Google, Apple, Mozilla may see compromise in EU digital identity bill's web security battle

25 Jan 2023 | 13:38 GMT | **Insight**
By Lucy Valeski and Matthew Newman

A dispute that pits Google, Microsoft, Apple and Mozilla against companies that offer website security certificates is close to being resolved after a group of European lawmakers agreed on a compromise legal text on how to regulate their use, MLex has learned. Browsers have lobbied against being forced to accept QWACs, arguing that the measure could increase users' cybersecurity risks.

A dispute that pits Google, Microsoft, Apple and Mozilla against companies that offer website security certificates is close to being resolved after a group of European lawmakers agreed on a compromise legal text on how to regulate their use.

Political groups in the European Parliament's industry committee voted today in favor of a compromise on Article 45 of the European Digital Identity Framework that will provide consumers with a secure way to authenticate their identities through a "digital wallet," MLex has learned.

Under the European Commission's proposal, which revises the 2014 EU regulation on electronic identification and trust services, web browsers must display the identity information contained in qualified web authentication certificates, or QWACs. The EU executive's goal is to ensure that users can identify who is behind a website.

Browser operators have raised concerns about being forced to accept QWACs, even if they don't meet the browser's security standards. They've argued that the legislation would "significantly increase the cybersecurity risks for users" (see here).

QWACS were introduced in the 2014 eIDAS regulation. The commission proposed to make the use of QWACs mandatory in Article 45. The compromise would still force browsers to accept the use of QWACs — but it will give them more flexibility in how to display the certification and they could reject the certificate authority, MLex understands.

Browsers may also immediately remove individual certificates they deem harmful, but the reasoning must be transparent and justified. Without a demonstrated justification, browsers may be at risk of being sued in court, MLex understands.

The political groups' compromise will now be put to the full industry committee for a vote on Feb. 9.

EU governments reached an agreement on their version of EU digital identity legislation in December (see here). Once lawmakers in the European Parliament agree on their stance on the measure, final negotiations can begin.

— The QWAC wars —

Discussion in the legislature's industry committee on the eID proposal had reached a "stalemate" because of the debate on mandatory QWAC acceptance. Big Tech browsers object to the regulation while citing user security concerns and certificate authorities believing the QWACs provide transparency to users, EU lawmaker Mikuláš Peksa told MLex in an interview.

"This situation is a bit unfortunate, because what we have seen in the area of browsers, the market is becoming more and more concentrated to what's like a couple of vendors. Their power over which certificates are being accepted is somehow growing," said Peksa, a member of the Czech Pirate Party, who is one of the legislators leading the parliament's work on the draft.

At issue are website certificates — a key building block for Internet security. Web browsers use these certificates to ensure that when users connect to a website, the link is protected with "transport layer security," or TLS, which encrypts data to prevent hackers from seeing what users transmit.

The TLS also ensures that the server on the other end of the website isn't a hacker impersonating the website. Certificates are issued by specific authorities, which are responsible for verifying that a given entity controls the site in question.

— Website security —

QWACs allow the EU to centralize the certification process and provide consistency in the display of safety information for users.

One purpose of QWACs is to provide users with information about the person on the other side of the website.

Paul van Brouwershaven, director of technology compliance at US-based certificate authority Entrust, says users will be able to understand who they are associating with online. If the certification is incorrect or users are subjected to a scam, they can hold the perpetrator liable because of the identifying information provided by the QWAC.

Objectors to this reasoning, such as Mozilla, argue that Internet users do not read “extended validation” certificates, which users can see if they click on the lock symbol on their browser’s address bar. Mozilla stopped using QWACs with the identity displays in 2019 after determining they weren’t useful and could potentially give users a false sense of security, as a legally valid entity could still abuse users.

Thomas Lohninger, the executive director of privacy NGO Epicenter Works, says that the certificates could act as a tool for government or law enforcement abuse. He worries they could enable mass surveillance, and digital privacy advocates have brought up the possibility of government-pushed certificates that compromise privacy to collect information about the user.

EU lawmaker Peksa expressed a similar concern, comparing the mandatory QWACs to a fictional law requiring citizens to give the government a house key.

Van Brouwershaven said people will read the certificates if their presentation is standardized. In the past, the display of the "extended validation" certificate varied between browsers, but the new revision should provide consistent displays regardless of country or browser.

Michael Butz, the chairman of European Signature Dialog, which represents European electronic signature providers, said in an interview with MLex that when compared to the situation in the past 20 years, QWACs were “easy to use.”

However, critics of QWACs, such as Mozilla, are concerned that they put too much responsibility on Internet users. Most users don’t read QWAC information because they prioritize the speed of reading websites and take cybersecurity for granted.

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):
Regulation - Data Privacy & Security - Digital Economy policy 2019-2024 (EU)

Areas of Interest: Data Privacy & Security, Sector Regulation

Industries: Communication Services, Information Technology

Geographies: Europe, EU

Topics:

5G technologies | Big Data | Cloud computing | Cybersecurity | Data Privacy | Digital tax | Future mobility