



# News about Qualified Certificates for Website Authentication

## Has the Gordian knot between QWAC and browsers been cut?

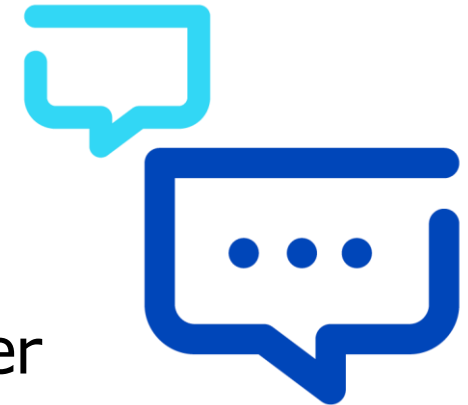
**Date:** 14.10.2021  
**Place:** Online / 54. F2F CA/B-Forum  
**Speaker:** Enrico Entschew



- Trust service of eIDAS
- Classic TLS certificate according to RFC 5280
- Check against eIDAS Trusted List
- According to eIDAS Recital 67 "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"
- QWAC is to be used in accordance with the rules of the EU

**QWACs are an important technical tool for establishing the European Digital Single Market as part of the Digital Agenda for Europe.**

- Rarely used in connection with the browser
- Use only if CA/B-Forum guidelines are followed
- Root CA must be included in the root store of the browser
- Some specific fields are not allowed or supported for QWAC by the browsers, for example European Payment Service Directive 2 (PSD2) extensions



**There were intense discussions between the EU Commission and browsers on the recognition of QWAC.**

- Different and competing solutions for implementation
  - tls-QWAC, nt-QWAC, ac-QWAC, self-signed QWAC
  - Parties agreed to disagree
- Browsers' positions
  - Purpose of QWAC: provider of identity credentials, not tls-handshake
  - Different responsibilities: CA/B-Forum/ Browsers versus ETSI/ Supervisory Bodies
  - Fear of website certificate whitelisting by government dictate / External trust source



**It was still an important and productive discussion to address the function and realization of the QWAC.**

- 2020: Consultation process on an eIDAS revision
- 3 options for revision: Improvement, expansion to private sector or introduction of an EUid
- June 2021: release of proposal of eIDAS revision
  - Commission chose EUid!
  - Milestone for digital identity improvement in Europe



**The introduction of an EUid-Solution is a major step ahead into the future of the European Digital Single Market.**

## New Recital 32:

- Assurance that there is a genuine and legitimate entity standing behind the website
- Use of website authentication services is voluntary
- Browsers should ensure support and interoperability with QWAC
- Browsers should recognise and display QWAC to the user



## Revised Article 45:

- Includes two new paragraphs
- Contains the rules in detail

**The importance of QWAC for Europe is addressed in the new revision.**

## New paragraph 2 of Article 45:

- QWACs shall be recognized by the browsers
- Browsers shall ensure that the identity data provided is displayed in a user friendly manner
- Browsers shall ensure support and interoperability with QWACs
- Exception: microenterprises and small enterprises in the first 5 years of operation



## New paragraph 3 of Article 45:

- Within 12 months after revision takes effect, implementing acts for QWAC will be published

**The commission integrates the role of the browser with the need of the European Digital Single Market.**



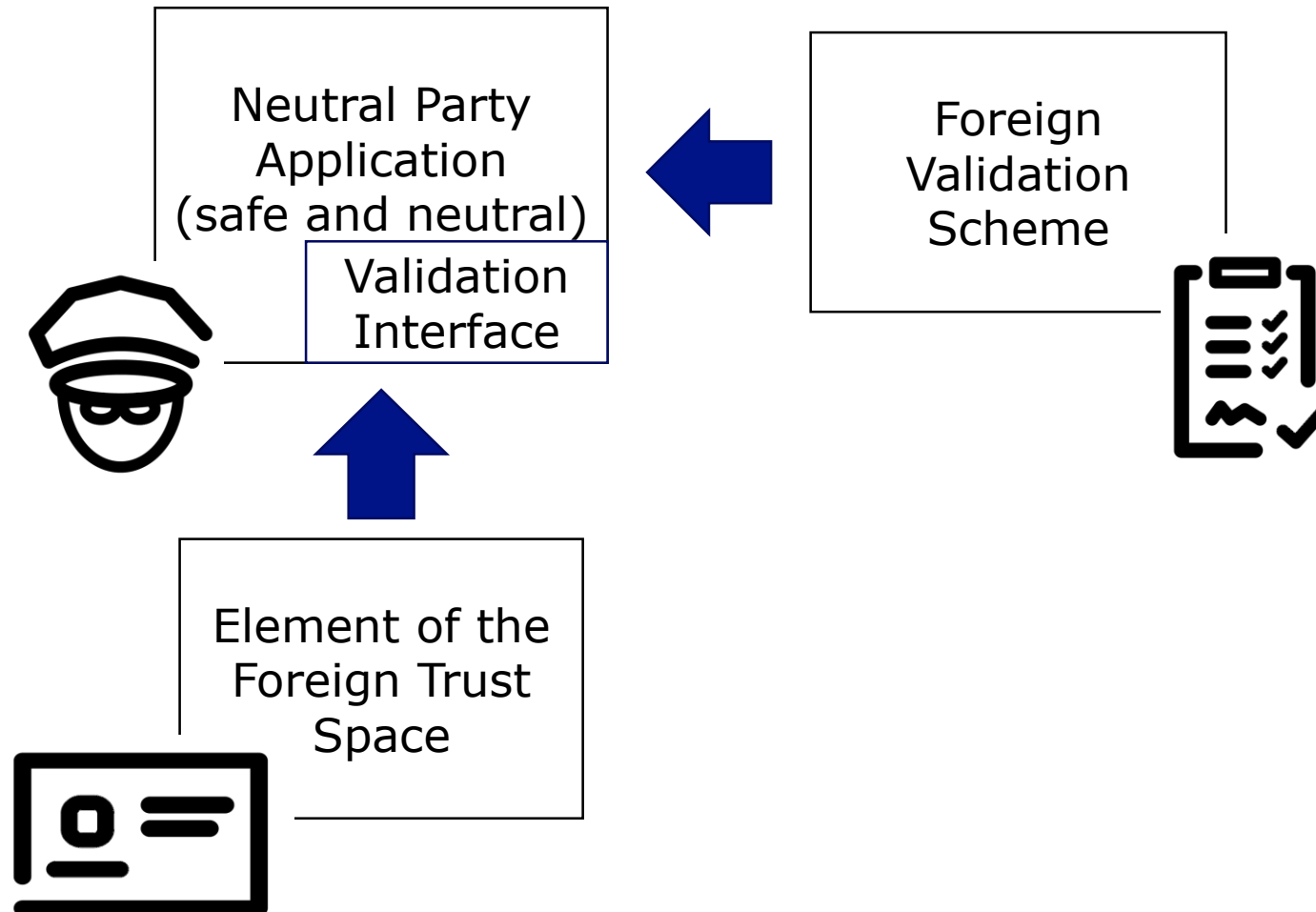
**We still need the bridge between the browsers and QWAC.**

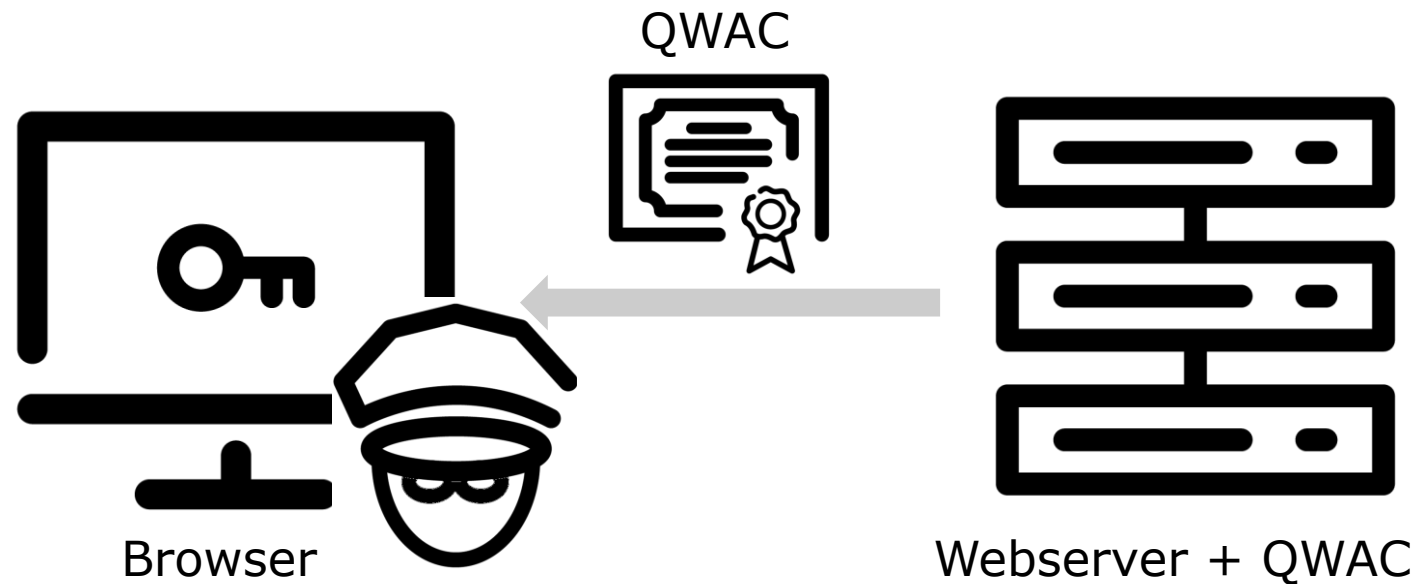


- Users and certificate holders can use QWACs in the browser
- Browser displays the QWAC information in a user friendly manner
- Browser ensures interoperability and support with QWACs
- EU retains sovereignty over the QWACs by providing the specifications and reference numbers of standards for QWACs

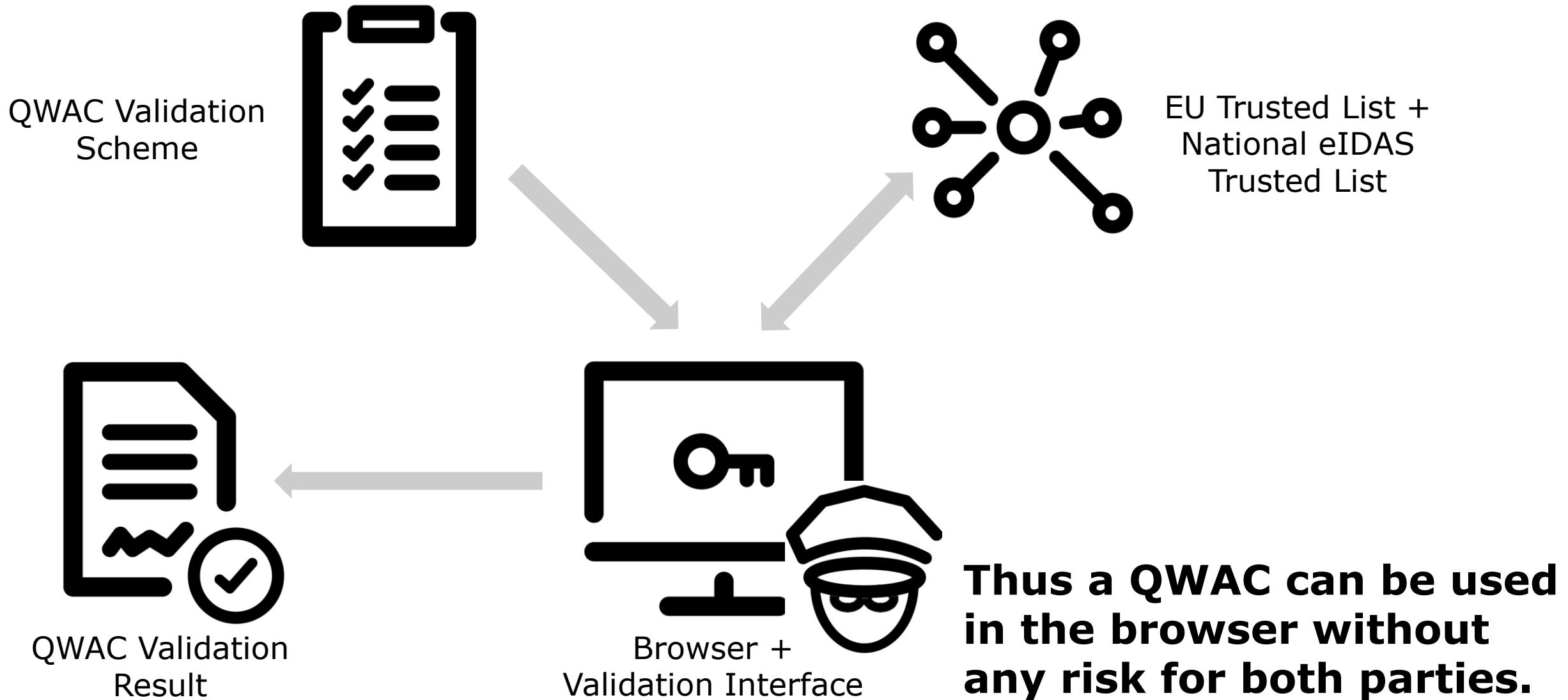


**A bridge taking into account all these interests is needed.**





**So far, everything is the same as with the normal TLS certificate.**



- All conditions are favorable at the moment.
- The complicated problem of fully exploiting QWACs has not yet been solved.
- The trust space concept can clearly help solve this problem.
- ETSI can make a valuable contribution by creating standards for machine-readable validation schemes according eIDAS and visualization of QWACs, among others.



**The QWAC journey is not over yet, but we are on a good path...**

**Enrico Entschew**

E-Mail: [e.entschew@d-trust.net](mailto:e.entschew@d-trust.net) or [enrico.entschew@bdr.de](mailto:enrico.entschew@bdr.de)

# Thank you!

**Please note:** This presentation is the property of D-Trust GmbH. All of the information contained herein may not be copied, distributed or published, as a whole or in part, without the approval of D-Trust GmbH.

©2021 by D-Trust GmbH.