New ETSI draft standard on QWACs is good news for safety of European internet users

In November 2023, Mozilla and many other stakeholders raised concerns about the finalised text for the eIDAS regulation. In response to these concerns, the text of the regulation was adjusted to add new safeguards :

> The obligation of recognition and interoperability of and support for qualified certificates for website authentication does not affect the freedom of providers of web-browsers to ensure web security, domain authentication and the encryption of web traffic in a manner and by means of technology that they consider to be the most appropriate. (Recital 65)

However, the practical implication of this regulation and the new safeguards remained unclear, with the implementation needing to be described in a technical standard by ETSI and adopted into EU law by the European Commission.

On December 9th 2024, the European Telecommunications Standards Institute (ETSI) published a draft technical specification for the support of Qualified Web Authentication Certificates (QWACs) in web browsers.

Mozilla has worked hard to engage with ETSI over the past year to ensure that the vital safeguards adopted by the European Parliament were reflected in this draft standard. Critically, the current draft standard is clear that it does not impose any restrictions or obligations on how browsers establish encrypted connections with websites, ensuring that browsers can continue to uphold the security and privacy of web users:

> Establish a secure TLS connection with the site using the web browsers' procedures and configuration, and evaluate the presented TLS Certificate with the security requirements of the web browser vendor and their policies for web security, domain authentication and the encryption of web traffic as outlined in Recital 65 of the Regulation (EU) No 2024/1183 [i.3]

The draft standard also introduces a new way for browsers to use the identity information contained in a QWAC without relying on the QWAC to establish an encrypted connection with the website. This approach, dubbed '2-QWACs' in the draft standard, allows any QTSP to issue a QWAC which can be used in web browsers to provide identity information about a website, without any risk to the privacy or security of user's encrypted connections with websites.

However, the draft standard still requires a final round of changes and formal approval from ETSI. Once approved, it will need to be included in the European Commission's upcoming implementing act on QWACs, expected to be published by May 2025. Mozilla will be continuing to engage with ETSI and other stakeholders over the coming months to ensure the final standard delivers the promised privacy and security safeguards for European web users.