Executive Summary

This document outlines a proposed change to the technical profile for Qualified Website Authentication Certificates (QWACs) defined by the ETSI Technical Committee (TC) Electronic Signatures and Infrastructure (ESI).

The technical profiles defined by ETSI ESI exist to support Trust Service Providers (TSPs), Conformity Assessment Bodies (CABs), National Accreditation Bodies (NABs), and Supervisory Bodies (SBs) in meeting the regulatory and legal requirements of the Regulation (EU) N°910/2014[1], also known as the eIDAS Regulation.

The objective of the proposed change is to align the technical profile for QWACs with the legal requirements specified in the eIDAS Regulation, as well as the technical profiles defined by ETSI ESI for other types of Qualified Certificates, such as Qualified Signature and Qualified Seal certificates. Such alignment encourages and permits the broader use of QWACs and the promotion of the Digital Single Market, by removing interoperability challenges and incompatibilities that currently exist with QWACs or which may be unintentionally introduced in the future.

By adopting the same approach to QWACs that is used for other forms of Qualified Certificates, the existing major barriers to the adoption of QWACs can be addressed or removed.

This document is structured so as to provide:

- a concrete proposal for how to remove the technical barriers to interoperability and adoption,
- an explanation of the background and motivation that led to this proposal,
- a demonstration of how this change complies with the existing obligations set forth under the eIDAS Regulation and requires no action by the Commission,
- questions and responses that arose during the informal discussions of this proposal, and
- examples of how this additional flexibility allows for more innovative approaches, facilitating the greater use and adoption of QWACs within the Digital Single Market.

Technical Proposal

The specific technical profile for Website Authentication Certificates, including that of Qualified Website Authentication Certificates, is set forth in the set of documents numbered x19 412-4, such as TS 119 412-4 or EN 319 412-4. The proposal is to remove the restriction that QWACs may only be used within the Transport Layer Security (TLS) protocol.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

This restriction is explicitly stated in x19 412-4 Section 1 “Scope” and implicitly part of Section 4.1 “Generic profile requirements” through the incorporation of the CA/Browser Forum Baseline Requirements. The CA/Browser Forum requirements are only applicable to the context of TLS certificates; directly referencing them restricts QWACs to only being usable as TLS certificates, limiting their potential uses and creating interoperability challenges.

To remove this restriction, Section 4.1 could simply state that the provisions related to the Extended Key Usage (EKU) extension within the CA/Browser Forum documents do not apply for website authentication certificates. ETSI ESI has precedent for making such exceptions, such as in ETSI TS 119 495, which sets forth technical requirements for PSD2 certificates. TS 119 495 specifically overrides and replaces requirements set forth in the CA/Browser Forum Extended Validation Guidelines, as noted in v1.3.2, Section 5.3, GEN-5.3-1 and Note 1.

Removing this limitation, indirectly incorporated, enables QWACs to be used in a variety of existing and new technologies, and not just the TLS protocol, thus ensuring true technological neutrality. This technological neutrality would align the specifications for QWACs with the specifications for other forms of Qualified Certificates developed by ETSI ESI.

The specifications for other forms of Qualified Certificates, including Qualified Signatures and Qualified Seals, do not place restrictions on what technologies can use Qualified Certificates. They also do not place limitations on how Qualified Certificates are delivered. This is done by separating out the specifications for how TSPs issue and create Qualified Certificates and the specifications for how such certificates are used or technically delivered. For example, the specifications in x19 122, x19 132, and x19 142 describe three separate ways for a single Qualified Certificate to be interoperably delivered with a signature that can be recognized as qualified under the eIDAS Regulation. A single Qualified Signature or Seal Certificate can be used with a variety of technologies, without requiring a distinct certificate for each technology be obtained, and without limiting innovation or integration by restricting what technologies can be used.

Potential uses of QWACs in technologies other than TLS are explored later in this document. While the full benefits of this proposal are only achieved once QWACs are delivered independently of TLS, specifying or harmonizing these alternative delivery methods is not required in order for TSPs and users to immediately benefit.

Background and Motivation

Recital 27 of the Regulation emphasizes the importance of technological neutrality. Provided that the obligations of the Regulation are met, then the legal effect may be achieved regardless of the technology used. For Qualified Website Authentication Services, the essential properties are enumerated in Annex IV of the Regulation.

Although the Regulation is technology neutral, ETSI ESI has developed a number of standards that support the use of specific and existing technologies to fulfill the requirements of the Regulation. This effort, directed by the Commission through Mandate 460[2], resulted in a number of standards that support a rationalized and interoperable use of eSignatures across the Digital Single Market. While the use of ETSI ESI standards is not mandatory under the Regulation, both the technical standards and the approach to Conformity Assessment provide the basis for much of the recognition, supervision, and implementation of the eIDAS Regulation, and specifically QWACs.

Since 2015, representatives from a variety of operating system and browser vendors have been engaged in informal meetings with representatives from the Directorate-General for Communications Networks, Content and Technology (DG CONNECT), the European Union Agency for Cybersecurity (ENISA), and ETSI regarding the use and recognition of QWACs within these software vendors' products. The meetings explored how these vendors' respective products might take advantage of Qualified Certificates and QWACs. In addition, discussions have focused on the interoperability challenges that TSPs face that prevent wider and interoperable use of QWACs with existing software, with the goal of reducing these challenges and incompatibilities.

As the primary method of implementing QWACs is through the use of the ETSI ESI standards, particularly ETSI EN 319 412-4, the primary implementation of QWACs is limited to only being usable with TLS. Due to the important role that TLS plays within browser and operating system vendors' products, each vendor has separate, independent technical and business requirements around the use of certificates within TLS in their products. A number of common technical requirements have been collected and documented through industry collaboration forums such as the CA/Browser Forum[3] (CA/B Forum) and the Common Certificate Authority Database[4] (CCADB).

In order for a certificate intended for TLS to work within a given browser or operating system vendor's products by default, the TSP responsible for issuing that certificate must undergo evaluation by that vendor. These evaluations are separate for each vendor, and undergone by each TSP. These evaluations consider technical interoperability, compliance as assessed by third-party conformity assessment bodies, and alignment with business, user, and product needs and policies. They may also involve additional legal agreements, contracts, or other forms of due diligence, in order to ensure the needs of the products' users and vendor are met.

Because ETSI ESI limits QWACs to only being usable with the TLS protocol, this means that in addition to undergoing assessment by a Conformity Assessment Body duly recognized by a National Accreditation Body, and the evaluation of a report by the relevant Supervisory Body, a

[2] https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=442#
[3] https://cabforum.org/
[4] https://www.ccadb.org/

TSP must also undergo evaluation and negotiation with each software vendor they wish their QWACs to seamlessly interoperate with. There is no other option available to TSPs when using the ETSI ESI standards for QWACs.

The need for these multiple assessments has made it difficult for TSPs and website operators to adopt QWACs. The process for evaluation by any single software vendor may take months or years, depending on the services the TSP offers and how their systems are designed, and even longer to complete evaluation by all the major software vendors. TSPs which do not go through this process, and only pursue recognition under eIDAS find that the certificates they issue to their customers do not work with common, off-the-shelf software. This is because they have not been evaluated as complying with the software vendors' security, privacy, and product requirements, which is necessary for these certificates to work with that software.

Much of the discussion over the past several years has focused on how best to reduce these challenges TSPs face, in order to remove barriers to the adoption and use of QWACs. One option that has been explored, and which browsers have found non-workable, has been the mutual or automatic recognition of the EU Qualified Trust List for use with TLS in these software vendors' products. This is because software vendors do not engage in any mutual recognition schemes; instead, they maintain direct involvement in the evaluation and review of all TSPs used for TLS within their products. This is due to the critical security role TSPs play in the security of these vendors' products as well as the substantial risk borne by these vendors in extending their users' security to external providers.

Another option that has been similarly explored – and browsers have determined to be non-viable – is harmonizing the assessment schemes used by CABs and Supervisory Bodies, such that the completion of an evaluation by a CAB or the evaluation of a CAR by a Supervisory Body might achieve the presumption of compliance with a given vendors' requirements. Similar to concerns around mutual or automatic recognition, the evaluations applied by browser software vendors frequently involve elements that are unique to that vendor. A common theme is each vendor requiring direct security assessment and evaluation of the TSP by the vendor's staff. This is because each vendor's requirements constantly evolve and adapt according to the product and security needs of that vendor, and involve additional requirements that extend beyond conformity assessment, such as legal contracts or additional obligations. Delegating these critical vendor assessment and security procedures to third parties is of significant concern for browser vendors.

One result of these discussions was a Trust Service Provider Technical Best Practices[5] document, developed through collaboration with multiple browser and operating system vendors. The objective of this document was to examine common challenges that TSPs face during the design and implementation of TLS certificate issuance that may present challenges for software vendors to interoperate with their certificates. Through implementing and adhering

[5] https://www.ccadb.org/documents/TSP_Technical_Best_Practices_eIDAS.pdf

to these best practices, potentially with the support of their Conformity Assessment Bodies, TSPs might expedite or streamline evaluations performed by software vendors, and address potential incompatibilities before they become insurmountable. While this was a positive step to reducing the challenges of TSPs, it could not wholly resolve the differences in requirements and objectives of the trust frameworks of the eIDAS Regulation and the various software vendors.

The proposal set forth in this document is the result of many years of productive discussion between browser and operating system vendors with the Commission, ENISA, and ETSI exploring these challenges. These challenges, communicated to ETSI as far back as 2013[6] [7], limit the ability to make use of QWACs without any additional configuration by users or actions by the issuing TSP. The underlying cause of these challenges was that by restricting QWACs to only be usable with TLS, the current ETSI standards themselves make it necessary for TSPs to be evaluated as complying with each vendor's requirements for TLS, in addition to the requirements under the eIDAS Regulation.

In adopting this proposal, x19 412-4 would no longer require that TSPs and QWACs interoperate with vendors' implementations and requirements for TLS, removing the primary challenge faced by TSPs and users of QWACs. The approach of separating out independent requirements reflects the approach being used by other industries and standards bodies, which have similarly seen challenges in trying to operate a single PKI to multiple compliance schemes and a single technological implementation.[8] [9]

This proposal does not directly address any special treatment within these software vendors' products. Special treatment is something that is specific to each software vendor, and depends on the specific needs of individual products and that product's users. However, by removing the main technical and procedural barriers for TSPs to issue QWACs, and for websites to deploy QWACs, it makes it easier to explore options to leverage the additional information QWACs provide and identify the most effective technological means of delivering that information, when not using TLS.

Compatibility with the eIDAS Regulation

Annex IV of the eIDAS Regulation[10] defines the requirement for what essential information must be present in a QWAC to achieve the desired legal effect. This information includes identifying the domain name of the website in question, as well as associating that with a legal or natural person. When all of the information required is bound by a Qualified Trust Service Provider, the desired legal effect is achieved.

[6] https://cabforum.org/2013/06/11/2013-06-11-minutes-of-munich-f2f/

[7] https://cabforum.org/2015/10/07/2015-10-07-face-to-face-meeting-minutes-meeting-36-istanbul/

[8] https://x9.org/__asc-x9-revives-pki-working-group-to-address-new-public-key-infrastructure-needs/

[9] https://www.digitaltransactions.net/divergent-online-security-needs-warrant-a-new-version-of-pki/

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e32-114-1

The eIDAS Regulation does not require the presence of “validation data” as defined in Article 3[11], nor does it limit QWACs to specific technical implementations. However, by limiting QWACs to the TLS protocol, ETSI ESI has directly imposed a requirement to include “validation data”, which is not required by the Regulation, nor is it necessary to achieve the desired effect. This requirement, along with the technical implementation of fulfilling this requirement, has been the root cause of the incompatibilities identified. These challenges with this approach were raised with the ETSI Liaisons to the CA/Browser Forum during the development of these profiles.

As the eIDAS Regulation is neutral with respect to both the technology and the conformity assessment scheme, deferring to the Supervisory Bodies in collaboration with the National Accreditation Bodies and Conformity Assessment Bodies, it is possible for TSPs to provide other implementations of QWACs. These alternative implementations could fully conform with all requirements of the eIDAS Regulation, achieving the desired legal effect, and without these unnecessary limitations. However, the widespread adoption of the current set of ETSI ESI conformity assessment standards and certificate profiles suggest that the most effective way to support and promote QWACs is by addressing these incompatibilities within the ETSI ESI specifications.

The technical proposal outlined in this document looks to harmonize the ETSI ESI technical requirements with the legal requirements set forth in the eIDAS Regulation, and with the technical approach used for other forms of Qualified Certificates. Because of the technological neutrality of the Regulation, and that the unnecessary “validation data” is not required by Annex IV, the change outlined can be adopted by ETSI ESI without requiring modification to the Regulation.

The technical proposal simply removes restrictions on QWACs that are not present in the Regulation, thus ensuring greater opportunity to use them within the Digital Single Market, and resolving the incompatibilities that the current restrictions lead to.

Questions and Answers

How does the removal of the mandatory requirement in ETSI x19 412-4 that QWACs only be used for TLS (specifically, the requirement to include the “id-kp-serverAuth” extendedKeyUsage as required by the CA/Browser Forum Baseline Requirements, or the use of the “id-kp-clientAuth” EKU) facilitate the use and acceptance of QWACs?

Software vendors use the Extended Key Usage (EKU) extension to indicate compliance with their certificate policies and practices. This approach dates back to the first implementations of SSL/TLS, well before certificate policies existed, which are an alternative way of signaling

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e791-73-1

compliance. This approach has seen significant discussion within the IETF[12] [13] [14] over the decades, and reflects the common approach used by industry in managing trust lists, even if it may not be the ideal approach for some use cases.

Requiring the id-kp-serverAuth EKU be included effectively requires that the TSP undergo evaluation according to each vendor's requirements for TLS. It also means that the TSP has to continue to comply with the vendors' requirements, which are constantly evolving – and at a much more rapid pace than the ETSI documents.

As shared by ENISA and by TSPs, this multi-stakeholder compliance requirement represents a significant and ongoing challenge for TSPs. Removing the requirement to include particular EKUs removes this compliance overhead. Because certificates with these EKUs also need to comply with all vendor requirements, this also limits ETSI's ability to specify a certificate profile suitable for the needs of the eIDAS community. Removing the EKU provides ETSI greater flexibility to specify, extend, and modify certificate profiles to support additional information for Qualified Certificates.

In addition, removing the EKU removes the restriction that QWACs can only be used with TLS. This limitation has prevented the use of QWACs in more situations, and removing it allows users and industry to make use of the additional assurances of QWACs in even more situations.

What other changes or new specifications by ETSI ESI will be required to use technologies other than TLS to deliver QWACs?

Removing the requirement to include particular EKUs does not impose any requirements on the use of other technologies. It simply allows other technologies to be used, depending on the needs of TSPs, websites, and users.

While it's too early to discuss the concrete requirements of particular technological approaches, the removal of any requirement to use a particular EKU within the ETSI set of documents allows for the exploration of these other technologies, while also reducing the challenges for TSPs to issue and use QWACs.

What impact will the proposed change, and potential future revisions, have on existing uses of QWACs within other software, such as non-web browser or server-to-server applications?

The CA/Browser Forum documents that ETSI ESI have incorporated primarily exist to support browser and operating system vendors' requirements for TLS and TSPs. This is why these documents require a particular EKU, and why this requirement subjects TSPs to the compliance and interoperability challenges identified.

[12] https://mailarchive.ietf.org/arch/msg/pkix/QQ4vHlYLyYFYnswc14_jTdHHbLg
[13] https://mailarchive.ietf.org/arch/msg/pkix/MHwcSWuuzezj4qHuzSmbYeGUbdI
[14] https://mailarchive.ietf.org/arch/msg/pkix/M80kRfzAX9bWcqibV97z4MOMqJI

Although removing the EKU requirement will no longer directly require compliance with browsers' root programs and policies, changes to these root programs may still end up affecting TSPs. This can happen if the browsers update or adopt changes to the CABF documents that ETSI has incorporated, as such changes would then also be required by ETSI. As a consequence, the removal of the EKU reduces, but does not wholly remove, the additional work TSPs have to do to comply with vendor requirements.

Removing the EKU requirement provides ETSI the flexibility to override or supercede those requirements, when such requirements are unnecessary or conflict with the goals of QWACs. This would reduce the challenges TSPs are subjected to, if ETSI deemed them undesirable or unnecessary. ETSI has previously done this for PSD2.

However, if and when ETSI exercises that flexibility, then only TSPs which do not assert the id-kp-serverAuth or id-kp-clientAuth EKUs will be able to comply with those new requirements. This is because any TSP that chooses to include id-kp-serverAuth or id-kp-clientAuth will still be subject to each vendors' requirements, and thus will be unable to resolve any conflicts if ETSI specifies conflicting requirements or overrides these requirements. TSPs that did not include these EKUs would not face these challenges, and the proposal is to let TSPs make that choice about whether to take that risk.

Because it allows TSPs and ETSI more flexibility, it's anticipated that the most preferable option for everyone is for TSPs to not assert the id-kp-serverAuth EKU at all for QWACs. This allows ETSI ESI the flexibility to further alter, improve, or reduce the profile from the CABF documents, and allows TSPs to adopt those changes without any additional requirements from browsers. However, ETSI ESI and TSPs can still incorporate industry best practices that are applicable and appropriate, and with less compatibility risks.

If QWACs are issued and used outside of TLS, what impact does that have on TSPs that also issue QWACs used in TLS?

The removal of the EKU requirement reduces the requirements of QWACs, and does not impose new or additional requirements.

For other technologies that don't use the ETSI ESI profile to define or issue QWACs, or don't use QWACs with TLS, there's no change. For systems that use QWACs in TLS, but which do not need nor desire to work with browsers or common operating systems, there's also no change. This is because they can continue to include the EKUs if necessary for the specialized software they use, and these EKUs will not be interpreted by browsers or operating systems, because the TSP is not used with browsers or operating systems.

The approach has the positive impact of allowing QWACs to be issued according to X.509v3 and RFC 5280, and the ETSI ESI profile, without requiring TLS be used to distribute or use them.

By not restricting QWACs to only supporting TLS, it also makes QWACs easier to use within existing browsers and with existing operating system APIs, without being subjected to additional OS-specific requirements.[15]

Will existing QWACs that are limited to TLS still be usable, or will new certificates have to be issued to comply with these changes and be usable in TLS?

TSPs which have already undergone multi-stakeholder evaluation, and which issue QWACs that contain the id-kp-serverAuth EKU, can continue to use and issue such certificates.

However, if a browser vendor or the CA/Browser Forum imposes a requirement that a QWAC cannot comply with, or if ETSI ESI imposes a requirement that conflicts with or replaces those of the CA/Browser Forum or browser and software vendors, TSPs will not be able to issue new certificates that are QWACs and that contain these EKUs, because they will only be able to comply with vendors or ETSI, but not both.

Further, TSPs already recognized will still continue to need to comply with all requirements from all stakeholders, which remains an acknowledged significant burden for these TSPs. Removing the EKU requirement will allow the TSPs the flexibility to separate their compliance obligations, no longer needing to have a single infrastructure that complies with all of these different requirements. Because of this, it’s expected that existing TSPs will prefer this flexibility and will prefer not to issue QWACs with id-kp-serverAuth or id-kp-clientAuth.

What other actions will TSPs need to perform for existing TLS-restricted QWACs?

TSPs can continue to offer TLS certificates (those containing the id-kp-serverAuth or id-kp-clientAuth EKUs) provided those certificates comply with vendors’ current and ongoing requirements. Under the existing set of requirements, it’s possible for a TSP to do this and comply with both the requirements of ETSI ESI and that of vendors.

If either ETSI ESI or vendors later adopt new or additional requirements, TSPs will have to update to meet those new requirements. If the requirements end up being incompatible, the TSP may have to make more significant changes, beyond the use of EKUs, in order to make sure their compliance obligations do not overlap.

However, as this proposal simply changes an existing mandatory requirement, making it optional, no immediate changes by TSPs are needed.

Should the proposal be adopted, will TSPs be able to immediately issue non-TLS-restricted QWACs?

[15] https://support.apple.com/en-us/HT210176

In theory, yes.

The exact details will depend on how individual, specific TSPs have configured their PKI hierarchy, so there is always the possibility of incompatibility in limited and TSP-specific ways. However, nothing fundamental in this proposal prevents such immediate adoption or would prevent changes by those specific TSPs. In practice, it is expected that the majority of TSPs will be prepared to issue certificates the moment such a change is adopted.

Should the proposal be adopted, will non-TLS-restricted QWACs be immediately adopted by browsers? If not, what additional actions will be required?

The discussion about removing the TLS restrictions is focused on the primary problem identified by the Commission and ENISA, which is the barriers for TSPs due to the added initial and ongoing compliance challenges with multiple stakeholders.

Special recognition or adoption of qualified certificates remains a separate conversation that will be specific to each browser vendor. However, by removing the primary cause of compatibility issues, these discussions can be far more productive in exploring technical options and trade-offs.

How will the use of QWACs, including those not restricted to TLS, be communicated to users in a browser environment?

The current mandate by ETSI ESI that these certificates can only be used in TLS, combined with the current mandate to comply with vendor requirements, significantly limits the ability to meaningfully discuss options for communicating in a browser environment.

Further, the approach currently used would require each vendor directly integrate such certificates with their product, which, due to the differences in each product, necessarily implies different and potentially inconsistent treatment between browsers.

The technology-neutral approach being described allows for a variety of technical options to be discussed, including solutions that do not require direct action by browser vendors in order for websites to leverage such certificates. This would allow for the consistent display of this information using existing web technologies.

One significant benefit, discussed in the course of prior meetings, is that it permits QWACs that can be integrated with existing web technologies by site operators, and displayed to users in a vendor-neutral, uniform way. One possible example is much like the site seals used in schemes such as S@fer Shopping or EMOTA trust marks.

How will the use of a non-TLS-restricted QWAC be used in combination with a TLS certificate? Will this create additional burden for users or issuers of QWACs?

It is already industry-standard practice that multiple certificates are used by server operators. The most common case is the support of both RSA and ECDSA certificates, necessary for websites to efficiently support the widest possible number of devices accessing their sites using modern and efficient cryptography. However, increasingly, technologies such as Delegated Credentials for TLS[16] and Secondary Certificate Authentication in HTTP/2[17] make use of additional, purpose-specific certificates.

The existence of tools such as Automatic Certificate Management Environment (ACME)[18] greatly simplify and automate this management experience, and thus the existence of an additional certificate, purpose-specific for eIDAS, does not represent a significant burden for a modern deployment. Increasingly on the Internet, the burdens involved for users or issuers in obtaining or issuing multiple certificates is offset by increasing the automation and ease of getting these certificates, by streamlining and potentially automating the experience.

Importantly, by separating out the TLS requirements from those of QWACs, the use and management of QWACs may no longer be impacted by the use and management of TLS certificates. This will reduce the overall burdens faced both by TSPs and site operators, as changes that impact a TLS certificate may not require replacing the QWAC, and similarly, any changes or improvements that impact QWACs may not affect the TLS certificate.

In effect, despite the existence of an additional certificate, the overall burden involved in maintaining such certificates will be meaningfully reduced.

Enabling Non-TLS Delivery Mechanisms

The specific focus of this proposal has been to remove unnecessary restrictions on QWACs that limit their use to TLS. By separating out how QWACs can fulfill the eIDAS Regulation from what technologies QWACs can be used with, this enables greater flexibility by users and greater opportunity by industry.

However, the greatest benefit is to be had when QWACs are delivered via means other than TLS. By not subjecting QWACs to the compatibility and interoperability requirements of TLS, software vendors can make better, interoperable use of the Trust Service Provider List, allowing for quicker and easier recognition of these non-TLS QWACs.

In the discussions, browser and operating system vendors shared several possible approaches that might be used, other than TLS. There is no requirement to pick a particular solution, as they are not mutually exclusive. This is similar to how a single Qualified Signature certificate may be

[16] https://tools.ietf.org/html/draft-ietf-tls-subcerts
[17] https://tools.ietf.org/html/draft-ietf-httpbis-http2-secondary-certs
[18] https://tools.ietf.org/html/rfc8555

used with PAdES, XAdES, and CAdES, depending on the technical requirements and needs of the sender and the recipient. Such flexibility is only possible when the restriction to use TLS is removed. This does not require picking a single option from the following list, as all of these can be explored with the use of a single non-TLS-restricted QWAC. The following descriptions are simply examples to show how technologies other than TLS can be used to deliver QWACs, while still providing the same assurances and certainty, and which are currently unnecessarily prohibited. These examples are not exhaustive; adoption of the technical proposal will likely lead to new ideas in the future – a process that is severely inhibited by the current restrictions placed on QWACs.

Expression within DNS

Domain operators could, upon obtaining a QWAC, make this information available through the use of a special DNS record. Such use has precedent within the CA/Browser Forum, which makes use of such special records to communicate ways in which to authenticate domain names. This approach has wide use on the Internet at large, most notably in the space of email security, using DMARC (RFC 7489[19]) and DKIM (RFC 6376[20]). These standards make use of the TXT record, as described in RFC 1464, to express arbitrary information about a domain.

In this model, there could be a specific TXT record that provides a URL that may be used to fetch and/or verify a QWAC. Using the model from DKIM, which utilizes a "_domainkeys" record, a prefixed label could be registered, consistent with RFC 8553[21], to provide information specific to the eIDAS Regulation. For example, a "_eidas" record could provide information to allow a client to either fetch the attestation from the domain in question or, if real time verification was desired, to verify the attestation with the Trust Service Provider automatically.

The benefit to such an expression within DNS is that it is agnostic to the protocol used and may provide assertions about a domain name independent of the TLS certificate(s) potentially used by that domain name. For example, such an expression could extend the utility of QWACs to cover other protocols, such as SMTP, to similarly provide assertions about the domain operator.

Expression as a well-known URI

As described within RFC 8615[22], an alternative to expressing within DNS is to express within a well-known URI. While conceptually similar to an expression within DNS, this would avoid the need to perform any additional DNS resolutions, instead allowing standard HTTP(S) exchanges to be made to fetch the certificate. A URI could be registered, as defined within RFC 8615, to provide information about the domain, such as "/.well-known/eidas".

[19] https://tools.ietf.org/html/rfc7489
[20] https://tools.ietf.org/html/rfc6376
[21] https://tools.ietf.org/html/rfc8553
[22] https://tools.ietf.org/html/rfc8615

The benefit of such an approach is that this information would be readily available in a variety of applications and protocols. For example, Web browsers do not expose information about the TLS connection to the calling page, and many browsers do not expose this information to extensions either, as revealing such information may reveal to the website or extension information about the user's local network that does not need to be exposed. However, Web pages and extensions are permitted to fetch resources, such as those at the well-known URI, and could use this information to display, either within a given page or as part of an extension, the additional information contained about the domain within the QWAC.

Such a solution allows for much more innovative use, allowing Web applications to detect information about their current domain, or potentially other domains, while also allowing the development of extensions that can be used to extend browser functionality, without requiring changes to the underlying browser software itself.

Expression as a JSON Web Token (JWT)

Under the ETSI ESI x19 412-4 specifications, in order to obtain information about a domain, it's necessary to perform a TLS handshake with it. However, there are a number of protocols which do not have a peer initiating a connection to a server, but instead accept a connection from the other party. Within TLS, this is commonly done via TLS mutual authentication, through the use of client certificates. However, in order for such TLS authentication to work, the receiving end must specifically request a certificate from the initiating party, which creates significant operational challenges to use and interoperate.

By decoupling a QWAC from a TLS certificate, alternative expressions such as JWT may also be used to deliver, or even embody, a QWAC. For such protocols, when a Qualified Website needs to send data, it can also communicate its Qualified status via a QWAC expressed within a JWT, providing additional information and assurance to the receiving end, and without requiring the receiver then initiate a TLS connection back to its peer.

It is important to note, this does not require redefining a QWAC or issuing a new form of certificate using something other than X.509v3 and ASN.1, even though the eIDAS Regulation permits such flexibility. This proposal is simply to deliver the QWAC with or as part of the JWT, such as via the "x5c" (X.509 Certificate Chain) or "x5u" (X.509 URL) attributes of JSON Web Signatures (RFC 7515[23]), rather than having to provide it within a TLS handshake. This enables the additional assurance provided by a QWAC to be used leveraged in situations where TLS handshakes are not possible.

[23] https://tools.ietf.org/html/rfc7515