FIDO Alliance White Paper:
Using FIDO with eIDAS Services

Deploying FIDO2 for eIDAS QTSPs and eID schemes

April 2020

Editors:
Sebastian Elfors, Yubico
Bernd Zwattendorfer, Infineon Technologies

Audience

This paper is aimed at governmental agencies that are interested in using FIDO2 as part of an eIDAS notified eID scheme, and Qualified Trust Service Providers (QTSPs) who are interested in deploying eIDAS remote signing services that leverage the FIDO2 standard. The intended readers are project managers, technical experts and developers.

Summary

This white paper describes how to use the FIDO2 standard with eIDAS compliant schemes and Qualified Trust Service Providers.

FIDO2 meets the eIDAS requirements on eID schemes for the authentication mechanism with assurance level substantial and high. In brief, FIDO2 meets the highest assurance level because WebAuthn is a non-phishable protocol and FIDO2 authenticators are tamper-proof hardware devices. In conjunction with proper registration, enrollment and issuance processes, FIDO2 authenticators can form the basis for eID schemes that can in turn be notified by the European Commission. Such eID schemes can be used within the EU's cross-border interoperability framework, which allows citizens of one EU Member State to access online services in another EU Member State.

FIDO2 can also be used as an authentication standard to attain an authentication process with high assurance to an eIDAS compliant Qualified Trust Service Provider. More precisely, a user can use FIDO2 for strong authentication to its Qualified Certificate's private key residing in a centralized Qualified Signature Creation Device, which is operated by a Qualified Trust Service Provider. When the end-user is authenticated to her remote private key, it can be used for creating remote Qualified Electronic Signatures. This fulfills the requirement of sole control. In this white paper, an architecture for using FIDO2 to trigger a remote resigning process is illustrated. The architecture is also compatible with the Committee European Normalization (CEN) standards, which specify the Signature Activation Protocol and Signature Activation Module for remotely operated Qualified Signature Creation Devices.

Table of Contents

1. Introduction to eIDAS

1.1 Overview of eIDAS

eIDAS (Electronic Identification, Authentication and Trust Services) [5] is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification. In addition to the EU regulation, eIDAS is legally constituted by the following set of Commission Implementing Regulations and Decisions.

- Commission Implementing Regulation EU 2015/1501 on the interoperability framework [6]
- Commission Implementing Regulation EU 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means [8]
- Commission Implementing Regulation EU 2015/1505 on laying down technical specifications and formats relating to trusted lists [8]
- Commission Implementing Regulation EU 2015/1506 on laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies [9]
- Commission Implementing Decision EU 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices [11]

The eIDAS regulation covers electronic identification and trust services for electronic transactions in the EU's internal market. It regulates electronic signatures, electronic identification, certification and supervisory bodies, and related processes to provide a secure way for EU citizens to communicate with public services.

Furthermore, eIDAS and the European standardization organizations European Telecommunications Standards Institute (ETSI) and Committee European Normalization (CEN) have created several standards for certification authorities, electronic signatures and seals, qualified digital certificates, timestamps, and authentication schemes. All EU Member States operating an electronic identification scheme are required to recognize eID schemes and electronic signatures that comply with the eIDAS regulation.

An overview of the electronic identification mechanisms and Qualified Trust Services is illustrated in Figure 1. The highlighted components are relevant to FIDO2 implementations for eIDAS.

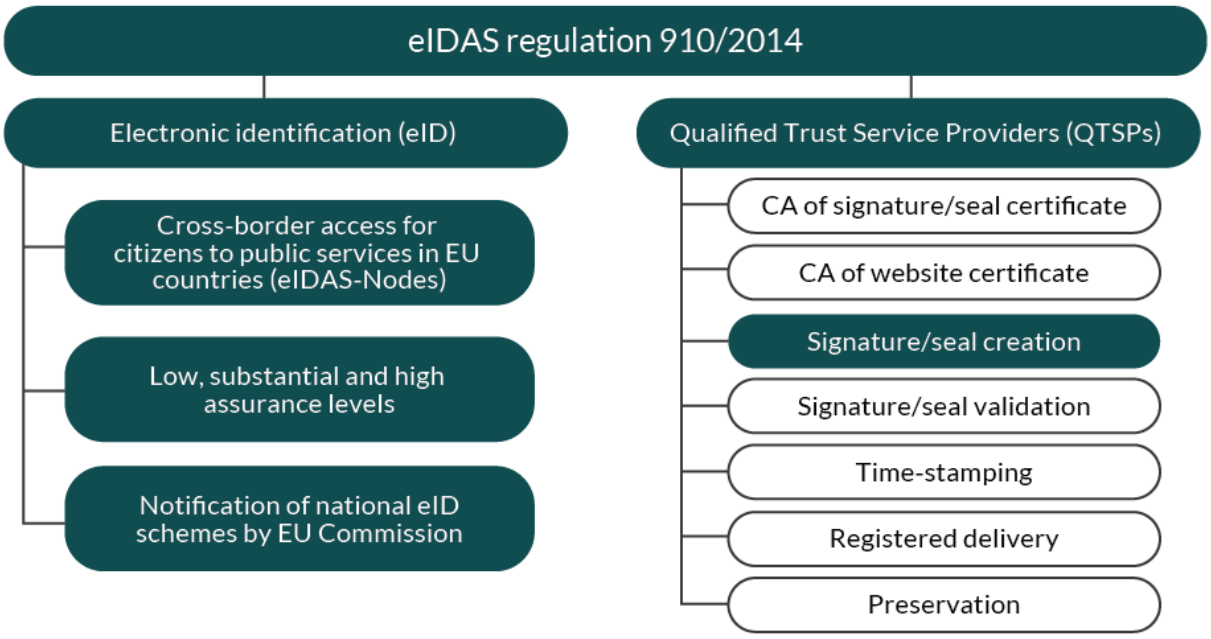

Figure 1 *– Overview of the eIDAS components*

1.2 Electronic Identification (eID Schemes)

The European Commission has obliged its EU Member States to create a common electronic identification framework that will recognize eIDs 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.

For example, German citizens are able to authenticate to an Italian online service using their national eID scheme (nPA – Personalausweis). Another example of cross-border identification is the Swedish tax authority, that has enabled access to their online service for EU citizens in Croatia, Estonia, Italy and Spain to log in using their national eID schemes.

The eIDAS regulation does not stipulate any technology-related implementation requirements on the eID scheme. Hence, it is the supervising agency in each EU Member State that approves the eID scheme on a national level.

Therefore, the eID schemes can be subject to different implementations in various countries. A typical implementation of an eID scheme is an eID smart card with Transport Layer Security (TLS) as authentication protocol; such eID schemes are implemented for the Belgian citizen eCard and the Spanish Nacional de Identidad electrónico (DNIe). In Germany, the national eID scheme is constituted by the German eID card in conjunction with the Extended Access Protocol. Estonia has created three main versions of eID schemes: the Estonian national eID card with TLS, SIM-card with PKI keys on a Wireless Identity Module (WIM), and a mobile phone app with a key-pair that is shared between the app and a central Hardware Security Module (HSM).

Each EU Member State can submit national eID scheme(s) to the European Commission, which will be subject to a pre-notification process, peer-review and (if approved) notification. When an eID scheme is getting notified by the European Commission, the process follows these steps:

- Pre-notified: The EU Member State has officially communicated its intention to notify its eID scheme to the European Commission.
- Peer reviewed: The eID scheme has been peer reviewed by other EU Member States' representatives.
- Notified: The EU Member State has notified its eID scheme to the European Commission and the information has been published to the Official Journal of the European Union.

Once a submitted national eID scheme has been approved by the European Commission, it will be formally recognized and published at the EU's official eID scheme web site. At the time of writing, roughly half of the EU Member States have had their eID schemes notified by the European Commission, while the rest of the EU Member States will apply for notification during 2020 and 2021.

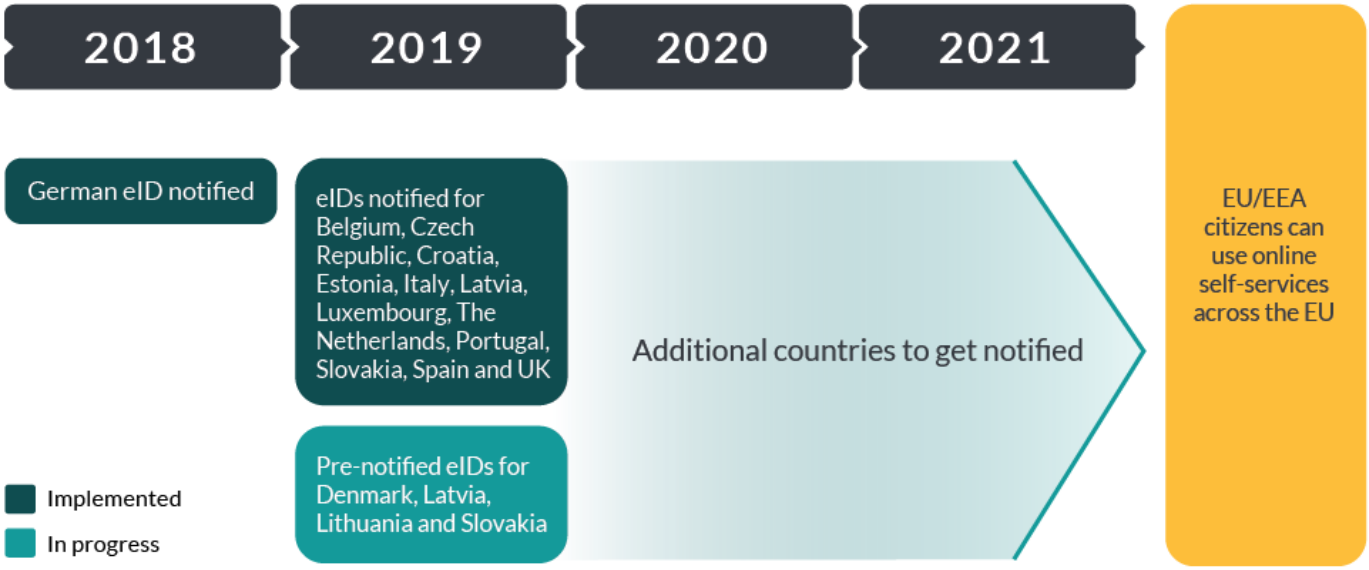

***Figure 2** – Rollout of eID schemes in the EU*

In order to establish an interoperability framework between the recognized eID schemes, each EU Member State is required to operate an eIDAS-Node. This interoperability framework including eIDAS-Nodes is described in legal terms in Commission Implementing Regulation (EU) 2015/1501 [6]. An eIDAS-Node is essentially a gateway that supports the Security Assertion Markup Language v2 (SAML v2) protocol [12], which is used for providing access for a citizen of one EU Member State to an online service in another EU Member State. In a nutshell, citizens authenticate at their domestic eIDAS-Node using their domestic eID scheme. Identity and authentication information is subsequently transferred from the domestic eIDAS-Node via the foreign eIDAS-Node to the foreign online service. For example, a citizen in Estonia is able to use her Estonian eID card for authentication and rely upon this authentication for getting access to the Swedish tax agency's online web service. Each EU Member State is required to assign an agency for operating the national eIDAS-Node; the official list of all agencies is available at the EU's eID web site.

More information on how the FIDO2 standard can be used as part of an eID scheme is available in section 2.

1.2.1 eIDAS Assurance Levels for Electronic Identification

The eIDAS regulation has also introduced three levels of assurance for electronic identification: low, substantial and high; those assurance levels are defined in article 8 in the eIDAS regulation [5].

- 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 inherent). In total, there are three different factors for authentication: something you are, something you have, and something you know. Two-factor authentication necessitates two separate authentication factors such as something you have (e.g., a mobile device) and something you know (e.g., a PIN-code). The user should be in control of or in possession of the authentication factors and the authentication process shall include dynamic authentication. An example of substantial assurance level is the use of one-time passwords that are distributed by text messages to mobile phones.
- 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. An example of high assurance level is a PKI-based authentication scheme with a hardware authentication token, such as a PKI certificate stored on a smart card plus PIN.

The requirements for the assurance levels are described in more detail in Implementing Regulation EU 2015/1502 [7].

More information on how the FIDO2 standard can be used for designing the authentication part of eID schemes according to assurance level high is available in section 2.

1.3 eIDAS QTSPs

The eIDAS regulation (EU 910/2014) [5] introduced the concept of Qualified Trust Service Providers (QTSPs), which are supervised service providers that are accredited to perform trusted services such as issuing signature/seal certificates, signature validation, timestamping, registered delivery, preservation, and signature/seal creation.

The QTSPs that are in scope of this document are Certification Authorities (CA) for issuing qualified electronic certificates and for the creation of Qualified Electronic Signatures (QES).

Hence, the QTSPs must be operated according to the accreditation made by the Conformity Assessment Body (according to ETSI TS 319 403) and the approval by the national supervisory body. Therefore, the QTSP CAs must adhere to the relevant policy, security and operational requirements in the relevant ETSI standards, which are listed at ETSI's ESI web site. Similarly, the QTSPs for remote signing services must adhere to the relevant policy, security and operational requirements in the applicable ETSI standards.

1.3.1 eIDAS Remote Signing and QSCDs

The eIDAS term Qualified Signature Creation Device (QSCD) originates from the term Secure Signature Creation Device (SSCD), which has been specified in the EU Electronic Signatures Directive 1999/93/EC. At that time, the SSCD requirements were tailored to the end-users to create signatures locally at their personal computers. Hence, several SSCDs were designed and implemented as Common Criteria certified smart cards. When the eIDAS regulation was written in 2014, the term QSCD was to a large extent based on its predecessor SSCD, with some broader context. The eIDAS QSCD is legally defined in Commission Implementing Decision EU 2016/650 [10], which specifies the standards for the security assessment of qualified signature and seal creation devices. In principle, each QSCD must be Common Criteria EAL 4+ certified and then be approved by the certification body in an EU Member State. Each EU Member State must have a certification body that is responsible for certifications of QSCDs; all certified QSCDs and legacy SSCDs are available at this official EU list.

QTSPs can offer the creation of electronic signatures locally or remotely. When the QTSP creates Qualified Electronic Signatures centrally for remote end-users, the process is denoted as remote signing. In this setup, the QTSP operates a QSCD, which is typically a Hardware Security Module, where the users' Qualified Certificates and associated private keys are securely stored and managed.

One important aspect is the concept of sole control, which is defined in recital 52 of the eIDAS regulation:

> *"In order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory."*

In brief, sole control constitutes the principle that only the signatory has access to her electronic signature creation data.

The user's authentication to the QTSP is therefore of major importance when creating a remote Qualified Electronic Signature by using a QSCD.

The security assessment of QSCDs is described in the Commission Implementing Decision (EU) 2016/650 [10]. However, this Implementing Decision is primarily focused on the security requirements and assessment of a QSCD that is managed locally by an individual. This has created uncertainty around how centrally deployed QSCDs at remote QTSPs should be operated. According to article 24(1) in the eIDAS regulation, the assurance level for authentication to a QTSP with a QSCD for remote signing is set to substantial or high. Although article 24(1) in the eIDAS regulation allows for assurance level substantial or high, it needs to be emphasized that authentication protocols according to assurance level substantial can be phishable.

More information on how FIDO2 can be used for implementing authentication with assurance level high to QTSPs is available in section 3.

2. How to Use FIDO2 as Part of an eID Scheme

2.1 FIDO2 Used with Electronic Identities

The FIDO2 standard referred to in this section, and throughout this document, is comprised of the W3C Web Authentication (WebAuthn) standard and the FIDO Client to Authenticator Protocol (CTAP). The FIDO2 standard is primarily designed for secure online authentication.

The registration procedure of the WebAuthn protocol does not provide any details about how the user can be identified when enrolling for the FIDO2 credentials. When accredited CAs issue traditional eID cards, however, the user is identified according to the policies and practices stipulated by the CA. Hence, eID cards support the processes of identification and authentication. These processes are typically followed by an authorization process, proving users' access to protected services or data. Such an authorization mechanism can be based on SAML v2, OpenID Connect or other access management systems and frameworks. Figure 3 illustrates the relationship of FIDO and eID cards with these security processes.

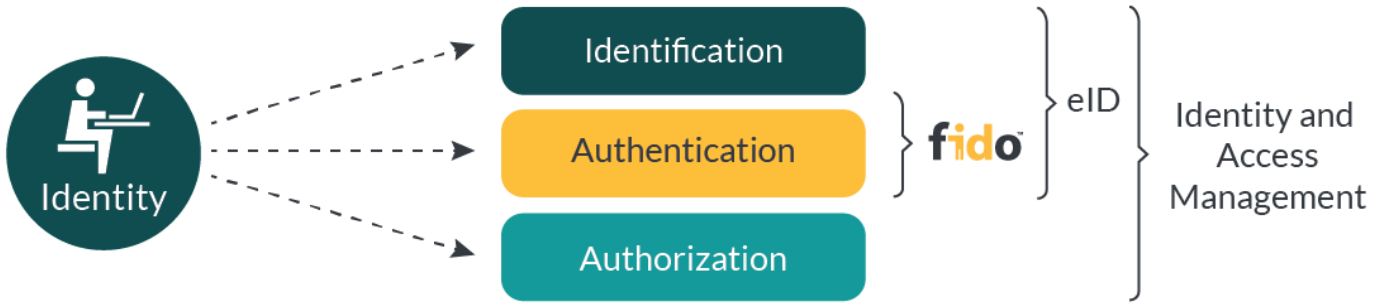

Figure 3 – *FIDO2 in relation to identification, authentication and authorization*

This means that the FIDO2 standard needs a complementary identification process when issuing the FIDO2 credentials as part of an eID scheme. Essentially, the following models can be applied when using FIDO2 as part of an eID scheme:

- Model 1: FIDO2 is used for strong authentication to a QTSP, where the FIDO2 credentials are associated with a Qualified Certificate (eID) residing centrally at the QTSP. In this case, FIDO2 can either be the authentication protocol to the QTSP, or FIDO2 can be part of an eID scheme used for access to the QTSP. In this model, the user is identified by the QTSP's registration authority, and the CA issues a Qualified Certificate and connected FIDO2 credentials to the user. This model is described in more detail in section 3.
- Model 2: FIDO2 is used as the authentication part of the eID scheme, where the FIDO2 authenticator serves as the eID card and WebAuthn as the authentication protocol. For this complementary identification setup, enrollment and issuance processes are needed to comply with the eIDAS regulation on eID schemes. A description of such processes is available in section 2.2.

2.2 FIDO2 as Part of an eID Scheme

The eIDAS regulation has introduced three levels of assurance for electronic identification: low, substantial and high; those assurance levels are defined in article 8 in the eIDAS regulation [5]. Furthermore, the requirements for the assurance levels are described in more detail in Commission Implementing Regulation (EU) 2015/1502 [7].

The FIDO standard allows for authentication implementations that can meet eIDAS requirements for assurance levels substantial or high, depending on the FIDO authenticators' security levels. This section analyzes specifically how the FIDO2 standard meets the eIDAS requirements for assurance level high for achieving EU notified and cross-border interoperable eID schemes. FIDO2 in itself can provide the authentication mechanisms for eIDAS assurance level high, but the additional processes need to be added in order to constitute a complete eID scheme.

Regulation (EU) 2015/1502 section	**Requirement(s)**	**How FIDO2 meets assurance level high**
2.1 Enrollment	See the requirements for assurance level high in sections "Application and registration", "Identity proofing and verification", and "Binding between the electronic identification means of natural and legal persons".	The enrollment requirements outlined in the eIDAS regulation are focused on how to properly identify a person. The WebAuthn specification, on the other hand, is agnostic with respect to the identification process of an individual. In other words, FIDO does not provide any means for identification. Hence, the issuer of the eID needs to ensure that the enrollment process complies with the eIDAS requirements. Therefore, the credentials enrollment to the FIDO2 authenticator needs to be done by other means, e.g. by identifying the user with a national ID card (during the initial identification process) or when the user authenticates to the CA online by using her eID. If enrollment in conjunction with a FIDO2 authenticator is carried out, the enrollment requirements set out in the eIDAS level of assurance implementing act need to be met accordingly. Thereby, the FIDO2 credentials stored either as resident credentials at the FIDO2 authenticator, or at the Relying Party server, should be associated with the national ID or eID to prove the identification of the user.
2.2.1 Electronic identification means characteristics and design	See the requirements for assurance level high in section 2.2.1.	The FIDO2 authenticator meets the requirements of assurance level high, since it is designed to be a two-factor authenticator, belongs to only one person, protects against duplication and tampering, and can be reliably protected by the person using the device.
2.2.2 Issuance, delivery and activation	See the requirements for assurance level high in section 2.2.2.	In order to meet the requirements of assurance level high, the FIDO2 authenticator basically should be delivered to the user by an accredited registration officer. If a PKI-based eID is used for identification, it can be used for authenticating the user online, which in turn can trigger the FIDO2 registration process. The FIDO2 credentials at the FIDO2 authenticator or the Relying Party can be associated with eID card. This even allows for remote activation of the FIDO2 authenticator without physically visiting an accredited office. Moreover, FIDO2 resident credentials should be used in conjunction with authentication by PIN-code or biometrics.
2.2.3 Suspension, revocation and reactivation	See the requirements for assurance level high in section 2.2.3.	The FIDO2 authenticator can be revoked by removing the credentials from the WebAuthn Relying Party, which will prevent the FIDO2 authenticator from being accepted for authentication at the relying party. Another option is to delete the credentials from the FIDO2 authenticator. In order to suspend the FIDO2 authenticator, the credentials can be temporarily removed and after a certain time be reinstated at the relying party. This way assurance level high can be implemented.

Regulation (EU) 2015/1502 section	Requirement(s)	How FIDO2 meets assurance level high
2.2.4 Renewal and replacement	See the requirements for assurance level high in section 2.2.4.	The FIDO2 authenticator can be renewed or replaced by registering new credentials for the WebAuthn Relying Party. In the event a previously registered user has all their keys deleted or deactivated by the Relying Party and is now permitted to register new FIDO2 credentials, it is expected that the user will go through the same process as any user enrolling a new key with the Relying Party. Whether the previously registered user must repeat a credentialing process to register new FIDO2 credentials is up to the Relying Party's policy and implementation for registration. Whether the revocation of a PKI credential should cascade to deleting/deactivating all registered FIDO2 credentials of a user or vice-versa depends on a specific implementation of the PKI and FIDO. Taking these policies into account, eIDAS assurance level high can be supported by FIDO.
2.3 Authentication	See "Authentication mechanism".	FIDO2 meets the requirements of a high level of assurance authentication mechanism, since the standard is designed to prevent against guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential. In particular, the FIDO2 design with origin bound keys protects the authentication protocol from phishing attacks. (For more information on how origin bound keys protects from phishing, see this FIDO Alliance article.) Furthermore, WebAuthn and CTAP2 provide dynamic authentication since they are PKI-based challenge response protocols.
2.4 Management and organization	See "General provisions", "Published notices and user information", "Information security management", "Record keeping", "Facilities and staff", "Technical controls", and "Compliance and audit".	The management and organization requirements outlined in the eIDAS regulation describe the processes, applicable law, organization and audits. The WebAuthn specification, on the other hand, is agnostic with respect to such processes. Hence, it is the responsibility of the issuer of the eID to ensure that its organization complies with the eIDAS requirements. If a FIDO2 authenticator is used as eID under such circumstances, the assurance level can be set to high.

***Table 1** – Analysis of FIDO2 compliance for eIDAS assurance level high*

A complementary analysis on how to design and deploy FIDO systems according to eIDAS assurance level high is available in BSI's report "Technical Guideline TR-03159 Mobile Identities" [1].

When it comes to certifications, each EU Member State decides on the eID scheme and its assurance level. Therefore, the requirements on eID devices differ from country to country. Typically, the protection profiles for secure signature creation devices (EN 419 211) are the means of choice for smart card based eID schemes. In addition, for eID schemes based on mobile apps in conjunction with authentication protocols that interact with a certificate/key residing in an HSM at a QTSP, the standard CEN 419241-2 (Protection profile for QSCD for Server Signing) could be used. Germany, for example, outlines that the cryptographic chip of the FIDO2 device should be at least Common Criteria EAL 4+ certified and the FIDO2 device should at least be subject to a light-weight certification such as BSZ (Accelerated Security Certification).

In addition to meeting the eIDAS requirements on assurance level high, FIDO2, with respect to authentication, provides the benefit of being implemented in a wide range of applications, web browsers, and operating systems. This allows for a simplified rollout of FIDO2, without the need for installing additional plugins in a heterogenous environment. The easy use of FIDO2 can also give a positive user experience among the citizens in an EU Member State.

2.3 Using FIDO2 in a Federated eIDAS-Node SAML v2 Environment

Cross-border interoperability between notified eID schemes in different EU Member States is achieved by a distributed cluster of national eIDAS-Nodes, which forms a SAML v2 [12] federation for EU online services. The notified eID scheme used for identification in one EU country must have the same or higher assurance level than the one required by the requested online service in another EU country. Since FIDO2 has the potential to be notified as the authentication part of an eID scheme, it is suitable for authentication to an identity provider, which in turn can connect to the national eIDAS-Node for issuance of a SAML v2 ticket. The SAML v2 ticket contains interoperable identity and authentication information and can in turn be used for access to a requested online service in another EU Member State.

An overview of cross-border interoperability between eIDAS-Nodes in different EU Member States is shown in Figure 4. In this scenario, FIDO2 is used as part of an eID scheme with assurance level high.

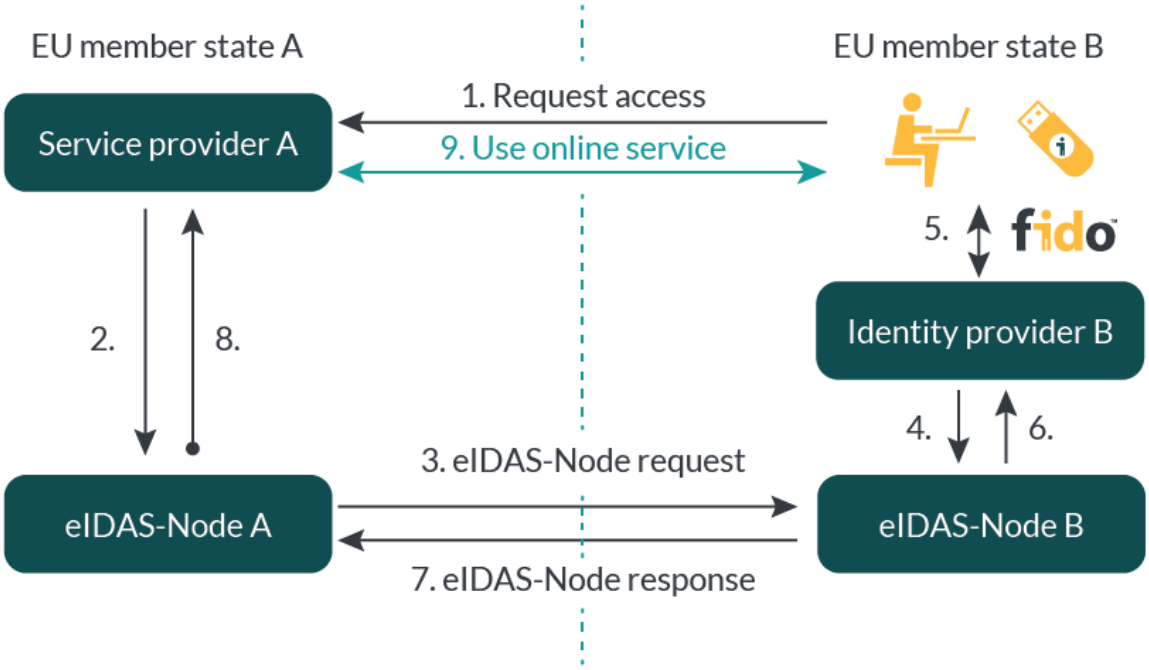

Figure 4 *– Overview of interoperability between eIDAS-Nodes*

The process steps in this cross-border interoperable model are the following:

1. A citizen residing in EU Member State B wants to connect to a governmental online service in EU Member State A. The citizen in EU Member State B selects to use an eID from EU Member State B.
2. The online service provider A detects that the user has requested to use an eID from EU Member State B, and redirects the authentication request to the eIDAS-Node in EU Member State A.
3. The eIDAS-Node in EU Member State A sends an eIDAS-Node request (i.e. SAML v2 request) to the eIDAS-Node in EU Member State B.
4. The eIDAS-Node in EU Member State B redirects the user to identity provider B.
5. The user in EU Member State B uses its FIDO2 authenticator with the FIDO2 standard for authentication to identity provider B. The different models for FIDO2 authentication are described in section 2.1.
6. The identity provider invokes eIDAS-Node B with the successful authentication response.
7. The eIDAS-Node in EU Member State B submits an eIDAS-Node response (i.e. SAML v2 ticket) to the eIDAS-Node in EU Member State A.
8. The eIDAS-Node in EU Member State A propagates the successful authentication to the governmental online service in EU Member State A that the user is authenticated.
9. The user in EU Member State B is granted access to the governmental online service in EU Member State A.

3. Using FIDO2 for Secured Access to QTSPs

3.1 The Challenge of Creating Remote Qualified Signatures

The eIDAS regulation from 2014 primarily focused on the QSCD as a device to be used for local signing by a user. Hence, when the Commission Implementing Decision (EU) 2016/650 was written, there were no available standards for remote signing devices operated by a trust service provider in a secure environment that could meet the requirements in Regulation (EU) 910/2014 Annex II for qualified signature or seal creation devices.

In order to implement a QTSP remote signing service that meets the sole control requirement set out in eIDAS recital 52, an electronic identification scheme with assurance level high is needed.

In order to close this gap, Committee European Normalization (CEN) has created three CEN standards that address how QTSPs should operate QSCDs in order to create remote Qualified Electronic Signatures.

3.2 Introducing the CEN/TC 224 Standards

The CEN technical committee TC 224 has published the following 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) [1]
- CEN EN 419 241-2 (Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing) [3]
- CEN EN 419 221-5 (Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services) [4]

If the CEN standards are implemented in conjunction with each other, the user will get sole control of the remote creation of qualified electronic signatures.

Furthermore, ENISA (European Union Agency for Cybersecurity) has published a report that discusses how the European Commission Implementing Decision 2016/650 may be updated to reference the CEN standards above to regulate the security and operations of a QSCD at a QTSP with the purpose of creating remote qualified electronic signatures.

3.2.1 CEN EN 419 241-1 (General System Security Requirements)

The CEN 419 241-1 standard [1] specifies security requirements and recommendations for Trustworthy Systems Supporting Server Signing that generate digital signatures. This system is composed of a Server Signing Application (SSA) and a remote Signature Creation Device. A remote Signature Creation Device is extended with remote control provided by a Signature Activation Module (SAM) executed in a tamper-protected environment. This SAM module uses the Signature Activation Data (SAD), collected through a Signature Activation Protocol (SAP), in order to guarantee that the signing keys are used under sole control of the signer (user). The SSA uses a remote Signature Creation Device in order to generate, maintain and use the signing keys under the sole control of their authorized signer. The standard is protocol agnostic, so the Signature Activation Protocol (SAP) is not specified in this standard, although FIDO2 is explicitly listed as a viable alternative.

3.2.2 CEN EN 419 241-2 (Protection Profile for QSCD for Server Signing)

The CEN 419 241-2 standard [3] specifies a Common Criteria protection profile for a Signature Activation Module (SAM), which aims to meet the requirements of a QSCD being operated remotely. To ensure that the signer (user) has sole control of her signing keys, the signature operation needs to be authorized. This is carried out by a Signature Activation Module (SAM), which can handle one endpoint of SAP, verify SAD and activate the signing key within a QSCD Cryptographic Module. Both the QSCD Cryptographic Module and the SAM must be located within a tamper protected environment such as an HSM. SAD verification means that the SAM checks the binding between the three SAD elements as well as checking that the signer is authenticated. The assurance requirement of the CEN EN 419 241-2 SAM Protection Profile is Common Criteria EAL4 augmented.

3.2.3 CEN EN 419 221-5 (Protection Profiles for TSP Cryptographic Modules)

The CEN EN 419 221-5 standard [4] specifies a Common Criteria Protection Profile for cryptographic modules, which is intended to be suitable for use by trust service providers supporting electronic signature and electronic sealing operations, certificate issuance and revocation, time-stamp operations, and authentication services, as identified by the eIDAS regulation. The protection profile also describes how the cryptographic module can be deployed as a remote QSCD at a QTSP.

3.3 System Overview Based on the CEN Standards

The CEN EN 419 241 and CEN EN 419 221-5 standards can be used as the basis for implementing a system whereby FIDO2 serves as the CEN Signature Activation Protocol. In this architecture, the CEN Signature Activation Module will validate the FIDO2 authentication credentials in the tamper proof HSM and unlock the user's signing key in the QSCD. Such implementation will ultimately give the user sole control of the remote signature process.

An overview of such a system, based on the FIDO2 standard and the CEN EN 419 241 and CEN EN 419 221-5 standards, is illustrated in Figure 5.

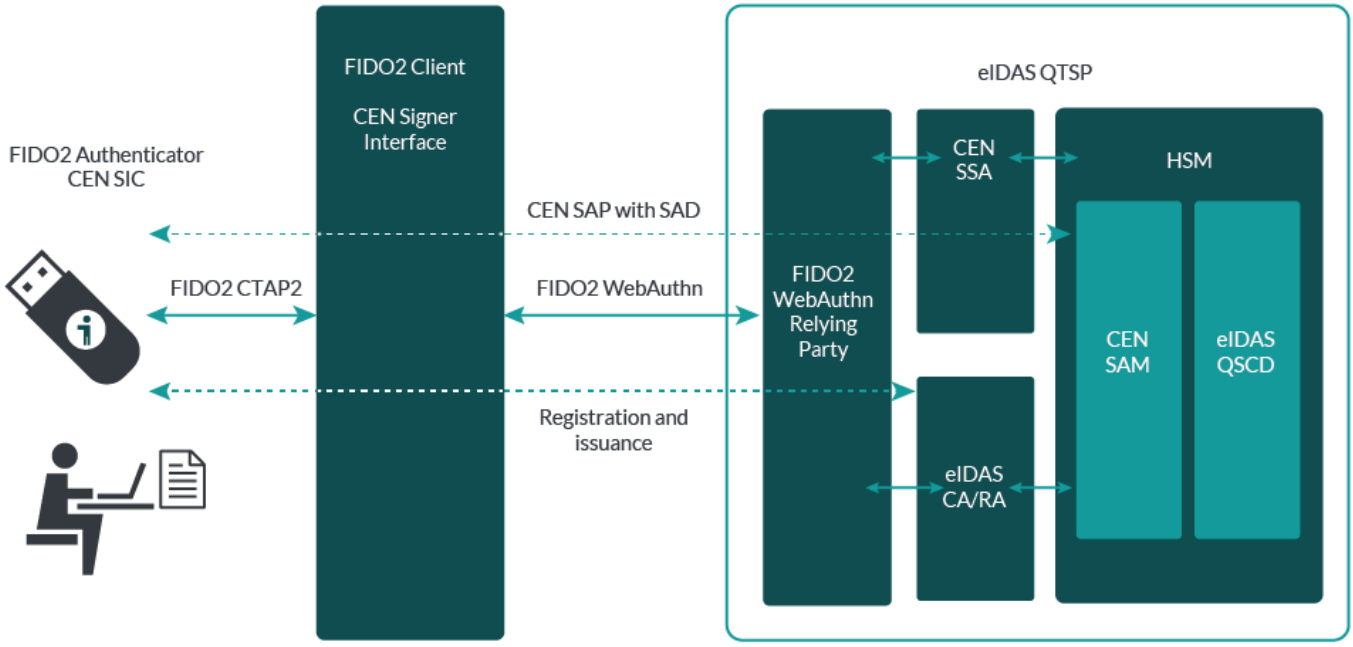

Figure 5 *– System overview based on CEN standards*

The entities in the system are described in the sub-sections (in alphabetic order) below.

3.3.1 Certification Authority (CA)

The Certification Authority (CA) is used for issuing Qualified Certificates to the users. The CA may be part of the same QTSP that provides remote signing services, or it can be external to the remote signing QTSP. Qualified Certificate (QC) is an eIDAS term that is defined in the eIDAS Regulation. A Qualified Certificate is issued under a QC-policy to a user by an accredited QTSP Certification Authority. The Certification Authority has also a Registration Authority (RA), which is the entity that is used when identifying and registering users as part of the certificate enrollment process. In this context, the users' Qualified Certificates and keys are stored and protected centrally in the QSCD's HSM at the QTSP, and are thus available to the QTSP's Remote Server Signing Application.

3.3.2 FIDO2 Authenticator

Authenticator is a FIDO2 term that is defined in the WebAuthn specification. An Authenticator is a cryptographic entity used by a WebAuthn Client to (i) generate a public key credential and register it with a Relying Party, and (ii) authenticate by potentially verifying the user, and then cryptographically signing and returning, in the form of an Authentication Assertion, a challenge and other data presented by a WebAuthn Relying Party.

3.3.3 FIDO2 Client

WebAuthn Client is a FIDO2 term that is defined in the WebAuthn specification. A WebAuthn Client is an intermediary entity typically implemented in the user agent, which is comprised of a platform and a web browser or app. Conceptually, it underlies the WebAuthn API and embodies the implementation of the internal WebAuthn methods. It is responsible for validating the RP ID of the Relying Party, marshalling the inputs for the underlying Authenticator operations, through the CTAP2 protocol, and for returning the results of the latter operations to the WebAuthn API's callers.

3.3.4 Hardware Security Module (HSM)

The Hardware Security Module (HSM) is deployed at the QTSP Remote Signing Service. The HSM generates, hosts, protects and operates the key-pairs of the users' Qualified Certificates. The connection between the QTSP and the HSM must be authenticated and encrypted. In particular, the HSM invokes the user's Qualified Certificate Private Key to sign the Document To Be Signed.

3.3.5 Qualified Signature Creation Device (QSCD)

A Qualified Signature Creation Device (QSCD) is an eIDAS term that is defined in Annex II of the eIDAS Regulation. The QSCD must be Common Criteria certified by an accredited certification body according to the requirements outlined in the eIDAS Implementing Decision (EU 2016/650) on QSCDs. A list of approved QSCDs is available at the official EU website. A typical QSCD is a secure smart card being able to create qualified electronic signatures. Hence, the secure key pair is stored in the user's domain. However, in the context of a QTSP operating Remote Signing Services, the QSCD is a centrally deployed HSM that generates, hosts, protects and operates the keypairs of the users' Qualified Certificates in a remote location.

3.3.6 Qualified Trust Service Provider (QTSP)

Qualified Trust Service Provider (QTSP) is an eIDAS term that is defined in the eIDAS Regulation in article 3, §20:

"(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;"

A QTSP is audited by a conformity assessment body according to ETSI guidelines and is accredited by the supervisory body in the relevant EU Member State. Furthermore, a QTSP can be accredited for different types of services. The trust services that are in scope of this document are Certification Authority (for issuing of Qualified Certificates that are stored centrally at the CA) and Remote Signing Service.

In this context, the eIDAS QTSP is described in section 1.3, and is comprised of the components described in this section. Furthermore, the QTSP is assumed to operate a database, which can be used for storing the end-user data, Qualified Certificates and associated FIDO2 elements per user record.

3.3.7 Server Signing Application (SSA)

The Server Signing Application (SSA) is the core service of the eIDAS compliant QTSP remote signing service. The SSA is operated by the eIDAS compliant Qualified Trust Service Provider (QTSP). It has the capability to create Qualified Electronic Signatures for authenticated remote users with the users' Qualified Certificates and Qualified Certificate Private Keys hosted in the Qualified Signature Creation Device (QSCD). The users' Qualified Certificates, issued previously by the QTSP CA, are available to the QTSP SSA.

3.3.8 Signature Activation Data (SAD)

The Signature Activation Data (SAD) is a CEN term defined in CEN EN 419 241-1 as follows:

"To reach the Sole Control Assurance Level 2 (SCAL2), the use of the SAD to ensure control over the signer's key SHALL be enforced by the SAM. Signature activation at SCAL2 requires fulfilment of several conditions as signer authentication and authenticity of signature operation request from the signer. Both properties MAY be given directly by the SAD. However, it is also possible to perform signer authentication prior to SAD generation, e.g. using delegation of authentication. SAD can be a set of data or be a result of cryptographic operations from which the same information can be derived. SAD contributes to authenticate directly or indirectly the signer. When the signer authentication takes place prior to collection of the SAD, the SAD SHALL contain items to identify the signer asserted by a known source. This assertion MAY come from either the Signer's Interaction Component (SIC) or from a trusted electronic identity provider. The source of the assertion SHALL be authenticated."

In the context of this document, the SAD is a combination of an Authentication Assertion, created by the user's Authenticator, and a cryptographic binding, which authorizes that Authenticator to authorize a signing process with a Qualified Certificate Private Key.

3.3.9 Signature Activation Module (SAM)

The Signature Activation Module (SAM) is implemented as safe code in the HSM. It is a CEN term defined in the CEN EN 419 241-1 standard as follows:

"The SAM is a software that uses the SAD in order to guarantee with a high level of confidence that the signing keys are used under sole control of the signer for SCAL2. The SAM is required to be used in a tamper protected environment. If the SAM is not used in the same tamper protected environment as the SCDev, then a secure channel between both tamper protected environments is required."

3.3.10 Signature Activation Protocol (SAP)

The Signature Activation Protocol (SAP) is a CEN term defined in the CEN EN 419 241-1 standard as follows:

"The SAP SHALL be designed to allow secure use of the signing key for the creation of a digital signature to be performed by the cryptographic module on behalf of a signer. The SAP is a protocol where the signer (via the SIC) and the Trustworthy System Supporting Server Signing (TW4S) communicate in order to generate the SAD. The design of the SAP SHALL include as a minimum the following verifications:

- *signer authentication when using the signing key,*
- *authenticity of the signature request with specific SAD,*
- *the selected signing key is valid and active,*
- *secure transfer of all the elements of the SAD.*

When the signing key is not used to sign a proof of possession in order to obtain a certificate, the SAP SHOULD include the following verification:

- *presence of valid certificate associated to signing key."*

The CEN-defined SAP protocol is implemented by a combination of the WebAuthn and CTAP2 protocols according to the FIDO2 standard.

3.3.11 WebAuthn Relying Party (RP)

The QTSP also needs to implement a WebAuthn Relying Party (RP) that is used for FIDO2 registration and authentication. The Relying Party is a FIDO2 term that is defined in the WebAuthn specification. This is the entity whose web application utilizes the WebAuthn API to register and authenticate users.

3.4 Mapping the CEN-standards to the FIDO2 Terms

In the table below, the CEN EN 419 241 terms are mapped to the FIDO2 terms (when applicable) and briefly explained.

CEN term	FIDO2 term	Description
Signature Activation Data (SAD)	Authenticator Response	The CEN Signature Activation Data is equivalent to the Authenticator Response in the WebAuthn protocol. This is the activation data to the Signature Activation Module for gaining remote access to the user's private key in the QSCD.
Signature Activation Protocol (SAP)	CTAP2 and WebAuthn	The CEN Signature Activation Protocol is equivalent to the combination of CTAP2 and WebAuthn protocols specified in the FIDO2 standard. This is the authentication protocol used to provide Signature Activation Data for remote access to the Signature Activation Module for gaining remote access to the user's private key in the QSCD.
Signer	User	The CEN Signer is equivalent to the FIDO2 User. This is the person who is operating the Client and authenticates with the Authenticator in order to sign a document remotely.
Signer's Interaction Component (SIC)	Authenticator	The CEN Signer's Interaction Component is equivalent to the FIDO2 Authenticator. This is the device with credentials used for creating the Signature Activation Data.
Signer Interface	Client	The CEN Signer Interface is equivalent to the FIDO2 Client. This is essentially the user's laptop or mobile device with a user agent (web-browser).

***Table 2** - Mapping of CEN and FIDO2 terms*

3.5 Registration and Issuance Process

3.5.1 Registration Process Overview

The registration process for issuing a Qualified Certificate and creating FIDO2 credentials, and associating them together, is illustrated in Figure 6.

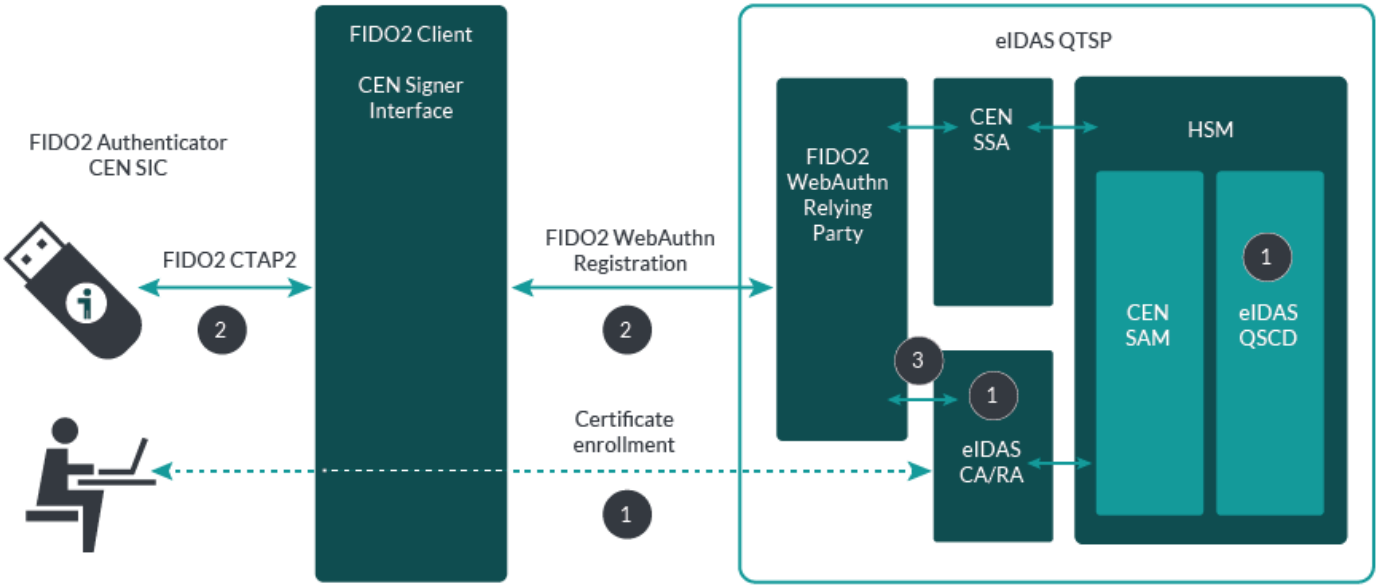

***Figure 6** – Registration and issuance process*

The steps in the registration process are described in the sub-sections below. The registration process in this section describes the initial registration and association of FIDO2 credentials with a Qualified Certificate and private key residing in the QSCD.

3.5.2 Registration Step 1

The user gets identified by the QTSP's Registration Authority (RA) in order for the QTSP Certification Authority (CA) to issue a Qualified Certificate. The identification process goes beyond the scope of this document, but it must adhere to the requirements on a QTSP CA for issuing a Qualified Certificate.

The QTSP registers the user's personal data, certificate application forms, identity document copies, etc., in its database. This is a sub-process for registering the certificate application documentation at the QTSP.

As part of this process, the QTSP CA invokes the HSM with a request to generate the Qualified Certificate key-pair in the QSCD.

Finally, the CA signs the Qualified Certificate based on the registered user information and the public key in the QSCD.

Since the QTSP is operating a remote signing server application, the Qualified Certificate remains at the QTSP CA, and the key-pair is protected in the remote QSCD.

3.5.3 Registration Step 2

Next, the user will enroll for the FIDO2 credentials. This step may be carried out immediately after the enrollment of the Qualified Certificate, or may be performed later for an existing Qualified Certificate. The recommended approach is to register the FIDO2 credentials immediately after the Qualified Certificate enrollment in order to get a stronger binding of the enrollee to the FIDO2 credentials.

The user should have a FIDO2 Authenticator available throughout the registration process. The FIDO2 Authenticator may be the user's personal device or may be handed out by the QTSP during or prior to the registration process.

The FIDO2 registration process follows the standardized enrollment procedure as described in the WebAuthn [13] and the CTAP2 [11] specifications. At the end of the FIDO2 procedure, the user's FIDO2 Authenticator is equipped with FIDO2 credentials, which are bound to the FIDO2 credentials at the WebAuthn Relying Party at the QTSP.

3.5.4 Registration Step 3

Finally, the FIDO2 credentials configured at the WebAuthn Relying Party are associated with the Qualified Certificate and key-pair in the QSCD; this association can be based on a cryptographic binding between the FIDO2 credentials key-pair with the Qualified Certificate's key-pair. Furthermore, the signature activation process in the SAM-module in conjunction with the QSCD is implemented to rely upon a successful FIDO2 authentication. How this association, potentially based on a cryptographic binding, and signature activation process is implemented goes beyond the scope of this document.

Hence, the FIDO2 registration process serves both the purpose of the usual FIDO2 registration at the WebAuthn Relying Party, and to implicitly associate the FIDO2 Authenticator with the user's signing key in QSCD. Therefore, the FIDO2 Authenticator can be used both for WebAuthn authentication to the WebAuthn Relying Party and for unlocking the user's key in the QSCD.

3.6 Authentication and Signing Process

3.6.1 Authentication and Signing Process Overview

The process for FIDO2 authentication to a QTSP remote signing service and creating a Qualified Electronic Signature is illustrated in Figure 7.

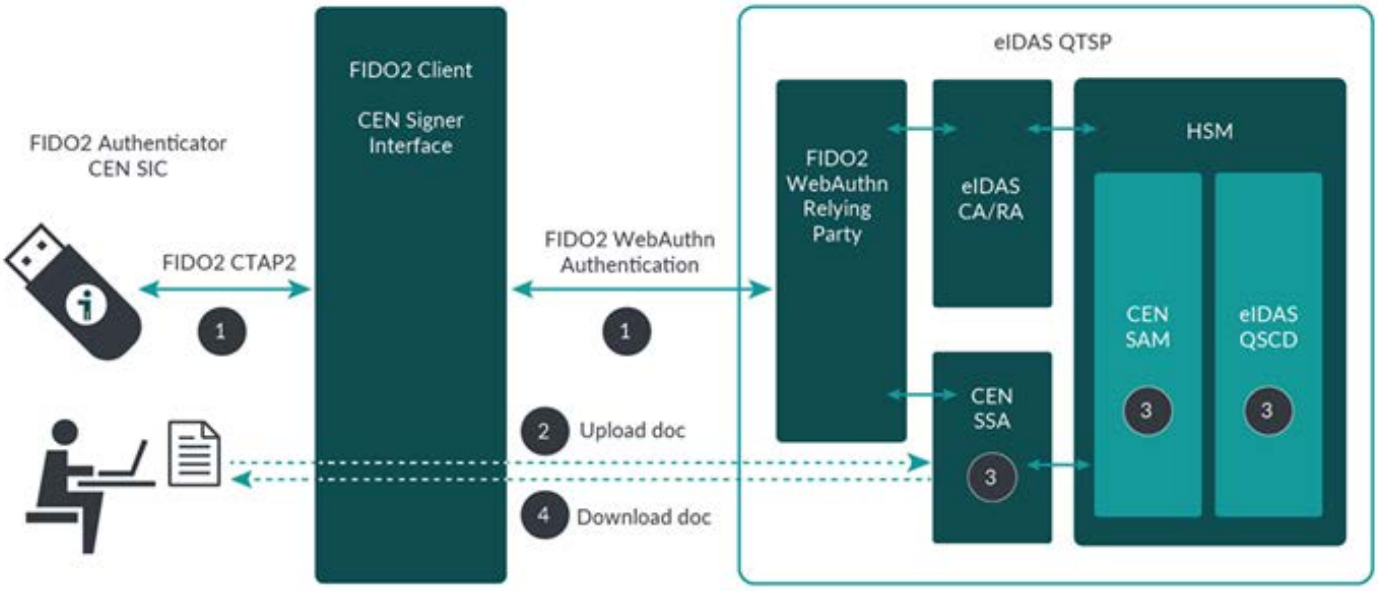

Figure 7 *– Authentication and signing process*

The steps in the authentication and signing process are described in the sub-sections below.

3.6.2 Authentication and Signing Step 1

The user performs the standard FIDO2 authentication procedure by using the FIDO2 Authenticator. The WebAuthn protocol is used for authenticating to the Relying Party, and the CTAP2 protocol is used for the interaction between the Client and the FIDO2 Authenticator. When the user is logged in to the WebAuthn Relying Party, she gets access to the online services at the QTSP.

3.6.3 Authentication and Signing Step 2

The user submits their Document To Be Signed (Doc-TBS) to the QTSP Server Signing Application. The Document To Be Signed can either be an electronic document (for example a PDF) that is uploaded from the Client to the Server Signing Application, or it can be a document that is previously stored centrally at the Server Signing Application. An example of a document that is stored centrally could be a tax declaration at a tax authority; in this scenario the user will be able to locate this document in her account at the Server Signing Application.

3.6.4 Authentication and Signing Step 3

The Server Signing Application uses the user's identity to find the Qualified Certificate (from the QTSP database) and the associated private key in the QSCD. The Server Signing Application invokes the Relying Party, which emits a second WebAuthn challenge, which includes a unique identifier (such as a hash value) of the document to be signed. The WebAuthn challenge is signed by the user's FIDO2 authenticator. The user's WebAuthn authentication response (AuthenticatorAssertionResponse) is propagated from the WebAuthn Relying Party to the Server Signing Application, which in turn invokes the SAM-module.

Next, the SAM-module, which is executed within the trusted HSM environment, validates (portions of) the user's WebAuthn authentication response. This validation can be based on the cryptographic binding or other association as described in section 3.5.4. When the SAM-module has ultimately validated the user's WebAuthn authentication response, the SAM-module gives the QSCD the privileges to unlock the user's private key residing in the QSCD and use this key to sign the document.

Finally, the Server Signing Application may extend the raw signature into an ETSI standardized CAdES, XAdES or PAdES advanced signature format.

3.6.5 Authentication and Signing Step 4

The document, which is now signed with a Qualified Electronic Signature, is returned back to the user's Client. Alternatively, the signed document can also be stored centrally at the user's account at QTSP.

4. Conclusions

FIDO2 meets the eIDAS requirements on eID schemes with respect to authentication with assurance level substantial or high, since FIDO2 is a non-phishable protocol and specific FIDO2 authenticators are tamper-proof devices. However, the identification, enrollment and issuance requirements according to the eIDAS regulations must be implemented in addition to the FIDO2 standard when deploying national eID schemes that can be notified by the European Commission. Such eID schemes can also be used within the EU's cross-border interoperability framework, which allows citizens residing in one EU Member State to access online services in another EU Member State. FIDO2 authenticators can be used as easy-to-use substantial or high assurance eID schemes according to eIDAS and thus can act as alternative or supplement for existing and non-user-friendly eID implementations.

In addition, FIDO2 can also be used for secured authentication at QTSPs. A design for a cryptographic binding of the FIDO2 authentication process with the remote eIDAS Qualified Electronic Signature creation process as defined in EU Regulation (EU) 910/2014 was presented. This design is compatible with the CEN EN 419 241 standard suite, so FIDO2 can be implemented as the Signature Activation Protocol that is supported by a Signature Activation Module. As a result, FIDO2 can be used for strong end-to-end authentication to unlock a user's Qualified Certificate's private key residing in a centralized Qualified Signature Creation Device, which is operated by a Qualified Trust Service Provider. This fulfills the concept of sole control defined in recital 52 of the eIDAS regulation. To summarize, FIDO2 provides an easy-to-use and secured alternative to other potentially phishable solutions.

The FIDO2 standard is suitable as the authentication mechanism for substantial or high assurance levels for both eID schemes and for authentication to a remote signing QTSP, as defined in the eIDAS regulation.

5. Acknowledgments

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

- Lorrayne Auld, MITRE
- Sridhar Bhupathiraju, Thales Group
- John Bradley, Yubico
- Tommaso De Orchi, Yubico
- Eric Deschamps, Thales Group
- John Fontana, Yubico
- Jeremy Grant, Venable
- Dennis Kügler, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bill Leddy, VISA Card
- Emil Lundberg, Yubico
- Michael Magrath, OneSpan
- Danielle Mattison, FIDO Alliance
- David Petch, VISA Card
- Megan Shamas, FIDO Alliance
- Mindy Souza, FIDO Alliance
- Kevin Turner, HYPR

6. Glossary of Terms

API .....Application Programming Interface
BSI .....Bundesamt für Sicherheit in der Informationstechnik
BSZ .....Beschleunigte Sicherheitszertifizierung (“Accelerated Security Certification”)
CA .....Certification Authority
CAdES .....CMS Advanced Electronic Signature
CC .....Common Criteria
CEF .....Connecting Europe Facility
CEN.....Committee European Normalization
CMS .....Cryptographic Message Syntax
CTAP2 .....Client To Authenticator Protocol v2
EAL .....Evaluation Assurance Level
eIDAS.....electronic IDentification Authentication and trust Services
ENISA.....European Union Agency for Cybersecurity
ETSI.....European Telecommunications Standards Institute
FIDO2 .....Fast Identity Online v2
HSM.....Hardware Security Module
HTTP .....HyperText Transfer Protocol
PAdES .....PDF Advanced Electronic Signatures
PDF .....Portable Document Format
PIN.....Personal Identification Number
PKI .....Public Key Infrastructure
PKCS .....Public Key Cryptography Standards
QC .....Qualified Certificate
QES.....Qualified Electronic Signature
QSCD .....Qualified Signature Creation Device
QTSP.....Qualified Trust Service Provider
RA.....Registration Authority
RFC .....Request For Comments
RP .....Relying Party
RP ID.....Relying Party Identifier
RSA .....Rivest Shamir Adleman
SAD.....Signature Activation Data
SAM.....Signature Activation Module
SAML .....Security Assertion Markup Language
SAP .....Signature Activation Protocol
SCAL2 .....Sole Control Assurance Level
SHA.....Secure Hash Algorithm
SIC .....Signer’s Interaction Component
SMS .....Short Messaging Service
SSA .....Server Signing Application
TC .....Technical Committee
TLS.....Transport Layer Security
TSP .....Trusted Service Provider
TW4S .....Trustworthy System Supporting Server Signing
W3C.....World Wide Web Consortium
WebAuthn.....Web Authentication
WIM .....Wireless Identity Module
XAdES .....XML based Advanced Electronic Signatures
XML .....eXtended Markup Language

7. References

[1] BSI, Technical Guideline TR-03159 Mobile Identities - Part 2: EAC and FIDO based mobile identities, August 2019, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-2.pdf?__blob=publicationFile&v=4

[2] CEN EN 419 241-1, Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements, July 2018, https://www.sis.se/en/produkter/information-technology-office-machines/it-security/ss-en-419241-12018

[3] CEN EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, May 2018, https://www.ssi.gouv.fr/uploads/2018/09/anssi-cc-pp-2018_02fr_pp.pdf

[4] CEN EN 419 221-5, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services, November 2016, https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-PP-2016_05%20PP.pdf

[5] eIDAS (electronic IDentification Authentication and trust Services), Regulation (EU) No 910/2014, July 2014, https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

[6] eIDAS Implementing Regulation EU 2015/1501, Commission Implementing Regulation EU 2015/1501 on the interoperability framework, September 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1501

[7] eIDAS Implementing Regulation EU 2015/1502, Commission Implementing Regulation EU 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means, September 2015, https://publications.europa.eu/en/publication-detail/-/publication/4735575a-56b7-11e5-afbf-01aa75ed71a1/language-en

[8] eIDAS Implementing Regulation EU 2015/1505, Commission Implementing Regulation EU 2015/1505 on laying down technical specifications and formats relating to trusted lists, September 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=EN

[9] eIDAS Implementing Regulation EU 2015/1506, 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, September 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506&from=EN

[10] eIDAS Implementing Decision EU 2016/650, Commission Implementing Decision EU 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices, April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D0650

[11] FIDO Alliance CTAP2, Client To Authenticator Protocol v2, January 2019, https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html

[12] OASIS, SAML v2 technical specifications, March 2005, https://wiki.oasis-open.org/security/FrontPage

[13] W3C WebAuthn, Web Authentication: An API for accessing Public Key Credentials, March 2019, https://www.w3.org/TR/webauthn/

Note: URL references to specific definitions can also be embedded in the document. Usually the cross-reference or link to a document or definition is inserted at the first occurrence of the term.