FIDO Alliance White Paper:
Introduction of FIDO & eIDAS Services

April 2020

Editors:
Sebastian Elfors, Yubico
John Fontana, 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 decision makers and C-level executives.

Summary

This introductory white paper describes the relationship between FIDO2 standards and eIDAS compliant schemes that can accommodate modern authentication protocols. eIDAS stands for electronic identification, authentication and trust services, building the legal basis for cross-border interoperability of electronic identification, authentication, and electronic signatures amongst EU Member States.

FIDO2 meets eIDAS requirements on eID schemes for authentication mechanisms at the highest of three eIDAS-defined assurance levels: low, substantial and high. FIDO2 meets requirements for inclusion in the EU's cross-border interoperability framework, which allows citizens in one EU Member State to get access to online services in another EU Member State. The FIDO2 WebAuthn API prevents phishing; FIDO2 authenticators are tamper-proof hardware devices, so FIDO2 meets the requirements for eIDAS-compliant electronic identification means. Combining FIDO2 and eIDAS, WebAuthn serves as the authentication protocol already implemented in the most prominent web browsers and FIDO2 supports a foundation for eID schemes that can be notified by the European Commission. Notified means that a national eID scheme has been approved by the European Commission, so it is recognized by all other EU Member States. FIDO2 is also suitable for authentication to a Qualified Trust Service Provider (QTSP) as defined in the eIDAS regulation, which typically offers remote signing capabilities.

This white paper discusses the relationship between FIDO2 and eIDAS services on a higher level. Details, including architectural concepts for integration of FIDO2 into the eIDAS interoperability framework, are presented in the FIDO Alliance White Paper, "Using FIDO with eIDAS Services" [2].

Table of Contents

1. Introduction to eIDAS

1.1 Overview of eIDAS

eIDAS (Electronic Identification, Authentication and Trust Services) [1] is an EU regulation on electronic identification and trust services for electronic transactions in the European Market, which guarantees the free movement within the European Union of goods, capital, services, and labor. Furthermore, eIDAS 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, primarily across Member States. eIDAS was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and supersedes the e-Signature Directive 1999/93/EC [5]. The eIDAS regulation is accompanied by several implementing acts, providing legislative guidance for its implementation.

Furthermore, the European standardization organization 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. The relevant ETSI and CEN standards for eIDAS are listed at ETSI's ESI web site. All EU Member States operating an electronic identification scheme are required to recognize an electronic identification from the scheme of another EU Member State.

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.

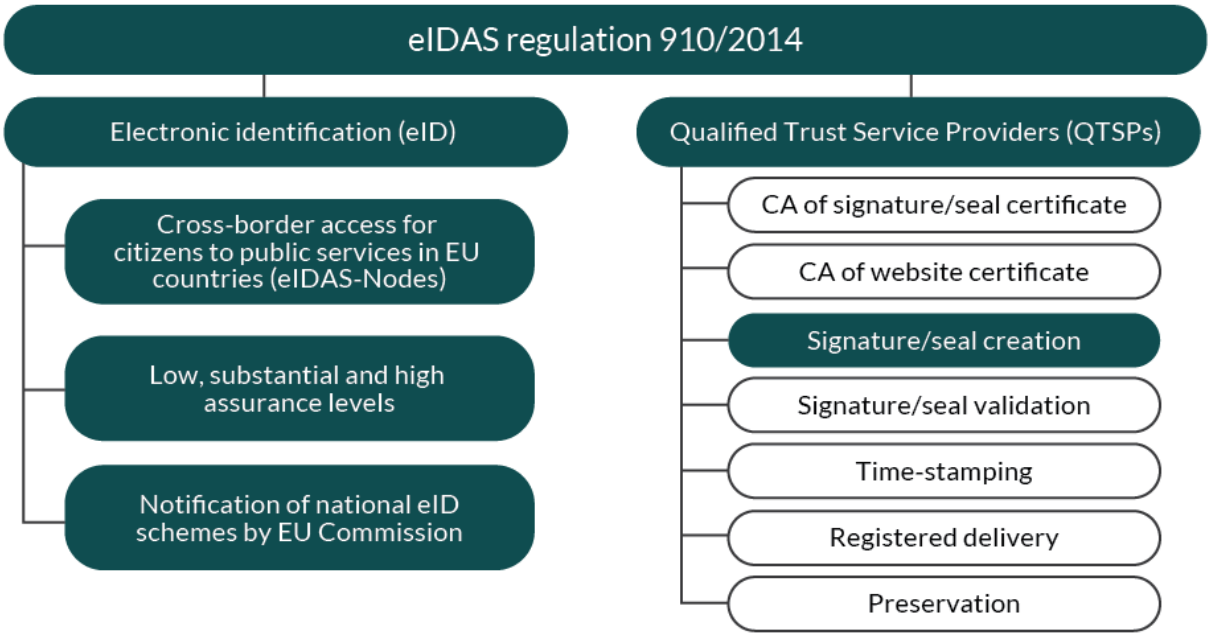

Figure 1 *– Overview of the eIDAS components*

1.2 Electronic Identification (eID Schemes)

The European Commission has obliged all EU Member States operating an electronic identification scheme to create a common electronic identification framework that recognizes eIDs from other EU Member States and ensure its authenticity and security. The goal with the interoperable identification and authentication framework is to allow EU citizens to access online services across borders within the EU.

Each EU Member State can submit national eID scheme(s) to the European Commission, which will be subject to a pre-notification process (the country has submitted its eID scheme to the European Commission) and peer-review (the eID scheme has been peer reviewed by other EU Member States). Once the eID scheme is notified, it is officially published to the EU website listing recognized eID schemes.

In order to establish an interoperability framework between the recognized eID schemes, each EU Member State is required to operate an eIDAS-Node. An eIDAS-Node is essentially a gateway which provides access for a citizen of one EU Member State to an online service in another EU Member State. As an example, German citizens can authenticate to an Italian online service using their national eID scheme (nPA – Personalausweis) with the help of these eIDAS-Nodes. In other words, authentication information is transferred between eIDAS-Nodes in various EU Member States.

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 introduces three levels of assurance for electronic identification: low, substantial and high; these assurance levels are defined in article 8 in the eIDAS regulation [1] and are elaborated in more detail in the corresponding implementing act (EU 2015/1502). The levels of assurance determine minimum technical specifications, standards, and procedures to ensure interoperability, reliability, and quality of these elements: enrollment, electronic identification means management, authentication, and management and organization. The authentication requirements are especially relevant for FIDO2.

- 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. 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). An example of an authentication mechanism providing a substantial assurance level is a one-time password.
- The high assurance level requires 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 a high assurance level mechanism is a PKI-based authentication scheme with a smart card plus PIN-code.

More information on how the FIDO2 standard can be used as part of an eID scheme according to assurance level substantial or high is available in section 2.

1.3 eIDAS QTSPs

The eIDAS regulation [1] introduced the concept of Qualified Trust Service Providers (QTSPs), which are supervised service providers that are accredited to perform trusted services. Trusted services include issuing signature/seal certificates, signature validation, timestamping, registered delivery, preservation, and signature/seal creation. Qualified signature/seal creation can be carried out using different means. Typically, secure smart cards have been the means of choice as Qualified Signature Creation Device (QSCD) so far.

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 remote Hardware Security Module (HSM), where the users' Qualified Certificates and associated private keys are securely stored and managed. Compared to smart cards, signature creation does not take place locally in the user's domain but rather in the remote HSM, triggered by a strong authentication mechanism.

The user's authentication to the QTSP is therefore of major importance when creating a remote Qualified Electronic Signature by using a centrally operated QSCD. In the current eIDAS regulation, assurance level substantial or high is sufficient when a user authenticates to a QTSP remote signing service. However, the eIDAS regulation also stipulates that the user must have sole control over the remote signing process. Sole control constitutes the principle that only the signatory has access to his or her electronic signature creation data.

More information on how the FIDO2 standard can be used for authentication to remote signing QTSPs, and thereby provide the user with sole control of the signing process, is available in section 3.

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

2.1 FIDO2 Used with Electronic Identities

The registration procedure of FIDO2 does not provide any details about how the user can be identified when enrolling for the FIDO2 credentials. When accredited Certification Authorities (CAs) issue traditional eID cards, however, the user is identified according to the policies and practices stipulated by the CA. eID cards typically store authentic identity information on the card, being transferred to a remote server during an authentication process. FIDO2 credentials may either be stored at the authenticator as resident credentials or at the Relying Party with secure access to the FIDO authenticator. Moreover, FIDO2 resident credentials should be used in conjunction with authentication by PIN-code or biometrics. Figure 2 illustrates the relationship of FIDO and eID cards with the process of identification and authentication. Both FIDO and eID cards can be used for subsequent authorization processes.

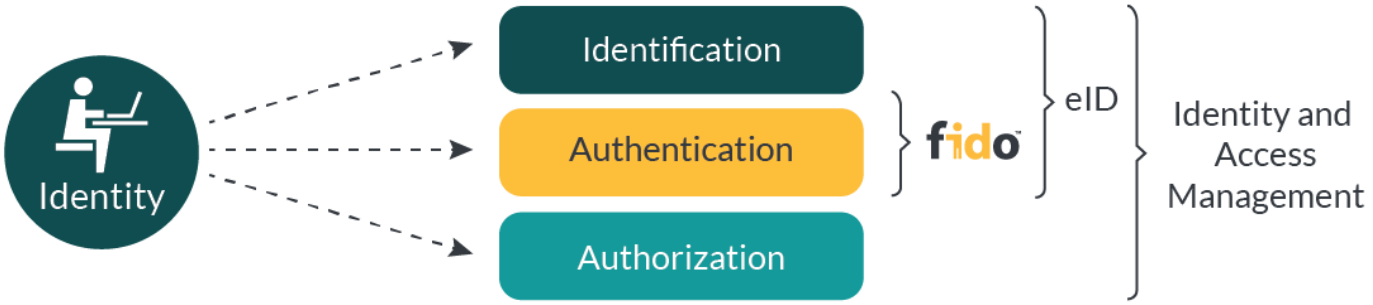

Figure 2 – *FIDO2 in relation to identification, authentication and authorization*

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. 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 scheme and WebAuthn as the authentication protocol. A description of such processes is available in section 2.2.

2.2 FIDO2 as Part of an eID Scheme

Smart card based electronic IDs are typically the means of choice for providing high confidence in the eID scheme as required by the eIDAS levels of assurance. However, even though they have been deployed in the field for many years, eIDs still lack broad applicability and wide user acceptance for accessing online services because of technical complexity or low usability for citizens. Continued widespread adoption of smartphones and FIDO2 can help in this instance to bypass these drawbacks.

FIDO2 meets the requirements of a substantial or 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. A complete analysis of how FIDO2 meets the requirements of assurance level high is available in [2].

In addition to meeting the eIDAS requirements for 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 or client software in a heterogenous environment. The easy use of FIDO2 also provides a positive user experience among the citizens in an EU Member State. More information on how to use FIDO2 as part of an eID scheme is available in [1].

2.3 Using FIDO2 in a Federated eIDAS-Node 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 an identity federation of EU Member States' online services. Essentially, identity information is federated amongst EU-located online services. Thereby, a citizen authenticates against her home eIDAS node, which in turn forwards identity information to the foreign eIDAS node and subsequently to the foreign online service being requested. The notified eID scheme used for identification in one EU Member State must have the same or higher assurance level than the requested online service in another EU Member State. FIDO2 is suitable for authentication to an identity provider, which in turn can connect to the national eIDAS-Node. Figure 3 illustrates the process flow of a cross-border and eIDAS-based identification and authentication process.

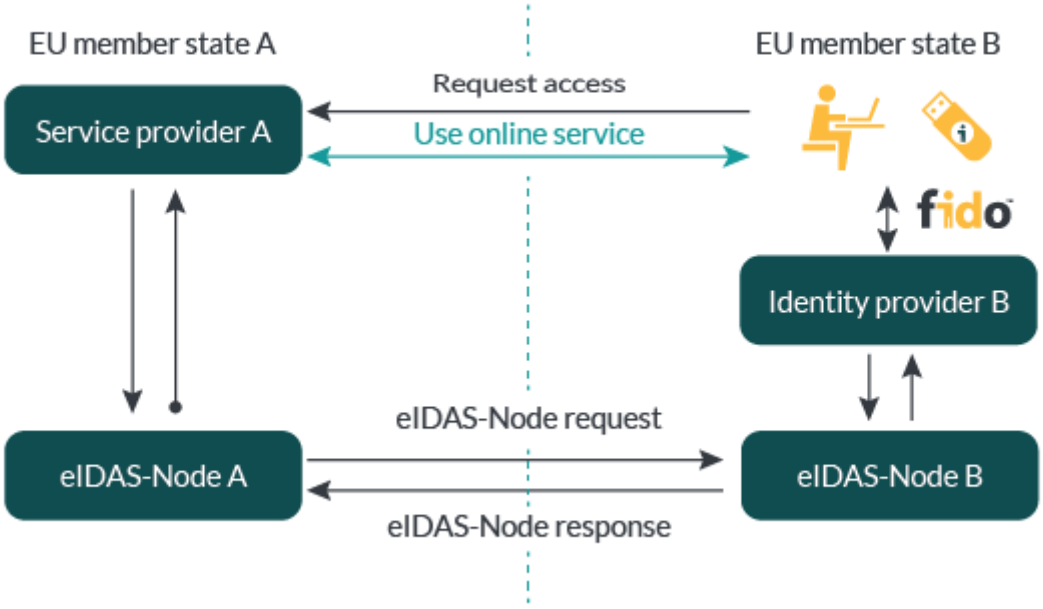

Figure 3 *– Using FIDO2 in a cross-border environment*

In Figure 3, a user in EU Member State B wants to access an online service provider in EU Member State A. Service provider A then redirects the request to the eIDAS-Node in Member State A, which connects to the eIDAS-Node in Member State B. Next, the user can authenticate with FIDO2 to the identity provider in Member State B; this authentication is channeled back through eIDAS-Node B to eIDAS-Node A, and grants the user access to service provider A.

More information on cross-border interoperability between eIDAS-Nodes is available in [1].

3. Using FIDO2 for Authentication to QTSPs

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

To close this gap, CEN (Committee European Normalization) has created three CEN standards (EN 419 241-1, EN 419 241-2 and EN 419 221-5) that address how QTSPs should operate QSCDs in order to create remote Qualified Electronic Signatures. However, no standard exists specifying how exactly to implement the sole control requirement. Hence, FIDO2 is a reliable option.

A FIDO2 Relying Party can be implemented based on the CEN standards to design a QTSP that allows for remote signatures under sole control. An overview of such remote signing QTSP, based on the FIDO2 standard, is illustrated in Figure 4.

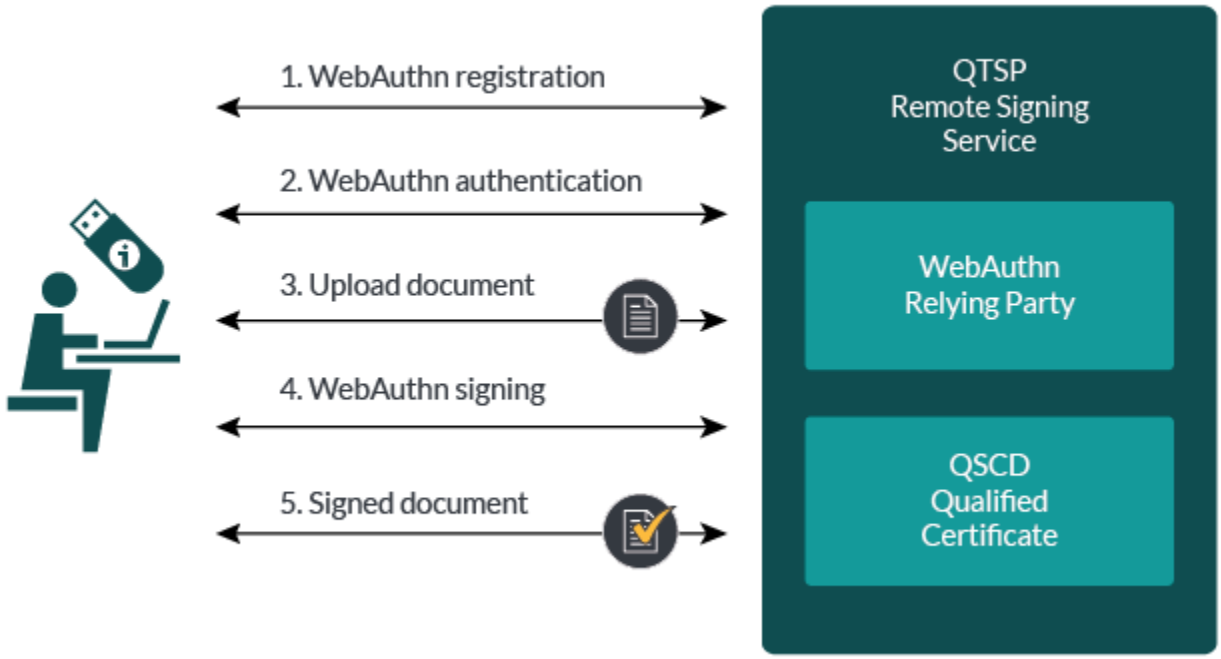

Figure 4 *– eIDAS QTSP with FIDO2 authentication*

There are five steps in this process:

1. The user's FIDO2 authenticator is registered with the WebAuthn Relying Party at the QTSP. The FIDO2 registration should take place immediately after the user has been identified at the QTSP CA for issuance of the Qualified Certificate. At this step, the FIDO2 credentials are associated with the user's key and Qualified Certificate that reside in the remote QSCD.
2. The user authenticates with the FIDO2 authenticator to the WebAuthn Relying Party at the QTSP.
3. The user uploads to the QTSP a document to be signed. The document may also be stored centrally at the QTSP in the user's account.
4. The user's FIDO2 authentication elements are propagated from the WebAuthn Relying Party to the QSCD at the QTSP. This operation unlocks the user's private key in the QSCD, and the document is signed with a Qualified Electronic Signature.
5. The signed document is returned to the user.

More information on how to use design a QTSP with FIDO2 for authentication and sole control is available in [1].

4. Conclusions

FIDO2 meets the eIDAS requirements on eID schemes with assurance level substantial or high with respect to authentication, because WebAuthn is a non-phishable protocol and FIDO2 authenticators are tamper-proof hardware devices. Therefore, FIDO2 authenticators are suitable as electronic identification devices with WebAuthn as the authentication protocol. However, the identification and enrollment processes outlined in the eIDAS regulation must be implemented in addition to FIDO2 to create national eID schemes that can be notified by the European Commission. If done in this way, FIDO2 could be used as part of an eID scheme within EU's cross-border interoperability framework, which allows for citizens in one EU Member State to access online services in another EU Member State.

FIDO2 can also be used for strong end-to-end authentication to a Qualified Trust Service Provider. Based on the WebAuthn authentication protocol, the FIDO2 device can be used to unlock a user 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 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
- 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

CEN	Committee European Normalization
CTAP2	Client To Authenticator Protocol v2
eIDAS	electronic IDentification Authentication and trust Services
ETSI	European Telecommunications Standards Institute
FIDO2	Fast Identity Online v2
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
PDF	Portable Document Format
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
SAML	Security Assertion Markup Language
SMS	Short Messaging Service
W3C	World Wide Web Consortium
WebAuthn	Web Authentication
XML	eXtended Markup Language

7. References

[1] 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

[2] FIDO Alliance white paper, Using FIDO with eIDAS services - Deploying FIDO2 for eIDAS QTSPs and notified eID schemes, April 2020, https://fidoalliance.org/white-paper-using-fido-with-eidas-services/

[3] 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

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

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, December 1999, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN

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.