IT'S QWACkers! EU's eIDAS PROPOSAL THREATENS ONLINE CYBERSECURITY AND ATTRACTS GROWING CRITICISM

- ***Proposed EU legislation poses security threat to internet users***
- ***In the wrong hands, the changes could enable state-sponsored internet surveillance***
- ***Brussels sees growing criticism of article 45.2 of the proposed eIDAS regulation***

Brussels, 13th July 2022: There is a serious threat to existing internet security measures stemming from the European Commission's proposed revision to the eIDAS regulation. The European Parliament ITRE Committee (leading on the file) has their last meeting before the summer recess today. If implemented, experts say it could open individuals browsing online to additional security risks and set a precedent to allow state sponsored internet surveillance. As currently drafted, article 45.2 could undermine the EU's own ambitions to be the frontrunner of a more secure, responsible and competitive internet that protects citizens, businesses and European democracy from illegal activity.

For close to 30 years, a web security ecosystem has existed that protects people from fraud, identity theft and surveillance, using website certificates. Under the revised article 45.2 of the eIDAS regulation, browsers would be mandated to accept the EU-designed Qualified Web Authentication Certificates (QWACs) even though they have weaker security properties than those most browsers currently allow. Moreover, browsers would be prevented from applying any of the existing security due diligence checks to the entities which issue these certificates, thereby bypassing the critical first line of defense against cybercrime on the web.

Article 45.2 is attracting growing attention from parliamentarians and cybersecurity experts alike. In her draft report, MEP Romana Jerković, the file's rapporteur, deleted it in order to have more time to figure out an approach that doesn't compromise security. Others have also expressed concerns. In a letter sent to MEPs and EU states, academics said that mandating the use of QWACs could introduce "*significant weaknesses into the global multi-stakeholder ecosystem for securing web browsing.*" The academics added that the move could make it "*more difficult to protect individuals from cybercriminals*."

Mozilla's Chief Security Officer, Marshall Erwin said: *"The proposal effectively removes existing cybersecurity checks which help to keep individuals safe online. 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."*

Attempts have been made in the past to forcefully bypass browser security checks for rights-interfering ends, most notably in Kazakhstan in 2020 and Mauritius in 2021. In both cases, the governments aimed to use so called "man-in-the-middle" attacks to carry out state-sponsored surveillance of internet traffic. These actors will be emboldened by the new norm this law would enshrine.

Marshall Erwin said: "*The bigger concern is the precedent that this regulation will set around the world. Because of the impressive growth in encrypted web traffic, what we've seen in the last few years is an increase in authoritarian regimes globally trying to undermine web security. While this is not the intent of the EU, the inclusion of article 45.2 in the eIDAS regulation will make it more difficult to push back on these surveillance attempts in future. The EU sets many global standards, and we're concerned that if this is copied elsewhere, the regulation would give the tools to governments to carry out state-sponsored surveillance of internet traffic. Such actions present a very real and dangerous unintended consequence of the EU's digital identity plans.*"

There are numerous examples of the serious consequences arising from state-sponsored surveillance of web traffic. In one notorious case almost 300,000 IP addresses in Iran were

redirected to falsified sites that enabled bad actors to monitor end-users communications. The attack reportedly could have put the lives of citizens in danger because the government would have had access to their private data and personal opinions.

Alexis Hancock, Director of Engineering, Certbot, Electronic Frontier Foundation said: *"We don't want to create a web security ceiling. We want to lay the foundations. I see the current proposal for Article 45 as that ceiling, where browsers aren't able to respond to security incidents quickly and efficiently. I hope to see continued collaboration around securing users across the internet equally, no matter where they are in the world."*

Thomas Lohninger, Executive Director, Epicenter.Works said: *"The eIDAS reform tries to establish an EU-wide general purpose infrastructure to electronically identify citizens vis-à-vis governments and corporations. Achieving this without throwing privacy out the window and losing the trust of citizens is already a huge task in front of EU lawmakers. It doesn't help that Article 45 of the same bill is a direct attack on the security of the world wide web and empowers governments to do mass surveillance against their citizens."*

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.