FAQ

How does web certification work?

When sharing sensitive data online web users expect assurance that they are sending it to the correct domain and not to a cybercriminal. When filling in credit card details for a Mozilla VPN, for example, it's clearly essential to trust that you are sharing the information in a secure manner.

There are three essential components to web certification:

Certificates - A website uses a certificate to prove to the browser that it controls the domain name the user has navigated to.

Certificate Authorities (CAs) - The organisations that issue these certificates. In the context of eIDAS, these are also referred to as TSPs (Trust Service Providers). They are responsible for, among other things, ensuring that certificates are only issued to the operators of a website. They are a critical part of the security process. If they mis-issue certificates to bad actors, the consequences for web users can be catastrophic. Some certificate authorities are state-owned companies.

Root Stores - To keep people safe, browsers ensure only certificate authorities that maintain high standards of security and transparency are trusted in the browser. The collection of trusted certificate authorities is called the Root Store. Once accepted in a browser's Root Store, any CA is trusted to issue certificates for any website. This also means that the system is only as strong as its weakest CA. Browsers continuously monitor the behaviour of certificate authorities and take prompt action in cases where a trusted certificate authority has been compromised. Mozilla operates an open Root Store program where decisions are discussed on a public mailing list allowing all stakeholders to weigh in.

What does eIDAS Article 45.2 propose?

Article 45.2 mandates browsers to

- Automatically accept any certificates which are issued by certificate authorities authorized by EU member states (so-called QTSPs, or Qualified Trust Service Providers)

This **overrides the rigorous and independent Root Store policies and vetting practices** done by browsers that ensure a system of online trust and replaces it with a weaker security architecture. See more info below ("what is at stake if…").

- Display the legal identity data of QWACs

QWACs are a type of web certificate that contains the legal identity of the company, organization or person behind the website. They were introduced in 2014 and are very similar to Extended Validation (EV) certificates, which also display the website operator's legal identity. Research has since demonstrated that EV certificates and QWACs provide users with a **false sense of security** that could be exploited for malicious purposes such as phishing and domain impersonation. Most browsers disabled EV certificates by 2019 and today no browsers showcase EV certificates directly in the URL address bar.

What are the security risks in eIDAS Article 45.2?

Article 45.2 overriding Root Store policies would mean that browsers will no longer be able to deliver on their promise of safeguarding users and security standards compliance. Browsers would be required to accept CAs that do not meet cybersecurity requirements merely by the virtue of them being present in the EU TSP list. They would also be prevented or delayed in distrusting CAs when there is evidence of misbehavior.

Article 45.2 would make it easier for criminals to execute "man-in-the-middle" attacks. One notorious case from 2011 where the Dutch certificate authority Diginotar was involved, occurred when users trying to access Google websites were redirected to falsified sites. This attack was carried out through EV certificates, a technology similar to QWACs (see below). Most of the IP addresses affected came from Iran.

Article 45.2 gives every EU member state the ability to let one or more certificate authorities override the security standards which are currently in place. Since several certificate authorities are also state-owned, this provides governments with new means to snoop on their citizens as it would compel users to allow their traffic to be intercepted and surveilled. Democracy is not a guarantee in any country, also not in Europe.

We have already seen attempts by Kazakhstan & Mauritius, trying to make users install their own certificates. The countries reversed the decision following pressure from Mozilla and other browsers. In 2019 a certificate authority associated with the United Arab Emirates was blocked by Mozilla because the company had a history of working for the rulers in surveillance operations targeting activists, political leaders and suspected terrorists.

Article 45.2 would also set an international precedent that could lead to harmful legislation in other, less democratic, parts of the world.

Also, if Article 45.2 is passed, EU-authorized certificate authorities would become a prime target for criminals, because they are a way to bypass existing web security protocols.

The display of the legal identity of a website operator through QWACs would also pose security risks to the everyday internet user. Just like EV certificates, QWACs can give users a false sense of security. See for example the Stripe case: a cybersecurity researcher set up a fake website, mimicking an existing payment website called stripe.com. He then obtained an EV certificate for it by registering a company under the same name (Stripe Inc.) but in another jurisdiction. The certificate showed that ‘Stripe Inc’ was behind the website, tricking visitors into a false sense of security.

In general, cybersecurity depending on user behaviour has been repeatedly demonstrated not to work. Normal people favour speed and convenience when browsing the web.

In the long term, Article 45.2 could negatively affect e-commerce, e-government, and the protection of fundamental rights in the EU.

What does Mozilla propose instead?

We suggest either deleting Article 45.2 from the Commission’s proposal or revising it to ensure a safety-first approach, giving Mozilla and other Root Stores the ability to distrust certificate authorities if this is appropriate.

How much does a QWAC cost?

QWACs are **expensive**. They currently cost between €700 and €1,400, depending on the Certificate Authority that is selling them. The cost of QWACs might further exacerbate economic divisions within the European Union.

Browsers do not gain from this charge, the figure is charged by Certificate Authorities who are the only ones to profit from QWACs.

Do other browsers have the same problem with Article 45.2?

Yes, Article 45.2 has an impact on the entire browser ecosystem. Mozilla is particularly vocal about the issue, as we consider our Root Store policy as core to our philosophy and an example of appropriate cybersecurity measures.

Have Mozilla or other browsers distrusted a Certificate Authority before?

Yes. In the past five years, there have been three removals from the major browser Root Programs**).** Certinomis is a Certificate Authority that remains authorized to issue QWACs under the EU TSP list, despite having been removed from browser root stores for repeated security related non-compliance. An example of the mismatch in security standards that could be set by Article 45.2.