FIDO Alliance Input to the European Commission

eIDAS Inception Impact Assessment

September 2020

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the European Commission's (EC) Inception Impact Assessment regarding the future of eIDAS.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 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.

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 MFA market, addressing concerns about 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 FIDO standards are being used across banking, health care, government, enterprises, and e-commerce to deliver authentication that is both more secure and also easier to use.

In the last year, FIDO has expanded its focus beyond authentication, launching a new effort to bring clarity to the market of solutions for remote identity verification. This new initiative is in the midst of developing performance standards and an independent, lab-tested certification process for remote identity verification solutions that scan and verify the authenticity of government-issued identity documents, as well as match the faces on those documents to "selfie" pictures.

Our comments here focus both on proposed changes to eIDAS that impact authentication, as well as broader identity verification issues.

Up front, we note that the eIDAS initiative has established an excellent model for enabling cross-border recognition of different eID solutions. While the Inception Impact Assessment outlines ways that eIDAS could support additional functionality, the model in place today is one that is impressive.

While we, as an Alliance, do not have strong views on every element of the three options outlined in the Inception Impact Assessment, we do want to offer comments in four areas for the EC's consideration:

1. **With regard to authentication – the EC should ensure that any LOA High solutions require high assurance authentication.**

   MFA adoption has been steadily increasing over the last 10 years – and with it, so have attacks seeking to defeat or circumvent MFA. Attackers have moved on to compromises of authentication tools that are also based on shared secrets, including both OTP and Push-based solutions. Here, we've seen a sharp increase in the number of phishing attacks looking to trick users into either handing over their OTP codes or pushing "approve" on a Push-based solution that has been activated as part of a phishing attack.

Google (a FIDO Alliance member) was one of the first to flag the problem, noting in 2015 that, a *"phisher can pretty successfully phish for an OTP just about as easily as they can a password"* and noted their shift to FIDO hardware-based solutions as the way to stop these targeted phishing attacks.[1] Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflected their experience with this technology.

2016 also saw what was perhaps the most visible and impactful phish of an OTP code, when the U.S. election was disrupted when Clinton campaign chair John Podesta's OTP-protected account was phished by the Russian government.

Since that time, the ability of adversaries to successfully phish OTP has only increased. Free, open source tools like Evilginx are easily available to anyone looking to phish a shared-secret-based authentication factor.[2] Per the release notes for Evilginx 2: *"Evilginx, being the man-in-the-middle, captures not only usernames and passwords, but also captures authentication tokens sent as cookies. Captured authentication tokens allow the attacker to bypass any form of 2FA enabled on user's account (except for FIDO U2F)."*[3]

OTP is routinely phishable, as attackers have figured out ways to phish OTP codes from users. Attackers have also found ways to phish authentication based on push notifications. If attackers can trick users into typing in a password, they can also trick them into sharing a six digit code or clicking "approve" on a push-based authentication app.

As a result, leaders in the security community have begun to move away from OTP and other authentication tools based on "shared secrets." Industry is shifting toward "high assurance" MFA where at least one factor is based on public key cryptography, and thus cannot be phished. Authentication using the FIDO standards is one such example.

As part of any eIDAS revision, the ED should ensure that any LOA High solutions require "high assurance" authentication in order to guard against these increasingly common attacks. The Commission Implementing Regulation EU 2015/1501 on the interoperability framework should require credential phishing resistance at LoA High; solutions unable to provide that protection should be relegated to LoA Substantial or Low.

Doing so would ensure eIDAS implementers clearly differentiate between tools that are phishing resistant and those that are not. Given how attackers have caught up with the latter, it no longer makes sense to allow LOA High solutions to use these authenticators.

2. **Extension of eIDAS to the private sector under Option 2 would be well-received by many companies.**

We note at a high level that the potential extension of eIDAS to the private sector under Option 2 would be of great interest to many firms, given the challenges with remote identity verification. In many countries, private sector remote identity verification tools are trying to "guess" what only the government actually knows.

Given this, the ability of eIDAS to support identity proofing not only for government transactions but also those in the private sector would help private entities have a higher level of confidence with regard to who they are dealing with online, and enable additional high-value transactions to be moved into the digital realm. We agree with the statement in the Inception Impact Assessment that *"an extension of eIDAS to the private sector is likely to generate considerable economic gains through an increased offer and uptake of identification and authentication for activities intermediated online*."

3. **All Europeans could benefit by creating new options for creating digital versions of physical identity documents.**

As the Inception Impact Analysis noted, *"the COVID-19 crisis has highlighted the urgency to provide all European citizens and businesses quickly with a universally accepted, trusted digital identity and with trust services such as eSignatures to allow for seamless business continuity in the Single Market, access to crucial and sensitive public online services such as in e-Health, eGovernment and e-Justice and mitigate against identity fraud."*

[1] See https://www.youtube.com/watch?v=UBjEfpfZ8w0

[2] See https://github.com/kgretzky/evilginx2

[3] See https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/. Note that while Evilginx is formally published as a tool for researchers, it and many other similar tools can be used for nefarious purposes.

One issue is that in some countries uptake of digital identity solutions may be mixed, and lag behind the number if individuals who have a physical identity credential issued by that country. Allowing individuals to leverage their physical credential to generate a companion digital credential – perhaps via a smartphone app – can help to extend the reach of digital identity and the eIDAS ecosystem. Essential to enabling this model, however, is the recognition of approaches to enable remote identity proofing.

We raise this issue largely to highlight that FIDO Alliance launched a new effort to bring clarity to the market of solutions for remote identity verification.[4] This new initiative is in the midst of developing performance standards and an independent, lab-tested certification process for remote identity verification solutions that scan and verify the authenticity of government-issued identity documents, as well as match the faces on those documents to "selfie" pictures. This new "Identity Verification and Binding Workgroup" features participation from a number of governments and companies who are looking for a global, credible, independent industry certification for remote ID proofing products; many of the leading vendors in this market are also contributing inputs and perspectives.

As the EC considers new ways to create and provision digital identity credentials, we would urge the EC to look to leverage this new identity certification program as one way to vet remote identity proofing tools for use in the eIDAS ecosystem.

4. **Mutual recognition and re-use of pre-approved ID products.**

   If a product has been approved for use with an eID scheme in one EU member state, it would be beneficial with an eIDAS framework that could allow for the same product to be re-approved for other eID schemes. That could simplify the approval processes for eID schemes, which in turn could increase the rollout pace and adoption of eID schemes in the EU.

   Per the point above – regarding FIDO Alliance's new initiative to create a certification program for remote identity proofing tools – we would welcome the chance to explore how eIDAS may be able to better leverage industry certification programs as part of the approval process. FIDO administers a number of industry certification programs including security certification for authentication products and independent lab testing for consumer-grade biometric components; these programs have been developed in concert with – and recognized by – other governments. Accordingly, leveraging these certifications may be helpful to the EC in efforts to increase the uptake and reach of the eIDAS ecosystem.

We greatly appreciate the EC's consideration of our comments. We look forward to further discussion with the EC and the eIDAS team 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 response.

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

[4] More on this effort is at https://fidoalliance.org/identity-verification-binding/