MEPs adapt eIDAS article 45.2 due to cybersecurity concerns

Trilogues will see final decision on future of web security

- Speaking at an event, MEP Mikuláš Peksa explained that the Parliament is amending the eIDAS text because MEPs feared it would set a ceiling on cybersecurity standards.
- Mozilla and the European Signature Dialogue went head-to-head in a discussion about this crucial article of the EU's proposed eID regulation.
- The lead committee (ITRE) is due to vote on the text on 9 February.

Brussels, 1 February 2023: A panel debate on 25 January about the revision of the European eID regulation brought together opposing viewpoints on the increasingly contentious Article 45.2. Cybersecurity experts and MEPs have expressed concern that it would push an outdated technology called Qualified Web Authentication Certificates (QWACs) and give governments the power to circumvent existing cybersecurity protocols. The panel discussion featured Paul van Brouwershaven from the European Signature Dialog, Thomas Lohninger, Board Member of European Digital Rights (EDRi) and Executive Director at Epicenter.Works, Mikuláš Peksa MEP, ITRE Shadow Rapporteur for the review of the eIDAS regulatory framework and Marshall Erwin, Chief Security Officer at Mozilla.

Speaking directly after a meeting of the Parliament's industry committee (ITRE), MEP Peksa revealed that the MEPs had agreed to a compromise on the article which will mean that browsers will be able to retain the integrity of their Root Stores. These are the lists of Certificate Authorities trusted by browsers. According to MEP Peksa, the compromise will mean that browsers will need to display QWACs, but they will still be able to vet Certificate Authorities before accepting them and will be able to block those that have not reached appropriate standards.

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 would be emboldened by the new norm this law would enshrine.

The eIDAS file is currently in the later stages of the EU's ordinary legislative procedure. The lead industry committee vote in the European Parliament is scheduled for the 9 February and the text will then go to a plenary vote. Following this, trilogue negotiations will start with the Council who adopted their general approach in December. The Council left article 45.2 as it was originally drafted in the Commission's proposal.

Last year MEP Romana Jerković, the file's rapporteur, deleted article 45.2 from her draft report. Several MEPs from different party groups have also tabled amendments removing the obligation for browsers to accept QWACs. Two committees for opinion in the European Parliament (the IMCO and JURI committees) either amended or deleted article 45.2 in autumn 2022.

Paul van Brouwershaven attended the panel as a member of the European Signature Dialog, a network of European Trust Service Providers who issue QWACs. Van Brouwershaven started the debate by setting out why the European Signature Dialogue believes that eIDAS article 45.2 should be adopted in its original wording. In particular, he emphasized that EU citizens have the right to know who they are dealing with online. He stated that article 45.2 would enable recourse by giving users the verified entity behind the website in a user-friendly manner.

In response, Marshall Erwin pointed to EV certificates which held similar functionality to QWACs and explained that most browsers had removed their visual indicators by 2019. Research has since demonstrated that EV certificates and QWACs provide users with a false sense of security that could be exploited for malicious purposes such as phishing and domain impersonation.

Despite this, he pointed that his main concern was that article 45.2 would impact Root Store policies which have been developed to protect individuals from attacks.

"While well intentioned, we believe that the original language in Article 45.2 poses grave risks to web security within Europe and will set a worrying precedent that will be leveraged by authoritarian regimes around the world.

As it stands, the draft parliament compromise will meaningfully protect the vital independence of browser root store programs while ensuring that the implementation of QWACs is based on cybersecurity best practices rather than political or financial considerations.

Any future compromises must continue to meet these two minimum criteria, especially in subsequent implementing acts, and we look forward to constructive engagement that implements QWACs in a safe, secure, and effective manner."

Thomas Lohninger of the EDRi pointed to wider security implications of the eID regulation. Speaking on article 45.2 he said: *"We saw a massive increase in encrypted web traffic after certificates were given away for free. Any form of business model around QWACs would be detrimental to security if we want to roll them out on a mass scale."*

QWACs are currently available for between €700 and €1,400, depending on the provider whilst there is no charge for some other web certificates. Browsers do not gain from this charge, the figure is charged by European Certificate Authorities known as Trusted Service Providers.

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.