Purpose and Agenda

Purpose:

- Discuss document sent to CA/Browser Forum on 15 January 2020 "*Soliciting feedback on potential changes to Qualified Website Authentication Certificates (QWACs)*"

Agenda:

- Background
- European Commission Working Group (ECWG) proposal
- Enabling Non-TLS Delivery Mechanisms (Examples)
- Next steps

Background

- Since 2015, operating system and browser vendors engaged in informal meetings on the use and recognition of QWACs within the vendors' products with representatives from:
  - The Directorate-General for Communications Networks, Content and Technology (DG CONNECT)
  - The European Union Agency for Cybersecurity (ENISA)
  - ETSI
- Meetings have led to a proposal that may reduce the interoperability challenges that TSPs face that prevent wider and interoperable use of QWACs with existing software
- In consultation with DG CONNECT, the proposal was shared for feedback from within the EC and from CAs

ECWG Proposal

- Make a minor change to the existing profile for QWACs, when embodied by ETSI ESI's set of documents, to facilitate easier interoperability of QWACs with existing software, as well as unlock new interoperability possibilities
- Remove the restriction that QWACs may only be used within the TLS protocol
  - 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
  - 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
- Removing this restriction, 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.

Enabling Non-TLS Delivery Mechanisms (Potential Examples)

- Expression within DNS
  - Domain operators could, upon obtaining a QWAC, make this information available through use of a special DNS record
- Expression as a well-known Uniform Resource Identifier (URI)
  - As described within RFC 8615 , an alternative to expressing within DNS is to express within a well-known URI
- Expression as a JSON Web Token (JWT)
  - 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), rather than providing it within a TLS handshake

Next Steps

- Remote ECWG meeting in early March
- Mockup prototype using “Expression as a well-known URI” option
  - Technical specifications to include formats, protocols, consumption (display and user experience)
- Testing and piloting of prototype
- Promotion among EC stakeholders