European
Signature Dialog

ESD Experts Support Trilogue Compromise and Emphasize Necessity for Highest Security of the Internet

The discussion on the eIDAS Regulation has entered its most important phase in the trilogue negotiations between the European Parliament, Council and Commission.

Recently, certain statements charging problems with the compromise reached in the trilogue have become public. The arguments presented by the ten companies in the Mozilla blog post shown have been raised many times since the eIDAS 2 legislation was initially introduced in June 2021. (*Note*: Mozilla is the only browser who has signed this "industry statement" – none of the other browsers are included. According to statcounter.com, Mozilla Firefox has only a 3.0% world market share, down from 30% in prior years.)

Experienced hands-on industry experts who enable secure digital interactions across Europe every day[1] respond to these claims in this blog post. We explain why the compromise reached in the Trilogue, following extensive discussions between Parliament and Council, is the right path forward, as it strikes a balance between various interests and enables Europe to assert its digital sovereignty while protecting its citizens.

1. The European Signature Dialog (ESD) represents the leading European trust service providers (TSPs). TSPs enable secure digital interactions across Europe - between public entities, businesses, and individuals.

European Signature Dialog

Mozilla Statement

1

Articles 45 and 45a mandate that all Web browsers recognize a new form of certificate for the purposes of authenticating websites.

We write to express our concern with the proposed eIDAS legislation. We appreciate efforts to use rulemaking to strengthen the security of the Internet and the leadership role that Europe has taken in fostering cross-border interoperability. However, leadership comes with a greater responsibility to consider the broader implications of changes.

Articles 45 and 45a of the proposed eIDAS provisions are likely to weaken the security of the Internet as a whole. These articles mandate that all Web browsers recognize a new form of certificate for the purposes of authenticating websites. The current language is imprecise, and this risks being interpreted as requiring that browsers recognize the certificate authorities that each EU member state appoints for the purposes of authenticating the domain name of websites.

FACT

QWACs are NOT new. Browsers have been accepting QWACs for the past 8 years.

Qualified Web Authentication Certificates (QWACs) are **not** "a new form of certificate for the purposes of authenticating websites".

They were defined under eIDAS (2014) Article 45 as part of Europe's push for "digital sovereignty" instead of domination by non-European big tech companies, and they work in *exactly the same way* as older forms of website server certificates that are also in use.

Browsers have been accepting QWACs for the past 8 years.

The current language in the eIDAS 2 legislation which has completed trilogue is not 'imprecise', at all. The arguments presented by Mozilla in this blog post have been presented **many times** since the eIDAS 2 legislation was first presented in June 2021.

They have been taken into account in trilogue negotiations – as well as the arguments from all other stakeholders. There is nothing new here.

Mozilla Statement

2

Browsers should be in control because other systems than websites rely on certificates

The root store programs operated by Web browsers and operating systems are the core of Internet security. The certificate authorities recognized by these programs are responsible for attesting to the authenticity of domain names for websites. However, this is not the only system that depends on these certificates. Certificates provided by certificate authorities also secure global commerce in many ways, including email, voice and video, messaging, software delivery, and many other proprietary forms of communication used by businesses.

FACT

QWACs today work with all systems that rely on certificates. This will not change with eIDAS 2.

QWACs are **fully compliant with all systems** that rely on certificates. The browsers have the ability to participate fully to make their voices heard in all rule and regulation approval by standards bodies such as ENISA and ETSI – and some do already participate.

In fact, multiple web browsers have already actively participated in ETSI meetings promoting their perspective to improve the ecosystem. ETSI has a history of collecting all member perspectives to derive the best consensus-based solution.

The point of eIDAS 2 is to ensure that the **browsers clearly display the identity information of website owners, and do not act unilaterally** and impose their own policy preferences while ignoring the EU's digital sovereignty and regulatory rules which protect EU citizens.

Mozilla Statement

3

The current system works

The current system works. Root store programs and certificate authorities have worked collaboratively in a joint body, the CA/Browser Forum, to develop baseline recommendations. These common rules ensure that trustworthy communication is possible at a global scale. People across the planet can trust that the operating systems or browsers they use can establish secure communications for Web browsing, apps, and other communications.

FACT

eIDAS 2 creates a *balance* between the EU and the browsers. Right now, there is no recourse or oversight to browsers' decisions.

Browsers are **BOTH competitors** of EU Qualified Trust Service Providers (QTSPs) – browsers also issue website certificates to their cloud hosting customers - **AND regulators** of QTSPs through the browsers' own root program rules.

Sadly, browsers have abused their monopoly regulatory powers in the past and are in the process of doing so again by forcing all website owners and QTSPs to move to automated 90-day website certificates (instead of the current 13-month certificate limit), even though there is **widespread opposition** in the internet ecosystem.

eIDAS 2 creates a *balance* between the EU and the browsers.

Under eIDAS 2, the EU is able to exercise its digital sovereignty to protect EU citizens, but the browsers are *also* able to (1) participate in future rulemaking and (2) report any certificate problems they encounter from QTSPs to EU regulatory bodies for investigation.

Browsers can participate in ETSI at any time – and **some** already do this – to strengthen the rules for the issuance of QWACs if they deem this necessary.

Right now, the browsers just do what they want, and there is **no recourse or oversight to their decisions**.

eIDAS 2 changes that.

Mozilla Statement

4

The draft mandates recognition of entities that do not meet established standards for security.

The current system is also delicate. Failure of any certificate authority has the potential to compromise communications with any website or service. The resilience of this system depends on multiple interdependent systems working together. The expertise and diligence of a diverse set of people is necessary to ensure that the system is robust and accountable. Intervention in this system therefore needs careful consideration and wide consultation.

The issues with Articles 45 and 45a of eIDAS are a result of mandating that browsers recognize entities nominated by European member states:

Mandating recognition of entities that do not meet established standards for security, as defined by the CA/Browser Forum.

FACT

This statement is untrue. In fact, the EU imposes stronger security requirements on QTSPs than the browsers do.

This browser statement is **untrue**.

The same security standards as defined by the CA/Browser Forum are *also* required for all QTSPs under ETSI audit standards. The EU actually imposes **stronger security requirements** on QTSPs than the browsers do under the EU's Digital Security Act and other EU laws.

There is also a defined process for supervising QTSPs by national state Supervisory Bodies (SB) and auditing by independent Conformity Assessment Bodies (CAB) under eIDAS. This means that QTSPs already operate uniformly under the framework conditions defined by eIDAS, and in the future also by NIS2.

QTSPs therefore operate under the strong legal framework defined by the EU, and this is audited every year. QTSPs are also compliant with all current browser program rules, which can be added to industry rules in the future by industry consensus.

Mozilla Statement

5

Article 45 potentially mandates the recognition of CAs that have been denied inclusion or removed from root store programs.

Article 45 potentially mandates the recognition of certificate authorities that have been denied inclusion in root store programs and those that have been removed after repeated failures to follow best practices in their operations.

FACT

This is misleading. eIDAS 2 does not enforce the inclusion of QTSPs in browser root stores unless a QTSP is listed on the EU Trusted List, indicating that the QTSP has undergone all rigorous checks and audits.

This is **misleading**.

The browsers can be arbitrary in their actions towards QTSPs, can take actions against QTSPs without justification, and are not transparent in their actions.

QTSPs must already follow all requirements specified by eIDAS, ETSI audit standards, and their national Supervisory Bodies. If browsers want to impose additional security requirements on QTSPs, they can bring their additional proposed requirements to ETSI and national Supervisory Bodies and ask them to be imposed on QTSPs. But under eIDAS 2, the browsers can no longer arbitrarily change the rules that affect everyone. They need to get broad industry and regulatory agreement first.

eIDAS 2 does not enforce the inclusion of QTSPs in the root store of browsers, as is often falsely claimed. The QWACs of an QTSP only need to be "recognized" or trusted by browsers on the basis of being listed on the EU Trusted List. How this is technically implemented by the browsers is not specified by eIDAS 2.

Mozilla Statement

6

Browsers are forbidden from specifying additional conditions for certificate authorities.

Browsers are forbidden from specifying additional conditions for certificate authorities.

All requirements will be specified by the nominated European Standards Organization: European Telecommunications Standards Institute (ETSI). Under Article 45 clause 2a, only conditions listed in these specifications can be required.

This means that root stores cannot apply policies that have been effective in the past, like requiring the use of Certificate Transparency to improve accountability, without permission. Similarly, changes in response to evolving needs, like the need to respond to the possibility of a cryptographically relevant quantum computer, would need to be developed by ETSI rather than a body that has demonstrated competence in this area.

FACT

This is wrong! Browsers can easily bring any additional rules to ETSI and other industry standards bodies to be adopted through an open process of consensus.

This statement is wrong!!

QTSPs follow *all the same rules*, including Certificate Transparency requirements that are currently imposed by the browsers, as other Certification Authorities in the US and rest of the world follow.

Plus QTSPs are subject to **even stricter requirements** under EU security laws.

The Browsers can easily bring any additional rules they want to impose on QTSPs such as Certificate Transparency to ETSI and other international standards bodies to be adopted through an **open process of consensus** by the internet community.

The browsers are objecting so loudly because they don't want to give up their current **unilateral** power over the EU.

Mozilla Statement 7

A single national supervisory body can mandate that a QTSP must be trusted.

A root store is permitted to temporarily remove a certificate authority under Article 45a. However, a supervisory authority can also mandate that the certificate authority be restored.

FACT

THIS CLAIM IS UNTRUE

This is a fair process that ensures all affected parties will be involved, and decisions on trust in the EU will not belong **solely** to non-EU browsers.

Mozilla Statement 8

An error of judgment by one member state will affect citizens in all other member states.

These changes have adverse extraterritorial effects.

Certificate authorities listed by member states will be recognized across the entire union. An error of judgment or deliberate action by one member state will affect citizens in all other member states.

FACT

This is no different than the situation today. And eIDAS 2 will guarantee more participation and transparency in all trust decisions.

This browser statement is no different than the situation today, where an error of judgment or deliberate action *by one browser* will affect citizens in *all EU* member states.

The new procedures in eIDAS 2 will guarantee more participation and transparency in all trust decisions by the internet community and will help the EU maintain its digital sovereignty against potential encroachment by browsers and others.

Mozilla Statement

9

Article 45 could fragment the Web.

Users and companies outside of Europe may opt to use a separate list of certificate authorities without the additional entries required inside the EU. This would limit the adverse security effects of these changes to European citizens but could lead to a fragmented Web where some sites are inaccessible outside of Europe.

FACT

This is an extremely unlikely scenario. Users and companies probably will not choose to distrust particular QWACs or QTSPs.

In case that users and companies outside the EU decide to not trust the EU trusted list by default, they would then see a pop-up warning when they navigate to websites secured by a QWACs – something users don't like. However, users and companies already have the ability to distrust particular TLS certificates in their browser settings today (but very few do). In any case, this scenario would be similar to national borders in the physical world, where users decide themselves to pass the border or not.

This is not a serious issue worth discussing.