FIDO Alliance Input to the European Commission

Using FIDO Standards in eIDAS 2.0

October 2021

Introduction to the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance welcomes the opportunity to comment on the selection of potential international and European standards for the European Union's digital identity (EUid) and digital wallet initiative, as detailed in the June 2021 draft amendments to the regulation on electronic identification and trust services (eIDAS).

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, whose logos are shown below, 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.

As the European Commission advances eIDAS 2.0 and considers the best way to ensure that every individual in Europe can benefit from new EU Digital Identity Wallets, FIDO standards and certification programs can provide essential components that will improve security, privacy, control, and convenience.

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.
- The W3C has formalized the Web Authentication JavaScript API (WebAuthn)[1] 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) and ITU X.1288 (FIDO Client to Authenticator Protocol (CTAP)/Universal 2-factor Framework).
- 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.

[1] https://www.w3.org/TR/webauthn/

As we detail below, FIDO standards can be used both to deliver part of EU Digital Identity Wallets that offer superior security, privacy, convenience, and usability, and to enhance remote Qualified Signature Creation Devices (QSCDs). We also provide details on FIDO Alliance certification programs, and the ways Europe can benefit by leveraging these programs.

How FIDO can be used as part of EU Digital Identity Wallets

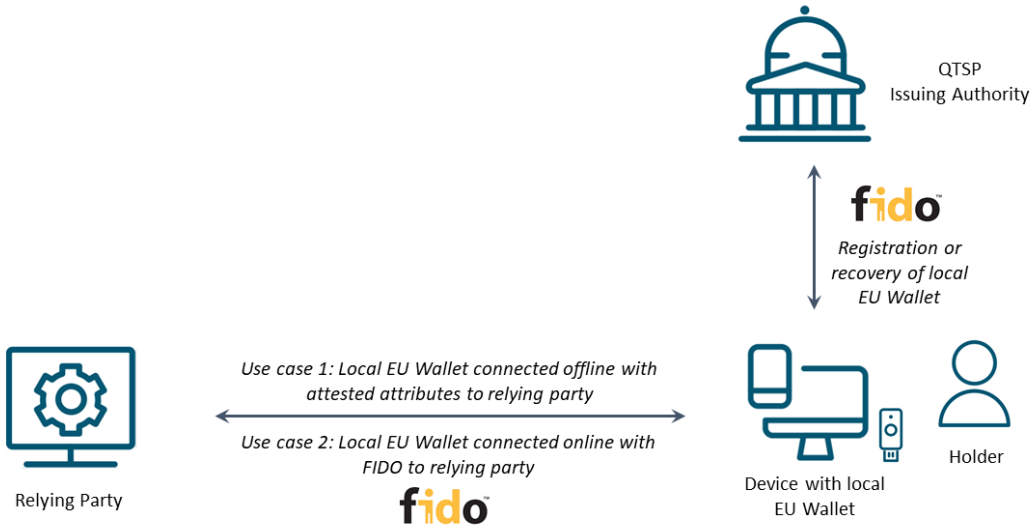
In its proposal to amend the eIDAS regulation, the EU Commission calls for a user wallet that can enable strong online authentication, and hold personal identity attributes and attestations used for identification to authorized relying parties in both online or offline contexts. The digital wallet may be stored locally at the holder's device or be hosted remotely as a SaaS wallet.

The eIDAS articles 6a(3), 6a(4) and 6a(5), which relate to the European Digital Identity Wallet (EU Wallet), can benefit from FIDO Authentication as described in the sub-sections below.

Using FIDO with local EU Wallets

When an EU Wallet is hosted locally at the holder's device, FIDO can be used for authentication to register or recover attested attributes to the EU Wallet in the holder's device. The EU Wallet can then use these attested attributes for offline authentication to the relying party (see use case 1 in the figure below).

The concept of local EU Wallets may also be expanded to hold FIDO credentials generated and stored locally at the device. Such a scenario would allow FIDO Authentication to be used for online authentication to relying parties (see use case 2 in the figure below).



Using FIDO with hosted EU Wallets

When an EU Wallet is hosted remotely at a Qualified Trust Service Provider (QTSP) or at an issuing authority, FIDO can be used for online authentication to release the EU Wallet's attested attributes (see use case 3 in the picture below).

As with local EU Wallets, a hosted EU Wallet may also hold FIDO credentials, generated and stored within the hosted EU Wallet, and be used for online identification to the relying party in this scenario (see use case 4 in the picture below).

Benefits of using FIDO with EU Wallets

Use of FIDO Authentication in EU Wallets offers Europeans a number of benefits:

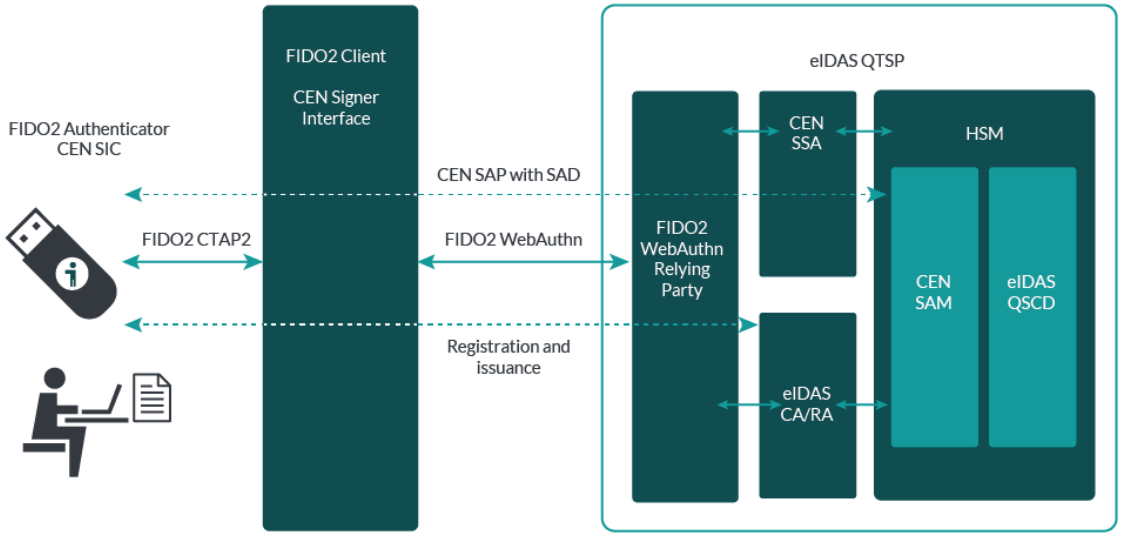
- FIDO could be used as the authentication method (via on-device match of a PIN, fingerprint, or face) for user authentication to a hosted EU Wallet.
- For frictionless user operation: if the Holder has lost or changed phone or computer, there is no need to revoke and reissue their attribute attestations. Roaming FIDO Authenticators – (aka *Security Keys*) that are device-independent and can be used across multiple devices – have the ability to recover attribute attestations from issuers into newly-created local or hosted EU Wallets, or the EU Wallets themselves from previously created backups. The precise recovery process will depend on the devices' implementations.
- The proposed FIDO solutions can be harmonized with the ISO standard ISO/IEC 18013-5 for Mobile Driver's License (mDL).

- Harmonization with QTSPs for remote signing: FIDO can be used for unlocking the private key at the hosted EU Wallet, which could be streamlined with how FIDO can be used with a hosted Signature Activation Module (SAM) for unlocking the private key in a remote QSCD, which is described in the next section.

How FIDO can be used to support a remote QSCD

The eIDAS articles 29a and 39a, with requirements for QTSP for the management of a remote QSCD, can also benefit from FIDO Authentication.

In this scenario, FIDO can be used as an authentication standard to attain an authentication process with high assurance to an eIDAS-compliant QTSP. More precisely, a user can use FIDO for authentication at eIDAS Level of Assurance High to its Qualified Certificate's private key residing in a centralized QSCD, which is operated by a QTSP. A FIDO Authenticator can be used standalone or as part of a local EU Wallet for authentication to the remote QSCD. When the end user is authenticated to their remote private key, it can be used for creating remote Qualified Electronic Signatures. A hash value of the document-to-be-signed can also be included in the FIDO2 WebAuthn challenge or the FIDO UAF transaction link, which allows for a strong (cryptographic) link between the authentication event and the document-to-be-signed. This fulfills the eIDAS Qualified Electronic Signature requirement of the user's sole control over the signing process with a remote QSCD.



This architecture is also compatible with the Committee European Normalization (CEN) standards CEN EN 419 241 and CEN EN 419 221, which specify the Signature Activation Protocol (SAP) and SAM for remotely operated QSCDs. For more details on how FIDO can be used for authentication to remote signing QTSPs, and explanations of the related abbreviations mentioned above, see the FIDO Alliance white paper "Using FIDO with eIDAS services".

Using FIDO for remote identification

The eIDAS article 24(1)c, regarding technical specifications for verification of identity and attributes of natural persons, can also benefit from FIDO.

As described in the report ETSI TR 119 460 V1.1.1, FIDO can be used as part of an eIDAS eID scheme on Level of Assurance High for authentication to a QTSP. FIDO can therefore be used as an authentication protocol for already identified individuals, which may be used as a complementary method for remote identity proofing procedures. It is also possible to redirect the user to an identity provider, which may support OpenID Connect or SAML v2, and use FIDO for authentication to the identity provider.

FIDO Certification Programs

The widespread adoption of FIDO Authentication has been fueled in large part by its robust certification programs that test and confirm that FIDO solutions adhere to FIDO standards.

Note that the FIDO certification program is the largest and most recognized certification program for authentication products in the world. It has been developed over several years by both industry and government,[2] ensuring that the certification requirements meet the needs of both the private and public sectors.

Europe can benefit by leveraging these certification programs – recognizing FIDO® Certified products where appropriate. Given the more than 850 FIDO® Certified products on the market today, recognition of FIDO certification can help to speed new digital ID solutions to market for all Europeans.

FIDO certification programs cover core specifications (UAF, U2F, and FIDO2) to validate product conformance and interoperability. In addition, FIDO Alliance has introduced programs to delineate security capabilities of FIDO® Certified Authenticators as well as to test and validate the efficacy of biometric components. The different levels of FIDO certifications are available at the FIDO certification website. This may be considered for ENISA's European Cybersecurity Certification Scheme (ECCS).

Collaboration with the FIDO Alliance

The FIDO Alliance greatly appreciates the EC's consideration of our comments. We would welcome the opportunity to present to the European Commission, and its Expert Toolbox Committee, a map of FIDO standards and credentials for consideration. Note that we have previously shared a similar proposal with ETSI on how FIDO can be used with the revised eIDAS regulation and in particular the EU Digital Wallet, and we can also share that proposal with the Commission and its Committee if helpful.

We would be happy to answer any questions or collaborate on approaches this map may raise through external meetings or industry subgroups supported at Commission level. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should the offices of DG CNECT or the Expert Toolbox Committee desire to learn more about how FIDO Authentication works.

[2] Note that Germany's Federal Office for Information Security (BSI) is among the agencies that have contributed to the creation of the FIDO Certification Program.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.