Internet Impact Brief

Mandated Browser Root Certificates in the European Union's eIDAS Regulation on the Internet

Marshall Erwin, Mozilla
Carl Gahnberg, Internet Society
Udbhav Tiwari, Mozilla
Robin Wilton, Internet Society

Version 1.0 (8 November 2021)

Abstract

In 2021, the European Union (EU) proposed an amendment to the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation that would change provisions related to Qualified Website Authentication Certificates (QWACs). The proposal could empower governments to compel browsers to validate specific Certificate Authorities (CAs) that may or may not comply with industry best practices for ensuring security online. This report uses the Internet Impact Assessment Toolkit[1] (IIAT) to assess how the EU's proposal may affect the global Internet by impacting what the Internet needs to thrive as an open, globally connected, secure and trustworthy resource for all.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.
To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally-connected, secure and trustworthy resource.

Context

Certificate Authorities (CAs) are a critical component of Public Key Infrastructure (PKI), which is a system of creating, managing, and using digital keys and certificates. The most familiar use of PKI in today's Internet is for secure web browsing using the Hypertext Transfer Protocol Secure (HTTPS), which relies on digital certificates and an encryption protocol called Transport Layer Security (TLS)[2].

The role of the CA is to issue digital certificates that certify the ownership and authenticity of a public encryption key. In the TLS

[1] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/ The IIAT was developed by the Internet Society[1] to be used by anyone who wants to check if a particular policy, development, or trend affects the critical properties of the Internet Way of Networking (IWN) and the Enablers of an Open, Globally-Connected, Secure and Trustworthy Internet. .

[2] In the context of TLS these certificates are, for historical reasons, sometimes referred to as SSL certificates.

protocol, the certified public key is used to create a secure connection between two or more parties[3], and to verify that the public key offered by a website does indeed belong to that website, and not someone else. The fact that the CA has signed the certificate – under a specific set of rules - gives assurance that the public key has been issued to a validated entity. Digital certificates used in this way ensure the authenticity, integrity, and confidentiality of the communication. By contrast, if a web browser is persuaded to accept a fake certificate, a third-party could impersonate the other communicating parties, eavesdrop on the conversation, and/or potentially tamper with or forge the messages exchanged. These vulnerabilities open the way to further malicious actions, such as the spreading of malware, or imitation of banks and other sites to steal users' credentials.

Since there is a risk of a CA issuing an incorrect certificate, the system of PKI is inherently dependent on trust in the CAs themselves. To this end, entities acting on behalf of the users, or "user agent," choose whether to trust a CA and a certificate. As user agents, browser vendors maintain a tightly controlled list of CAs (known as "root stores") that meet their own policies and industry security standards developed by the CA/Browser Forum. If a CA is not able to meet these requirements the root store owner (browser vendor) excludes it from the list of trusted CAs.

What are eIDAS and QWACS?

The Regulation on electronic identification and trust services[4] for electronic transactions in the internal market (eIDAS Regulation) aims to make electronic transactions between businesses safer, quicker, and more efficient in the European Union. Adopted in 2014, the eIDAS regulation has applied to the EU since 1 July 2016, meaning public services in the Member States must recognize national electronic identification schemes (eIDs).

One of the main goals of eIDAS was to make public and business services more accessible, especially across EU Member States. This included the development of eIDAS standards, building on the 1999 e-Signature Directive[5] which gave the same legal standing as ink-and-paper signatures to transactions using electronic signatures, qualified digital certificates, electronic seals, timestamps, and other authentication techniques.

eIDAS proposes the issuing of Qualified Website Authentication Certificates (QWACs) by a Trusted Service Provider (TSP), to act as "[…]an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued". This QWAC standard is in turn based on the Extended Validation Certificate for Transport Layer Security (EV TLS), which is a

[3] To learn more about Public Key Infrastructure and Certificate Authorities, see: https://www.internetsociety.org/resources/deploy360/2017/introduction-to-pkis-cas/

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

set of guidelines originally created by the CA/Browser Forum to denote that the owner of a certificate has been extensively vetted by the CA beyond the baseline requirements. However, after many years of deployment, the CA/browser community has, by mutual agreement, moved away from EV certificates because they were not felt to provide users with clear, actionable cues about online trust, and were therefore adding cost and complexity but little or no benefit.

2021 proposal to amend the eIDAS regulation

The European Commission is currently evaluating this regulatory framework. It organized a public consultation in 2020 to collect feedback on drivers and barriers to the development and uptake of trust services and eID in Europe. On this basis, the Commission has proposed an amendment to the 2014 regulation to try to stimulate adoption of the framework and the availability of secure eID schemes across the internal market.

Among the changes in the new proposal are provisions around QWACs that could have the effect of forcing browsers to include TSPs (i.e. CAs) authorized by national governments into their root stores, without guaranteeing security parity with current best practices. In other words, it would require browsers to add these CAs to the list of trusted middlemen – even if they do not meet industry standards or are recognized as a trusted party.

Although the text of the proposal may seem uncontentious, the high-level goals have unstated technical consequences which we believe are unpalatable regardless of which option is put into practice (For more information about our interpretation of the proposed revisions, see Annex A).

How Do the Proposed Amendments Affect the Realization of the Full Potential of the Internet?

In order to assess the proposed amendments affect how we get to an Internet that is Open, Globally-Connected, Secure and Trustworthy, we will look at them through the lens of the enablers of these goals[6].

Collaborative development, management, and governance

A key feature of an open Internet is that its resources are developed, managed, and governed in a collaborative way. This means that standards, technologies, and products are developed following

[6] https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

principles of collaboration, expertise, transparency, and consensus, and on the basis of leading to global accessibility. ETSI's assumption that browsers would add eIDAS-approved Trust Service Providers (TSPs – the issuers of QWACS) to the trusted root list violates this concept of voluntary collaboration. This is because the requirement to include a Trusted Service Provider (TSP) would override the trust criteria mutually agreed among the certificate authorities, browser manufacturers and other relevant stakeholders (such as mobile handset vendors and IoT manufacturers).

Unrestricted Reachability

A globally connected Internet is premised on the ability of Internet users to access and use resources in other networks without unnecessary restrictions. If incorrect or insecure certificates are issued, this can be used to impose drastic restrictions (e.g., through spoofing or Man-in-the-Middle (MiTM) attacks[7]) on users' confidence that the resources they are accessing are the ones they intended to reach across the global Internet.

Integrity of Information, Applications, and Services

Since the use of digital certificates assures the data transmitted is both complete and accurate, as well as confidential, the proposed measures are also a direct threat to Internet security. Digital certificates safeguard the integrity of information by preventing transmitted data from manipulation, and a CA that does not meet the required security standards increases the risk of incorrect certificates being issued, either by accident or by malicious intent (e.g. the certificate could itself be used as a MiTM by a malicious actor).

Data Confidentiality of Information, Devices, and Applications

Digital certificates also play a key role in encryption, which enables data confidentiality by allowing users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. This ability to communicate confidentially is put at risk if a CA does not meet the required security standards.

Reliability, Resilience, and Availability

The risks associated with incorrect certificates undermines the ideal of a trustworthy Internet as the reliability of online services could be affected both by the issuing of incorrect certificates, and inability to rapidly address security incidents. A legal mandate requiring browsers to include TSPs in their root store and validate QWACs means browser manufacturers will be unable to respond as promptly to

[7] https://www.internetsociety.org/news/statements/2019/internet-society-concerns-kazakhstan-encryption

security incidents. Security concerns can arise suddenly and can impact large numbers of users in a short period of time: browser manufacturers need a response procedure that is as simple and timely as possible. This mandate would introduce greater complexity, and increase the time needed to respond to security incidents.

Accountability

The provisions would also undermine the ability of users and root store owners to hold a designated TSP accountable for any incorrect behaviour, and introduce a new and grave risk that a designated TSP may also engage as a MitM mechanism. Furthermore, since a mandate would hamper the ability of a root store owner to respond to issues of this kind, and to adhere to their own policies, it risks producing an additional accountability gap between users and the browser vendor.

Privacy

Finally, the risks associated with incorrect certificates could also undermine privacy since incorrect certificates provide the means for third parties to intercept and modify traffic without the knowledge or consent of the sender and recipient. This extends to ETSI's interpretation of the process for validating QWACs, since at least one of the technical options (See Annex A, Option 2) would reveal a user's browsing activity to a third-party validation service (which in turn would be positioned to track and profile users based on this information) as can be seen from previous presentations at industry meetings by relevant participants in the CA Browser Forum[8].

[8] Slide 50, "Trust Zones -The Gordian knot between QWAC and Browser: Proposal for a Solution", CA Day, 23 September 2020.:https://www.enisa.europa.eu/events/tsforum-caday-2020/presentations/CAD-presentations

Summary & Recommendations

The proposed changes to eIDAS are based on the principle that TSPs, by issuing QWACs, should provide an online experience that increases users' level of trust in the authenticity of websites.

Therefore, TSPs should exceed the technical and best practice standards of web PKI Certificate Authorities. This would start with TSPs complying with existing CA/Browser forum standards, and adding further trust-enhancing measures on top of those. This would be more effective and inherently less risky than the eIDAS proposal to establish a parallel assurance scheme that is decoupled from existing certification standards and processes.

Mandating browsers to include CAs authorized by national governments into their root stores, without guaranteeing security parity with current best practices, poses a significant risk to the global Internet. It undermines the security of the Internet and the integrity of the browser experience and erodes trust in the global public key infrastructure.

In this light we recommend that provisions that would mandate browsers to include TSPs in their root stores be removed and replaced with guidance to the effect that TSPs should meet industry best practices and requirements to be included in relevant root stores.

While this analysis has focused on the impact on the global Internet, it should be noted that there are other means for enabling the regulatory environment established by eIDAS. For instance, there are several alternative solutions that would not interfere with the global system of TLS, as noted by Mozilla in their contribution[9] to the European Commission. The Internet thrives on collaboration to address challenges, and this approach is key to achieve our shared goals for a more secure Internet for everyone.

[9] https://blog.mozilla.org/netpolicy/files/2020/10/2020-10-01-eIDAS-Open-Public-Consultation-EU-Commission-.pdf

Appendix A: Article 45 of the eIDAS proposal

Source: Regulation COM(2021) 281
https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

Article 45
Requirements for qualified certificates for website authentication
1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.
2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.
3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Annex A - Interpretation of the proposed revisions

The Commission's proposal text itself says nothing about *how* the envisaged changes should technically underpin the desired assurance of website authenticity – only that qualified certificates "shall be recognised by web-browsers", and web-browsers shall ensure support and interoperability with qualified certificates for website authentication". (See Appendix A, which contains Article 45 of the proposal). As a result, much of the browser community's understanding of the technical strategy is based not on the proposal itself, but on discussions with ETSI, the European Technical Standards Institute, about technical options[10].

There appear to be three technical options, each with their own risks:

1. Cryptographically bind QWACs to TLS certificates. This violates the principle of technology neutrality, because it means that QWACs will only work if used in conjunction with a TLS session. However, as eIDAS is not in a position to require TLS, in fact its own "technology neutrality" requirements prevent this option from being implemented.
2. Have separate protocols for (i) TLS certificate validation and session establishment, and (ii) QWAC validation and user interface. This option introduces new threats to users' security and privacy, in the form of opportunities for machine-in-the-middle (MitM) attacks on the separate QWAC validation protocol, disclosure of users' browsing behaviour to third parties, and an over-all increase in the attack surface through added complexity.
3. Add eIDAS-approved Trust Service Providers (TSPs – the issuers of QWACS) to the trusted root list. This represents a security risk because it violates the strict vetting rules for inclusion in the list of trusted CAs, and opens up the dangerous possibility of a government mandating inclusion of a CA over which it exercises inappropriate control (the Kazakhstan- or Mauritius-style "government root" attack).

ETSI's core assumption is that browsers will validate ("recognise") a QWAC by binding it to a TLS certificate for the domain it is intended to represent (Option 3). Since TLS certificates themselves do not provide the level of authenticity eIDAS wants to achieve, this means that QWACs must be issued according to a separate set of processes and criteria for eIDAS-compliant Trust Service Providers[11].

[10] CA Day, 23 September 2020: https://www.enisa.europa.eu/events/tsforum-caday-2020/presentations/CAD-presentations

[11] These processes and criteria are set out in an ETSI normative reference: https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf