EU Digital Identity framework (eIDAS)

November 2021 position paper on the European Commission's legislative proposal to revise the eIDAS Regulation

At Mozilla, we're a global community of technologists, thinkers, and builders.

Our mission is to ensure the internet is a global public resource, open and accessible to all. An internet with trust at its core, where individuals can shape their own experience and are empowered, safe, and independent.

Executive summary 2

About Mozilla 4

Security is fundamental to Mozilla, Firefox, and our Root Store Program 4

Browsers defend the privacy and security of users online 5

Browsers help secure everyone against attackers 5

There are three essential parts to website authentication - Certificates, Certificate Authorities, and browser Root Stores 7

The revision to Article 45 - what it includes and what it does 9

The 2014 eIDAS Regulation was premised on discredited security technology 9

The revised Article 45 overrides independent Root Programs and undermines their security assurances 11

The revised Article 45 creates vulnerabilities to be exploited by authoritarian regimes 12

How can we address this 12

Conclusion 13

1. Executive summary

Our modern digital life requires us to navigate across billions of websites. This is made possible through a web browser, which is an unusual type of software in that it represents the individual person using it. It helps people visit the sites and services they want to use, and it protects them while they are there.

The legislative proposal to revise the eIDAS regulation contains a set of provisions that will undermine the independence and security assurances of our "Root Program" and "Root Store", which is the basis for website security. This will have a significantly negative effect on e-commerce, e-government, and the protection of fundamental rights in the EU.

In a nutshell, the revised Article 45 of the eIDAS regulation would circumvent established browser Root Store policies and security protocols that have been working for many years to protect people browsing across websites. These are rigorous and independent policies and vetting practices developed by major browser companies to establish a system of online trust. This system of trust is put into practice every single second and is fundamental to ensuring the online security of every person on the planet who uses a browser to navigate the web.

The security architecture that the revised Article 45 seeks to mandate has been shown to be ineffective and counterproductive when it comes to online security, and so no web browser has been able to support it. Put simply, the proposal's revision to Article 45 has a significant cost: it would worsen online security without providing any additional value for consumers or businesses. It is unprecedented, dangerous, and will not achieve the legislator's desired objective, namely to improve trust and security for e-commerce and e-government.

Instead, the 'real world' impact of the revised Article 45 would be to increase the risk of individuals' web traffic being intercepted and redirected. It would compromise privacy and security by increasing the likelihood that passwords, credit card details, and personal activity conducted on a website could be exposed to an unauthorised party. Should the revised Article 45 be adopted as is, Mozilla would no longer be able to honour the security commitments we make to the hundreds of millions of people who use our Firefox browser or any of the other browser and email products that also depend on Mozilla's Root Program. It would amount to an unprecedented weakening of the website security ecosystem.

Mozilla does not submit these comments out of financial self-interest. Mozilla's Root Store Program is free and we do not generate revenue through it. To the contrary, we are a public benefit organisation and our open source browser Firefox has an established privacy and security reputation. We are deeply concerned about the harms that will result should EU legislators adopt the proposed Article 45 and its security flaws.

The grave security risks elaborated in this position paper should be addressed by, at a minimum, reverting back to the status quo of the existing eIDAS regime. That means dropping the provisions of Article 45.2 that would override our ability to independently develop and enforce our independent Root Store security policies.

2. About Mozilla

Mozilla Corporation builds the open-source Firefox web browser, Mozilla VPN, and the Pocket "read-it-later" application. These products are used by hundreds of millions of individuals around the world. Mozilla Corporation is a private company fully owned by its sole shareholder, the non-profit Mozilla Foundation. The Mozilla Foundation furthers our mission to protect an open and accessible internet, by investing in advocacy, research, and movement-building. It is guided by the set of principles in the Mozilla Manifesto that recognise, among other things, that the internet is integral to modern life; the internet must remain open and accessible; security and privacy are fundamental; and that a balance between commercial profit and public benefit is critical.

We have worked hard to make the Mozilla Manifesto's vision for privacy and security a reality for the billions of users of the web. We do this by leading and participating in the creation of web standards that make the internet more secure and more protective of privacy, and by pioneering the product-level implementation of privacy and security-enhancing browser technologies through Firefox.

Mozilla has been a proponent of many of the key EU regulatory interventions concerning the tech sector in recent years. We advocated in favour of the General Data Protection Regulation (GDPR) and the E-Privacy Regulation; we are a founding signatory of the EU Code of Practice on Disinformation; and we have been at the forefront of the stakeholder efforts to implement the next-generation of internet laws through the Digital Services Act and the Digital Markets Act.

Our concern with the legislative proposal to revise the eIDAS Regulation is limited to Article 45. This is a rare instance where we are obliged to voice not support — but serious concerns — with the EU legislative trajectory and the risks it poses for online security architecture and the security assurances behind Firefox.

3. Security is fundamental to Mozilla, Firefox, and our Root Program

Mozilla has spent years building the internet as an open and interoperable platform that is private and secure. Mozilla has influenced major companies to adopt better privacy practices such as browser anti-tracking measures and has influenced consumers directly with tools to improve digital literacy and better understand third-party data collection. We have made online commerce and navigation safe through protocols and initiatives like TLS 1.3 and Let's Encrypt.

TLS 1.3 is the protocol that powers every secure transaction on the internet. Prior versions of TLS involved privacy leakage, outdated cryptography, and slower web page loading. As the lead editor of the TLS 1.3 specification at the IETF, Mozilla drove the development of security innovations to improve the prior version and also forged collaboration between communications experts, standards organisations, and academic security communities.

Let's Encrypt is another major internet security success story of which Mozilla is a proud co-founder. It's creation has resulted in more than 85% of online traffic being encrypted with HTTPS (signaled by a green padlock on many web browsers), compared to less than 30% in 2014. This protects consumers by ensuring that the websites they visit are in fact the real websites.

Mozilla has also been instrumental to improving security properties in foundational compilers, programming languages, and other communications protocols used not only in browser technology, but other applications such as Content Delivery Networks, video conferencing, AI, IoT and so on. Put simply, Mozilla is deeply invested in the effort to create a trusted online ecosystem, both as a browser maker and as a stakeholder in the broader internet ecosystem.

4. Browsers defend the privacy and security of users online

a. Browsers help secure everyone against attackers

The browser is the cornerstone of web access and necessary to the open internet. Browsers are unique because they represent every *individual* as they navigate across billions of websites. They enable individuals to express themselves, communicate and engage with others, engage in commerce, education and work, and participate in democratic society.

While browsers protect individuals in many ways, **website authentication** is fundamental to user security. Encryption of web traffic protects users against some dangers, such as eavesdropping. But encryption alone cannot keep people safe online. Users also need assurance that they are sending data to the correct party. If a user sends their private data to an attacker instead of to their bank, for example, it is of little consolation that the data was encrypted while in transit. This is why to be effective in practice, the communication protocol TLS (Transport Layer Security) that is used by modern browsers, must be coupled with website authentication.

For instance, if a person wants to visit Europa.eu, the web browser must reliably ensure that the site is actually under control of the owner of the domain 'Europa.eu', and not an attacker on the network *impersonating* the European Commission's domain. Absent that assurance, users might send passwords, personal details, and other compromising information to the wrong party, putting them at risk of identity theft, fraud, and other privacy interferences. Insecurity in website authentication can lead to significant harms, both online and off, as was seen during the DigiNotar attacks in 2011 that had EU-wide implications.

Examples of these harms include:

- **Privacy violations:** By interfering with the connection between an end-user and a server, an attacker can monitor communications between the two end-points and eavesdrop on communications between the parties.

- **Identity and credential theft**: Users who wrongly believe they are communicating with a trusted website may share passwords and other login credentials with attackers. Attackers can then use those credentials to impersonate users and compromise online accounts.

- **Financial Crimes and loss of trust:** One of the most dangerous consequences of an insecure website authentication ecosystem is the interception and illegal utilisation of financial instruments. Malicious actors can compromise the security of e-commerce websites by stealing such data (esp. credit card transactions) which can cause tremendous financial loss, reduce the trust in online transactions, and disincentivise digitisation.

- **Malware and targeting:** Attacks can redirect an end-user's web traffic to a different location on the web where they can directly install malware onto the end-user's machine, thus setting off a secondary chain of security and privacy harms. This can also be actively exploited to harm politicians, human rights activists, dissidents, and journalists, by targeting their traffic for interception and manipulation.

For these reasons, the trust benefits of website authentication are essential for the Digital Single Market, e-government, as well as to facilitate everyday uses of the internet and to protect the public interest work of journalists, politicians, and human rights defenders.

b. There are three essential parts to website authentication - Certificates, Certificate Authorities, and browser Root Stores

Digital certificates

Website authentication depends on a "**digital certificate"**.

A digital certificate is a document that ties the website server's name (e.g. "europa.eu") to a cryptographic key. The website's server can then prove its identity to the browser using that key, and once it has done so, the browser knows it has connected to the server identified in the certificate and can encrypt the connection (the padlock 🔒 on the left side of the URL bar in the browser symbolises this). This authentication and encryption are the cornerstone of trust on the web, driving e-commerce and enabling secure interactions for billions of users around the world.

Certificate Authorities

The digital certificates used by browsers for website authentication are issued by distinct entities called "**Certificate Authorities**" (CAs).

These organisations are responsible for verifying the website server's identity before issuing a certificate. This is a significant responsibility – if a Certificate Authority issues a website certificate that is incorrect or the certificate-issuing process is otherwise compromised, whether for malign intent or because of poor operational standards – the consequences for EU residents and organisations can be catastrophic. Put simply, for website authentication and encryption to work, and by extension e-commerce and e-government, Certificate Authorities must be reliable and trustworthy.

Root Programs and Root Stores

To ensure that Certificate Authorities can be trusted, most major browsers have a rigorous vetting process before a Certificate Authority can enter its ecosystem. This vetting process manifests through the "**root program**". Mozilla's root program has a large set of rigorous, public policies and practices that Certificate Authorities must meet in order to be trusted by web browsers and operating systems. The standards and criteria that underpin root programs are regularly discussed and improved at common industry fora such as the CA/Browser Forum.

Certificate Authorities must meet the criteria of the Root Program to be eligible for inclusion in the "**Root Store**" of browsers and operating systems. The Root Store is the collection of certificate authorities that both meet this vetting criteria and are actively trusted by browsers, which in turn recognise certificates issued by these CAs for websites/service providers. Mozilla does not charge Certificate Authorities any fee to be included in its Root Store.[1]

Crucially, web browsers continually monitor the Certificate Authorities that have been admitted into their Root Store. A Certificate Authority that fails to adhere continuously to the Root Program policies can be removed from Root Stores. This ability is vital in protecting users from inadvertent errors and malicious actors that can compromise the security and privacy of the open web. For example, in the past, browsers have denied entry into Root Stores to Certificate Authorities on grounds such as the CA had compromised security processes; the CA has links to authoritarian state actors; or because the CA was issuing certificates that impersonate other websites.

Mozilla's role in this space

Mozilla's Root Program is the most widely-recognised forum for open, public discussion of policy issues in this space. In addition to security, controlling our own Root Program allows us to share our values of transparency and public participation:

1. our policies and criteria are public;
2. we publicly publish findings for root certificate inclusion or removal from our Root Store;
3. we have a public incident reporting process that emphasises disclosure and learning from experts in the field; and,

[1] More detail about Mozilla's Root Store is available at:
https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

4. we hold public discussions to allow others to have a voice in these decisions, and this includes participants from many CAs, CA auditors, and other Root Store operators.

Mozilla's decisions on root certificate inclusion and exclusion are not dependent on any other organisation, government or fee. This enables Mozilla to make independent decisions that are best for individuals, and it supports the security assurances we make of the trust anchors in our program.

The value delivered by Mozilla's Root Program extends far beyond just Firefox. Because our Root Store is part of the NSS cryptographic library and is open source, it has become a de-facto standard for many Linux distributions and other products, like email clients, that need a Root Store but don't have the resources to curate their own. These developers, and their downstream users, all rely on the security assurances provided by Mozilla's Root Program.

5. The revision to Article 45 - what it includes and what it does

a. The 2014 eIDAS Regulation was premised on discredited security technology

The original eIDAS regulation was written in 2014 on a faulty assumption that Extended Validation (EV) TLS certificates would evolve into a widely-used basis for website authentication. These types of certificates relied on verifying the legal identity of website operators prior to issuance. However, subsequent research has demonstrated that EV certificates provide users with a false sense of security that is often exploited for malicious purposes such as phishing and domain impersonation. All prominent browsers disabled EV certificates by 2019 and none today showcase EV certificates directly in the URL address bar.

Unfortunately, the existing eIDAS Regulation, passed in 2014, had already created a distinct framework for website certificates and authentication, known as '**Qualified Website Authentication Certificates' (QWACs)** A **QWAC** is a type of certificate for website authentication that makes it possible to authenticate a website **and to** link the website to the natural or legal person to whom the certificate is issued. The problem is that QWACs were inspired by the aforementioned EV TLS certificates. As such, the fundamental motivating factor behind QWACs is flawed – they rely on a discredited security architecture that weakens trust and security online.

Developments since the adoption of the 2014 eIDAS regulation

Given this context, Mozilla and the wider browser community's preference would have been for the latest eIDAS revision to acknowledge recent security developments and drop outdated technology. Yet beyond these principle-based concerns regarding the effectiveness of QWAC-type certificates as a solution for trust on the web, no web browser has *in any case* been able to support QWACs since the adoption of the 2014 regulation.

This is because the **technical implementation framework** for QWACs that has been favoured by the European Commission and ETSI suffers from significant security and operational weaknesses, as the browser community has stated in its work with relevant European stakeholders between 2015 and 2020. These weaknesses are largely premised on technical incompatibility with how the web certificate ecosystem operates and tangibly weaker privacy characteristics, along with the reality that any certificate form based on EV certificate architectures are fundamentally ill-suited for web authentication. These points have been raised multiple times in bilateral conversations and industry fora by the entire browser community to no avail. The browser community has even offered several technical proposals in an attempt to mitigate the implementation weaknesses, none of which have been accepted by ETSI despite offering concrete ways to allow QWACs to co-exist with how other web authentication certificates work.

Unfortunately the 2021 regulatory proposal makes the risks associated with the QWAC framework much more dramatic, and will lead to a regression in the security assurances that users have come to expect from their browsers. This is because through Article 45.2, the legislative proposal, in effect, ***mandates* that browsers *automatically* include Trust Service Providers (TSPs) in their browser root programs**. '**Trust Service Providers**' (TSPs), in this context, are essentially Certificate Authorities (CAs) that can issue QWACs under the eIDAS regime. These TSPs are notified by member states and as Mozilla has highlighted in the past, many of them do not meet the criteria required to also be included in our Root Store. By mandating that TSPs be supported by browsers in general, and in particular when they fail to meet the security and audit criteria of their root program, Article 45.2 will negatively transform the website security ecosystem in a fundamental way. This is outlined in the following subsection in more detail.

b. The revised Article 45 overrides independent Root Programs and undermines their security assurances

The revised Article 45.2 creates a legal mandate for web browsers to support QWACs and accept TSPs into their Root Stores. This is unprecedented. It would replace the security expertise of major browser companies such as Mozilla who have developed a widely-acclaimed Root Program with legislation premised on weaker and discredited security architectures.

In practice, this legal compulsion means that a web browser like Firefox will no longer be able to ensure compliance with the security standards and safeguards that web users need and expect when it comes to website authentication. As noted above, these standards and safeguards are set out in our Root Program policies, and they include audit requirements, encryption strengths, public transparency requirements, and practice requirements that are far more rigorous than TSP standards.

Independently setting, monitoring, and enforcing our Root Store policies is an essential pillar of how we secure the browsing experience today. We pride ourselves on having in place robust, industry-leading policies, and it is a key expression of our Manifesto commitment that privacy and security are fundamental and should never be treated as optional. As a parallel, the internet as we know it largely exists due to the creation and adoption of web standards at standard development organisations (SDOs) like the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the CA/Browser Forum. In these fora, processes and policies are independently determined by participants and on the basis of shared expertise and diverse equities. Just like those processes, which are widely recognised as being responsible for the rapid pace of innovation on the internet, the independence of browser Root Program policies is a fundamental enabler of a dynamic and responsive website security ecosystem.

Mozilla has provided evidence in the past of how the security practices for TSPs that issue QWACs are tangibly weaker than Mozilla's own Root Program policies. Should Article 45.2 be adopted in its current form, with its obligation that Mozilla suspends our security policies and procedures where QWACs are concerned, we would no longer be able to effectuate our commitment to keep our users' browsing experience secure. Crucially, this would apply to all the other products that also use Mozilla's Root Store and have massive 'downstream' impact.

6. The revised Article 45 creates vulnerabilities to be exploited by authoritarian regimes

If adopted in its current form, the revised Article 45 of the eIDAS regulation will set a radical negative precedent for web browsers' ability to implement and enforce Root Program policies. Authoritarian regimes in other parts of the world have long sought to override web browsers' Root Program security policies – a trusted website authentication ecosystem is a barrier to surveillance and censorship. For example, the Kazakhstan government has tried to force its citizens to install (in 2015, 2019 and 2020) certificates that would have compelled users to allow their traffic to be intercepted and surveill internet traffic. The government of Mauritius also considered amending its laws to force browsers and platforms to carry out similar interception for social media traffic in mid-2021.

The browser community and a broader coalition of civil society advocates have long resisted these efforts by authoritarian regimes to undermine web security, and our efforts have been buttressed by the fact that interference with Root Program policies by a regime is incompatible with fundamental rights and the rules-based international order globally. Indeed, we have been able to resist these interferences *precisely because* there is a trusted, robust, and multi-stakeholder ecosystem that governs website authentication.

Unfortunately, our ability to resist these efforts by authoritarian regimes would be undermined by the revised Article 45. As currently proposed, the EU framework green-lights the precise kind of security overrides that authoritarian regimes demand. Worst of all, these risks to cybersecurity and fundamental rights are not locally-contained to the region where they are demanded. A locally-mandated Certificate Authority can execute network interference attacks *globally*, thereby posing a risk to EU residents and businesses.

7. How can we address this

Based on the above, the elements of the eIDAS revision that concern QWACs, TSPs, and browsers' relation to them **must be revisited as a matter of urgency in the co-decision procedure.**

At a minimum, the revised Article 45.2 should be amended such that support for QWACs is not mandatory for web browsers. Further, as discussed, the entire security architecture on which QWACS are premised has serious security challenges that can compromise privacy, security, and democracy in ways that legislators should not endorse.

8. Conclusion

In conclusion, browsers are the front line of security on the web through the role they play in the website authentication ecosystem. A key element of this work is the operation of independent Root Stores. By rigorously implementing and enforcing security standards that determine who gets to issue website certificates to users and under what circumstances, browsers ensure trusted and secure interactions between users and service providers. This underlying trust and security is an essential prerequisite for the digitalised economy and society.

By stripping browsers of their ability to implement and enforce their Root Program policies as is the case today, the revised Article 45 would significantly increase cybersecurity risk for EU residents and businesses, and indeed individuals around the world. Browsers will not be able to ensure this trust is present for critical transactions like financial transfers, credit card transactions, and login authentication.

Ironically, this will greatly exacerbate the very mistrust and security risk that QWACs are apparently designed to mitigate, and undercut progress towards a deeper EU Digital Single Market.

We urge lawmakers in the European Parliament and the EU Council to address these fundamental flaws in the eIDAS revision.

****

To discuss this position paper in more detail and how the above concern can be practically addressed in the mark-up phase, please contact Owen Bennett, Senior Policy Manager (obennett@mozilla.com) and Udbhav Tiwari, Public Policy Advisor (utiwari@mozilla.com)