European Commission Review of the eIDAS Regulation

Attachment to Mozilla's Survey Response

31 August, 2020

About Mozilla

Mozilla is the Corporation behind the Firefox web browser and the Pocket "read-it-later" application; products that are used by hundreds of millions of individuals around the world. Mozilla's parent is a not-for-profit foundation that focuses on fuelling a healthy internet. Finally, Mozilla is a global community of thousands of contributors and developers who work together to keep the internet open and accessible for all.

Since its founding in 1998, Mozilla has championed human-rights-compliant innovation as well as choice, control, and privacy for people on the internet. According to Mozilla, the internet is a global public resource that should remain open and accessible to all. As stated in our Manifesto, we believe individuals' security and privacy on the internet are fundamental and must not be treated as optional. We have worked hard to actualise this belief for the billions of users on the web by actively leading and participating in the creation of web standards that drive the internet.

Mozilla's crucial role in laying the foundations of web security can be seen from our history and involvement with the Transport Layer Security (TLS) standard--our CTO, Eric Rescorla, served as the editor for both the TLS 1.2 and 1.3 standards. Firefox, our premier product, is based on the source code of Netscape, which Mozilla inherited and open-sourced in the early 2000s. Netscape created the Secure Sockets Layer (SSL) protocol, which has evolved into TLS. This critical protocol provides server authentication and transmission encryption on the web and beyond.

To allow for server authentication, TLS certificates bind cryptographic keys to fully qualified domain names (e.g. https://www.mozilla.org). This linking of domain names to cryptographic keys has been the bedrock of reliable, safe and secure interactions on the internet for over two decades. Since that time, Mozilla has been pivotal in the evolution of standards that have made the modern web more secure, including the most recent version of TLS, version 1.3.

Feedback on QWACs in the eIDAS Regulation

Given our background in the creation of the standard for website security (TLS), we believe that mandating an interpretation of eIDAS that requires QWACs to be bound with TLS certificates is deeply concerning. Along with weakening user security, it will cause

serious harm to the single European digital market and its place within the global internet.

Some high-level reasons for this position, as elucidated in this attachment to our survey responses, are:

1. **It violates the eIDAS Requirements:** The cryptographic binding of a QWAC to a connection or TLS certificate will **violate Recital 67 of the eIDAS regulation** ("this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation"), as well as Recital 26 (innovation), Recital 27 (technological neutrality), and Recital 72 (interoperability). Annex IV of the Regulation, which lays out the precise requirements for website authentication certificates, does not require an X.509 certificate or other technology-specific binding of digitally signed data. Annex IV basically requires that the domain name(s) operated by a natural or legal person are digitally signed with an advanced electronic signature or advanced electronic seal. The EU Parliament and Council have shown excellent foresight in ensuring the technological neutrality of QWACs, and they ensured that all of the information necessary and sufficient to authenticate a website (i.e. a domain name) to a legal or natural entity is present in the Regulation. The move to cryptographically bind a QWAC to a connection or TLS certificate will negate this wise consideration and go against the legislative intent of the Council.

2. **It will undermine technical neutrality and interoperability:** Mandating TLS binding with QWACs will hinder **technological neutrality and interoperability**, as it will go against established best practices which have successfully helped keep the web secure for the past two decades. Even the recent ac-QWAC proposal by ETSI still requires a binding to the TLS server certificate. The proposed ac-QWAC would be limited to only providing that information if the TLS protocol is used. The Origin-centric nt-QWAC alternative proposed by browsers would, instead, provide information about the genuine and legitimate entity of a website. Apart from being central to the goals of the eIDAS regulation itself, technological neutrality and interoperability are the pillars upon which innovation and competition take place on the web. Limiting them will severely hinder the ability of the EU digital single market to remain competitive within the global economy in a safe and secure manner.

3. **It will undermine privacy for end users:** Validating QWACs, as currently envisaged by ESIA within ETSI, **poses serious privacy risks** to end users. While subsection (j) of Annex IV sets forth an ability to check the validity status of QWACs, ETSI's interpretation would require revealing a user's browsing activity to a third-party validation service. This third party service would be in a position to track and profile users based on this information. Even if this were to be limited by policy, this information is largely indistinguishable from a privacy-problematic tracking technique known as "link decoration". This **external validation also serves no security purpose**, as there is no way to guarantee that the third-party service's view of the server's certificate does not reveal any properties of any of the user's connections, past or present.

4. **It will create dangerous security risks for the web:** It has been repeatedly suggested that Trust Service Providers (TSPs) who issue QWACs under the eIDAS automatically be included in the root certificate authority (CA) stores of all browsers. Such a move will amount to forced website certificate whitelisting by government dictate and will **irremediably harm users' safety and security.** It goes against established best practices of website authentication that have been created by consensus from the varied experiences of the internet's explosive growth. The technical and policy requirements to be included in the root CA store of Mozilla Firefox, for example, compare much more favourably than the framework created by the eIDAS for TSPs. They are more transparent, have more stringent audit requirements and provide for improved public oversight as compared to what eIDAS requires of TSPs.

Historical Background of QWACs and TLS Certification

According to subsection (38) of Article 3, "'certificate for website authentication' means 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." (Emphasis added.)

According to the Regulation, the QWAC needs to:

1. provide 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;
2. be issued by a qualified trust service provider and

3. meet the other requirements laid down in Annex IV.

The presumed goal of these sections of eIDAS is for the TSP to provide "a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website." (Recital 67). Based on this history of eIDAS, it has been inaccurately presumed that this goal can only be achieved with a specific technology - the Extended Validation Certificate for Transport Layer Security (EV TLS).

The QWAC was apparently based on the CA/Browser Forum's EV TLS certificate. At the time of eIDAS' adoption, the EV TLS certificate was the model for what advocates of the QWAC thought it could become--an augmented EV TLS certificate. It was thought that QWACs would be better than EV TLS certificates and that browser software would display QWAC information with even better displays of enhanced messaging to browser users. In EN 319 412-4, ETSI added what it interpreted was required by Annex IV to augment the EV TLS certificate so that it could be a QWAC, and it mandated the use of the TLS certificate and associated criteria developed by the CA/Browser Forum. Since that time, however, the presentation of EV certificates in the browser's user interface has evolved. Browsers previously displayed the asserted domain owner's name from the EV TLS certificate in the address bar. However, research over the years has established that users do not act upon security indicators in the browser address bar, and so in 2019 Mozilla removed EV indicators. Other browsers have taken similar steps.

TLS server certificates are not the correct place to store QWAC identity information.

The current debate makes it appear there are different interests at stake—the security of the Web versus the regulatory environment established by eIDAS. However, Web security and the provision of trust credentials for websites should be complementary tools to the regulatory objective established by eIDAS. The reason this has been difficult to achieve with the current TLS-oriented approach towards QWACs is that there are substantial differences between QWACs and TLS server certificates. The standards for TLS and QWACs have been developed by different bodies, and there are different rules for liability, audits, and supervision. The intent of eIDAS is to enable secure cross-border electronic transactions and create central building blocks of the Digital Single Market, both of which benefit the industry. The following table attempts to illustrate some of these differences.

TLS Server Certificates and QWACs

TLS Server Certificates	QWACs
1. Purpose is to support the TLS handshake between a browser and a website's origin server to protect HTTP application-layer traffic with encryption.	Purpose is to provide an identity credential for website with associated benefits of the eIDAS regulation (to give legal effect to interactions, to increase accountability of TSPs, and to protect EU citizens).
2. Certificate agility allows rapid roll-over of TLS certificates with revocations and shorter certificate lifetimes.	It is unclear how often QWACs should be renewed, but coordinating the validity of QWAC certificate content with TLS certificates becomes complicated. Similarly challenging is the expectation that the TSP issue a new QWAC whenever one of the TLS certificates or keys change.
3. The CA/Browser Forum and Browsers quickly react to security issues and update requirements based on new threats and industry developments.	EU standards are slow to change and be adopted because the regulatory process takes more time.
4. Each OS/Browser has separate, independent technical/business requirements for the use of TLS certificates in software.	Evaluation based on ETSI standards, subject to TSP and auditor oversight by country-specific Supervisory Bodies, followed by uniform, mutual recognition among EU countries.

The primary purpose of a TLS certificate is to authenticate a server as part of a TLS connection and not necessarily to provide a guarantee of the legal identity of the website

owner. One way to think about the communication of identity in a TLS certificate is that the domain name is the native identity, or an "Origin". (Mozilla collaborated with other browsers in previously providing a paper on the topic of QWAC bindings to TLS to an informal working group of EU representatives.) We believe that the TLS certificate should not be bound to the QWAC. A domain name and organizational legal identity are two different things, so there should be two different kinds of certificates – they should be separate and independently changeable. This is the concept of agility. The domain registration cycle is different from legal entity renewal cycles. The renewal date for a domain registration will rarely ever coincide with corporate renewal deadlines. Also, many things can affect the legitimacy of an organization's identity, including name changes, mergers/acquisitions, bankruptcy, physical re-location, charter cancelation, dissolution, etc. If organization information is included in a TLS-based QWAC certificate, then it will have to be revoked and replaced whenever any of these events occurs.

Proposed Technical Alternatives to TLS binding in eIDAS

Over the past couple of years, an informal working group of EU and browser representatives has discussed the gaps between these two trust frameworks. Mozilla and other browsers have proposed the "ntQWAC" – a non-TLS QWAC. EN 319 412-4 should be amended to remove all TLS requirements for ntQWACs. By removing this TLS requirement, TSPs could issue ntQWACs that are not TLS certificates. This would reduce the burden on TSPs and also some of the burden on ETSI to keep in sync with quickly evolving CA/Browser Forum requirements, and it would give ETSI, and possibly the CA/Browser Forum, more flexibility to adjust requirements when dealing with ntQWACs.

ntQWACs

The ntQWAC does not need to be cryptographically linked to a TLS server certificate.

The strict (and technically infeasible) interpretation and corresponding implementation of the QWAC provisions of eIDAS have led to challenges with the browser community. Placing an excessive emphasis on an interpretation of "website authentication" that necessitates the use of TLS goes against global web security best practices. The ESIA at ETSI has made an argument that because "authentication" is defined by eIDAS as "an electronic process that enables the electronic identification of a natural or legal person" and because a certificate for website authentication is "an attestation that makes it possible to authenticate a website," a TLS component is the only way that QWACs can

meet eIDAS requirements. This is despite the fact that nowhere in eIDAS is TLS specifically mandated and as illustrated throughout this submission, there exist alternative means of authentication. Similarly, eIDAS does not define "certificate" as an X.509 digital certificate, so an ntQWAC can be any digitally signed blob, such as a JSON Web Token, or some other type of regular, non-TLS X.509 certificate.

Article 3 of eIDAS has definitions for "authentication" and "certificate for website authentication." Subsection (5) states: "(5) 'authentication' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed," and subsection (38) states, "(38) 'certificate for website authentication' means 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." Subsection (38) does not require a TLS certificate. Even the definition of "qualified certificate for website authentication" in subsection (39), which incorporates by reference "the requirements laid down in Annex IV" does not require a TLS certificate. Annex IV of eIDAS only requires that QWACs consist of some basic components: the website's domain name, the domain owner's legal name, an official government registration number, and other identifying information.

If it decides that it should not amend the eIDAS, Mozilla recommends that the Commission explicitly issue guidance that cements technological neutrality and interoperability by stating a QWAC does not have to be cryptographically tied to a TLS certificate. As a part of this recommendation, some technical illustrations on how alternatives can be used to achieve similar outcomes are given below.

Non-TLS QWAC Delivery Mechanisms

While TLS certificate information is exchanged during the TLS handshake, several non-TLS delivery mechanisms exist to communicate ntQWAC information. Note that according to Annex IV, ntQWACs will contain "(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider." Thus, they can be distributed and authenticated without TLS. Three non-exclusive, non-TLS mechanisms have been identified to provision ntQWACs: (1) reference the ntQWAC in a DNS TXT record; (2) store the ntQWAC in a well-known URI; or (3) communicate the ntQWAC as a JSON Web Token.

1. DNS TXT Record

Internet traffic is routed by the Domain Name System (DNS), which is a distributed set of tables that maps numerical addresses to more familiar alphanumeric names. There are different record types for DNS table entries. One is known as the DNS TXT record. RFC 1464 allows broad use of the DNS TXT record. An "_eidas" format could be defined for a TXT record that could point to the ntQWAC for the domain in question. For example, _eidas.example.com. IN TXT "ntQWAC".

2. Well-known URI

A Uniform Resource Identified (URI) is a string of characters that contains a fully qualified domain name and a path to a particular digital resource on the Internet. RFC 8615 describes a scheme for well-known URIs. It avoids DNS lookups altogether and can be used as a storage location for ntQWACs. All that is needed is for the URI to be registered, per RFC 8615, as e.g. "/.well-known/eidas". The ntQWAC could be retrieved and displayed, either within a given page or as part of an extension. Web applications could be modified to detect information about the domain and extensions could be developed to extend browser functionality without requiring changes to the underlying browser software itself.

3. JSON Web Token

A JSON Web Token is a digitally signed object Thus, it can be used to either transmit, or even embody, an ntQWAC. Because the JSON Web Token is digitally signed, it can embody an ntQWAC and be served over a non-TLS connection. For example, section 4.1.6 of RFC 7515 describes how to create an X.509 Certificate Chain, which can be used to convey the information normally sent in a TLS handshake (without having to provide it in a TLS handshake).

Additional Transparency and Security Concerns with the EU TSP List

Article 22 of eIDAS, "Trusted lists", states:

> *"1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them."*

It has been previously argued by some that Mozilla and other browsers should be required to automatically recognise the EU TSP List for issuers of QWACs.

Lack of Transparency

To become a qualified TSP, the TSP applies (under Article 21) to a Supervisory Body (Article 17) which must verify that the TSP "[complies] with the requirements for qualified trust service providers and for the qualified trust services they provide."[Art. 21] eIDAS does not specify the degree of preliminary due diligence that a Supervisory Body has to perform in order to determine such compliance. Furthermore, there is currently no transparency in how the approval process operates at each Supervisory Body. By comparison, Mozilla has a very thorough and transparent root inclusion process, which is conducted over a public email list.

Irregular Audits

Ongoing supervision of TSPs on the EU Trust List for QWACs is performed under Article 20, which states that TSPs must be "audited at their own expense at least every 24 months by a conformity assessment body." Whereas, the regular cadence for audits required by browsers is 12 months--"*Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually.*"

Insufficient Risk Management

Mozilla and the other browser providers follow well-established technical and policy requirements and a risk-management approach for ongoing supervision of the issuers of TLS certificates. Mozilla and the other browsers have well-established root certificate inclusion programs such as those by Microsoft, Apple and Google. As the ongoing supervision of qualified TSPs by Supervisory Bodies is opaque, there is not sufficient

information if these meet the rigorous security standards followed by the comparable peers in the browser industry.

Enforced Trust is Bad for User Security

For the reasons given above, Mozilla should not be forced by government dictate to blindly accept TSP QWAC issuers as trusted, without further evaluation of the TSPs' policies, practice statements, operational procedures, security practices, or audit results. Such a move would deny Mozilla the autonomy to choose who to trust, leaving it in the hands of third parties, and would potentially expose Mozilla, and its users, to the risk of relying on false information. Furthermore, it has also been suggested that Mozilla would be prohibited by eIDAS from suggesting such certificates are untrusted or untrustworthy, if for example a security incident occurred with a TSP. An equal, if not greater concern about having to use the EU Trust List is that we will lose our ability to enforce our own security and trust-framework policies. Currently, the only real power we can effectively use is the ability to de-list or distrust the TSP's root certificate(s). We do this in our code by removing the TSP's root certificate or public key. Limiting our ability (and that of other browsers) to do so will place the security of billions of users at risk and increase instances of fraud or other crimes on the internet.

In summary, independently performing oversight of TSPs using a risk-management approach and well-known, public criteria is the well-documented approach. Additionally, we need transparency and insight into the approval and regulatory processes, which we do not have under the current eIDAS audit framework.

Recommendations

Given the above reasons, we believe that the current interpretation of the QWAC provisions in Recital 67, Article 45, and Annex IV of eIDAS are based on erroneous assumptions about website authentication performed by Trust Service Providers (TSPs), and the way that browsers function. Therefore, Mozilla recommends that eIDAS be re-written to exclude website authentication via QWACs from its purview in its entirety.

Alternatively, we suggest that the Commission provide guidance with respect to how QWACs would operate in a manner that retains compatibility with the global internet. The only way to achieve such compatibility would be to ensure explicit instructions in the Regulation or accompanying guidance that ensure:

1. The QWACs are not cryptographically linked via TLS (or any other certificate or connection-specific technology) and are technologically neutral. We propose that the concept of website "Origin" should be used as an acceptable means of complying with the Regulation (where websites that have the same scheme, hostname, and port are considered to have the same "Origin", which is the keystone for today's web security infrastructure.)
2. The government-mandated whitelisting of TSPs that issue QWACs in the root store of browsers is explicitly disallowed and instead the safer technical, policy, and procedural requirements currently required by browsers is followed.

Finally, even if eIDAS is not re-written or reinterpreted, we maintain that there is no reason why a QWAC needs to be cryptographically linked to a TLS certificate. Therefore, we recommend that alternative Origin-based proposals, such as nt-QWACS, be explicitly recognised as valid means of complying with the Regulation in upcoming changes. We thank the Commission for this valuable opportunity and remain committed to working with all stakeholders to achieve an effective solution.

Appendix A: Relevant Language from the eIDAS Regulation

Recital 26 provides,

> *Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.*

Recital 27 states,

> *This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.*

Recital 67 reads,

> *Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and*

the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

Recital 72 states,

When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.

Article 45 provides,

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Annex IV states,

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least the Member State in which that provider is established and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

— for a natural person: the person's name;

(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;

for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) details of the beginning and end of the certificate's period of validity;

(g) the certificate identity code, which must be unique for the qualified trust service provider;

(h) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

(i) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (h) is available free of charge;

(j) the location of the certificate validity status services that can be used to enquire as to the validity status of the qualified certificate.