MEP Melchior, tech experts and civil society debate cybersecurity risks within the eIDAS revision

- ***Proposed eIDAS revision poses security threat to internet users, according to tech experts***
- **Scott Helme, independent security researcher: *"If it's on the internet and it's communicating, it's probably using certificates, so the stakes are high."***
- ***Panelists warned that the changes could enable state-sponsored internet surveillance.***

Brussels, 17 November 2022: Cybersecurity risks in eIDAS were the topic of a breakfast event (*Web security in an insecure world: risks within the eIDAS revision*) on 15 November 2022 with panelists Karen Melchior MEP, Eric Rescorla Chief Technology Officer at Firefox, Scott Helme, Security Researcher and Thomas Lohninger, Executive Director at Epicenter.Works and Vice President at EDRi. They discussed the differences of opinion around the European Commission's proposed revision to the eIDAS regulation. Member of the European Parliament Karen Melchior gave the keynote speech in her role as shadow rapporteur on the eIDAS revision in the EP Committee on Legal Affairs (JURI).

Article 45, which formed the main part of the discussion, deals with Qualified Web Authentication Certificates (QWACs,) a new form of web certificate which ties a website to a legal entity. The article as proposed by the Commission mandates the acceptance of QWACs into a browsers' root store, purportedly bypassing existing checks put in place by the browsers.

The panelists engaged with the audience about several cybersecurity concerns with the proposed revision. They explored how the context of an increasingly volatile world where democracies are under pressure meant that web security is of utmost importance.

Karen Melchior (Renew), Member of the European Parliament and shadow rapporteur on eIDAS in EP Committee on Legal Affairs (JURI), said: *"I initially thought the eIDAS revision would be a good idea, and then we got to article 45. While having a European digital wallet is crucial, the Commission's proposal […] is dangerous for a number of reasons, including facilitating phishing and state-sponsored surveillance. Unfortunately, we must regulate with worst case scenarios in mind, that not all EU governments are going to be democratic and act democratically. This must and can be fixed."*

In effect, the proposal removes the transparent process whereby browsers vet the authorities which issue web certificates, before accepting them into their root store. Removing these existing audits would mean that users are less protected. The panelists warned that forcing browsers to accept QWACs would lower the security standard for internet users all over Europe, opening them up to serious risk. It would make it easier for actors with bad intent to steal data or commit crime online.

Mozilla's Eric Rescorla mentioned that while there is no malicious intent in the EU's proposals, the approach can be copied by others, and cited past cases where states such as Kazakhstan attempted to impose similar processes, opening users to risks of state-sponsored surveillance. Within Europe the European Parliament voted recently to confirm Hungary's status as a non-democracy, which highlights the importance of maintaining the independence of security verification processes.

Interventions from audience participants focused on the importance of linking a website to a legal entity via a QWAC. Security researcher Scott Helme, said that he failed to see the advantage of this,

highlighting that it could lull users into a false sense of security just because they have a small piece of extra information. Commenting on QWACs, he added that "*QWACs are a reincarnation of EV certificates which died a few years ago. It's unclear why the Commission would want to reintroduce them when they've already been discredited.*"

Extended Validation (EV) certificates, which QWACs are based on, also linked websites to a legal entity and notified web users of this via a green padlock in the URL address bar. Despite this, it was found that they could be used to create believable phishing sites and most browsers removed the visual indicators by the end of 2019.

An intervention from Thomas Lohninger, Vice-President of the European Digital Rights NGO EDRI and Executive Director at Epicenter.Works included wider concerns regarding the eIDAS regulation. Lohninger commented that: "*The eIDAS reform aims to create a trusted environment for our most sensitive health, financial and identity data. We have yet to see if the final legislation includes the privacy safeguards to deliver on that promise. But it's ludicrous that this same legislation also includes a direct attack on the security of the World Wide Web in the form of QWACs*."

In the concluding remarks, independent security researcher Scott Helme said: *"I've tried to understand the proposal and I am failing to see the benefits of imposing QWACs on browsers. It's seems to me that the one group that are strongly in favour of them are the people that will make a lot of money."*

The panelists also drew a link between the recent issues faced by Twitter with verified profiles being acquired by third parties, highlighting that paying for extra verification and showing a visual signifier is not a guarantee of safety and good intent.

Learn more at **securityriskahead.eu**

For media enquiries please contact harriet.fry@hkstrategies.com

---

About #SecurityRiskAhead

#SecurityRiskAhead is a campaign backed by Mozilla. Its main aim is to provide up to date information about the eIDAS regulation and its potential impacts. For more information visit www.securityriskahead.eu

About Mozilla

Mozilla is the public benefit technology company and maker of the open-source Firefox web browser, Mozilla VPN, and the Pocket "read-it-later" application. These products are used by hundreds of millions of individuals around the world. Mozilla Corporation is a private company fully owned by its sole shareholder, the non-profit Mozilla Foundation. The Mozilla Foundation furthers our mission to protect an open and accessible internet, by investing in advocacy, research, and movement-building. It is guided by the set of principles in the Mozilla Manifesto that recognise, among other things, that the internet must remain open and accessible; and that security and privacy are fundamental.

Notes to editors

Web authentication – how it currently works:

Web authentication is the technical mechanism that ensures that users are visiting the website they want to visit and are not directed to entities masquerading as that website. In order to do so, websites are given a certificate (issued by a Certificate Authority or CA) that confirms they control the domain name that the user navigates to and that it has not been compromised by a cybercriminal.

Most major browsers have a rigorous process to vet CAs for trustworthiness before the certificates they issue are trusted in the browser (i.e included in the browser 'root certificate store'). These programs are responsible for evaluating candidate CAs based on published criteria and requirements for what makes a trustworthy CA. Root stores are also responsible for removing CAs which violate those requirements.

What are QWACs?

A Qualified Website Authentication Certificate (QWAC) aims to make it possible to authenticate a website and link the website to the natural or legal person to whom the certificate is issued. QWACs rely on a discredited security architecture and have a lower bar for security than other website certificates.

The 2021 proposed changes to eIDAS mandate that browsers automatically include QWAC-issuing certificate authorities (CAs) identified by EU member states in their browser root stores, without any restrictions or caveats. This effectively removes some of the existing checks in place and could erase web security gains made over the last decade. By pushing QWACs and overriding browser security protections to do so, the eIDAS regime will expose web users to new cybersecurity risks.

What does Mozilla propose instead?

Mozilla, a not-for-profit dedicated to improving internet security and supportive of the EU's regulatory efforts, proposes to amend article 45.2 so that it does not establish a limitation on cybersecurity and averts future harm. In practice, this means ensuring browsers can continue to block certificate authorities that don't meet security standards. As a result, this will keep potential malign actions at bay while also continuing to protect individuals' sensitive data.