

QWACs EXPLAINED SIMPLY

What are the facts regarding the statement about spying on EU citizens?

Currently, headlines are increasingly warning of EU citizen surveillance by member states, allegedly facilitated by the eIDAS compromise reached in the trilogue. The discussion often centers around the so-called QWACs (Qualified Websites Authentication Certificates), with browsers claiming they compromise internet security.

However, looking behind the scenes reveals that the core issue is a question of **governance**. And here, which entity should oversee the reliability of TLS certificates?

Is it **profit-driven, U.S. big-tech corporations** who are not transparent and not accountable to anyone but their stockholders, or is it the **democratically authorized bodies of the EU and its member states**?

Or a **coexistence of both**, operating independently as provided for in the regulation?

Claiming that the amended Article 45 poses the risk of comprehensive surveillance on EU citizens is **unfounded** and there are no relevant examples cited to support this claim. Any such alleged surveillance is unrelated to Article 45; quite the contrary.

Rather, the existing governance system of browsers already allows for this possibility. Browsers can function as gatekeepers through new trust service providers (TSP - root CAs) or existing ones (e.g., their own TSP), which browsers themselves use to issue certificates to their web hosting customers and others that facilitate internet traffic monitoring. They can unilaterally deactivate verification mechanisms (such as CT log mechanisms) on a case-by-case basis secretly and without scrutiny.

Unlike the EU governance system authorities, browser manufacturers are not bound by the principle of administrative legality. They operate profit-oriented, free from judicial review, deciding at their discretion whether and how transparently to communicate their decisions and actions to governments and the public. Additionally, there is no arbitration board to address potential abuses of market position by browsers.

FACT

QWACs are secure and adhere to all current standards, a commitment that will hold true, and even be strengthened, with the implementation of the new version of Article 45 eIDAS. They are issued by qualified trust service providers (QTSPs), they are audited and certified and the security requirements are constantly being developed and adapted by open industry consensus.

- ✓ As critical infrastructure, QTSPs will in future be subject to the NIS2 Directive and thus to **higher IT security requirements** than those non-EU certificate issuers that browsers include in their proprietary trusted root store. Unlike non-EU certificate issuers, QTSPs are **continuously supervised** by a national supervisory body and **audited** ex ante every two years by an independent conformity assessment body.
- ✓ In addition to the IT security requirements, the **European standard is generally higher** than the browser requirements for non-EU TSPs to get into the root store.
- ✓ Technically, QWACs are TLS-certificates with a **more reliable identification** of the customer – for example, they require the TSP to conduct face-to-face identity verification of the customer's representative, which other TSPs don't do. QWACs are based on the industry-consensus requirements of the CA/Browser Forum and thus essentially correspond to the known EV certificates, which have been in use and trusted by browsers since 2008.
- ✓ Contrary to common portrayal, Article 45 of eIDAS ONLY prohibits browsers from **imposing additional requirements before recognizing and displaying certificates**. What is **explicitly NOT covered** by this prohibition are browser security checks conducted during operation, such as evaluating CT logs or implementing monitoring measures for unusual behavior. This ensures that browsers can still detect any errors or security breaches in the certificates.

FACT

Browsers sometimes set their proprietary root program rules to suit their own commercial purposes rather than security, and their rules often don't represent industry consensus.

- ✓ Presently, browsers wield direct influence over the structure of TLS certificates, including QWACs, through their root store programs. However, modifications to these requirements are frequently **motivated more by market dynamics than by considerations of IT security**. Significant technical alterations to QWAC certificates, such as reducing the maximum validity period to 90 days, ought to undergo extensive discussion, be approved by broad industry consensus outside of the browser root stores, and be anchored in legal frameworks.
- ✓ More can be done to improve internet security by moving root program rules to a recognized legal framework. These added measures include steps to maximize transparency, such as the logging of QWACs in CT logs, and can be made mandatory for QWACs via implementing acts.

FACT

Contrary to common assertions, QWACs are not required to be incorporated into browser root stores. The stipulation is solely that the EU Trusted List, functioning as an EU governance system, must be acknowledged in parallel.

- ✓ Browsers run a root store which includes, among others, all root certificates of those QTSPs whose TLS certificates they trust. They operate their own supervising regime for this.
- ✓ With the eIDAS Regulation, the EU has created its own supervising regime for the QTSPs that issue QWACs. It lists the QTSPs that are allowed to issue QWACs on an EU Trusted List. This is the "root store of the EU", so to speak.
- ✓ Unlike the browser root store, the "EU root store" is administered by democratically legitimized institutions of the EU and its member states. It is subject to constitutional mechanisms and the rule of law.
- ✓ The root stores and infrastructure of browsers **remain unaffected by Article 45 of eIDAS**. In the context of QWACs, browsers are only required to conduct validation against the EU Trusted List. Therefore, browsers can expressly label QWACs as EU certificates, underscoring their obligation as dictated by the eIDAS Regulation. There are **no** specific regulations in Article 45 regarding specific technological processing of the EU Trusted List by browsers; this discretion is left to the decision of the browsers themselves.

FACT

The EU governance system covering QWAC brings an end to the existing proprietary governance practices of browsers for TLS certificates. At present, browsers unilaterally establish rules as gatekeepers while simultaneously functioning as market participants in competition with EU TSPs. This is clearly a conflict of interest.

- ✓ Currently, browser manufacturers wear the **dual hats of "regulators"** – unilaterally determining who can issue publicly trustworthy TLS certificates – and **competitors of trust service providers**. Browsers also issue website certificates for their cloud hosting customers, showcasing a firm integration of the trusted service provider ecosystem into their business model.
- ✓ The dual role of simultaneously serving as a gatekeeper and being a market provider, often illustrated by examples like Amazon, is inherently problematic. The EU, in line with its stance against digital sector monopolies through the Digital Markets Act (DMA), should adopt a similar guiding principle in this context.

FACT

The compromise solution for Article 45 reached in the trilogue also empowers web browsers to promptly address any security concerns about a TSP they may have. In suspicious cases, browsers can suspend QWACs or QTSPs and subject them to examination within the EU governance system.

- ✓ Importantly, this does not necessitate approval by EU or member state regulators for immediate suspension by supervisory bodies; **browsers continue to hold the initial decision-making prerogative** in this regard.

CONCLUSION

The eIDAS Regulation serves as a legal framework to safeguard the digital sovereignty of the EU and to facilitate the European Digital Single Market.

Importantly, it is not a security law and does not grant additional rights or powers to police and security authorities. It does not establish the groundwork for surveillance or expanded data access rights.

On the contrary, the goal of eIDAS is to establish trust anchors for digital transactions through stringent and comprehensive regulation, earning trust universally across legal and business transactions.

Spying on citizens under the new eIDAS regulation is not possible, thanks to the comprehensive safeguards of supervision and auditing already in place. This has been further strengthened by the eIDAS 2 version negotiated in the Trilogue.

In the future, the Certificate Transparency (CT) system can serve as an additional safeguard. This CT system ensures that all certificates issued by Certificate Authorities (CAs) are logged in publicly verifiable CT logs, visible to everyone. If a fake certificate is logged for an important domain, anyone can raise the alarm, making it impossible for rogue EU member states to issue fraudulent certificates unnoticed. ESD strongly supports this initiative.

Browsers, as part of their precautionary measures, can distrust and block any suspicious certificates under new Article 45, while promptly notifying the relevant authorities and even the media. Moreover, QWAC issuers are legally liable for any intentional or negligent damage caused by non-compliance with eIDAS regulations. Therefore, the eIDAS 2 regulation effectively prevents spying on citizens and ensures their privacy and security.