European Parliament

Qualified certificates for website authentication

Qualified certificates for website authentication (QWACs) allow users to identify who is behind a website. Aiming to increase QWAC uptake, the Commission has proposed an obligation for web-browsers to recognise them and make them more visible. The proposal has prompted fierce debate. While the Council agrees with the Commission and the Parliament is still debating its position, many stakeholders have raised concerns.

Introduction

More and more **EU citizens do not feel secure online**. As revealed in a recent Eurobarometer survey, more than seven in ten internet users in the EU believe there is an increasing risk of falling victim to cybercrime, and nearly seven in ten are concerned that websites do not store personal information securely.

Website authentication is an important part of security online. It can have a major impact on the user experience, while not being immediately apparent. Website authentication is done with website **certificates** issued by certificate authorities (CAs), which can be companies or organisations. CAs validate the identities of websites, email addresses and such like, and bind them to cryptographic keys by issuing electronic documents known as digital certificates. Digital certificates that authenticate website identity are known as secure sockets layer (SSL) and transport layer security (TLS) certificates. The website visitor can see that the website has some kind of website certificate when 'https' (hypertext transfer protocol secure) appears in the web address.

The global **CA market** was valued at around US$130 million (€124 million) in 2021 and could reach US$260 million (€247 million) by 2027. Every day CAs issue millions of new certificates. There are hundreds of CAs on the market, such as IdenTrust, DigiCert, Sectigo and Let's Encrypt. They cooperate in the CA/Browser Forum, which publishes guidelines on website certificates.

What is a qualified certificate for website authentication (QWAC)?

A QWAC (SSL certificate) is a website authentication certificate governed by the eIDAS Regulation. Each QWAC contains information about the entities issuing and receiving the certificate, as well as information about the certificate itself. QWACs are issued by qualified trust service providers (QTSPs) as defined in the eIDAS Regulation. QWACs are used beyond websites as they authenticate the connection and the identity of the entity or person in control of the connection. Standards on implementation of QWACs are set by the European Telecommunications Standards Institute (ETSI). ETSI decides if QWACs are compatible with EV certificates (see text below).

Source: eIDAS Regulation, ENISA and ETSI.

Types of website certificate

There are many types of website certificate, varying in quality and purpose. One way to categorise them is by data validation level, with the following levels possible.

- **DV (domain validated)**: this is the most commonly used certificate and provides a relatively low level of trust. It checks only that the applicant actually owns the domain, not that they are a valid business entity.
- **OV (organisation validated)**: this is the second most commonly used certificate. It checks in detail if the applicant is a registered legal entity, if the registration is valid, if the applicant actually owns the domain and if they have the authority to apply for such a certificate.
- **EV (extended validation)**: this is a much less commonly used certificate and has the strictest requirements. It checks in detail the legal, physical and operational existence of the applicant and their exclusive right to use the domain.

Another way to classify these certificates is by number of domains. There are single domain and multi-domain certificates. Wildcard certificates meanwhile secure an unlimited number of first-level subdomains

Author: Maria Niestadt, Members' Research Service
PE 739.285 – January 2023

within a single domain. Single and multi-domain certificates are available as DV, OV or EV. EV is not available for wildcards.

QWACs are also a type of website certificate. While QWACs are issued by several EU companies and organisations, their uptake has so far been relatively limited. The delegated regulation supplementing the Payment Services Directive makes the use of QWACs mandatory in communications between players in the payment circuit. Spain is a particular case, as a national law obliges public administrations to use QWACs for their websites. However, web browsers do not include QWACs in their list of trusted root SSL certificates and do not display them clearly, making QWACs unusable for traders and consumers at present.

The cost of website certificates varies greatly. DVs can be free-of-charge but EVs usually cost a couple of hundred euros. This cost means that certificates providing less trust are much more popular than those providing a high level of trust. According to search platform Censys, the proportion of DVs is about 80 % (around 400 million certificates in use currently), while the market share of EVs and QWACs is less than 1 %.

The eIDAS Regulation revision proposal

In 2021, the **European Commission** proposed to update the eIDAS Regulation. In article 45 of the revised regulation, the Commission proposes to oblige web browsers (which are located predominantly in the United States) to recognise QWACs and make them more visible. The Commission believes that QWACs provide secure and trustworthy information on who is behind a website, and thus reduce fraud.

The **Council**'s general approach, adopted on 6 December 2022, did not introduce any significant changes to the Commission proposal on QWACs.

Parliament has still to adopt its position on the file. The Committee on Industry, Research and Energy (ITRE), the lead committee, is preparing its report, while the associated committees (Committee on the Internal Market and Consumer Protection (IMCO), Committee on Legal Affairs (JURI) and Committee on Civil Liberties, Justice and Home Affairs (LIBE) have already adopted their opinions. So far, the positions expressed in the Parliament are split. Rapporteur Romana Jerković (S&D, Croatia) proposed in her draft report to delete the amending of article 45. The JURI committee agrees with this deletion. Meanwhile, IMCO wishes to allow web browsers not to recognise QWACs when they can demonstrate that QWACs significantly undermine user security. LIBE did not change article 45 as proposed by the Commission.

Stakeholder views

Since the Commission's proposal could have a significant impact on the web authentication market, it has raised many questions and concerns among stakeholders.

- **Security**: a group of cybersecurity researchers and advocates, web browser Mozilla, advocacy group EDRi, the American Chamber of Commerce to the EU and Internet Society believe that the article 45 amendment proposed by the Commission could dramatically weaken web security. They claim that web browsers have rigorous security standards and criticise the proposal for giving greater power to government-appointed CAs.
  Government IT security company Bundesdruckerei does not agree with this criticism. It says that an independent third party (QTPS) checks in advance the identity and communication information contained in QWACs. It also praises QWACs for increasing EU sovereignty.
- **Conflicting standards bodies**: as highlighted by the European Union Agency for Cybersecurity (ENISA), there is some confusion as to how different requirements adopted at different levels will interplay and whether they conflict.
- **Technical neutrality and interoperability**: Mozilla claims that the Commission proposal undermines technical neutrality and interoperability and is in contradiction with other parts of the proposal (namely recitals 27 and 72).
- **Privacy**: Mozilla and Internet Society also believe that there are serious privacy risks in validating QWACs. They believe that the validation procedures and protocols used in the proposal would reveal users' browsing activities to third-party validation services.
- **Visual differentiation**: some stakeholders are against the visual differentiation of QWACs from other website certificates. As highlighted by some stakeholders and researchers, users do not pay attention to site identity indicators.