A law of unintended consequences

The revision of the EU's digital identity law, eIDAS, could undermine security on the world wide web.

In this report, we outline what parts of the web security ecosystem eIDAS Article 45.2 will affect and what it will be casting aside. Four experts explain the risks within Article 45.2

Table of Contents

3 Introduction

4 An attempt to “fix” web security risks breaking it

6 HTTPS - securing the web since the 20th century

8 Four authentication and encryption experts explain why eIDAS Article 45.2 should be revoked

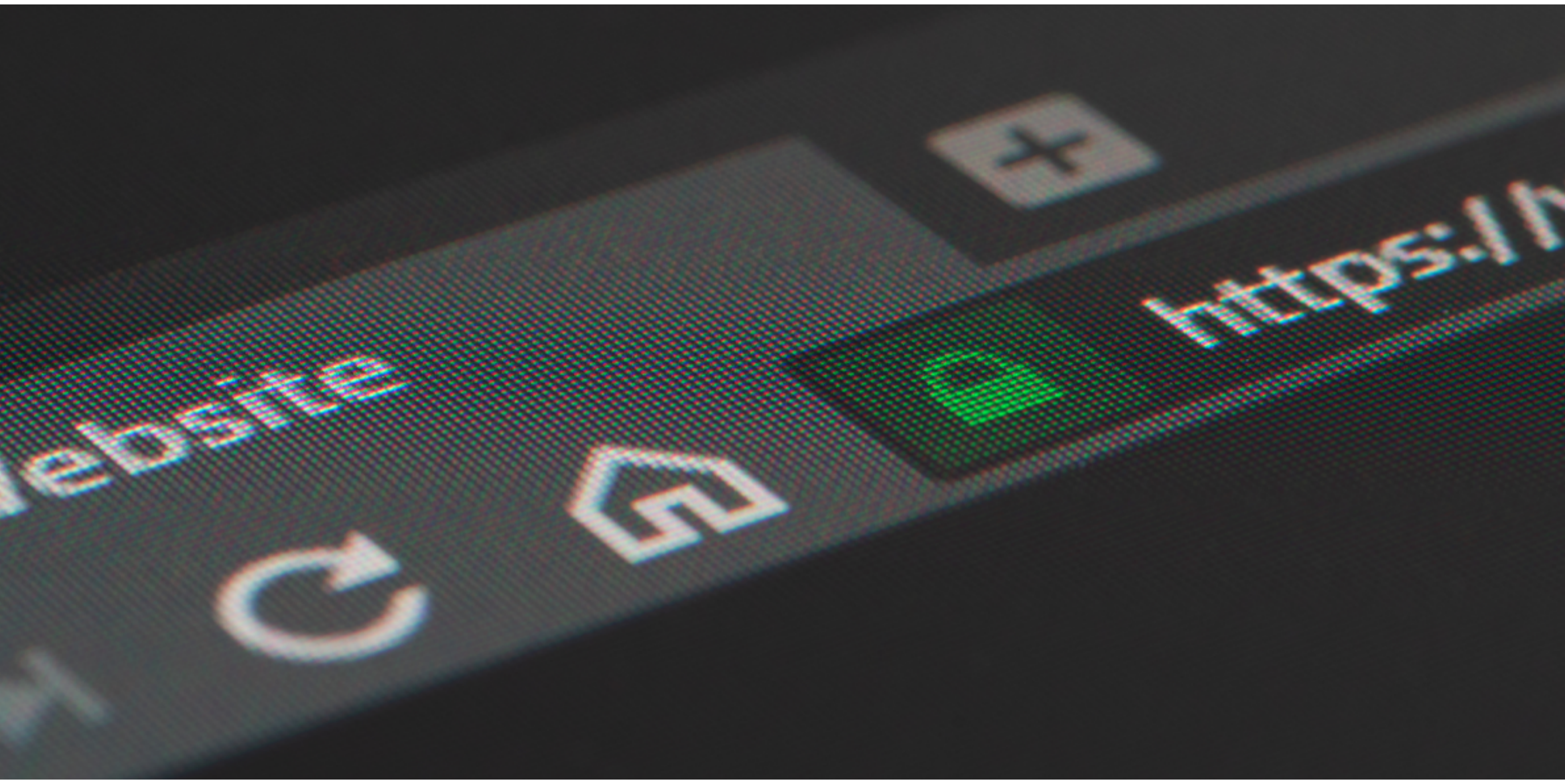
12 Conclusion: It’s time to come together for the good of web security

Introduction

A revision the European Commission has proposed to the EU's digital identity law, eIDAS, could undermine security on the world wide web – potentially risking an increase in ID theft, phishing and financial fraud. It could even aid in the surveillance of dissidents by repressive regimes.

The revision, known as eIDAS Article 45.2, will legitimise the establishment of new Certificate Authorities (CAs) in all 27 EU member states – with each empowered to force web browser makers to automatically recognise a discredited technology: Qualified Website Authentication Certificates (QWACs). But QWACs for websites were never adopted as they relied on an approach that cybersecurity specialists call "security theatre", in which web users enjoy only a false sense of security.

In this report, we outline what parts of the web security ecosystem Article 45.2 will affect and what it will be casting aside, before asking four of the world's leading digital authentication and cybersecurity experts to explain why the risks that Article 45.2 exposes us to mean that it must be revoked.



An attempt to “fix” web security risks breaking it

If, as is likely, you are reading this report on the web, or have downloaded it from a website, there are two things you can be pretty sure of. First, the browser will have authenticated it as the genuine website that you entered, ensuring that it was not a fraudulent fake designed to steal your credentials. And, second, that data encryption will have been harnessed to ensure that nobody can intercept, eavesdrop on, or modify the information exchanged between your browser and the website.

These may sound like simple measures, but the fact that this process happens transparently to you – in the background, instantly and securely – is actually the result of a quiet miracle that has been many years in the making.

For almost three decades, browser makers such as Mozilla, Microsoft, Apple and Google have worked with internet security engineering groups worldwide to build trust into the very fabric of the web. Together, they have developed methods, policies and standards that ensure that HTTPS – the technology underlying website authentication and traffic encryption – is trustworthy.

Trust online is assured by requiring website operators to acquire a secure digital code, known as a certificate, from an approved organisation called a Certificate Authority (CA). CAs are heavily vetted by each browser maker, through what are known as root programs, before they can be deemed secure enough to issue web certificates.

Once approved, a CA is listed as legitimate in the root store in the browser. Users can then access websites with certificates signed and issued by those CAs. If a certificate is invalid, or non-existent, the user will be warned that pressing ahead and accessing the site would be a major security risk.

> **HTTPS is at the very heart of security in today's thriving web ecosystem. But the security of this critical certificate-based technology – and, with it, the online safety of all web users – is now in jeopardy.**

Consequently, HTTPS is at the very heart of security in today's thriving web ecosystem. But the security of this critical certificate-based technology – and, with it, the online safety of all web users – is now in jeopardy.

The reason? A decision by the European Commission to revise eIDAS, the EU's Electronic Identification, Authentication and Trust Services law. For many, these revisions, known as eIDAS Article 45.2, are regarded as a clear and present threat to web security, one that can only help cybercriminals commit fraud and enable repressive regimes to undertake surveillance of dissidents and whistleblowers.

In short, the Commission's aim is to enforce the acceptance of a type of certificate, known as a Qualified Website Authentication Certificate (QWAC), across the EU. It wants to allow a new breed of CAs, operating in each of the EU's 27 member states, to issue these QWACs. It also wants to have the power to force browser makers to recognise QWACs as valid certificates without the extensive vetting and auditing process that is required at present.

One of the Commission's aims with Article 45.2 is for certificates to include user-readable data about the name and registered address of the legal entity behind the enterprise or organisation that owns and operates the website. This aligns with the bloc's data privacy law, the General Data Protection Regulation (GDPR), which allows people (such as website users) to know exactly who is acquiring and using their data (the website operators).

Although a shallow analysis of this idea might suggest that it could be a good thing, a closer look at recent history suggests otherwise. Including a website's legal entity data in a certificate has been attempted before, with Extended Validation (EV) certificates. EVs displayed information on websites' legal operators in the browser bar in the user interface – just before the URL – although extensive research showed that web users widely ignored that information.[1] Problematically, it also proved too difficult and expensive to acquire accurate legal entity data on every company or organisation across different nations, and even across different US states. With the measure failing to improve web security, in 2019 browser makers effectively ended the use of EVs by removing the legal entity data from the user interface display.

In that context, it is clear that what the Commission is actually doing by advocating the adoption of QWACs is providing users with a false perception of improved security. This is a concept that security professionals term "security theatre".

To push these QWACs, the Commission is willing to allow the establishment in each EU member state of CAs that would potentially be subject to less secure standards. This has the potential to generate a wave of security risks and undermine nearly three decades of progress driven by browser makers and organisations such as the Internet Engineering Task Force.

[1] https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/ev-to-page-info.md

HTTPS - securing the web since the 20th century

So just what, in security development terms, will the Commission be throwing away if eIDAS Article 45.2 is allowed to stand and leads to the introduction of insecure CAs?

Securing the web began in 1994, when Netscape Communications Corporation, author of the Navigator browser, developed and introduced HTTPS. But by the turn of the century, the technology was still what Marshall Erwin, vice president and chief security officer at Mozilla, describes as a bit of a “boutique” security feature, one that few knew about.

“It was a privately managed system that was not public-facing. There was very little transparency in it. If you were on that list, you got to issue certificates that would then work in the browser – but there was no real public policy saying how you got on the list, how you were removed from the list, and exactly what standards you needed to meet,” he explains.

Mozilla consulted widely and drafted a policy that brought public-facing transparency to the governance of certificate management in Mozilla’s root store, says Mr Erwin. “We published that groundbreaking, innovative policy in 2004. Although it has evolved since, the basic pieces have stood the test of time – it’s been pretty foundational.”

By 2014 HTTPS was securing only 30% of website page loads globally – and the Electronic Frontier Foundation (EFF, a digital rights group) and Mozilla thought they knew why: having to buy certificates was deterring people from using HTTPS, as was having to manually renew certificates on expiry. So in 2014 – alongside content delivery provider Akamai Technologies, networking giant Cisco Systems and the University of Michigan – they launched Let’s Encrypt, a next-generation, not-for-profit CA. This democratised the entire process, giving out certificates for free,

> It is clear that what the Commission is actually doing by advocating the adoption of QWACs is providing users with a false perception of improved security.

and using automation to do so at scale – and renewals were handled automatically.

“What we saw as a result was a sudden increase in the percentage of web traffic that was being encrypted around the time that Let’s Encrypt was founded. Although HTTPS technology was mature, the deployment model wasn’t working as well – Let’s Encrypt changed that in a fundamental way,” says Mr Erwin.

Independent observers agree. Scott Helme, a UK-based cybersecurity researcher who specialises in authentication technology, says that Let’s Encrypt and other free CAs raised website page loads using HTTPS from 30% in 2014 to an astonishing 85% in 2021. It is this kind of web security level that today’s slow and steady improvements in root certificate programs have led to – and which the European Commission is willing to jeopardise with Article 45.2.

Four authentication and encryption experts explain why eIDAS Article 45.2 should be revoked

Arvid Vermote

Worldwide chief information security officer,
GlobalSign

Few security specialists have seen the web authentication issue from so many critical angles as Arvid Vermote. Before assuming his current role at GlobalSign, a CA, he was a Webtrust auditor of Cas around the world at the EY (Ernst & Young) Global.

“I’ve seen the best of both the CA and the CA auditor worlds. The root program supervisory bodies have solid and long-lasting technical experts in place, and they really know their stuff: they do a strong evaluation and properly ‘roast’ applicants before accepting them as a CA,” Mr Vermote says.

“The big concern for me, in eIDAS Article 45.2, is the part that says browsers should accept any Certificate Authority in its root store when any of the EU member states says they should be accepted. With the Article 45.2 revision, suddenly, apart from the four browser root programs, we will now have 30 extra supervisory bodies, because that’s how many EU/EEA countries there are, all with the capability to decide for a Certificate Authority to be trusted in the browser. So suddenly, from four, we’d have 34 instances that can define a company as globally trusted. That technical trust comes, with the implication that any traffic on the internet could be targeted for interception if those CA are compromised. For me, that would be an astronomical problem.”

> **So suddenly, from four, we’d have 34 instances that can define a company as globally trusted. That technical trust comes, with the implication that any traffic on the internet could be targeted for interception if those CA are compromised. For me, that would be an astronomical problem.**

Joseph Lorenzo Hall

Senior vice president for strong internet,
Internet Society

To Joseph Lorenzo Hall, what is deeply wrong with the Article 45.2 revision to eIDAS is that it shows the European Commission does not seem to understand that web security is always evolving, because security in general is an ever-moving target.

"The only way this certificate technology, based on public key cryptography, works is if it's continually evolving and adapting. The fact that it seems like it's been stable for nearly 30 years is a huge success, because in fact it changes all the time. It changes because someone, for instance, will break a certain kind of encryption and we'll then have to get everyone to use a new kind – but getting hundreds of millions of people to do that online is really, really hard."

What is clear, Mr Hall says, is that the EU is letting geopolitics cloud clear, sound, security thinking. "There's tons of people from around the world involved in the EU certificate debates, but to anyone who's been part of the regulatory discussion for the last two to three years, it's clearly very anti-American, and particularly anti-Silicon Valley, on a whole range of issues." Wanting to wrest some control from Silicon Valley is no reason to back a discredited technology like QWACs and use insecure CAs to push them out unaudited, he adds.

"The root certificate system is brittle but extremely well policed. There are things that can happen in a moment that can dramatically undermine the trustworthiness of millions of websites online: if someone breaks a popular form of cryptography, suddenly any website that uses it could be undermined, and people – from e-commerce users to dissidents and whistleblowers – may not be secure any more. So you have to police these things and be extremely agile about it. Because the last thing you want is to go on a holiday and find all your purchases were actually funnelled into a criminal bank account because we weren't vigilant about the little flaws that keep popping up."

Continually managing these "little flaws", and through that vigilance nailing down HTTPS security, is undertaken by a dedicated group known as the Certificate Authority/Browser Forum. Mr Hall describes their tireless, evolutionary work as a process of constant gardening.

He is clear that the EU cannot just legislatively insert its Article 45.2 ideas into the current ecosystem without causing problems. "What they don't seem to understand is that by bolting an exception mechanism on for EU government trusted entities, browsers will be forbidden, for example, from revoking trust for certain things. This means that you could have a group of websites online that are being spoofed, or being eavesdropped upon, by some compromised EU-anointed authority. And we are handcuffed and cannot do things that we would normally do very quickly to protect the people of the internet," he explains.

Mr Hall predicts that this could have serious unintended consequences for the future of e-commerce, too – the opposite of what eIDAS advocates want. "If browsers are unable to take action when a QWAC domain is breached, or has a problem, and we can't respond in the community, trustworthiness will be lost. That could lead to less e-commerce and less online transactions," he warns.

> **If browsers are unable to take action when a QWAC domain is breached, or has a problem, and we can't respond in the community, trustworthiness will be lost.**

Marshall Erwin

Vice president & chief security officer,
Mozilla Corporation

According to Marshall Erwin, enforcing the use of the already discredited QWAC technology, and the egregious step of forcing unaudited CAs into browser root stores, amounts to a two-pronged government attack on web authentication and encryption standards.

"The EU is trying to establish that QWACs should be used because they allow the user to determine the legal entity that is sitting behind the certificate. But many studies have asked if this information is something users would actually benefit from – and the answer to that is 'no.'"

"That's why all of the major browsers removed EV certificates, which do the same thing as QWACs, because we found that users just really didn't benefit from it. It was intended as a phishing mitigation but it didn't work – yet the EU has not realised this and is aiming to mandate QWAC use," says Mr Erwin.

The QWAC format will require CAs in the EU's 27 member states to vet the legal entity information that is included in them – and that process will cost money, Mr Erwin explains. "The companies that benefit from this are those that want to be able to charge website operators for certificates. This will turn back the clock on web security to where it was prior to Let's Encrypt founding in 2014."

"There's a community of CAs in the EU, roughly 50 of them, and I think they would all stand to gain from being able to charge for certificates. Twenty of them are already in the browser, but that leaves 30 who have not met our security standards. And I think that's the interest group that really stands to gain the most from QWACs."

Another issue is that Article 45.2 demands that QWAC-issuing CAs are automatically recognised by browsers. "It is very problematic that the EU would require Mozilla to include CAs in our root store that issue QWACs that have not met our security standards. After roughly three decades' work developing security standards, this essentially amounts to government circumvention of them. And that, in our view, is the really problematic part as it sets a precedent globally that we think will be quite damaging."

It would only take a compromised employee in one of the new unaudited CAs to breach security, Mr Erwin says – and they know this because it has been attempted before.

"We know that repressive regimes around the world are really interested in conducting men-in-the-middle attacks, surveillance in the middle of the network, and they have actively tried to compromise Mozilla's CA program to surveil dissidents and journalists. We had a case about three years ago where a front company for a United Arab Emirates intelligence agency attempted to gain access to Mozilla's root store, essentially because they wanted to surveil dissidents and journalists operating locally. This is something we've seen over and over again: repressive regimes want to compromise encrypted web traffic and gain clear text access to traffic on the internet. And the real problem with Article 45.2 of eIDAS is it's going to set a precedent that regimes around the globe are going to follow – and as a result not only undermine web encryption in general, but then also put dissidents, and journalists, at immediate risk."

> **"The real problem with Article 45.2 of eIDAS is it's going to set a precedent that regimes around the globe are going to follow – and as a result not only undermine web encryption in general, but then also put dissidents, and journalists, at immediate risk.**

Scott Helme

Authentication & security researcher

Scott Helme knows just how important free certificates are to website security. “In terms of how much encryption is used on the web, you can see quite clearly, up to 2014 we’d been making 1% or 2% progress a year. But when we got to 2015 [and the launch of Let’s Encrypt], we got a hockey stick effect, and off we went. By 2021, it had shot up to 85%. So free certificates have been fundamental in completely transitioning web security.”

But if eIDAS Article 45.2 stands and QWACs are enforced, paying for certificates could return, he believes, with a concomitant downward pressure expected on security levels. The reason, says Mr Helme, is that QWACs incorporate expensive-to-find data on the legal entity behind a website, so costs are incurred that someone – almost certainly the website operator – will have to pay.

“With QWACs, as with EVs before them, there’s an additional overhead on the CA side because they have to check the registered company the operator trades under. That’s a human process and human processes are very expensive,” he explains.

Whereas today HTTPS certificates can be purchased for between $10 and $30 (or obtained for free from the likes of Let’s Encrypt), Mr Helme predicts that in the future, QWACs could cost as much as $1,000. But as he explains, paying for a QWAC could all be for nothing in any case, as scammers and fraudsters can easily register businesses that sound similar to legitimate ones.

“With EV certificates, the previous generation of QWACs, they published very clear guidelines in the rules that said just because somebody has registered a company, it doesn’t mean they’re legitimate. Here in the UK, for instance, it only costs £12 to get a registered company name – and there’s zero checks that happen, so it’s no barrier to entry,” says Mr Helme.

What is baffling, he adds, is precisely what is driving a lot of the smart, highly respected people he has met at the European Commission to pursue QWAC technology, when all the evidence says they should do otherwise.

“I’m curious to understand more about why it is that the EU is independently seeing a benefit in this,” he says. “Or are they being sold really hard that there is a benefit by organisations that stand to make a large amount of money? I feel like this is driven more by the organisations that will be selling these products in the future. So I wonder if the evidence that’s been presented to them is perhaps a little skewed.”

> **I’m curious to understand more about why it is that the EU is independently seeing a benefit in this. Or are they being sold really hard that there is a benefit by organisations that stand to make a large amount of money?**

CONCLUSION

It’s time to come together for the good of web security

The European Commission is leading security technology down the wrong path with its insistence on auto-recognised CAs and its attempts to enforce QWACs, a technology that is identical to the previously discarded generation of EV certificates. Such moves pose a threat to the integrity of today’s browser root stores.

It shouldn’t be this way. With legislation such as GDPR and the forthcoming Artificial Intelligence Act, the Commission often leads the world on technological matters. As such, it also needs to lead on internet regulation across the EU’s 27 member states. Yet, with Article 45.2, it is in danger of needlessly placing a limit on web security for citizens, users, the wider economy and even democracy, as repression loves insecurity.

What is needed instead is dialogue and collaboration between all the global parties involved in web authentication and encryption, rather than the establishment by the European Commission of a separate cybersecurity regime for the EU – a move that risks instilling an insecure future for the web.

For more information, visit

SecurityRiskAhead.EU