Mandated Qualified Web Authentication Certificates (QWACs)

October 2023

The Internet Society, Center for Democracy and Technology, Electronic Frontier Foundation, and Epicenter.works are concerned that despite previous discussions at which the goals and concerns of relevant stakeholders, including the Commission, were debated, the text relating to Qualified Web Authentication Certificates (QWACs) in the eIDAS proposals remains ambiguous, and risks undermining trust in browsers as a globally deployed element of the Internet ecosystem.

Analysis

Browsers process certificates to secure and authenticate their connection to servers: this underpins trustworthy and safe browsing, for countless purposes, worldwide. Browser certificates and their issuers are subject to a legitimate and stringent set of requirements which differ from and, in some respects, exceed the policy requirements expressed in Article 45 of the proposed eIDAS regulation[1] and the technical and security requirements for QWACs.

A vetting process that establishes whether a certificate authority (CA) is fit to issue QWACs, by definition, does not establish that the CA is fit to issue the Transport Layer Security (TLS) certificates used to secure browsers' Internet connections. Conflating these two sets of assurance requirements undermines the trustworthiness of the browser, the connections it can establish, and the governance regime for CAs globally. It erodes the value of established CA-supported trust schemes.

Previous multi-stakeholder discussions resulted in an apparent compromise, establishing a clear functional separation between QWACs and browser connection security, and limiting QWACs to the delivery of identity information in a verifiable form. This reflects the reality that QWACs and browser certificates have different functional goals. Those different goals also lead to two substantively different sets of user interface (UI) requirements. On the one hand, Article 45 envisions the clear display of data asserting the identity of a website owner; on the other, years of experience to date indicate that displaying more *security* information to users does not result in greater safety and security. In practice, the most constructive user experience comes from: secure defaults; trustworthiness of the

[1] https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2021/0281/COM_COM(2021)0281_EN.pdf

underlying CA infrastructure and its governance; and only alerting the user in case of a violation of the browser certificate rules.

The current Article 45 text lacks sufficient clarity and detail about relevant functional differences between QWACs and browser connection certificates. If users mistake one for the other, they are likely to make misguided trust decisions based on mistaken assumptions about what each type of certificate "means". This is more likely to confuse users than to help them, since as far as users are concerned, there will be no apparent difference between one type of certificate and another. This outcome represents a systemic threat to trust in the Internet and online services.

The browser ecosystem is global, not EU-bounded. Once a mechanism like QWACs is implemented in browsers, it is open to abuse by governments that do not aspire to the same governance principles as the EU. For instance, the same mechanism can be used to insert a "government root" certificate, and thereby gain access to all browser sessions secured with those certificates. This represents a serious threat to fundamental rights, including those of EU citizens communicating with those countries, and it represents a cybersecurity threat to the EU. The threat is not hypothetical: this approach has already been attempted in at least two countries.[2] Furthermore, we do not believe that this risk can be mitigated by applying procedural safeguards once the mechanism is in place.

Recommendations

1. That the Commission re-introduce text previously proposed in the trilogue, making it clear that web browsers may take steps to address breaches of security, privacy and integrity arising from QWACs. Reintroducing this text would restore proven safeguards, building trust with citizens and experts.

2. Ambiguities in Article 45 and related Recitals must be resolved. Ambiguity may sometimes be helpful in achieving consensus on contentious issues, but technical measures require clear and explicit specifications. The text should clearly state that the purpose of QWACs is to provide a verifiable assertion of website ownership, and thus distinct from the purpose of certificates used to establish transport layer security.

3. The current text of Article 45 creates the risk of "bad" government-mandated root certificates which will impact the EU and, in our view, cannot be mitigated by procedural safeguards "after the fact". If the risks cannot be ruled out by technical design, the current QWACs approach to asserting the ownership of website should be discarded.

[2] https://www.internetsociety.org/news/statements/2019/internet-society-concerns-kazakhstan-encryption/