

After Trilogue is Over:

Browsers Make One More Effort to Stop eIDAS Article 45 Changes

The EU has been considering changes to eIDAS since June 2021 when the Commission released its draft proposal with improvements to existing law and new provisions for an EU digital wallet to help create “digital sovereignty” for Europe.

The goal was to reduce Europe’s existing dependance on US-based big tech companies for trust decisions affecting EU citizens – and included new provisions in Article 45 on *Qualified Certificates for Website Authentication (QWACs)* to make them even better at securing and identifying European websites and their owners.

The US-based browsers strongly resisted all these Article 45 proposals, saying that the browsers should continue to have exclusive supremacy on which EU QWAC issuers should be trusted by their proprietary trusted root programs. Through months of hearings before Parliament, the browsers presented exaggerated arguments that sharing control with the EU and its member state Supervisory Bodies as to which EU QWACs should be trusted would – in effect – destroy the internet! As part of their scare campaign, they have even argued that EU member states would force browsers to accept rogue QWACs and QWAC issuers, and then use these bad QWACs to spy on their citizens.

The browsers never presented any evidence to justify these claims, and in fact the final Article 45 text as agreed to in the Trilogue allows **any** browser to publicly **challenge** any QWAC or QWAC issuer and force the Commission and applicable Supervisory Body to **investigate** the QWACs in question and report their findings. This Article 45 change has the effect of making EU security and trust decisions a **joint responsibility** of both browsers and member states **working together** for the first time.

The Trilogue ended on 8 November 2023,¹ with new language added to address browser concerns – yet the browsers are still trying to block the eIDAS legislation. Their basic argument is this: “You can’t trust the EU and its member states – you can only trust browsers for security decisions applying to EU citizens.”

Browser decisions that weakened security for EU citizens

The browsers themselves have made many decisions in the past that have weakened security for EU citizens – so the browsers should no longer have exclusive control over QWAC issuer trust. See, for example, a list of the top browser security threats to users.²

“So far this year [2023], Google has disclosed six vulnerabilities that attackers were actively exploiting before the company had a patch for them [three alone in September 2023].”³ “These weaknesses pose significant risks for organizations relying on widely used browser applications like Google Chrome and Mozilla Firefox.”⁴

Browsers have also made poor decisions in the past concerning which server certificate issuers they should trust. For example, in 2015 the certificate issuer Let’s Encrypt decided it would not revoke any of its certificates even after Let’s Encrypt was notified (with evidence) that they were being used by phishers to harm users – and even though the existing CA/Browser Forum (CABF) rules required all certificate issuers to revoke such certificates. The browsers did nothing in response and chose not to enforce the industry standard.⁵

As a second example of poor trust decisions, Let’s Encrypt mis-issued 3,000,000 certificates over a 7-month period in 2020, failing again to follow CABF rules that apply to all issuers.⁶ Let’s Encrypt initially said it would revoke all those bad certificates, as the CABF rules require certificate issuers to do in a very short period. However, just two days later Let’s Encrypt said it would not revoke 1,300,000 of the mis-issued certificates because it would be too hard, and that it didn’t even have an email address to contact some customers whose websites were using the mis-issued certificates – thus again violating the CABF rules applicable to all certificate issuers.⁷ Once again, the browsers did nothing, and did not enforce the industry standards.

Let’s Encrypt made another mistake in early 2022 – this time mis-issuing another 2,000,000 website certificates under industry rules.⁸ Again the browsers did nothing. All of these phishing and mis-issued certificates posed a significant security risk for EU users, but the browsers chose not to act.

1. <https://www.consilium.europa.eu/en/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid/>

2. <https://www.forbes.com/sites/forbestechcouncil/2023/08/14/web-browsers-examining-the-latest-threats-solutions-and-trends/?sh=6129c7b42187>

3. <https://perception-point.io/blog/browser-security-threats-solutions-user-education/>

4. <https://www.bleepingcomputer.com/forums/t/771639/google-identifies-security-problems-update/>

5. <https://www.forbes.com/sites/forbestechcouncil/2023/08/14/web-browsers-examining-the-latest-threats-solutions-and-trends/?sh=7142deed2187>

Many observers believe the browsers' decision to do *nothing* about certificate errors by Let's Encrypt is because... some of the browsers like Google and Mozilla are major contributors to Let's Encrypt, involved in its management, or users of its certificates.⁹

What is the point of these examples of problematic browser decisions about trust concerning server certificate issuers? ESD believes that in general the browsers do a very good job in trying to protect EU users – but NOT a perfect job. In fact, some of the browsers seem to apply different standards for certificate issuers they like or have an investment in, versus other certificate issuers who compete with them, like the European issuers of QWACs. On this basis, US-based browsers should not continue to have the current exclusive supremacy they want when it comes to trust decisions affecting EU citizens.

The Parliament should support the strong compromise for Article 45 on QWACs created by the Trilogue last month and should ignore the ongoing campaign by browsers to stop the eIDAS Trilogue legislation through fear-mongering and tales of spying by governments or the end of the internet.

This Trilogue compromise for the first time shares control between browsers and the EU, requiring browsers to trust QWACs from QTSPs on the EU Trusted List (after extensive audits and member supervision) but also allowing browsers to challenge any QWACs before the Commission and Supervisory Body for a full review. That is the right balance.

For additional information about existing problems with exclusive browser control over certificate issuer trust decisions in the EU, see the attached information "How encrypted internet traffic is ensured today."

6. https://bugzilla.mozilla.org/show_bug.cgi?id=1619047#c9
<https://www.ssl.support/blog/lets-encrypt-certificates-been-revoked/>

7. https://bugzilla.mozilla.org/show_bug.cgi?id=1619179

8. <https://www.bleepingcomputer.com/news/security/lets-encrypt-is-revoking-lots-of-ssl-certificates-in-two-days/>

9. <https://letsencrypt.org/sponsors/>

ANNEX

Additional information

How encrypted internet traffic is ensured today

Internet traffic is encrypted because browsers support the TLS certificates DV, OV and EV. Browsers do not support “native” Qualified Certificates for Website Authentication Certificates (QWACs) – those on the EU Trust List, but not in the browser trust store - as of today. QWACs are only supported in browsers when they include a marker also used by EV certificates.

In general, browsers determine which requirements trust service providers must comply with. On top come guidelines of the CA/Browser Forum. But they are of secondary importance, as the browsers believe they can always be overridden in detail through browsers’ own root store programs.

Browsers accept root certificates from trust service providers or remove them at their own discretion. How does this work in practice?

Browsers have their own **trusted root store** that is pre-loaded in the browser software installed (and updated) in clients. The root store contains the root certificates or issuing certificates of trust service providers that the browser software is coded to trust automatically. Trust service providers can apply for inclusion of their certificates in each respective root store.

To do so, they must, among other things, **comply with the respective individual root store programs of the browsers, which are ALL different**. The root store programs contain browser-specific requirements but also general requirements, such as that they must comply with the specifications of the CA/Browser Forum. So, in consequence, the **security requirements are not harmonized and a bit opaque**. In addition, a trust service provider is not guaranteed to be accepted by a browser or can be subject to delays of years without explanation.

Trust service providers who wish to issue TLS certificates that are publicly recognized by the browsers must also always follow the rules of the CA/Browser Forum. These are the Baseline Requirements for TLS certificates, plus the EV Guidelines if Extended Validated (EV) TLS certificates are to be issued.

EV TLS certificates are TLS certificates in which the identity of the certificate holder has been verified more thoroughly and information about the certificate holder has been included in the certificate. In addition, trust service providers must always follow the Network and Certificate System Security Requirements of the CA/Browser Forum.

It's important to note that trust service providers have taken the lead since the CA/Browser Forum was created in 2005 in constantly improving security and audit requirements that apply to their certificates – they have been willing partners to the browsers in creating a safer internet.

CAB Forum guidelines

The CA/Browser Forum is a non-institutionalized standardization industrial federation. See cabforum.org. Its members consist of three groups, namely certificate issuers (trust service providers), certificate consumers (e.g. browsers), and associated members (e.g. auditing organizations). Interested parties may also participate, but not vote on Forum ballots setting standards. The CA/Browser Forum has its own bylaws.

The content-related work is carried out in working groups and their subcommittees. Every two years, a chair and a vice chair are elected for the CA/Browser Forum as well as for each of the working groups and subcommittees, and these officers come from both browser and certificate issuer members. Minutes are prepared for the meetings and are publicly accessible.

Physical meetings are held three times a year, organized and hosted by a member organization of the CA/Browser Forum. The CA/Browser Forum does not charge membership fees, has no office and no employees. The work is carried out for free. The CA/Browser Forum is not registered as a corporation, and nothing can be physically delivered to it. For this reason, it is considered non-institutional.

Compliance with the guidelines of the CA/Browser Forum is carried out by **audit organizations** on the basis of the WebTrust for Certification Authorities program or by audit organizations organized in the Accredited Conformity Assessment Bodies' Council (ACAB-C) on the basis of ETSI standards. The two audit standards are very similar, and both are accepted by browsers. The audit of the trust service providers is carried out annually and at the expense of the trust service providers. After each audit, an audit attestation letter is issued by the audit organization and sent by the trust service provider to Mozilla, Apple, Google and Microsoft via the Common **Certification Authority** Data Base (CCADB) platform and available to the world for public inspection.

The CCADB is a platform by which the browsers manage the respective trust service providers (TSPs) with their root and issuing CA certificates. The trust service providers (certificate issuers) communicate formally via this platform if, for example, they wish to make changes to their existing root or issuing CA-certificates.

Such change must always undergo a public and transparent discussion period of minimum 6 weeks, during which any interested party can comment on the request. Only then do the browsers decide individually and separately whether they want to comply with the TSP request and include the new CA certificates in their trusted root stores. This decision also depends, among other things, on whether the applicant complies with the individual requirements of the respective root store programs. Whether when and how quickly an application is processed by each browser, however, is not specified and in some cases, there have been very long delays.

If a trust service provider violates the specifications of the CA/Browser Forum or a browser root store program, it must report this publicly and transparently on the **Bugzilla platform** once it learns of the violation. See https://wiki.mozilla.org/CA/Bug_Triage. In this process, the trust service provider describes the reason for the violation, what effects it has, how it has been rectified and what measures will be taken to prevent a recurrence. In this way, the incident is dealt with publicly so that other trust service providers can also learn from the process. The aim of this mechanism is to improve the industry as a whole. However, multiple and persistent violations can lead to the removal of the trust service provider from a browser's root store using whatever procedure each browser chooses. In some cases, this process, also known as the **distrust process**, is not transparent to the public.

Root store programs by browsers

Each root store program is managed by each browser itself, and the programs can be quite different. As a rule, planned changes to root store programs are communicated in advance and interested parties can comment on them. Responses may also be collected via surveys in which all trust services that are located in the respective root store program are obliged to participate.

Ultimately, however, each browser decides which changes it considers appropriate. For example, in 2020 at the face-to-face meeting of the CA/Browser Forum in Bratislava, Apple announced that it would enforce a shortening of the TLS certificate validity period to 398 days via its root store program, regardless of the regulations in the Forum's Baseline Requirements and related audit standards or the views of other Forum members or website owners.

The example of the reduction of certificate validity period to 398 days shows that while the CA/Browser Forum can define standards, enforcement of standards takes place exclusively through the anchoring in the root store program of each respective browser. In this sense, the CA/Browser Forum merely issues "best practices" standards via ecosystem consensus but has no power whatsoever as to whether the standards are implemented by the browsers.

If the specifications of the root store programs and the CA/Browser Forum diverge or even conflict in certain areas, a clean-up ballot is periodically drafted to ensure that the guidelines of the CA/Browser Forum also comply with the specifications of the root store programs. If the CA/Browser Forum as a whole decides against the ballot by vote, the conflicting browser rules will take precedence and still apply due to the requirements of the root store programs.

In this way, browsers can also enforce requirements that shape the market or whose benefits are controversial, i.e. not necessarily aimed at strengthening IT security but perhaps to favor the market plans of the browsers. Since they have market power, they act autonomously. Nothing can be done to counter this market power of the browsers.

No possibility to appeal

If a trust service provider does not agree with a trust decision made by a browser or does not feel that it has been treated appropriately, it cannot appeal to an institution such as an arbitration tribunal. There is therefore no supervisory body that can independently review a browser's decisions. In this sense, there is no access to justice and the rule of law in this important area of internet security. The sole decision-making authority lies exclusively with the respective browser.

Apart from the imbalance in the governance of the browsers vis-à-vis trust service providers, there is another important fact to be considered in the further discussion of the best way to supervise trust service providers: Most of the browsers are US companies. They are obliged under the US Homeland Security Act to forward data to US intelligence services on request, without giving notice to anyone. In fact, under US law the browsers are prohibited from publicly protesting or discussing these mandatory data orders, so that the targets of the orders never learn what has happened to them. Maybe it is time to regulate the browsers to some degree?

Conclusion

The governance of browsers is based on market power. The design of guidelines for Trust Service Providers (TSPs) is indeed influenced by the economic interests of browsers, and not solely, as often portrayed, by IT security considerations of the browsers. Allowing this browser governance for Qualified Website Authentication Certificates (QWACs) means browsers will continue to shape an EU trust service based on their own economic considerations, thereby undermining European sovereignty.