Input to the European Commission

Draft Implementing Act

European Digital Identity Wallets – Integrity and Core Functionalities

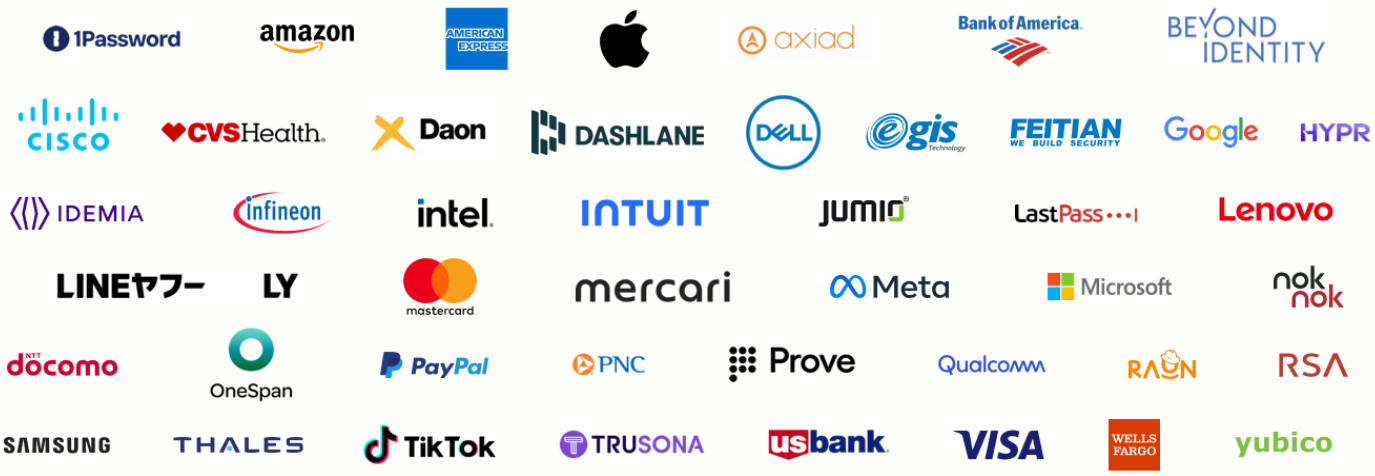
September 2024

To whom it may concern,

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to submit comments to the European Commission (EC) on the Draft Implementing Act for European Digital Identity Wallets – Integrity and Core Functionalities.

As background, 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 included 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, telecommunications, and fintech, as well as those in security, health care, information technology, and government services.



The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the twelve 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 have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is more secure, easier to use, and more privacy-preserving than legacy authentication tools.

Against this backdrop, we were thrilled to see the EC propose the use of the Web Authentication (WebAuthn) standard – which was developed by FIDO Alliance in partnership with the World Wide Web Consortium (W3C) – as the proposed technical specification for pseudonym generation referred to in Article 14 of the Implementing Act for European Digital Identity Wallets – Integrity and Core Functionalities.

The WebAuthn standard was specifically designed to enable pseudonymous and anonymous authentication, and at a time when WebAuthn is becoming the preferred approach to enabling phishing-resistant authentication in government and private sector applications across the globe, it is ideally suited for this purpose.

The use of WebAuthn for pseudonymous authentication in European Digital Identity Wallets is exciting for two reasons:

1) **EUDI Wallets can be "passkey providers" in the authentication ecosystem to enable pseudonymous authentication.**

   As use of the WebAuthn standard for authentication has gained traction across the globe, we have seen increasing use of WebAuthn as a "passkey" – which enables users to have a completely passwordless login experience that is phishing-resistant and delivers multiple factors of authentication. Passkeys may be carried on a specialized hardware device such as a FIDO security key, or carried in protected environments in devices such as laptops and smartphones.

   In this latter case, we are seeing the emergence of two types of "passkey providers" which ensure that a user's passkeys are made available in a secure fashion across all of their devices. Broadly speaking, these passkey providers are either tech platforms that provide this service as a feature of their operating system, or third-party software firms that have historically been known as "password managers," but are now evolving to support passkeys as we push toward a post-password world.

   With the introduction of the ability for a consumer to now also choose to store their passkeys in an EUDI Wallet, we believe these wallets could also become a new form of passkey provider – or, alternatively, in some wallet architectures, stored with a passkey provider that is then made accessible through the WebAuthn API to the EUDI Wallet. To that point, we note that there is active work in FIDO Alliance around creating security requirements for passkey providers, and we would welcome the EC's participation in these activities, as well as input from the EC as to whether there are any challenges they see in a Relying Party using WebAuthn to access passkeys from an EUDI Wallet.

2) **Use of WebAuthn in EUDI Wallets can help to address privacy concerns related to requirements for very large online platforms to accept and facilitate the use of EUDI Wallets.**

   A potentially troubling privacy implication of the requirement in the eIDAS 2 regulation is the requirement that very large online platforms accept and facilitate the use of EUDI Wallets. The concern here is that – in an attempt to give Europeans more privacy-preserving options to log in to different sites – the regulation inadvertently could require very large online platforms to accept credentials that will effectively "over-identify" consumers.

To that point: there has been some discomfort in the authentication community that this requirement could be interpreted to mean that a very large online platform must accept a credential that is bound to identifying data even for applications where the platform does not have a reason or desire to know who a user is. European consumers should not have to over-identify themselves when dealing with very large online platforms just to enjoy the convenience of authenticating via a credential in their wallet.

Put simply, if a platform has no need to know the identity of the individual accessing its services, a requirement that a platform leverage a government-issued credential to authenticate that user would put both the platform and the individual at risk, in that it would share more information than the platform requires to use its service.

Recital 57 of the eIDAS 2 regulation notes that *"if users wish to (use their wallet), very large online platforms should accept them for that purpose, while respecting the principle of data minimsation and the right of the users to use freely chosen pseudonyms."* And Article 5f(3) makes clear that while very large online platforms must accept and facilitate the use of EUDI Wallets for authentication, they must do so *"in respect of the minimum data necessary for the specific online service for which authentication is requested."*

We suggest that the EC should interpret these clauses to allow a very large online platform to only support pseudonymous authentication via WebAuthn credentials stored with an EUDI wallet, rather than require those platforms to also accept credentials that are issued by and tied to a government-issued credential.

By making clear that a very large online platform can choose to support only a pseudonymous WebAuthn passkey for authentication in the EUDI wallet, the EC can avoid a scenario where platforms might inadvertently end up with more information than is necessary on an individual because that individual chose to authenticate with a credential that fully identifies them. This will deliver added privacy protection.

Of course, for applications where anonymity pseudonymity are not possible or desirable, the idea of using a different type of EUDI Wallet credential makes sense. But authentication is not a "one size fits all" situation, and so platforms should be able to choose to leverage only pseudonymous authenticators from the wallet in cases where gathering additional information from an identifiable credential would create additional privacy risks.

This has the added benefit of ensuring that Europeans authenticating to very large online platforms can do so without dependency on a state-issued credential; using WebAuthn enables the creation of a "private credential" that is created without the government having any role, but that can still be stored for convenience and security in the EUDI Wallet under the control of the user.

In addition to the points we raised above, we have three additional comments:

1) The WebAuthn standard is referenced in the Annex of Integrity and Core Functionalities draft implementing act, but not in the draft which outlines Protocols and Interfaces to be supported. We believe it would make sense to include WebAuthn in the Annex of both of these acts.

2) While the draft implementing acts reference the WebAuthn Level 2 specification, WebAuthn is an evolving standard. The EC could future-proof the implementing act by instead calling out "Level 2 or any future version of WebAuthn that meets the requirements of the EUDI initiative."

3) It would also be sensible for the EC to provide more guidance on the standards and protocols to be used with cloud-based wallets.

   Recital 30 of the eIDAS 2 regulation states: *"European Digital Identity Wallets should ensure the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions, taking due account of the different levels of risk."*

   The use of cloud-based wallets is an interesting use case for several EUDI Large Scale Pilots, in particular the EU Digital Wallet Consortium (EWC), which is evaluating the cloud-based wwWallet with leverages WebAuthn support.

   Assuming that some countries will wish to leverage cloud-based wallets, additional guidance from the EC on the requirements for authenticating to and accessing a cloud-based wallet – or a cloud Wallet Secure Cryptographic Device (WSCD) from a native application wallet – would be helpful. Here, we believe WebAuthn is ideally suited as the authentication standard for enabling secure access from the local device to the cloud-based wallet. Among other things, use of WebAuthn will allow for easy recovery if a mobile device is lost: the user needs only to recover the WebAuthn credentials to regain access to their credentials. And if the wallet's backend is supported by a passkey provider, the passkey can be restored seamlessly.

   Additionally, we note that the new WebAuthn pseudo-random function (PRF) extension can be used to encrypt web wallets or cloud WSCD private information at rest so that users' information is safe from compromise while they are not actively accessing it. Future WebAuthn extensions will allow for some or all of the WSCD functionality to be placed inside the FIDO authenticator secure boundary.

We greatly appreciate consideration of our comments. We look forward to further discussion on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this letter.

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