July 25, 2024

To whom it may concern:

We appreciate the opportunity to provide comments to the European Commission on the draft implementing act under the NIS2 Directive.

As background, the Fast Identity Online (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, and information technology.

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 both more secure and also easier to use than legacy authentication tools. However, as we detail in our comments below, we are concerned that the draft implementing act for NIS2 does not sufficiently differentiate between phishing resistant authentication and legacy authentication tools that are increasingly vulnerable to phishing attacks.

The importance of phishing-resistant authentication – and FIDO standards – are recognized across the globe.

- ENISA and CERT-EU highlighted the importance of FIDO in a 2022 publication entitled "Boosting Your Organization's Cyber Resilience (JP-22-01),"[1] noting:

  > *"If possible, avoid using SMS and voice calls to provide one-time codes and consider deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."*

- The Netherlands National Cyber Security Center (NCSC) highlighted the importance of phishing-resistant authentication in its publication "Mature Authentication – Use of Secure Authentication Tools."[2] That guidance notes:

  > "A distinction can be made between the implementation of two-factor authentication (2FA) and phishing-resistant authentication" and goes on to note that SMS, software tokens and hardware tokens are all *"not totally resistant to phishing."*
  >
  > It goes on to advise that *"A standard from the FIDO Alliance, known as FIDO2, is resistant to phishing. Therefore, tokens that implement this standard provide the most comprehensive protection for authentication at this time."*

- In the US, the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory[3] echoing the concerns of ENISA and the NCSC, noting:

  > *"Not all forms of MFA are equally secure. Some forms are vulnerable to phishing, "push bombing" attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM Swap attacks. These attacks, if successful, may allow a threat actor to gain access to MFA authentication credentials or bypass MFA and access the MFA-protected systems."*

  The CISA guidance goes on to note:

  > *"While any form of MFA is better than no MFA and will reduce an organization's attack surface, phishing-resistant MFA is the gold standard and organizations should make migrating to it a high priority effort,"* and also notes that *"The only widely available phishing-resistant authentication is FIDO/WebAuthn authentication."* – although it notes that PKI-based MFA is also phishing-resistant, if not as widely available.

[1] See https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

[2] See https://english.ncsc.nl/publications/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools

[3] See https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

- Also in the US, an August 11, 2022 circular[4] from the U.S. Consumer Financial Protection Bureau (CFPB) states:

> *"MFA solutions that protect against credential phishing, such as those using the (FIDO) Web Authentication standard supported by web browsers, are especially important."*

Concerns with the draft implementing act

Against this backdrop, we wanted to flag our concerns that the draft implementing act and accompanying Annex are both silent when it comes to acknowledging the concerns that ENISA and other agencies have flagged about legacy authentication tools. It would seem that the draft act or annex should echo these points, and note that legacy authentication tools are increasingly vulnerable to phishing attacks and encourage implementers to select authentication technology that can stand up against these attacks.

- The draft implementing act points to "passwords and other authentication means" (paragraph 18). This was surprising to see given the very limited efficacy of passwords as a security tool; we would expect that in 2024, use of passwords alone would not be considered a reasonable part of any "cyber hygiene practices." When later discussing MFA (paragraph 21), the draft act is silent on the type of MFA that should be used.

- The draft annex does contain more detailed sections on authentication (11.6) and MFA (11.7), however, neither gets into the specifics of whether authentication solutions should be phishing resistant.

While we understand that this draft annex may not wish to be overly specific, we do note that section 11.6.2 does get into very specific, prescriptive requirements for authentication, such as requiring "the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts," as well as "terminating inactive sessions after a predefined period of inactivity."

Given that the draft act already includes some specific security requirements on authentication, it would seem logical that it should go further to address the threat that authentication credentials can be phished.

To be clear, we do not believe it would make sense to call out FIDO or any other authentication standards in the text of the act or the annex itself. Indeed, as CISA notes, PKI-based MFA is also phishing-resistant, and there are certainly non-standard proprietary products on the market that also have this quality.

However, we do believe it is worth highlighting the threat of authentication being phished – much as the annex points to other security concerns and requirements – and calling for implementers to leverage phishing-resistant authentication wherever possible.

[4] https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

We greatly appreciate the Commission's consideration of our comments. We look forward to further discussion with the Commission 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.

Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should Commission officials wish to learn more about how FIDO authentication and how its certification programs work.

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