2: In this case, the EUDI Wallet will be hosted as a web application at a cloud service provider. The users' credentials will typically be protected by an HSM that is hosted in the cloud service, which the user will get access to by using a web browser. Hence, the user needs to get authenticated to the cloud-based wallet, and the user's specific credentials will be selected and released based on this authentication.
- Form factor 3: This is a secure application that will run on a desktop PC, with similar design principles as form factor 1.

However, the ARF has only specified the technical architecture of an EUDI Wallet as a mobile app, i.e., according to Form Factor 1. The other form factors that are described in the ARF outline are reserved for future use.

There are several standards for digital wallet architecture and security that will be of relevance for the EUDI Wallet:

- ISO/IEC 23220 "Cards and security devices for personal identification — Building blocks for identity management via mobile devices." The ISO/IEC 23220 standards will be published as parts 1-6: ISO/IEC 23220-1 describes the generic system architectures of mobile eID systems [38], ISO/IEC 23220-5 [42] is a draft standard that will describe the trust models and confidence level assessment, and the ISO/IEC 23220-6 [43] draft will describe certification on the trustworthiness of a secure area. The ISO/IEC 23220-6 standard in conjunction with the forthcoming EU Common Criteria (EUCC) cybersecurity certification scheme [68] will form the basis for certification of the EUDI Wallet.
- ETSI TS 119 462 "Wallet interfaces for trust services and signing" [28]. This is a draft standard by ETSI ESI, which will specify the technical interfaces for a wallet with respect to issuance of credentials and signing operations. To a large extent, the ETSI TS 119 462 standard will be based on ISO/IEC 23220.
- W3C Universal Wallet [57]. This specification describes a portable and extensible JSON-LD wallet, which supports digital currencies and credentials. The standard has a pending section for wallet security.
- DIF Wallet Security Group [78]. This is a working group within the Digital Identity Foundation (DIF) with the purpose of describing the security features of a digital wallet.
- OpenWallet Foundation [75]. This is an initiative launched by the Linux Foundation with the purpose to develop an open-source engine to build interoperable, secure, and privacy-protecting wallets.
- Hyperledger Indy SDK Wallet [74] is a cloud-based wallet, which is accessed by the Hyperledger Aries protocols. This cloud-based architecture is most relevant for the EUDI Wallet Form Factor 2.

2.4 Issuance of the EUDI Wallet and the PID

2.4.1 Legal Definition

The issuance of the EUDI Wallet is described in eIDAS2 Article 6a.6 [10]:

"The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'."

Furthermore, eIDAS2 Article 6a.4.e states the following about the onboarding of user's Person Identification Data (PID) to the EUDI Wallet:

"ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural or legal person is associated with it."

2.4.2 Technical Solutions and Standards

The user first needs to install the EUDI wallet, which has been issued by the wallet provider, and secondly, the user needs to enroll for the PID.

To enroll the PID, the user will be identified according to the "Identity proofing and verification" section of the Commission Implementing Regulation (EU) 2015/1502 on assurance levels for electronic identification means [2]. For Level of Assurance (LoA) High, the user can be identified based on identification documents issued by authentic sources, or by using a previously enrolled eID scheme on LoA High.

The ARF [9] has specified the PID formats as ISO 13801-5 mobile driving license (ISO mDL) [37] and W3C Verifiable Credentials (W3C VC) [62]. How to achieve selective disclosure with these formats is described in section 2.11.

Furthermore, the ARF has specified ISO/IEC 23220-3 [40], which is based on OpenID for Verifiable Credentials Issuance (OID4VCI) [50], as the enrollment protocol for the PID. The ISO/IEC 23220-3 draft standard will describe protocols and services for the installation and issuing phase of a digital wallet. The European standardization organization CEN has introduced the concept of EUDI Wallet PID onboarding in a proposed standard by the CEN/TC224/WG20 working group. Furthermore, the ETSI TS 119 461 standard "Policy and security requirements for trust service components providing identity proofing of trust service subjects" [13] includes appendix A.5, which describes how remote identity proofing can meet the requirements for LoA High.

2.5 Issuance of Qualified Certificates

2.5.1 Legal Definition

The Qualified Certificates are issued by accredited Qualified Trust Service Providers (QTSPs) according to Article 24 in eIDAS [11].

Specifically, Article 24.1b of eIDAS2 [10] declares that the user can be identified accordingly for issuance of a Qualified Certificate:

"(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high';"

Article 24.1b implies that the user has previously enrolled for an eID on LoA Substantial or High, which can be used for identification to a QTSP in order to issue a qualified certificate.

2.5.2 Technical Solutions and Standards

The ETSI EN 319 401 standard "General Policy Requirements for Trust Service Providers" [24] describes the policies, audit,s and operations that apply for trust service providers and qualified trust service providers. The issuance of Qualified Certificates are performed in accordance with the Certification Authority's CP/CPS by using a Registration Authority with traditional PKIX protocols such as CMP [16], CMC [15], or SCEP [57].

The details of the QTSP Certification Authority issuance procedures go beyond the scope of this white paper, but it is worthwhile highlighting that the ETSI TS 119 461 standard "Policy and security requirements for trust service components providing identity proofing of trust service subjects" [13] describes how a user can be identified with remote identity proofing according to eIDAS Article 24.1b.

2.6 Issuance of qEAAs

2.6.1 Legal Definition

The qualified Electronic Attribute Attestations (qEAAs) were introduced in eIDAS2 [10] for use with the EUDI Wallet. Hence, Article 24 in eIDAS2 has been updated to allow for QTSPs to issue qualified Electronic Attribute Attestations (qEAAs) as well as Qualified Certificates.

Furthermore, eIDAS2 Article 24.1a [10] has been updated with respect to identification for issuance of qEEAs and Qualified Certificates:

"by means of a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high';"

Another change to the eIDAS2 regulation with regards to QTSPs is that the proposed EU NIS2 directive will shift some of the auditing and reporting requirements to the supervisory bodies.

2.6.2 Technical Solutions and Standards

The ETSI EN 319 401 standard "General Policy Requirements for Trust Service Providers" [24] will be updated to take the qTSP operational changes in the eIDAS2 regulation into account, for instance, to reflect that the NIS2 directive will regulate the reporting to supervisory bodies. Furthermore, ETSI TS 119 471 is a new standard that will describe the policy and security requirements for qTSPs issuing qEAAs.

During the development of eIDAS2, the ESSIF project eIDAS Bridge investigated how qEAAs could be sealed with Qualified Electronic Seals (QES) by a third-party issuer. This bridged the gap between the concept of Self-Sovereign Identity (SSI) and the eIDAS trust framework in the sense that qEAAs were issued by a trusted party. The eIDAS Bridge project served as a prototype, but the qEAA issuance will be an integral feature of the qTSPs under eIDAS2.

As regards to technical protocols for issuance of qEEAs, typically in the form of W3C Verifiable Credentials, the following standards can be considered:

- OpenID for Verifiable Credentials Issuance (OID4VCI) [50]: This specification defines an API and corresponding OAuth 2.0-based authorization mechanisms for the issuance of Verifiable Credentials.
- WACI-DIDComm [63]: This specification provides an initial protocol definition for the two main interactions (issuance and presentation) required for Verifiable Credentials.

The ARF has specified OID4VCI to be used as the issuance protocol for qEAAs.

2.7 Credential Formats

2.7.1 Legal Definition

The eIDAS2 regulation [10] defines the EUDI Wallet utilization of Electronic Attribute Attestations (Electronic Attestion of Attributes) as follows:

"6a.3. European Digital Identity Wallets shall enable the user to:

"securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services;"

The technical specifics of the various forms of Electronic Attribute Attestations will be defined in a set of standards, which are discussed in the next section.

2.7.2 Technical Solutions and Standards

Ultimately, the ARF [8] will specify the qEEA formats that will be in scope of the EUDI Wallet. Below is a list of the most significant credentials to be supported by the EUDI Wallet:

- W3C Verifiable Credentials (VC) [62] in conjunction with W3C Decentralized Identifiers (DIDs) [19] are becoming the de facto standards for Self-Sovereign Identity (SSI) and digital wallets. The W3C Verifiable Credentials are encoded as JSON [44] objects, either in JWT [45] or JSON-LD [46] formats. A set of Verifiable Credentials can be combined in a Verifiable Presentation, which is presented to a verifier.
- ISO 18013-5 mobile Driving License (mDL) [37] is the digital equivalence to a driving license. ISO mDL is implemented in Apple iOS and Google Android and has been deployed in several states in the United States. The ISO mDL format is based on CBOR-encoded MDOC, which can be presented to a verifier either offline or online by using OIDC [49] or the ISO mDL WebAPI.
- ICAO electronic Machine Readable Travel Document (eMRTD) [23] is the basis for passports issued around the globe and is used by IATA and its associated airlines for identification of travelers. The ICAO Digital Travel Credential (DTC) [22] is an electronic version of passports, which is suitable for use with digital wallets.

The ISO 23220-2 draft standard [39] will specify how the different types of credentials should be stored and protected by a digital wallet.

In parallel, ETSI ESI is working on the draft standard ETSI TS 119 472 "Profiles for Attribute Attestations" [29] that will specify the formats of the Electronic Attribute Attestations for the EUDI Wallet.

Note: X.509 certificates, according to the IETF PKIX profile [35], will not be considered as qEAA formats. However, the traditional X.509 certificates constitute the backbone of a Public Key Infrastructure (PKI), and will remain as the fundamental credentials for digital signature creation and internet security protocols such as Transport Layer Security (TLS) [60] and IP Security (IPsec) and Internet Key Exchange (IKE) [36]. Hence, X.509 certificates will be used for auxiliary functions in the eIDAS2 eco-system, such as signing qEAAs during the issuance phase and allow for secure TLS access to websites that are protected with Qualified Web Authentication Certificates (QWACs).

2.8 Access to Relying Parties

2.8.1 Legal Definition

The eIDAS2 regulation [10] defines access to Relying Parties as follows:

"6b.3. Relying parties shall be responsible for carrying out the procedure for authenticating person identification data and electronic attestation of attributes originating from European Digital Identity Wallets."

2.8.2 Technical Solutions and Standards

The ARF has specified the protocol to be used for presentment of PIDs and/or qEAAs to ISO 23220-4 [41], which in turn is based on OpenID for Verifiable Presentations (OID4VP) [51]. Hence, ISO 23220-4 will be used when an EUDI Wallet is authenticated to a Relying Party.

Furthermore, the ARF has classified two configuration types of the EUDI Wallet in section 6.5.2 "Initial Configurations":

"EUDI Wallet Solutions will initially support two configurations:

- *Type 1 configuration is aimed specifically at use cases where the Relying Party relies on guarantees required for the LoA High as defined in CIR 2015/150215, to enable cross border identification using PID attributes at LoA High. Type 1 configuration is mainly designed for purposes of PID.*
- *Type 2 configuration aims to enable flexibility and additional feature support for possible (Q)EAA use cases that cannot be met by Type 1 configuration (e.g., possibly in areas of health, education credentials, …).*

Note that the Type 1 configuration is not meant for the PID set only. It is likely that many (Q)EAAs are used in elevated security areas (e.g., finance, health, access to premises) and will have requirements that are satisfied by Type 1 configuration. If so, these (Q)EAAs will be issued in accordance with Type 1 configuration."

2.9 Interoperability

2.9.1 Legal Definition

The Relying Parties in the EUDI Wallet ecosystem are the online services the user needs access to. Examples of Relying Parties are citizen portals, hospitals, banks, airports, police authorities, etc.

Interoperability for access to the Relying Parties is of importance to the eIDAS2 regulation [10], as stated in recital 9:

"To achieve simplification and cost reduction benefits to persons and businesses across the EU, including by enabling powers of representation and e-mandates, Member States should issue European Digital Identity Wallets relying on common standards to ensure seamless interoperability and a high level of security."

This requirement is reiterated in the ARF outline [8]:

"As provided by the legislative proposal, EUDI Wallets shall be interoperable across the European Union and have externally oriented interfaces specified by common, technical standards."

2.9.2 Technical Solutions and Standards

Under the eIDAS regulation of 2014, interoperability of eID schemes between EU member states was based on SAML v2 as federation protocol. Each EU member state operates eIDAS-Nodes, which are used for receiving and submitting SAML v2 transactions. However, this system has suffered from scalability issues and is not used on a large scale.

At the time of writing, eIDAS2 and the ARF have not yet defined any federation protocols that could be used for interoperability between EUDI Wallets, Identity Providers, and Relying Parties.

Two candidate protocols for achieving interoperability are OAuth2 [47] and OpenID Connect (OIDC) [49], which are modernized federation protocols that are widely deployed in the private and public sectors.

The OAuth 2.0 authorization framework would enable the EUDI Wallet to obtain access to a Relying Party: the user's EUDI Wallet will authenticate itself to the OAuth2 Authorization Server to retrieve an OAuth2 access token, which can be used for accessing the Relying Party's protected resources. OpenID Connect 1.0 (OIDC) is an identity layer on top of the OAuth 2.0 protocol: it enables Relying Parties to verify the identity of the user based on the authentication performed by an Authorization Server.

The OAuth2 and OIDC authorization code flows are illustrated below:

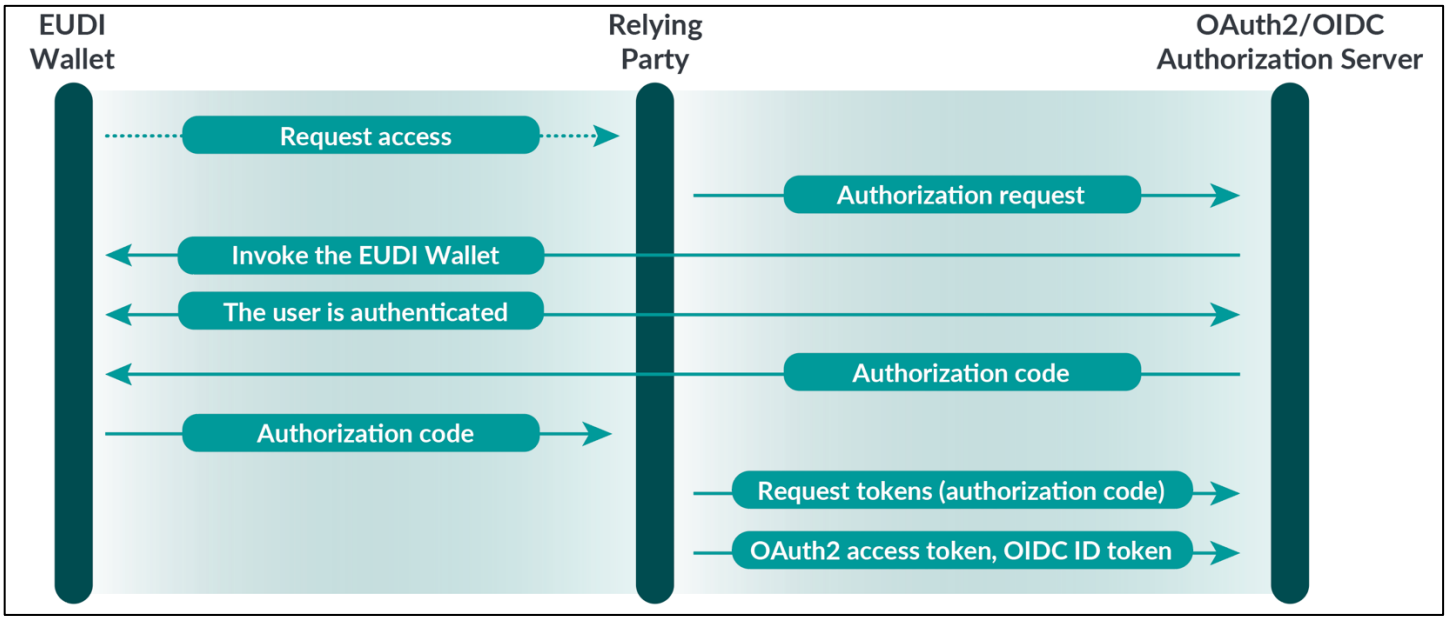

Figure 3 – Oauth2 and OpenID Connect (OIDC) illustrated

2.10 Authentication

2.10.1 Legal Definition

The ARF outline [8] includes the following statements regarding mutual authentication for the EUDI Wallet:

*"**Section 4.4 Mutual Authentication***

To ensure informed actions from the user and adequate security levels, the EUDI Wallet shall implement mutual authentication capabilities. The mutual identification and authentication capability shall cover both the EUDI Wallet end and the third party end as, depending on the use case, the EUDI Wallet may identify and authenticate itself or the user, however it shall be able to identify and authenticate the third party it is interacting with. Additionally, this mutual identification and authentication shall be possible both online (over the Internet) and offline."

*"**4.6.2 User authorization mechanism***

The EUDI Wallet shall require the user to use two-factor authentication in a combination of at least two authentication factors for certain use cases, satisfying the requirements for LOA high:

- a proof of knowledge;
- a proof of possession;
- a proof of inherence."

2.10.2 Technical Solutions and Standards

There are several standards available for mutual authentication with a digital wallet. Below is a list with the most significant standards for two-factor authentication:

- FIDO2 standard [34], comprised of FIDO Alliance CTAP v2.1 [17] and W3C WebAuthn [64].
- IETF Transport Layer Security (TLS) [60].
- IETF IP Security (IPsec) and Internet Key Exchange (IKE) [36].
- IETF OATH Time-Based One-Time Password (TOTP) [59].

In addition to the widely deployed authentication standards above, there are emerging standards for verifiable presentations that are suitable for digital wallets with verifiable credentials:

- OpenID for Verifiable Presentations (OID4VP) [51].
- DIF WACI-DIDComm [63].

A more extensive description of FIDO as an authentication standard for the EUDI Wallet is available in section 4.

When using OAuth2 with a mobile native app, it is recommended to use the system browser for the authentication protocol. This architecture is described in the standard IETF "OAuth 2.0 for Native Apps" [48].

2.11 Selective Disclosure

2.11.1 Legal Definition

Selective disclosure is defined as follows in recital 29 of the eIDAS2 regulation [10]:

"The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data."

2.11.2 Technical Solutions and Standards

From a technical perspective, there are different ways to design and implement privacy systems that cater to selective disclosure of credentials' claims:

- Short-lived atomic credentials that are enrolled upon request. The atomic credentials should only contain the bare minimum claims that are needed to disclose to a verifier. One or more short-lived atomic credentials can be combined into a verifiable presentation that is exposed to the verifier. The verifiable credentials issuance protocols described in section 2.6 could be considered for the enrollment procedures.

- Zero Knowledge Proof (ZKP) schemes. A ZKP is a method by which the user can prove to the verifier that a given statement is true, while the user is only revealing the requested information. For example, a ZKP scheme can be used by a user to prove that their age is above 18 years. Examples of ZKP schemes are DIF BBS+ Signatures [14], Hyperledger AnonCreds (which are based on CL-signatures) [13], and zkSNARK [67].
- Create a list with hashed values of salted claims and combine them in an object which is signed by the issuer. The holder can present the selected claims and related salts and provide the object with hashed salted claims, to the verifier. IETF SD-JWT [55] is an example of such salted claims in JSON [44] format, which can be used with DIF Presentation Exchange [52] and presentment protocols such as WACI-DIDComm [63] or OIDC4VP [51]. Another example of the same technique is the Mobile Security Object (MSO) in the ISO mDL 18013-5, which is used for offline selective disclosure of MDOCs.
- Use OIDC [49] such that the verifier requests an ID Token with selected claims by the Identity Provider (IdP). This is how the ISO 18013-5 (mDL) [37] has designed selective disclosure for online verification.

The ARF stipulates that selective disclosure of attributes in the EUDI Wallet must be performed using SD-JWT for W3C Verifiable Credentials or the MSO for ISO mDL in offline mode.

One reason for this selection is that SD-JWTs and MSOs can be signed with cryptographic algorithms that are approved in the EU and listed at SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [58]. The SD-JWT and MSO cryptographic algorithms can also be upgraded to future-proof Post Quantum Cryptography (PQC) algorithms such as Kyber, Dilithium, and SPHINCS+.

2.12 Privacy Aspects

2.12.1 Legal Definition

Privacy is in important aspect of eIDAS2 [10], which is articulated in Article 6a.7:

"The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it."

2.12.2 Technical solutions and standards

This requirement is implicitly fulfilled by the network protocols that only involve communication between a client and server, and can be implemented straightforward with authentication standards such as FIDO, TLS, and IPsec (see section 2.10).

This requirement is, however, a bit more challenging for ISO mDL online checks. As mentioned in section 2.11, ISO 18013-5 has designed the online verification checks such that the verifier connects over OIDC to the issuer's authorization server to request selected claims in the user's MDOC. This is not ideal from a privacy perspective according to Article 6a.7 in the eIDAS2 regulation, but for the EUDI Wallet to be compatible with this standard, the ISO mDL application needs to use OIDC. The IdP may not be operated by the issuer, which could increase privacy. There is also the caveat in the eIDAS2 Article 6a.7 that the user could expressly request to release claims to the issuer's authorization server, so the EUDI Wallet will accept ISO 18013-5 for legacy and interoperability reasons.

Hence, the ARF specifies the privacy enhancements to be based on OID4VP [51] in conjunction with SIOP2 [56], whereby selected claims of a credential are presented by the user to the verifier without the involvement of the issuer. The draft standards ISO 23220-4 and ISO 18013-7 will take OID4VP and SIOP2 into account for this purpose.

2.13 Remote Qualified Signature Creation Device (QSCD)

2.13.1 Legal Definition

In eIDAS2 Article 29 [10] the new paragraph 1a is added:

"Generating, managing and duplicating electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote electronic qualified signature creation device."

This means that the operation of a remote Qualified Signature Creation Device (QSCD) has become a fully-fledged qualified trust service under eIDAS2. The remote QSCD can hold millions of users' keys and certificates and thereby create Qualified Electronic Signatures on behalf of the users in a secure cloud-based QTSP.

Under the first eIDAS revision of 2014, however, operation of remote QSCD was (legally speaking) a module, which could be operated by a Qualified Trust Service Provider (QTSP) that was accredited for another qualified trust service, such as issuance of qualified certificates.

The initial eIDAS Commission Implementing Directive (CID) 2016/650 [5] specified the certification requirements of QSCDs. When the initial eIDAS CID 2016/650 [5] was written in 2016, however, it was focused on handheld QSCDs such as smart cards. Hence, there were no available standards for remote QSCDs operated by a QSTP in a secure environment that could meet the requirements in eIDAS Annex II for qualified signature or seal creation devices. Therefore, there existed a gap on how to achieve sole control of the remote qualified signing process.

2.13.2 Technical Solutions and Standards

To close this gap, the European Committee for Standardization (CEN) technical committee TC 224 published three CEN standards that address how QTSPs should operate QSCDs and manage signature creation data on behalf of a remote user to create qualified electronic signatures or seals:

- CEN EN 419 241-1 (Trustworthy Systems Supporting Server Signing Part 1: General Security Requirements) [30];
- CEN EN 419 241-2 (Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing) [31];
- CEN EN 419 221-5 (Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services) [32].

The CEN standards above introduced the following concepts:

- SAM: Signature Activation Module, which authenticates the user and provides access to the user's key and certificate in the remote QSCD;
- SAP: Signature Activation Protocol, which is used by the user for authentication to the SAM;
- SAD: Signature Activation Data, which is part of the SAP that is presented to the SAM, and unlocks the user's key and certificate in the remote QCSD;

In other words, the user will authenticate with SAP and provide the SAD to the SAM, which will give the user access to its private key in the remote QSCD. Hence, the user will get sole control at assurance level 2 (SCAL2) over the remote QES creation process. The EUDI Wallet can implement a SAP for authenticating the user and provide access to the remote QSCD.

There are three additional standards worth mentioning for remote creation of qualified signatures:

- OASIS Digital Signature Services eXtended (DSS-X) [21]: This is an XML-based protocol for remote signing and validation operations by using a SAM and remote QSCD;
- Cloud Signature Consortium (CSC) API [18]: This API is based on the Oauth2 protocol to provide a user access to an IdP, which in turn issues a SAD that can be presented to the SAM for access to the remote QSCD. The CSC API is a modernized version of OASIS DSS-X, although it only provides remote signing while OASIS DSS-X also provides remote validation;
- ETSI TS 119 432 [25]: This is the ETSI technical standard that describes the protocols for remote signatures, i.e., DSS-X (in XML format) and the CSC Oauth2 access token (in JSON format).

3. EUDI Pilot Projects

3.1 EUDI Wallet Reference Implementation

In addition to the ARF, which specifies the architecture framework of the EUDI Wallet, there will also be an EUDI Wallet reference implementation provided as an open-source project. The EUDI Wallet reference project was announced as an EU public tender [73] with a deadline of July 2022. The reference implementation will be a full-fledged implementation with modular architecture, so that software components can be replaced, added or removed independently.

The first release of the core EUDI Wallet will be implemented as mobile apps for Google Android and Apple iOS, with the cryptographic keys stored in the mobile devices' Trusted Execution Environment (TEE). Later releases may include the possibility to develop cloud-based or hybrid applications. The EUDI Wallet reference implementation is defined by several requirements, which specifies technical details such as:

- Native app programming languages: Java, Kotlin and Swift;
- Cloud/hybrid programming techniques: HTML, JavaScript and CSS;
- Protocols: CTAP [17], DIDComm [20], Extended Access Control (EAC) [33], OAuth [47], OpenID Connect [49], and SAML [54];
- Credentials: Hyperledger AnonCreds [13], ISO 18013 (mDL) [37], and W3C Verifiable Credentials [62];

From a FIDO perspective, it is interesting to observe that the EUDI Wallet reference implementation must be able to interact with external cryptographic tokens. In the table below, FIDO/U2F, WebAuthn, and CTAP are explicitly mentioned.

Requirement ID:	**Support for external storage of cryptographic materials** **Clarification: Smartcard vs. non-physical/certificate based eID schemes**
Description	The mobile application must be able to interface and interact with cryptographic material stored externally for example on a smartcard or other remote HSM (e.g. FIDO/U2F) solutions. The interface must be based on existing standards eg. WebAuthn, CTAP, CT-API and similar The interface must be compliant with specific security requirements, standards, and certification schemes. The mobile application must be able to validate the remotely stored cryptographic material.
Comments	The mobile application does not need to alter the remotely stored cryptographic material.
Conditions	

Figure 4 – Interaction with external cryptographic tokens

3.2 Large Scale Pilots

In addition to the EUDI Wallet reference implementation, the EU has also issued a public tender for Large Scale Pilots (LSPs) to evaluate the EUDI framework under the Digital Europe Programme. The main use cases for the LSPs are as follows:

- Mobile driving license. Obviously, the ISO 18013-5 (mDL) will be the most relevant standard for this use case. The privacy aspects described in section 2.12 need to be considered for the ISO mDL deployment in the EU, so the modernized standards ISO 18013-7 and ISO 23220-4 may be used for privacy preserving purposes.
- Payments. Both offline and online payments in the Single Euro Payments Area (SEPA) will be in scope. For offline payments, the EMV protocol will be implemented in the EUDI Wallet mobile app with support for NFC and virtualized credit cards. Online payments will be implemented in accordance with the EU PSD2 directive [7]. One important aspect of the PSD2 directive is the requirement on dynamic linking, which can be fulfilled by Strong Customer Authentication (SCA) as described in the “Regulatory Technical Standards (RTS) on strong customer authentication and secure communication under PSD2” [12].
- eHealthcare. For eHealthcare, the EU Digital COVID Certificate is the most significant use case example the past years. There may, however, be other use cases in the eHealthcare sector, such as issuance of electronic prescriptions from hospitals to pharmacies, etc.
- Educational and qualifications (diploma). The educational diploma use case has been investigated as part of the eIDAS Bridge project, where qualified electronic seals were applied on diplomas in verifiable credential formats. The receiving party could validate the electronic seal on the verifiable credential and thereby trust the issuer.

There could also be other use cases, such as flight travel with ICAO DTC or eMRTD, access to government portals, check-in at hotels and conferences, etc. A number of consortia have been established with the purpose to respond to the EU public tender on LSPs. Each consortium is supposed to implement one use case with three roles: wallet issuer, credentials issuer, and relying party. These three roles must be represented in three different EU member states.

The use of the EUDI Wallet reference implementation is required, although certain extensions can be implemented as modules if necessary. Interoperability will be of the essence for the LSPs, and federation protocols such as OIDC and OAuth2 will play an important role in the EUDI Framework.

3.3 Timeline

A tentative timeline of the eIDAS2 project is illustrated below:

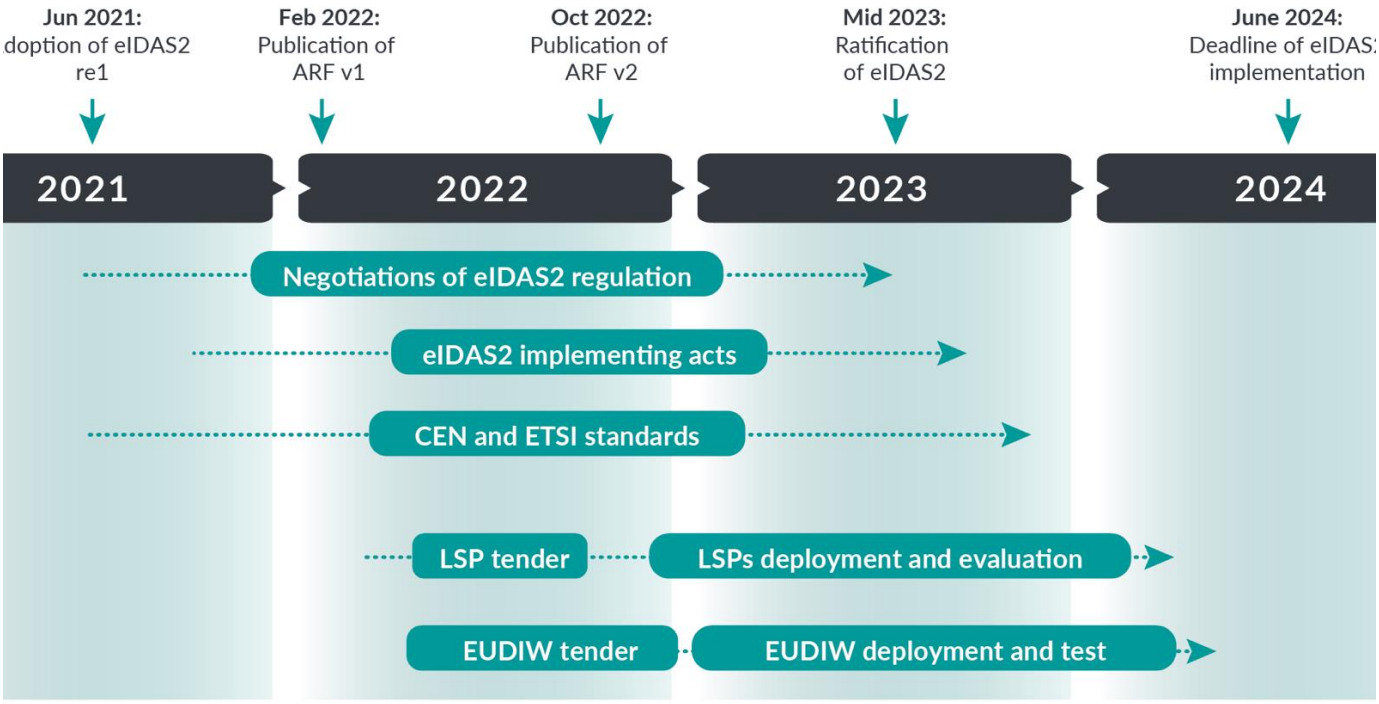

Figure 5 – Timeline for the eIDAS2 project

Note: This is a tentative timeline and may change due to political or technical reasons.

4. How FIDO Can be Used with the EUDI Wallet

This section describes how FIDO can be used with the EUDI Wallet ecosystem.

All editions of the FIDO standards – FIDO2/WebAuthn, FIDO U2F and FIDO UAF – can be used unless a specific standard is explicitly mentioned.

Where applicable, there will be references to the previous sections that outlined the general EUDI Wallet features, protocols, credentials, and APIs.

4.1 Scope of FIDO for eIDAS2

The eIDAS2 regulation [10] and the ARF [9] put forth a set of requirements that define the scope of how FIDO can be utilized within the EUDI Wallet eco-system.

The eIDAS2 proposal declares that PIDs, QCs, and QEAAs can be issued based on identification with eID means at LoA High (see sections 2.4, 2.5 and 2.6). Since FIDO based eID schemes exist at LoA High in Norway and the Czech Republic, FIDO can be used as an existing eID scheme for identification when issuing PIDs, QCs, or QEAAs.

The ARF outline mentions cloud wallets as a form factor (see section 2.3), which may be specified by a future edition of the ARF. The technical details are not yet specified by the ARF, but FIDO is a candidate to allow for authentication access to a cloud wallet.

As described in section 2.4, the ARF limits the scope of PID formats to W3C VC (with SD-JWT for selective disclosure) and ISO mDL. The PID must also be presented by OID4VP in accordance with the ISO 23220-4 standard. Hence, FIDO is out of scope as PID.

Furthermore, the ARF specifies two types of the EUDI Wallet configuration (see section 0):

- Type 1 configuration is aimed specifically at use cases where the Relying Party relies on guarantees required for the LoA High as defined in CIR 2015/150215, to enable cross border identification using PID attributes at LoA High.
- Type 2 configuration aims to enable flexibility and additional feature support for possible (Q)EAA use cases that cannot be met by Type 1 configuration (e.g., possibly in areas of health, education credentials, etc).

Since QEAAs must be issued by QTSPs, FIDO credentials are limited to the group of EAAs and their use cases. In other words, FIDO can be used with the EUDI Wallet as an EAA for access to Relying Parties at LoA Substantial. This allows for using FIDO with use cases such as authentication in the online ISO mDL flow, PSD2, etc.

The sub-sections below elaborate how FIDO can be integrated with the EUDI Wallet and be used for the use cases that are in scope.

4.2 Integrating FIDO with the EUDI Wallet

As mentioned in section 2.3, the ARF specifies the following types of cryptographic key management systems:

- Embedded Secure Element or Trusted Execution Environment (for mobile devices),
- reliance on an external device (Secure Elements / Smart Cards), and
- a backend (remote Hardware Security Module).

Hence, the FIDO authenticator can either be a platform authenticator (“trusted execution environment” or “embedded secure element”) or a roaming FIDO authenticator (“external device”). The FIDO based eIDAS eID schemes in Norway and the Czech Republic, which are recognized at LoA High, require roaming FIDO authenticators that have been certified according to FIPS 140-2, Common Criteria EAL4 + AVA_VAN.5 and/or FIDO certification at Level 2 (see section 1.1.3). FIDO platform authenticators, however, can be used at eIDAS LoA Substantial.

Since the ARF v1.0.0 specifies the EUDI Wallet as a mobile app, the mobile operating systems’ FIDO APIs are recommended for integration: Google Android FIDO2 API and Apple iOS Passkey API. If FIDO is used in conjunction with a web browser’s WebAuthn API, the design principles in the IETF RFC 8252 “OAuth2 for Native Apps” [48] can be considered.

Combining a FIDO authenticator, which is certified as an existing eID under eIDAS, with the mobile operating system’s or web browser’s WebAuthn API can result in an eID scheme at LoA Substantial or High. Hence, the EUDI Wallet may invoke the mobile operating system’s or web browser’s WebAuthn APIs [48] in order to achieve FIDO authentication to Relying Parties at LoA High.

4.3 Deployment of FIDO in the eIDAS2 Ecosystem

As described in section 2.2, there are several roles in the EUDI Wallet ecosystem: authentic source, identity verification provider, PID provider, issuers of certificates or electronic attribute attestations, relying parties, and remote qualified signature creation devices, etc. An overview of how FIDO can be used in the EUDI Wallet ecosystem is illustrated below:

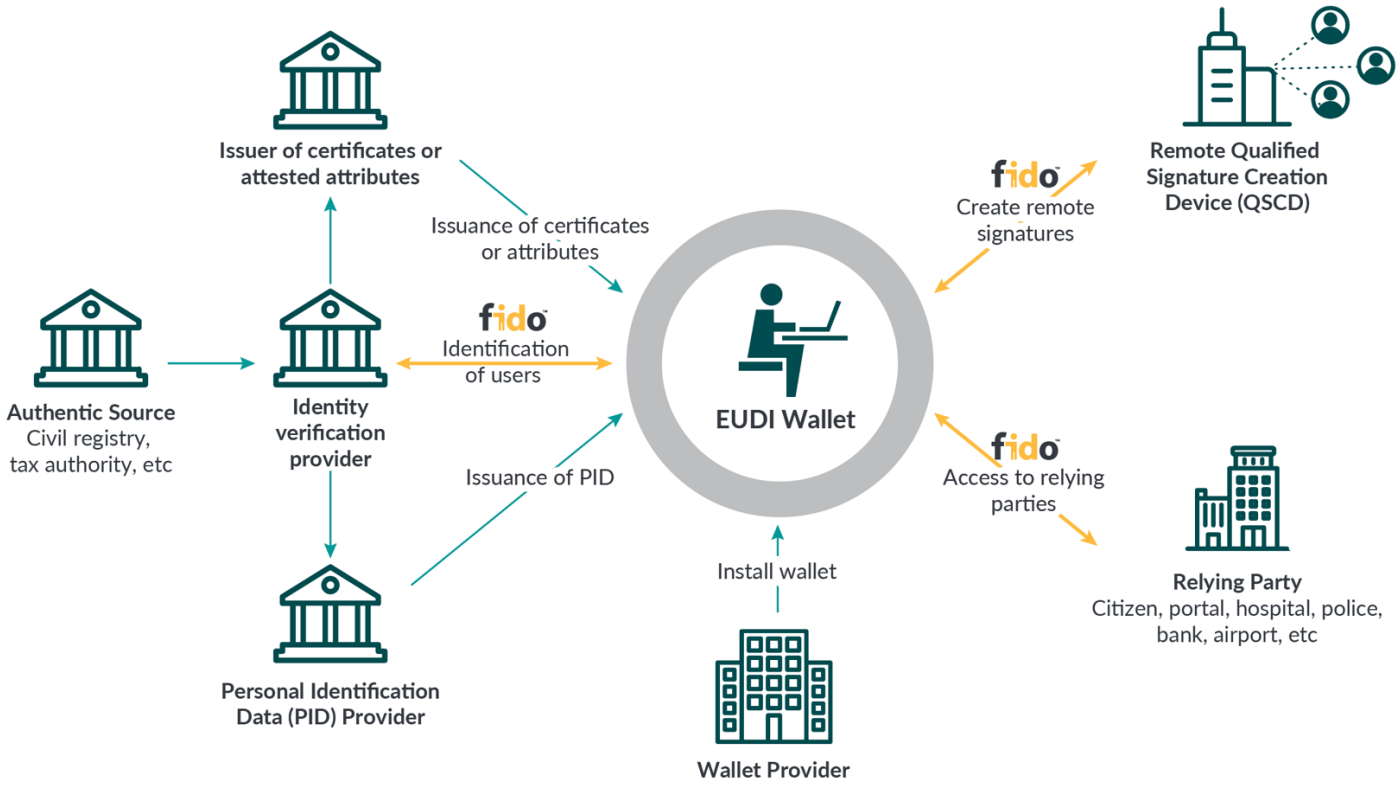

Figure 6 – eIDAS2 ecosystem with FIDO deployments

Essentially, FIDO can be used for the following scenarios in the EUDI Wallet ecosystem:

- FIDO can be used as part of an eIDAS eID scheme for authentication to an identity verification provider, which in turn can be used for onboarding of PID to the EUDI Wallet (section 4.4), issuance of qualified certificates/attestations (section 0), or issuance of short-lived Electronic Attribute Attestations (section 4.6).
- FIDO can be used for authentication and access to cloud-based hosted wallets (section 4.7).
- FIDO can be used for access to Relying Parties in several ways. One option is to use FIDO as the authentication mechanism in an OIDC flow (section 0), which allows for federated authorization to numerous Relying Parties. Two more specific use cases with Relying Parties are the ISO mDL online access (section 4.10) and PSD2 SCA compliant online payments (section 4.11).
- FIDO can be used as authentication standard for access to remote QSCDs (section 4.9).

4.4 eID Scheme for Onboarding of PID

As described in section 2.4, the user can be identified for EUDI Wallet PID onboarding by using an eID scheme at Level of Assurance (LoA) High. Furthermore, FIDO can be used as part of an existing eIDAS eID scheme at LoA High, which is described in section 1.1.3. Hence, FIDO can be used for onboarding of PID to an EUDI Wallet.

The FIDO based identification process for PID onboarding is shown below. In this illustration, FIDO is used for authentication to an identity verification provider, which may be either an integral part of the PID provider or a separate entity that identifies the user on behalf of the PID provider.

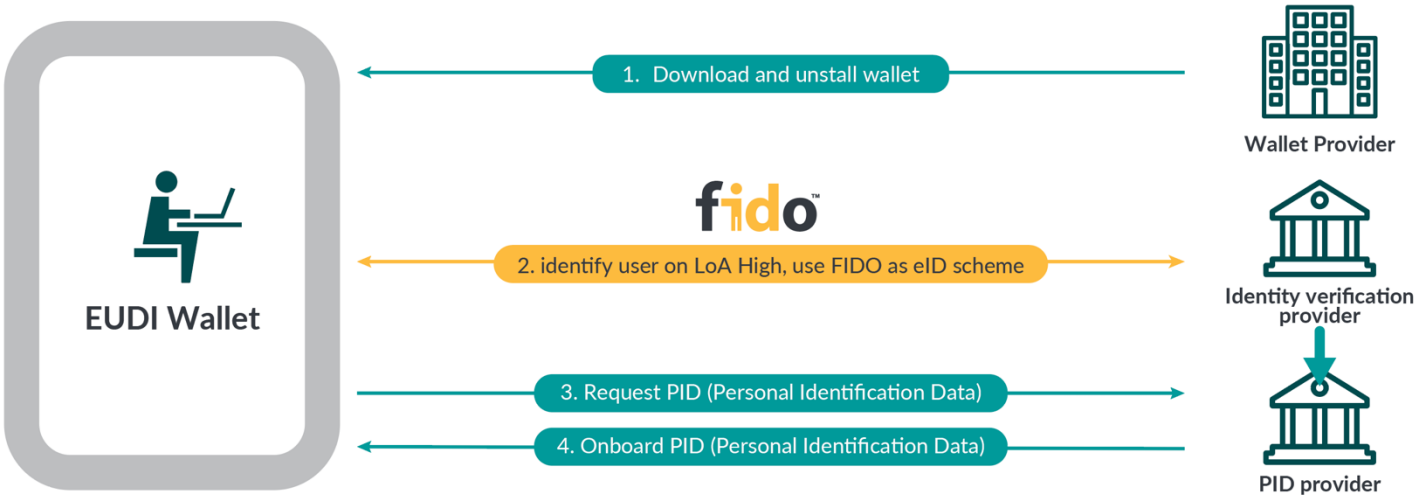

Figure 7 – PID onboarding with FIDO to the EUDI Wallet

More specifically, FIDO is used for authentication in two eID schemes that have been recognized at LoA High in the Czech Republic and Norway, so there are FIDO-based eID schemes deployed in production, which could potentially be expanded into the use case of PID onboarding to EUDI Wallets.

More details on the eID schemes in the Czech Republic and Norway, such as the FIDO authenticator certification requirements and onboarding of the users, are described in section 1.1.3.

4.5 eID Scheme for Issuance of QC or QEAA

Article 24.1.a in the eIDAS2 regulation [10] stipulates that eID schemes at LoA High can be used for identification of a user to a QTSP for the purpose of enrolling a Qualified Certificate (QC) as described in section 2.5 or a Qualified Electronic Attribute Attestations (QEAA) as described in section 2.6.

Hence, the same principle as in section 4.4 applies: FIDO can be used as part of an eID scheme at LoA High for the enrollment of QCs or QEAAs.

The FIDO-based process for identifying users for QC or QEAA enrollment is shown below. In this illustration, FIDO is used for authentication to an identity verification provider, which may be either an integral part of the QTSP or a separate entity that identifies the user on behalf of the QTSP.

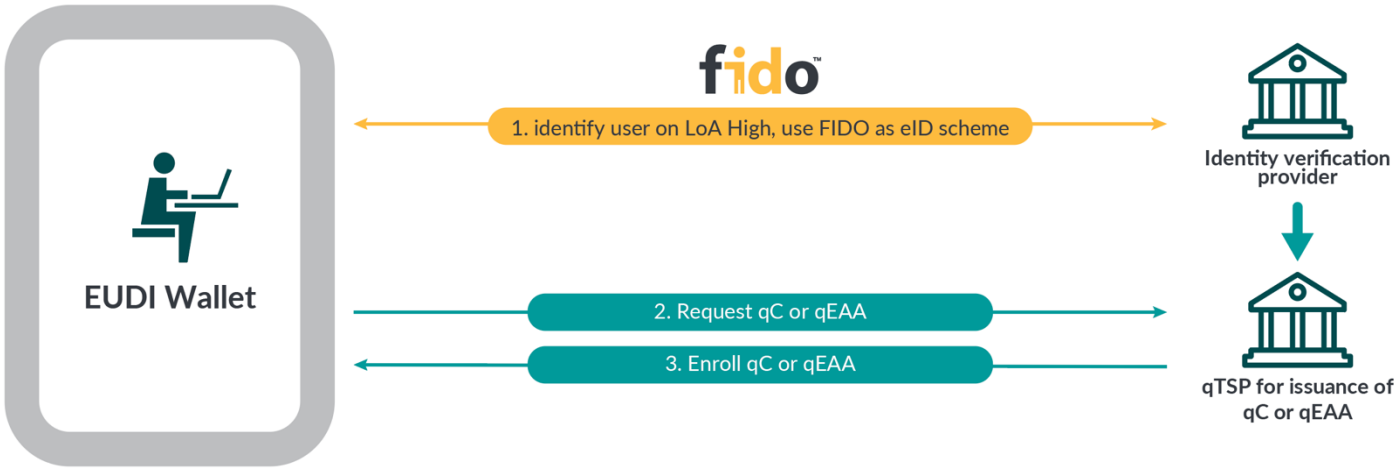

Figure 8 – qC or qEAA enrollment with FIDO to the EUDI Wallet

The enrollment protocols for issuance of QCs are typically the PKIX protocols such as CMP [16], CMC [15], or SCEP [57], while WACI-DIDComm [63] or OIDC4VCI [50] can be used for the enrollment of QEAAs; however, the details of such enrollment protocols go beyond the scope of this white paper.

4.6 Issuance of Short-Lived EAA for Selective Disclosure

Selective disclosure is an important aspect of the EUDI Wallet architecture. As described in section 2.11, one alternative to implement selective disclosure is to enroll for short-lived (qualified) Electronic Attribute Attestations (qEAAs) with atomic claims, which can be combined in a verifiable presentation. In other words, such solution for selective disclosure is special case of enrollment of qEAAs according to the principles in section 0.

FIDO is well-suited for designing such a solution, since FIDO can be used for the authentication mechanism of the eID scheme used for identification to the qTSP(s) that issues the EAAs. More specifically, each Identity Verification Provider could deploy a FIDO Relying Party, for which the users' FIDO credentials are configured. When the user needs to enroll the short-lived EAAs, the EUDI Wallet will use FIDO for authentication to the Identity Verification Provider, such that the qTSPs can rely upon this identification for issuance of an EAAs to the users' EUDI Wallets.

Such a FIDO based solution for selective disclosure is illustrated below:

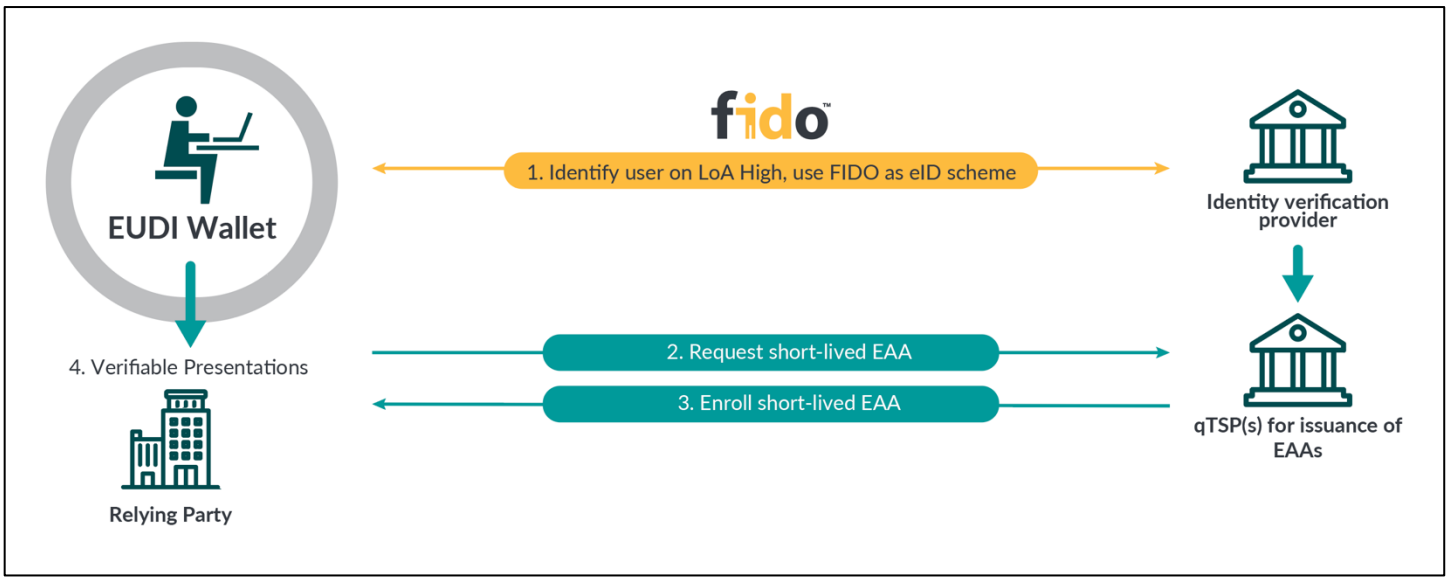

Figure 9 – Enrollment with FIDO of short-lived EAAs for selective disclosure

Kent University has designed and implemented a solution called the VC-FIDO integration, which utilizes multiple FIDO credentials to enroll for short-lived Verifiable Credentials that are combined in a Verifiable Presentation. Technically, the WebAuthn stack is integrated with the Verifiable Credentials enrollment protocol, resulting in a client that can rapidly enroll for multiple atomic short-lived Verifiable Credentials based on Credential templates. These atomic short-lived Verifiable Credentials can be combined into a Verifiable Presentation that is presented to the verifier. It is possible to migrate the VC-FIDO client and the Credential templates to another device given that the FIDO credentials are roamed as well to the new device, for example, by using FIDO passkeys.

The VC-FIDO integration was presented by David Chadwick at SHACK2020. This presentation explains the VC-FIDO architecture diagrams and shows a demo of how the client enrolls for three atomic Verifiable Credentials (address, driving license, and credit card) that are combined into a Verifiable Presentation as a parking ticket. The team at Kent University has also implemented a prototype based on this design and deployed it as a pilot at National Health Services (NHS) in the UK.

4.7 Access to Hosted Wallets

According to the ARF outline, one of the form factors of the EUDI Wallet is a hosted wallet (also known as cloud wallet, web wallet, or remote wallet). A hosted wallet (section 2.3) is a secured cloud or web service that is hosting the users' qEAAs and private keys, which are associated with the credentials of an authentication protocol that the user can utilize for accessing its wallet and qEAAs/keys.

Hence, the complexity of the credential and key management is outsourced to a hosted wallet, so the user only needs a mobile device or desktop computer with a web browser that supports the authentication protocol. There are other benefits with a hosted wallet: the credentials/certificates are protected in the hosted wallet that makes recovery easy if the device is lost or changed, upgrades can be performed centrally at the cloud provider, the security level is guaranteed by the HSM at the hosted wallet, there are synergy effects with backend integrations with QTSPs, etc.

Although a hosted wallet is described as a form factor in the ARF outline, it is not yet technically specified by the ARF v1.0.0. A future version may describe the hosted wallet form factor in more detail.

FIDO is a viable authentication standard for accessing hosted wallets, and is therefore a suitable candidate for providing secure access in a future version of the ARF.

First, the users will register their FIDO credentials at their hosted wallet, and then they can use their devices with standard web browsers that invoke the WebAuthn API by JavaScript or React. A FIDO based solution for accessing hosted wallets is illustrated below:

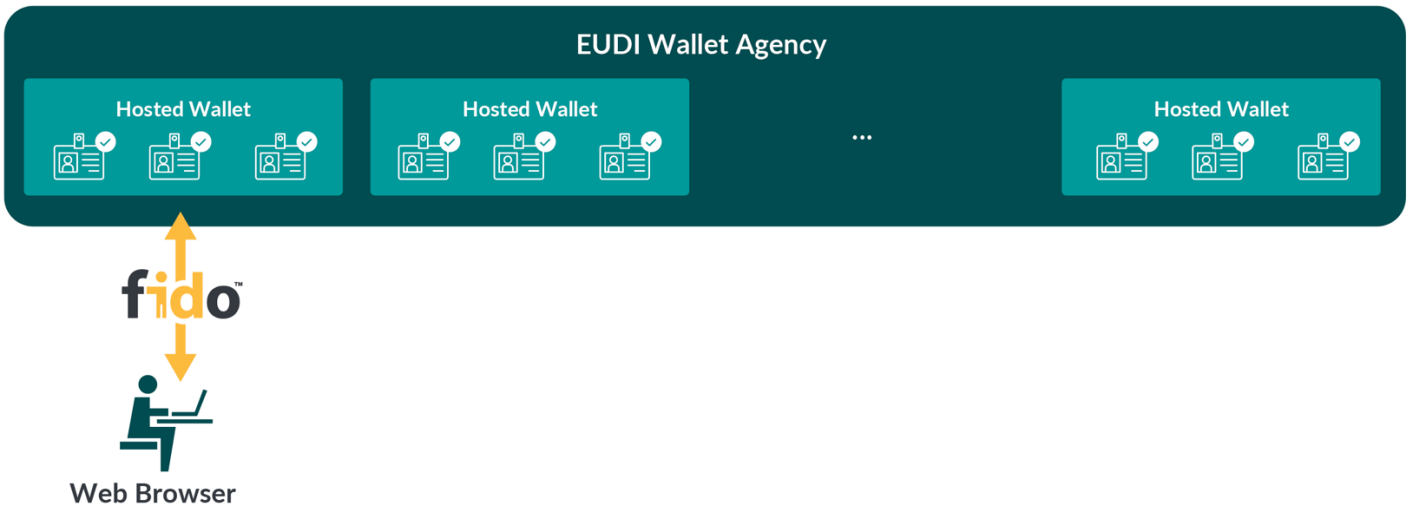

Figure 10 – Access to hosted wallet with FIDO

The Findy Agency is an open-source project that developed a Hyperledger Aries compatible identity agent service based on the Hyperledger Indy SDK Wallet [74]. The Findy Agency hosted wallet can be used by individuals and exposes an API for organizations to utilize functionality related to verified data exchange such as issuing, holding, verifying, and proving credentials. Access to the Findy Agency from the user's device is performed with FIDO2/WebAuthn authentication.

The Findy Agency architecture is divided in two server layers:

- The Agency, which is comprised of the Authentication service (that registers and authenticates all users with FIDO2/WebAuthn), the Agent service (that handles the Aries protocols), and the Vault service (that maintains a database of agents' data).
- The Service Agent(s), which are applications integrated in the backend of the Agency that handle verified data. Also, the backend calls from the Agency to the Service Agents are authenticated with FIDO2/WebAuthn.

There is also potential synergy of FIDO-based hosted wallets with Multi-Device FIDO Credentials [70], since all credentials in such a scenario will be hosted at cloud service providers: the wallet provider will host the Multi-Device FIDO Credentials, and the hosted wallet (as FIDO Relying Party) will protect the qEAAs that are associated with the FIDO credentials. This will allow for rapid recovery of a wallet since the user can first download the Multi-Device FIDO Credentials to a device, and then use the FIDO credentials for getting access to the hosted wallet.

4.8 Interoperability

Interoperability is an important aspect of the EUDI Wallet, in order to ensure that the clients using the EUDI Wallet can get access to a wide range of Relying Parties across the EU.

As mentioned in section 1.2.1, the SAML v2 protocol is used as federation standard for the eIDAS-Nodes under the eIDAS regulation (EU 910/2014). However, there are performance and scalability issues with SAML v2 [54], so the EUDI Wallet ARF and the Large Scale Pilots may need modernized protocols for delegated authorization instead.

The ARF v1.0.0 does not explicitly define federations or delegated authorization, but two viable candidates for delegated authorization are OAuth2 [47] and OpenID Connect (OIDC) [49].

OAuth2 and OIDC requires the user to be authenticated to the Authorization Server. The standards do not specify what user authentication protocol to use, so there are a wide range of implementations using different authentication standards.

FIDO is well-suited to be used as authentication standard for the OAuth2 and OIDC federation protocols, which is described in the FIDO Alliance white paper “Integrating FIDO & Federation Protocols” [70]. Below, there is an illustration of how FIDO can be used with the OAuth2 or OIDC protocols.

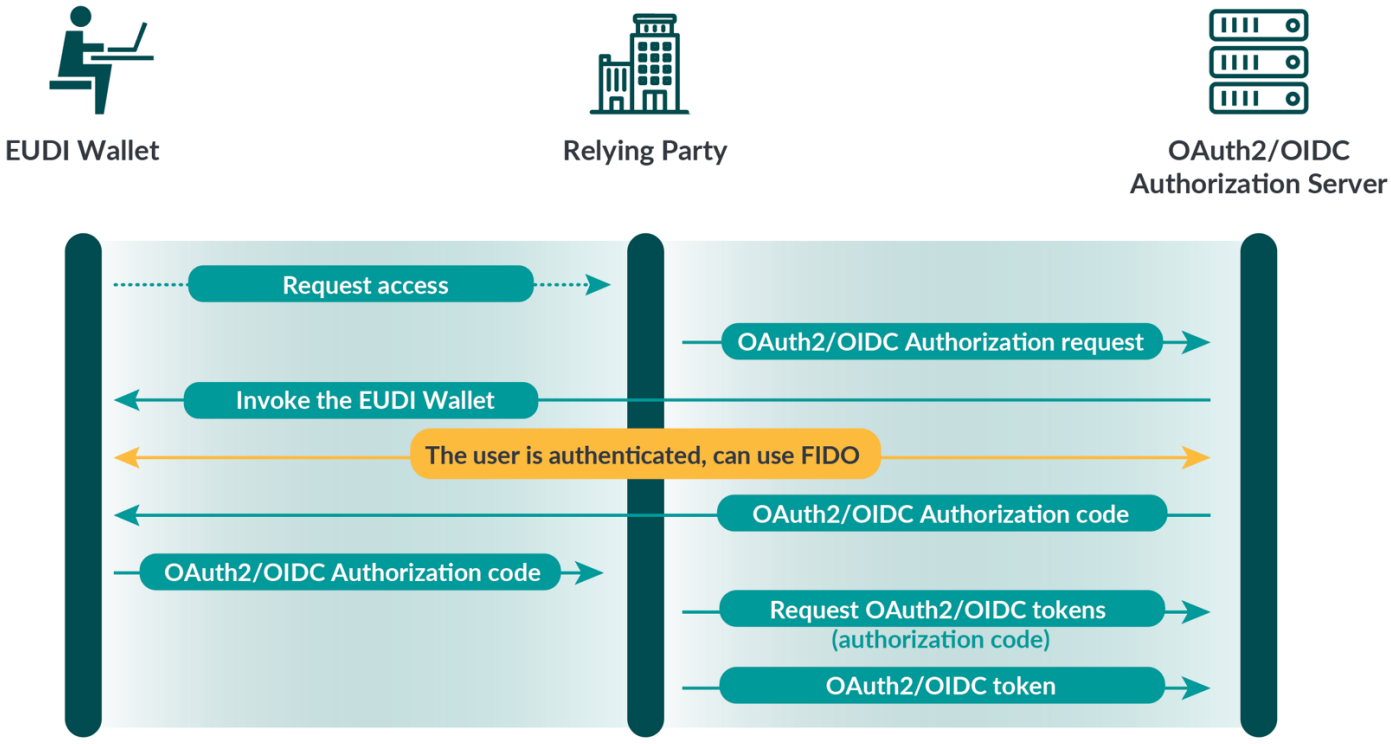

Figure 11 – Authentication with FIDO for OIDC/OAuth2

In the example shown above, FIDO is used with OAuth2/OIDC in authorization code flow, but other flows of OAuth2/OIDC could also be considered.

In brief, an OAuth2 access token is issued by the Authorization Server to grant the user access to protected resources at the Relying Party, while in the case of OIDC it is the Relying Party that requests the Authorization Server for an OIDC ID Token with additional information of the user.

In the next two sections, there are practical use case examples of how to use OAuth2 for getting access to a remote signing service, and OIDC for requesting online selective user claims for the ISO mobile driving license.

4.9 Access to Remote QSCD

The EUDI Wallet will also have the capability of accessing QTSPs that operate remote Qualified Signature Creation Devices (QSCDs) for creating Qualified Electronic Signatures (QES) on behalf of the users. As described in section 0, the QTSP will operate a Signature Activation Module (SAM) that authenticates the user based on Signature Activation Data (SAD), which in turn can be used for activating the user's private key in the remote QSCD and thereby creating a QES.

In the FIDO Alliance white paper "Using FIDO with eIDAS Services" [72], there is a comprehensive description of how to use FIDO as authentication standard for access to SAM on SCAL2 (Sole Control Access Level 2). Below is an illustration of how FIDO can be used for access using an EUDI Wallet with an embedded CEN Signer Interface to a QTSP that operates a remote QSCD; in this scenario, FIDO is used as Signature Activation Protocol (SAP) to create the SAD, which is used for getting access to the SAM and the remote QSCD. In order to reach eID at LoA High when accessing the SAM, the EUDI Wallet needs to invoke a system browser's WebAuthn API (4.2) using a roaming FIDO authenticator that is certified as eID at LoA High (see section 1.1.3).

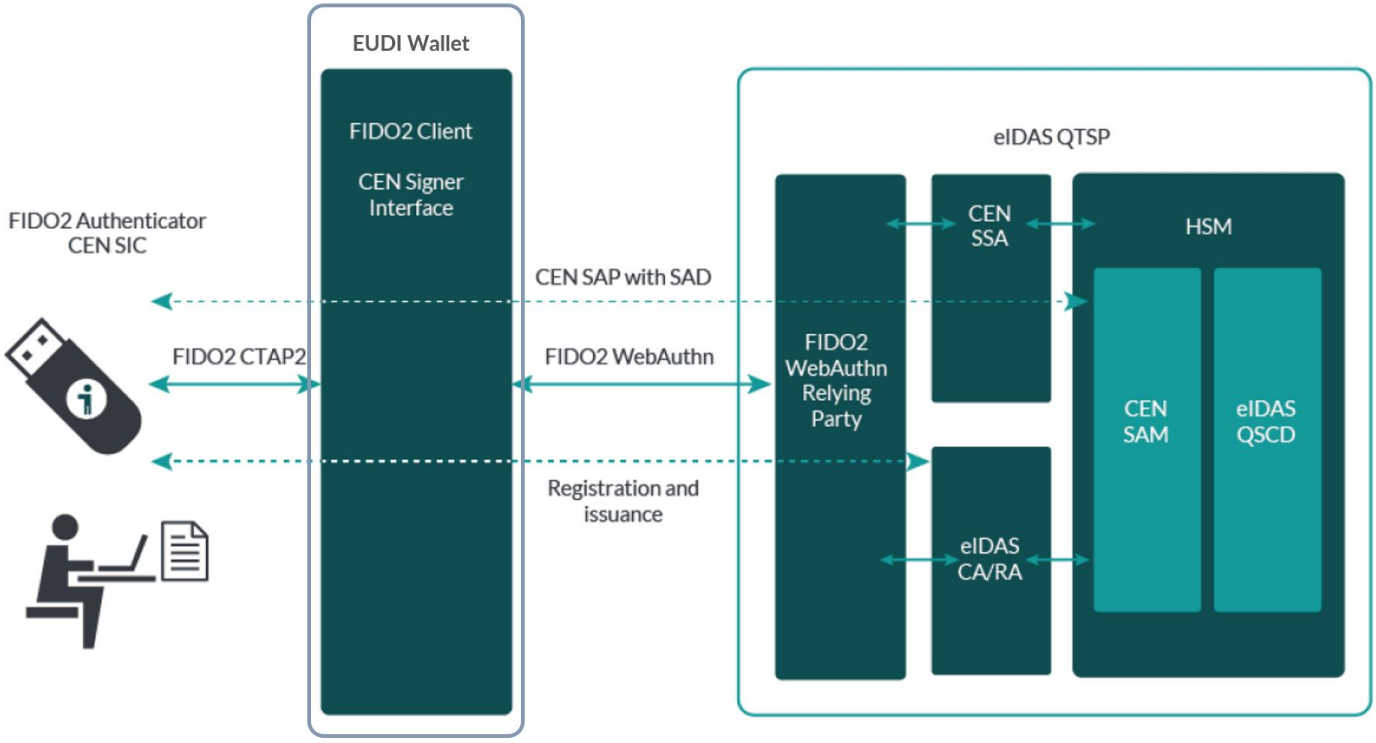

Figure 12 – Using FIDO for access to remote QSCD

The Cloud Signature Consortium (CSC) has developed a protocol that allows for a separate OAuth2 Authorization Server to authenticate the user and issue an OAuth2 Access Token. How to use FIDO in such a scenario is illustrated below:

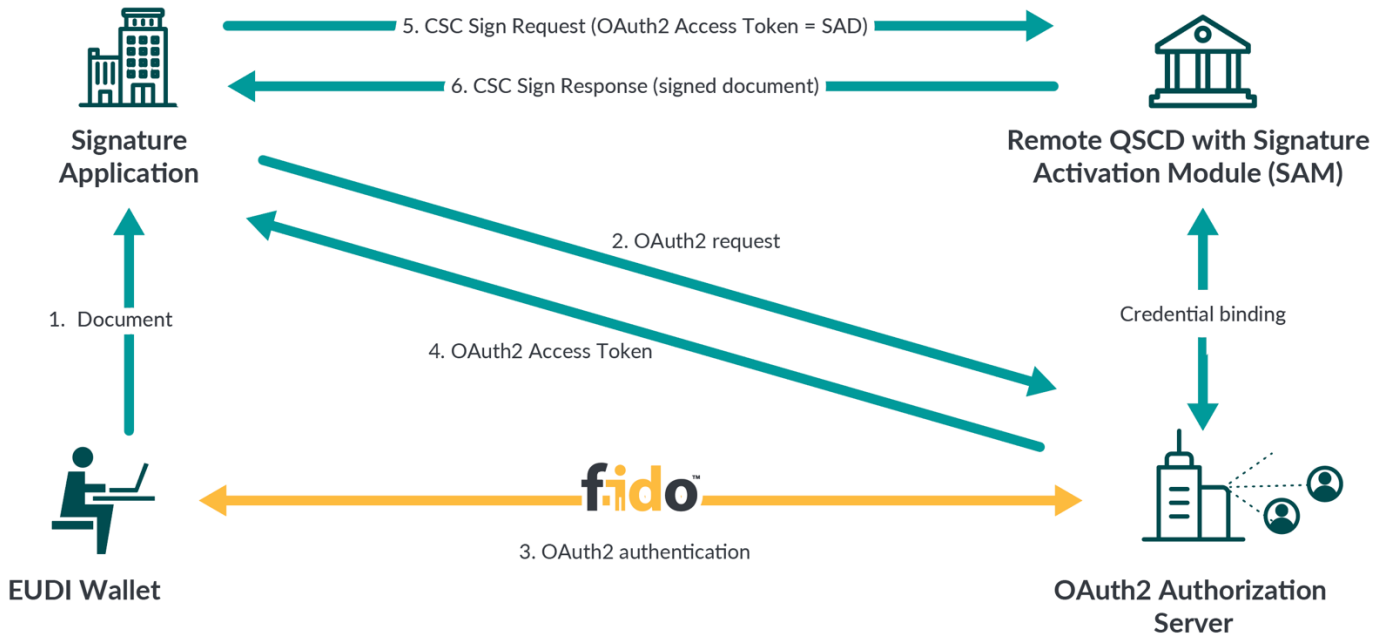

Figure 13 – Using FIDO with the CSC API

In the case of the CSC API, FIDO is the authentication standard between the EUDI Wallet and the OAuth2 Authorization Server, which issues an OAuth2 access token that also serves the purpose of a SAD for getting access to the SAM and the backend remote QSCD.

4.10 ISO Mobile Driving License

The mobile driving license is a prioritized use case for the EUDI Large Scale Pilots (see section 3.2). The dominating standard in this regard is ISO/IEC 18013-5:2021 “ISO-compliant driving licence - Part 5: Mobile driving licence (mDL) application” [37]. The ISO mDL application is implemented in Apple iOS and Google Android and is deployed in production across the globe, for example in Utah and Arizona in the US. The ISO mDL application can be used for offline identification, online identification, or a hybrid combination of offline initialization and online identification.

The ISO mDL online identification process is performed with the ISO mDL WebAPI or OpenID Connect (OIDC). Essentially, the ISO mDL reader/verifier connects online over OIDC or the WebAPI to the mDL issuer’s authorization server to request claims about the user. The users need to give their consent for the mDL issuer to release the claims to the verifier; in order to do so, the user needs to authenticate to the authorization server, review the request from the reader/verifier, and accept to release certain claims. This way, online selective disclosure of claims is designed in the ISO 18013-5 standard.

The authentication process between the user's EUDI Wallet and the mDL issuer's authorization server can be implemented by using FIDO as authentication standard, which is illustrated below:

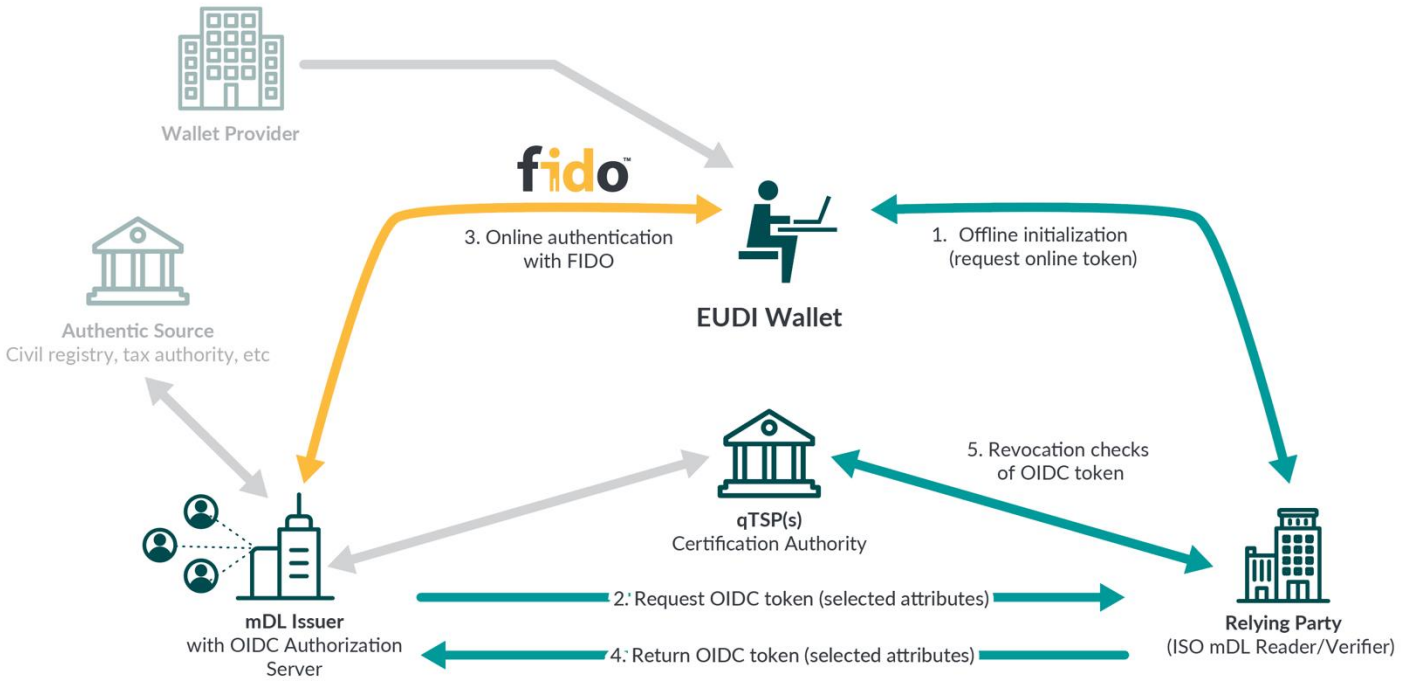

Figure 14 – Using FIDO with the ISO 18013-5 (mDL) online flow

However, the eIDAS2 regulation [10] includes Article 6a.7, which declares that "the issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services" (see section 2.12). This requirement is a bit challenging for the ISO mDL online checks since the verifier needs to connect to the mDL issuer's authorization server. This is not perfect from a privacy perspective, but there is also the disclaimer in the eIDAS2 Article 6a.7 that the user could expressly request to release claims to the issuer's authorization server if necessary for the EUDI Wallet operations. So the EUDI Wallet will accept ISO 18013-5 for legacy and interoperability reasons, and FIDO will be a viable authentication standard for this use case.

A privacy enhancement that is planned for the ISO mDL standard is to use OIDC4VP [51] in conjunction with SIOP2 [56], whereby selected claims of a credential is presented by the user to the verifier without the involvement of the issuer. The draft standards ISO 23220-4 and ISO 18013-7 will be based on OIDC4VP and SIOP2 for this purpose.

In this scenario, FIDO can be used as authentication standard if the EUDI Wallet is hosted at a cloud-based service, which is shown below.

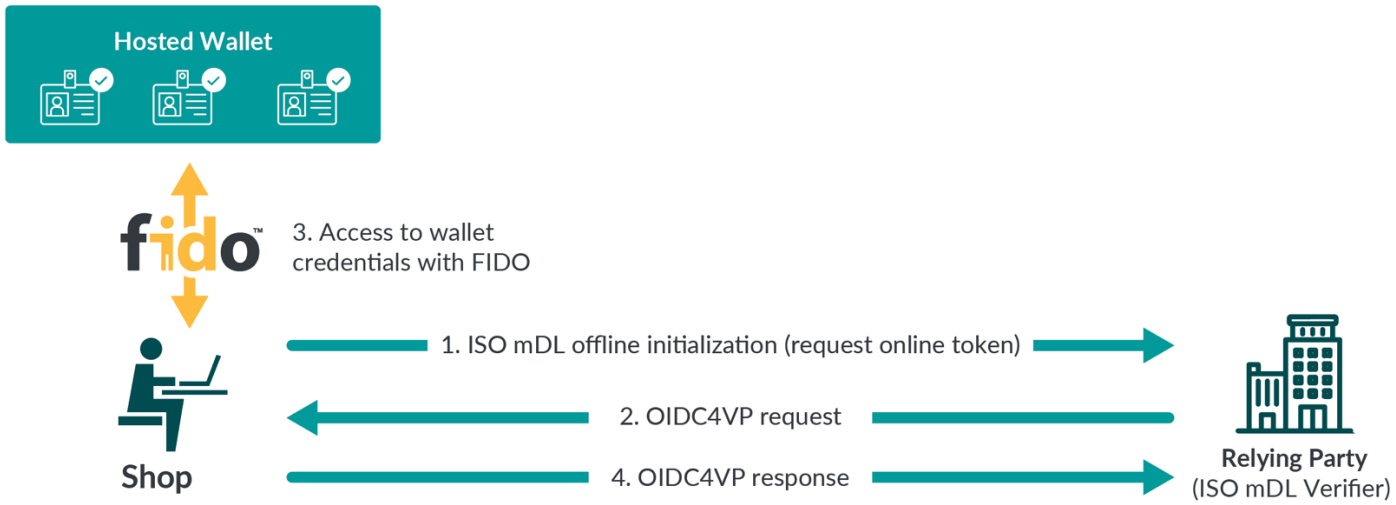

Figure 15 – Using FIDO with the ISO 23220-4 flow

More specifically, the SIOP2 app that is running at the user's EUDI Wallet will connect over FIDO to the hosted wallet in order to get access to its centrally stored credentials.

4.11 Compliance with PSD2 for Online Payments

One of the most important and complex use cases for the EUDI Wallet Large Scale Pilots is payments (see section 3.2). In essence, the payments use case can be divided into Point of Sales (PoS) payments at physical stores and online payments to web merchants, both operating in the Single Euro Payments Area (SEPA).

For PoS payments, the EUDI Wallet may contain the user's virtualized credit cards, which can be used for payments over the EMV protocol by tapping the phone to a PoS cashier reader over NFC.

The online web payments use case is regulated by the EU PSD2 directive [7]. One important aspect of the PSD2 directive is the requirement on dynamic linking, which can be fulfilled by Strong Customer Authentication (SCA) as described in the "Regulatory Technical Standards (RTS) on strong customer authentication and secure communication under PSD2" [12]. What this means in practice is that the Payment Service Provider, which serves the merchant for online payments, sends the financial transaction to the user's device, which displays the information so the user can sign it. Technically, online payment solutions are implemented based on systems such as 3D-Secure v2 (3DS2), which are designed to be compliant with PSD2.

As illustrated below, FIDO can be used for online payment solutions that comply with the PSD2 requirement on dynamic linking in conjunction with RTS SCA.

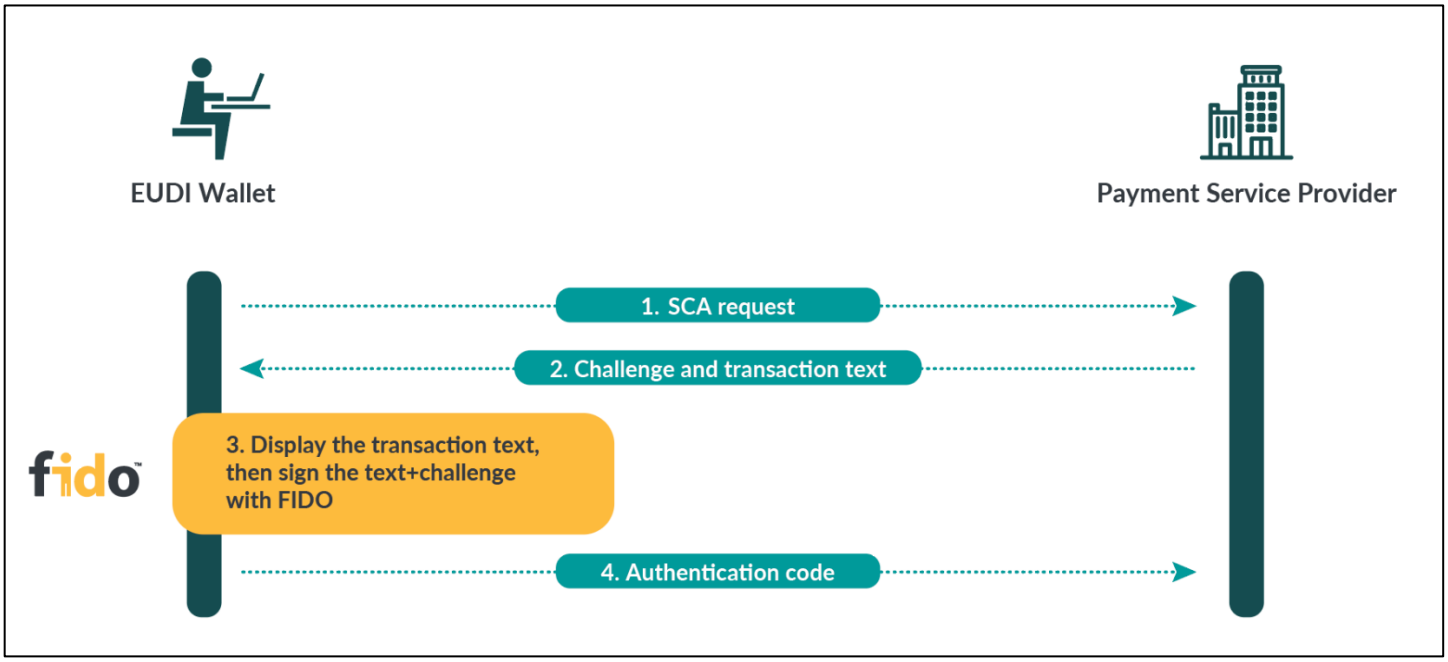

Figure 16 – Using FIDO with PSD2 Strong Customer Authentication

The FIDO Alliance white paper “FIDO for PSD2 - Providing for a satisfactory customer journey” [69] is recommended for further reading on this subject.

Furthermore, W3C has published the specification “Secure Payment Confirmation” [53], which uses the WebAuthn Extension “payment" to sign the web payment transaction with FIDO.

5. Why Use FIDO for the EUDI Wallet?

5.1 The FIDO Alliance

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, who are listed at the FIDO Alliance membership website, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO Authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today the FIDO standards are being used across government and industry to deliver authentication that is more secure, better able to protect privacy, and easier to use; FIDO Authentication is increasingly being embraced by every sector as the preferred way to deliver high-assurance MFA to consumers.

The FIDO Alliance's work to standardize the use of on-device biometric matching coupled with public key cryptography has transformed the identity and authentication market, creating a standards-based alternative to legacy authentication tools such as central-match biometric systems, OTPs, and traditional PKI X.509 digital certificates.

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

5.2 FIDO is a Global Standard Supported by Every Major Platform

Over the last eight years, the FIDO Alliance has delivered a comprehensive framework of open industry standards for MFA that addressed significant security and usability shortcomings in previous MFA tools, and that provide practitioners with new options for crafting digital identity solutions.

FIDO standards have delivered improvements in online authentication by means of open, interoperable technical specifications that leverage proven public key cryptography and on-device match of biometrics for stronger security and device-based user verification for better usability. The impact of FIDO standards, and formal certification testing to those standards, is notable:

- Leading firms in banking, payments, fintech, insurance, technology, telecommunications, health, and cloud services have deployed authentication solutions based on FIDO standards. In total, FIDO solutions are available to protect more than 4 billion accounts worldwide.
- Governments around the world that are either using FIDO today for citizen identity or have announced plans to modernize citizen identity systems around a FIDO-centric architecture include South Korea, Thailand, Taiwan, the United Kingdom, Australia, and the United States. In addition, the governments of France, the United States, Australia, South Korea, Taiwan, and the United Kingdom have all explicitly recognized FIDO standards in their own digital identity and authentication guidance to organizations in those countries. Lastly, FIDO is approved as part of eIDAS eID schemes on LoA High or Substantial in the EU (see section 1.1.3).
- The W3C has formalized the Web Authentication API (WebAuthn) [64] as part of the FIDO2 standards. This standard enables FIDO functionality to be embedded in major browsers (i.e. Chrome, Edge, Firefox, Safari, Opera) – meaning that FIDO-standard MFA can be deployed for any web application without any significant burden on the part of an implementer.
- The ITU has formally adopted the FIDO specifications as standards, through ITU X.1277 (FIDO Universal Authentication Framework) [65] and ITU X.1278 (FIDO Client to Authenticator Protocol (CTAP)/Universal 2 factor Framework) [66].
- More than 850 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.
- Core device platforms have also become FIDO® Certified; nearly every commercially available smartphone and laptop on the market today ships with support for FIDO Authentication built in, and FIDO is also supported natively into browsers. This means that neither implementers nor their customers need to buy a separate technology to enable MFA.

6. Conclusions

The maturity of the FIDO standard and its wide implementation by the major smartphone and laptop vendors cater for successful technical deployments with the EUDI Wallet ecosystem. Furthermore, FIDO has been certified under eIDAS (EU 910/2014) as part of eID schemes on LoA High and Substantial in the Czech Republic and Norway, which proves that FIDO is compliant with the eIDAS regulation in the EU.

As discussed in section 0, the EUDI Wallet PID must be an ISO mDL or W3C VC formatted credential, which must be presented over OID4VP according to ISO 23220-4. Hence, FIDO is out of scope as PID, which is used in the Type 1 configuration of the EUDI Wallet.

FIDO is, however, well-suited as an authentication standard for the Type 2 configuration EUDI Wallet, which allows EAAs to be used for access to Relying Parties. The strong combination of being a widely adopted technical standard and compliant to the eIDAS regulation, FIDO can be used for several use cases with the EUDI Wallet, which are illustrated below.

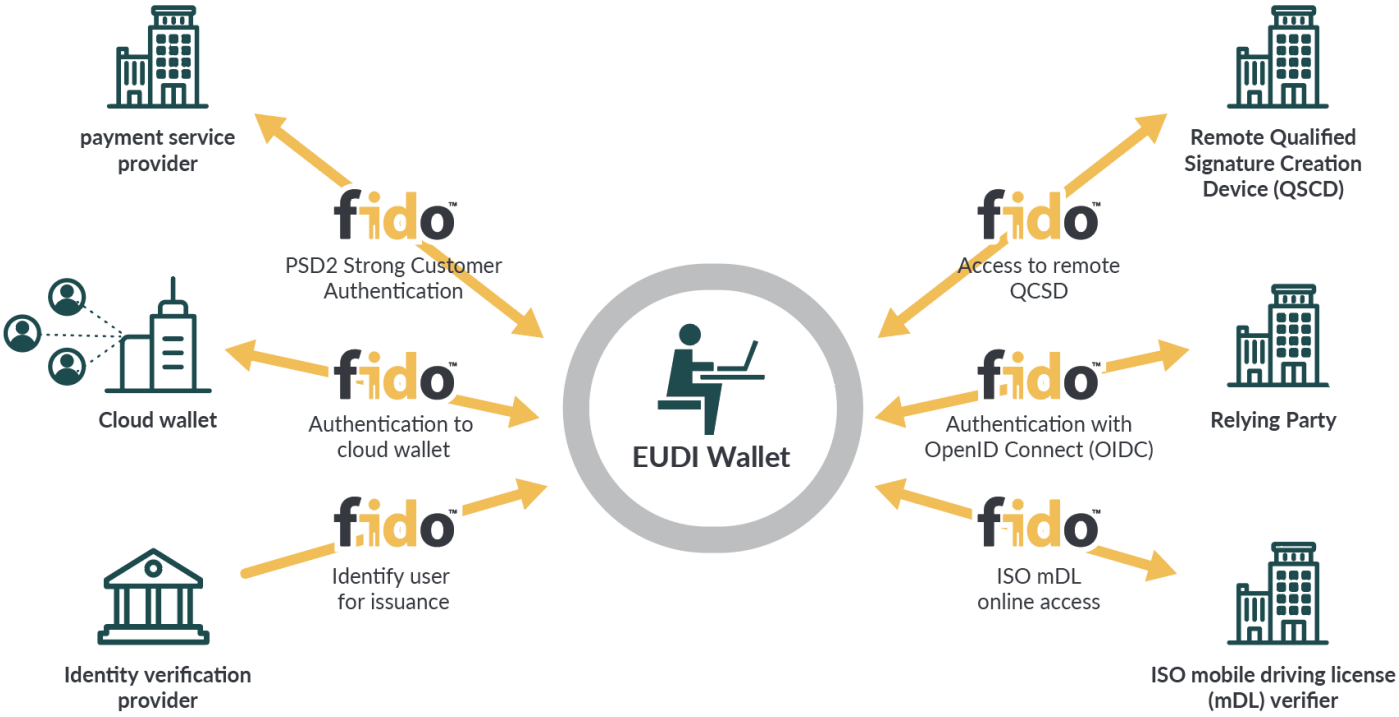

Figure 17 – FIDO use cases for the EUDI Wallet

To conclude, FIDO can be used as authentication standard for the following use cases in the EUDI Wallet ecosystem:

- eID scheme for onboarding of Person Identification Data (PID): FIDO can be used as part of an eID scheme on LoA High for enrollment of PID the EUDI Wallet in accordance with eIDAS2 Article 6a.6 and eIDAS2 Article 6a.4.e (see section 4.4).
- eID scheme for issuance of Qualified Certificates (QCs) or Qualified Electronic Attribute Attestations (QEAAs): FIDO can be used as part of an eID scheme on LoA High for identification to a Qualified Trust Services Provider (QTSP) as issuer in accordance with eIDAS2 Article 24.1.c (see section 0).

- Issuance of short-lived Electronic Attribute Attestations (EAAs) for selective disclosure: This is a special case where FIDO is used for identification when issuing short-lived EAAs that can be combined in a verifiable presentation (see section 4.6).
- Access to hosted wallets: This is a form factor that is described in the ARF outline but is not yet specified in the first version of the ARF. When/if the EUDI Wallet can be deployed as a hosted wallet at a cloud-based service provider, FIDO is a viable candidate to be used as an authentication standard for getting access to the centrally stored qEAAs (see section 4.7).
- OAuth2 and OpenID Connect (OIDC) for access to relying parties: FIDO can be used as authentication standard for the authorization protocols OAuth2 and OIDC, which may be used under eIDAS2 for federation of relying parties across the EU (see section 0).
- Access to remote Qualified Signature Creation Device (QSCD): When the users' Qualified Certificates and keys are protected in a remote QSCD, FIDO can be used as authentication standard for sole control access to a Signature Activation Module that protects the remote QSCD (see section 4.9). In order to reach eID LoA High for this use case, existing FIDO based eID schemes (such as a roaming FIDO authenticator being used with WebAuthn in a system browser) may be invoked by the EUDI Wallet.
- ISO Mobile Driving License (mDL): The ISO mDL online verification checks based on OIDC or the ISO WebAPI can utilize FIDO when the user authenticates to the issuer's authorization server to release the mDL claims (see section 4.10).
- Compliance with PSD2 for online payments: FIDO can be used as authentication standard in compliance with the PSD2 requirement on dynamic linking in conjunction with Strong Customer Authentication (see section 4.11).

Hence, FIDO is already compliant under the existing eIDAS regulation and has the potential to continue to expand its use cases under eIDAS2.

7. Acknowledgments

The authors acknowledge the following people (in alphabetic order) for their valuable assistance, feedback, and comments:

- Adrian Loth, FIDO Alliance
- Alain Martin, Thales
- Alban Feraud, Idemia
- Andrew Shikiar, FIDO Alliance
- Arshad Noor, Strongkey
- Carmen Schwarzenbeck, IDnow
- David Turner, FIDO Alliance
- Derek Hanson, Yubico
- Dirk Balfanz, Google
- Frank-Michael Kamm, Giesecke+Devrient
- Jeremy Grant, Venable
- John Bradley, Yubico
- Lee Campbell, Google
- Megan Shamas, FIDO Alliance
- Mike Jones, Microsoft
- Mindy Souza, FIDO Alliance
- Paul Bastian, Bundesdruckerei
- Peter Altmann, Digitaliseringsmyndigheten
- Pieter Kasselman, Microsoft
- Rayissa Armata, IDnow
- Teresa Wu, Idemia
- Tim Cappalli, Microsoft
- Tobias Looker, MATTR
- Torsten Lodderstedt, Yes.com
- Vittorio Bertocci, Okta

8. Glossary of Terms

Term	Definition
3DES2	3D-Secure v2
AES	Advanced Electronic Signature
API	Application Programming Interface
ARF	Architecture Reference Framework
ASN.1	Abstract Syntax Notation no 1
AVA_VAN	Advanced Methodical Vulnerability Analysis
CA	Certification Authority
CC	Common Criteria
CEN	European Committee for Standardization
CID	Commission Implementing Directive
CL	Camenisch-Lysyanskaya
CMC	Certificate Management messages over CMS
CMP	Certificate Management Protocol
CMS	Cryptographic Message Syntax
COVID	Coronavirus Disease
CP	Certificate Policy
CPS	Certificate Practice Statement
CSC	Cloud Signature Consortium
CSS	Cascading Style Sheets
CTAP	Client to Authenticator Protocol
DER	Distinguished Encoding Rules
DID	Decentralized Identifier
DIDComm	DID Communication protocol
DIF	Decentralized Identity Foundation
DSS	Digital Signature Service
DTC	Digital Travel Credential
EAA	Electronic Attribute Attestation
EAL	Evaluation Assurance Level
eID	Electronic Identity
eIDAS	electronic IDentification, Authentication and trust Services
eMRTD	Electronic Machine Readable Travel Document
EMV	Europay, Mastercard, and Visa
EN	European Norm
ENISA	EU Cybersecurity Agency
ESSIF	European Self Sovereign Identity Framework
ETSI	European Telecommunication Standardization Institute
EU	European Union
EUCC	European Union Cybersecurity Certification
EUDI	European Digital Identity
EUDIW	European Digital Identity Wallet
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTML	Hypertext Markup Language
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
JSON-LD	JSON for Linking Data
JWT	JSON Web Token
LoA	Level of Assurance

LSP	Large Scale Pilot
mDL	Mobile Driving License
MDOC	Mobile Driving License Document
MFA	Multi Factor Authentication
MSO	Mobile Security Object
NFC	Near Field Communication
NHS	National Health Services
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
OIDC	OpenID Connect
OIDC4VCI	OpenID Connect for Verifiable Credentials Issuance
OIDC4VP	OpenID Connect for Verifiable Presentations
OTP	One Time Password
PC	Personal Computer
PID	Person Identification Data
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PoS	Point of Sales
PQC	Post Quantum Cryptography
PSD2	Payment Services Directive v2
QEAA	Qualified Electronic Attribute Attestation
QES	Qualified Electronic Signature
QC	Qualified Certificate
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RTS	Regulatory Technical Standard
SAD	Signature Activation Data
SAM	Signature Activation Module
SAML	Security Assertion Markup Language
SAP	Signature Activation Protocol
SCA	Strong Customer Authentication
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SD-JWT	Selective Disclosure JWT
SEPA	Single European Payment Area
SIC	Signer's Interaction Component
SIOP	Self-Issued OpenID Provider
SOG-IS	Senior Officials Group Information Systems Security
SSA	Signature Server Application
SSCD	Secure Signature Creation Device
SSI	Self-Sovereign Identity
TC	Technical Committee
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOTP	Time-based One Time Password
TS	Technical Standard
TSP	Trust Service Provider
U2F	Universal Two-Factor
VC	Verifiable Credential
W3C	World Wide Web Consortium
WACI	Wallet and Credential Interaction
XML	Extensible Markup Language
ZKP	Zero Knowledge Proof

9. References

9.1 Legal references

[1] "Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework." European Commission. September 2015. https://eur-lex.europa.eu/eli/reg_impl/2015/1501/oj.

[2] "Commission Implementing Regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means." European Commission. September 2015. https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

[3] "Commission Implementing Decision (EU) 2015/1505 laying down technical specifications and formats relating to trusted lists." European Commission. September 2015. https://eur-lex.europa.eu/eli/dec_impl/2015/1505/oj.

[4] "Commission Implementing Regulation EU 2015/1506 on laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies." European Commission. September 2015. https://eur-lex.europa.eu/eli/dec_impl/2015/1506/oj.

[5] "Commission Implementing Decision (EU) 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices." European Commission. April 2016. https://eur-lex.europa.eu/eli/dec_impl/2016/650/oj.

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

[7] "Directive (EU) 2015/2366 of the European Parliament of the Council on payment services in the internal market." European Commission. November 2015. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

[8] "European Digital Identity Architecture and Reference Framework (ARF) Outline." eIDAS Expert Group. February 2022. https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/73759/download.

[9] "European Digital Identity Architecture and Reference Framework (ARF) v1.0.0." eIDAS Expert Group. February 2023. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[10] "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." European Commission. June 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281.

[11] "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." European Commission. July 2014. https://eur-lex.europa.eu/eli/reg/2014/910/oj.

[12] "Regulatory Technical Standards on strong customer authentication and secure communication under PSD2." European Banking Authority. April 2022. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2.

9.2 Technical standards

[13] "AnonCreds Specification v1.0." Hyperledger. January 2022. https://anoncreds-wg.github.io/anoncreds-spec/.

[14] "BBS Signature Scheme." Digital Identity Foundation (DIF). September 2022. https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html.

[15] "Certificate Management over CMS (CMC)." IETF. June 2008. https://datatracker.ietf.org/doc/html/rfc5272.

[16] "Certificate Management Protocol (CMP)." IETF. September 2005. https://www.rfc-editor.org/rfc/rfc4210.

[17] "Client to Authenticator Protocol (CTAP) v2.1." FIDO Alliance. June 2021. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[18] "CSC API Specification v1.0." Cloud Signature Consortium (CSC). June 2018. https://cloudsignatureconsortium.org/resources/download-api-specifications/.

[19] "Decentralized Identifiers (DIDs) v1.0." W3C. July 2022. https://www.w3.org/TR/did-core/.

[20] "DIDComm Messaging v2." DIF. https://identity.foundation/didcomm-messaging/spec/.

[21] "Digital Signature Services eXtended (DSS-X)." OASIS. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x.

[22] "Digital Travel Credentials (DTC)." ICAO. October 2020. https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Digital%20Travel%20Credential%20(DTC).pdf.

[23] "Doc 9303 Machine Readable Travel Documents." ICAO. 2021. https://www.icao.int/publications/pages/publication.aspx?docnum=9303.

[24] "Electronic Signatures and Infrastructures (ESI); EN 319 401: General Policy Requirements for Trust Service Providers." ETSI ESI. May 2021. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf.

[25] "Electronic Signatures and Infrastructures (ESI); TS 119 432: Protocols for remote digital signature creation." ETSI ESI. March 2019. https://www.etsi.org/deliver/etsi_ts/119400_119499/119432/01.01.01_60/ts_119432v010101p.pdf.

[26] "Electronic Signatures and Infrastructures (ESI); TR 119 460: Survey of technologies and regulatory requirements for identity proofing for trust service subjects." ETSI ESI. February 2021. https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf.

[27] "Electronic Signatures and Infrastructures (ESI); TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects." ETSI ESI. July 2021. https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf.

[28] "Electronic Signatures and Infrastructures (ESI); TS 119 462: Wallet interfaces for trust services and signing." ETSI ESI. September 2022. The specification is still a draft that is not yet published.

[29] "Electronic Signatures and Infrastructures (ESI); TS 119 472: Profiles for Attribute Attestations." ETSI ESI. September 2022. The specification is still a draft that is not yet published.

[30] "EN 419 241-1 (Trustworthy Systems Supporting Server Signing Part 1: General Security Requirements)." CEN. October 2018. https://www.sis.se/en/produkter/information-technology-office-machines/it-security/ss-en-419241-12018/.

[31] "EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing." CEN. January 2019. https://www.en-standard.eu/csn-en-419241-2-trustworthy-systems-supporting-server-signing-part-2-protection-profile-for-qscd-for-server-signing/.

[32] "EN 419 221-5: Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services." CEN. October 2018. https://www.en-standard.eu/csn-en-419221-5-protection-profiles-for-tsp-cryptographic-modules-part-5-cryptographic-module-for-trust-services/.

[33] "Extended Access Control (EAC)." BSI. March 2012. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/Sicherheitsmechanismen/EAC/eac_node.html.

[34] "Fast Identity Online v2 (FIDO2)." FIDO Alliance. https://fidoalliance.org/fido2/.

[35] "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." IETF. May 2008. https://www.rfc-editor.org/rfc/rfc5280.

[36] "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap." IETF. February 2011. https://datatracker.ietf.org/doc/rfc6071/.

[37] "ISO/IEC 18013-5:2021 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application." ISO/IEC. September 2021. https://www.iso.org/standard/69084.html.

[38] "ISO/IEC DIS 23220-1: 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. November 2021. https://www.iso.org/standard/74910.html.

[39] "ISO/IEC DIS 23220-2 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 systems." ISO/IEC. September 2022. The specification is still a draft that is not yet published.

[40] "ISO/IEC DIS 23220-3 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. September 2022. The specification is still a draft that is not yet published.

[41] "ISO/IEC DIS 23220-4 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. September 2022. The specification is still a draft that is not yet published.

[42] "ISO/IEC DIS 23220-5 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. September 2022. The specification is still a draft that is not yet published.

[43] "ISO/IEC DIS 23220-6 Cards and security devices for personal identification — Building blocks for identity management via mobile devices - Part 6: Mechanism for use of certification on trustworthiness of secure area." ISO/IEC. September 2022. The specification is still a draft that is not yet published.

[44] "JavaScript Object Notation (JSON) Data Interchange Format." IETF. December 2017. https://www.rfc-editor.org/rfc/rfc8259.

[45] "JSON Web Token (JWT)." IETF. May 2015. https://www.rfc-editor.org/rfc/rfc7519.html.

[46] "JSON-LD 1.1 - A JSON-based Serialization for Linked Data." W3C. July 2020. https://www.w3.org/TR/json-ld11/.

[47] "OAuth 2.0 Authorization Framework." IETF. October 2012. https://www.rfc-editor.org/rfc/rfc6749.html.

[48] "OAuth2 for Native Apps." IETF. October 2017. https://datatracker.ietf.org/doc/html/rfc8252.

[49] "OpenID Connect Core 1.0." OpenID Foundation. April 2014. https://openid.net/specs/openid-connect-core-1_0.html.

[50] "OpenID for Verifiable Credential Issuance." OpenID Foundation. September 2022. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

[51] "OpenID for Verifiable Presentations." OpenID Foundation. September 2022. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

[52] "Presentation Exchange v1.0.0." Digital Identity Foundation. https://identity.foundation/presentation-exchange/spec/v1.0.0/.

[53] "Secure Payment Confirmation." W3C. September 2022. https://www.w3.org/TR/secure-payment-confirmation/.

[54] "Security Assertion Markup Language (SAML) V2.0 Technical Overview." OASIS. March 2008. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[55] "Selective Disclosure for JWTs (SD-JWT)." IETF. August 2022. https://www.ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-00.html.

[56] "Self-Issued OpenID Provider v2." OpenID Foundation. September 2022. https://openid.net/specs/openid-connect-self-issued-v2-1_0.html.

[57] "Simple Certificate Enrollment Protocol (SCEP)." IETF. September 2020. https://datatracker.ietf.org/doc/html/rfc8894.

[58] "SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms." SOG-IS Crypto Working Group. January 2020. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf.

[59] "TOTP: Time-Based One-Time Password Algorithm". IETF. May 2011. https://www.ietf.org/rfc/rfc6238.txt.

[60] "Transport Layer Security (TLS) Protocol Version 1.3." IETF. August 2018. https://datatracker.ietf.org/doc/rfc8446/.

[61] "Universal Wallet 2020". W3C. August 2022. https://w3c-ccg.github.io/universal-wallet-interop-spec/.

[62] "Verifiable Credentials Data Model v1.1." W3C. March 2022. https://www.w3.org/TR/vc-data-model/.

[63] "WACI-DIDComm Interop Profile." OpenID Foundation. September 2022. https://identity.foundation/waci-didcomm/.

[64] "Web Authentication: An API for accessing Public Key Credentials Level 2." W3C. April 2021. https://www.w3.org/TR/webauthn/.

[65] "X.1277 : Universal authentication framework." ITU. November 2018. https://www.itu.int/rec/T-REC-X.1277-201811-I.

[66] "X.1278: Client to authenticator protocol/Universal 2-factor framework." ITU. November 2018. https://www.itu.int/rec/T-REC-X.1278-201811-I/en.

[67] "zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure." University of Maryland. July 2022. https://eprint.iacr.org/2022/878.pdf.

9.3 Other references

[68] "Cybersecurity Certification: Candidate EUCC Scheme V1.1.1." ENISA. May 2021. https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

[69] "FIDO Alliance White Paper: FIDO for PSD2 - Providing for a satisfactory customer journey." The FIDO Alliance. September 2018. https://media.fidoalliance.org/wp-content/uploads/FIDO-PSD2_Customer_Journey_White_Paper.pdf.

[70] "FIDO Alliance White Paper: Integrating FIDO & Federation Protocols." The FIDO Alliance. December 2017. https://media.fidoalliance.org/wp-content/uploads/Enterprise_Adoption_Best_Practices_Federation_FIDO_Alliance.pdf.

[71] "FIDO Alliance White Paper: Multi-Device FIDO Credentials." The FIDO Alliance. March 2022. https://fidoalliance.org/white-paper-multi-device-fido-credentials/.

[72] "FIDO Alliance White Paper: Using FIDO with eIDAS Services." The FIDO Alliance. April 2020. https://media.fidoalliance.org/wp-content/uploads/2020/06/FIDO_Using-FIDO-with-eIDAS-Services-White-Paper.pdf.

[73] "Framework Contract for Fixed Price and Quoted Time and Means for Development, Consultancy and Support for the European Digital Identity Wallet." EU Tenders Electronic Daily. July 2022. https://ted.europa.eu/udl?uri=TED:NOTICE:309685-2022:TEXT:EN:HTML&src=0.

[74] "Hyperledger Indy SDK: Wallet Storage Design." Hyperledger. June 2018. https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/design/003-wallet-storage/README.html.

[75] "OpenWallet Foundation." The Linux Foundation. September 2022. https://openwallet.foundation/.

[76] "Remote ID Proofing." ENISA. March 2021. https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing.

[77] "Support to the implementation of the European Digital Identity Framework." The EU. March 2022. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-deploy-02-electronic-id.

[78] "Wallet Security Working Group." Digital Identity Foundation. June 2021. https://identity.foundation/working-groups/wallet-security.html.