Latest wording on QWACs does not correspond with the principles agreed in trilogue

Mozilla, through its #SecurityRiskAhead campaign, has been building awareness around internet safety and the role of web certification in ensuring the safety of users on the web in the context of the new EU eIDAS Regulation. As the negotiations on this file are coming to a close, we wish to continue the constructive dialogue with all stakeholders towards a solution for Article 45 that reflects the principles agreed at the political level between the institutions and keeps internet users safe.

What is the latest news on Article 45?

The Commission's proposal for Article 45 in eIDAS was concerning to us and many other cybersecurity experts in that it upended many of the norms and practices of web certification that have made the internet as safe as it is today. The security of the web is at the heart of Mozilla's mission and we consider the safety of our users paramount. As such, we felt compelled to make our voice heard to ensure the best possible outcome for European Citizens. We believe that eIDAS should seek only to improve the security of web users and not not undermine existing security practices through clauses mandating exceptional treatment.

As a solution to the security risks of this obligation, the European legislators have agreed in the last political trilogue to allow browsers to take precautionary and preventive measures against QWACs that were deemed unsafe (Article 45a). This is a very welcome addition and seemingly a win for the safety of users online.

In the same trilogue, there was also a political agreement to limit the obligation to recognize QWACs solely to the display of the identity information contained in the certificate. We believe this is a sensible approach because it fulfills the objectives of QWACs (to show internet users which legal entity owns a website) while not overriding existing cryptographic protocols that keep the connection between internet users and websites secure.

However, the latest wording of Article 45, fails to reflect these principles and leaves it ambiguous as to whether Article 45's provisions, especially paragraph 2a's requirement not to impose additional security checks, applies to the types of certificates used to web browser's connections. If enacted, this obligation would fatally undermine the agreement not to override existing security protocols, jeopardize the security of user's private communications with websites and make any precautionary measures effectively toothless.

Two security issues stand out in the latest legal text, as agreed in technical meetings, especially when compared to the principles agreed in trilogues.

Issue 1: The addition of paragraph 2a in Article 45 undermines the agreed trilogue principles and renders the cybersecurity exemption of Article 45a moot. According to the latest wording of Art. 45 para 2a QWACs *"shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1."* This wording would establish a security ceiling for browsers, making it impossible to adopt new security technology and checks. For example, browsers are already looking

to adopt new technology like post-quantum cryptography in certificates which is essential for the security of the web. Browsers cannot enforce the use of this technology without introducing a new mandatory check.

This is especially problematic as the current text of Article 45 does not reflect the agreement to scope QWACs to identity information only (see Issue 2), meaning that information carried in certificates which is not part of eIDAS Annex IV (e.g. website public keys) falls within these provisions.

It is also important to note that this provision was never part of either the Council's or the European Parliament's original positions before entering into interinstitutional negotiations. We do not believe a regulation banning browsers from adopting new security checks is in anyone's interests. To the extent that there are legitimate concerns around discriminatory treatment of QWACs, these could be addressed with a requirement not to subject QWACs to any excessive requirements beyond what browsers apply to all other certificates.

Issue 2: The obligation to recognize only the identity information in QWAC should be clarified explicitly in Article 45 in order to remove any ambiguity when interpreting text in Recital 32.

As written, the current eIDAS text has a raft of unintended consequences because the scope of the requirement placed on browsers is unclear. If the requirement to recognise QWACs extends to the information used to establish secure connections with websites (e.g. public keys) then eIDAS2 will be placing the security and privacy of European citizens in the hands of the least effective supervisory body. This means, for example, that a national supervisory body in one member state could substantially damage internet commerce and user privacy in another member state due to reluctance to enforce decisions against local QTSP who contribute to the local economy.

This could be easily fixed by ensuring the legislative text of Article 45 reflects the agreed position that the requirement to recognise QWACs will only extend to identity information. This will ensure that browsers can carry out their own security checks on the cryptographic material contained in certificates and used to establish secure connections, whilst still ensuring the browsers are required to authenticate and make available the identity information according to EU rules

What is the solution

We seek a compromise that would maintain the merits of QWACs, i.e., the display of identity information, while at the same time ensuring that only the QWACs that have passed browsers' cybersecurity standards would be used to ensure the security of the connection. We believe that this is the only effective way to decouple the otherwise contradictory policy requirements of certificates for legal identity and certificates used for securing browser's internet connections.

Concretely, we urge policymakers to include the principles of separation agreed at the political level and in Recital 32 in the binding terms of the Regulation and specifically in Article 45 by amending as follows:

- **Recital 32:** [...] Recognition of QWACs means that the providers of web browsers should not deny the authenticity of qualified certificates for website authentication. ***Such recognition solely means that web browsers shall attest*** ~~***attesting***~~ the link between the website domain

name and the natural or legal person to whom the certificate is issued and ***confirm*** ~~***confirming***~~ the identity of that person. [...]

- **Art 45 - paragraph 2**: Qualified certificates for website authentication issued in accordance with paragraph 1 shall be recognised by web browsers~~***. Web-browsers shall ensure***~~ ***solely by ensuring*** that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner [...]

These changes will ensure that browsers have a duty to recognise QWACs and make legal identity information available, without compromising the security of user's browsing connections.

We urge policymakers to adopt the above recommendations before the conclusion of the trilogue discussions on the eIDAS Regulation, ensuring that users safety online will remain intact and in accordance with the highest cybersecurity standards and norms.