ETSI TR 119 411-5 V1.1.1 (2023-01)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 5: Guidelines for the coexistence of
web browser and EU trust controls

Reference
DTR/ESI-0019411-5

Keywords
cyber security, electronic signature, extended validation certificate, internet, public key, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Transport Layer Security (TLS) [i.7], including earlier versions based on Secure Socket Layer (SSL), is an integral part of the security environment for the web. TLS/SSL is widely supported by web browsers and websites. A TLS connection between a browser and a website depends on a website's authentication certificate, often referred to as a "server certificate" which binds its domain name, and optionally, the genuine and legitimate entity standing behind the website, to a public key.

Browser Vendors operate individual Root Programs to review and approve root certificates linked via a certificate chain to website authentication certificates. Trusted root certificates are included in a Root Store used by the web browser to validate website certificates used in TLS/SSL.

Regulation (EU) No 910/2014 [i.4] is a regulation on electronic identification and trust services for electronic transactions in the internal market. Under Regulation (EU) No 910/2014 [i.4], EU Commission and EU member states operate a trust scheme for the approval of trust services, including issuers of qualified certificates for website authentication. Trusted issuers of website certificates are listed in EU Trusted Lists according to EU Commission Implementing Decision 2015/1505. Further requirements on web browsers for recognition and display of website certificates are under review.

The CA/Browser Forum is an unincorporated association of separate certificate issuers (i.e. EU Qualified Trust Service Providers and Certification Authorities), certificate consumers (e.g. web browsers), and interested parties. Members of the CA/Browser Forum maintain a standard set of minimum requirements and expectations for the issuance of publicly-trusted website certificates. Both Browser Vendor Root Stores, the EU trust scheme, and the ETSI policy and security requirements for QTSPs and QWACs incorporate features of the CA/Browser Forum Requirements [i.6].

So far, browsers were not checking website's certificates against any EU Trusted List. Therefore, the present document provides guidance to perform such a check and enable the coexistence of trust controls applied by the Browser Vendors and EU trust scheme to EU qualified certificates for website authentication.

1 Scope

The present document provides guidance on how a single TLS certificate can support both Browser Vendor controls and EU trust controls for website authentication, commonly referred to as "server authentication".

In particular, the present document provides guidance on the issuance and verification of website authentication certificates which:

a) Are based on trust controls defined in existing ETSI standards and CA/Browser Forum specifications as referenced in the present document.

b) Include requirements of qualified certificates for website authentication as specified in Regulation (EU) No 910/2014 [i.4].

c) Include requirements of web browsers for certificates based on CA/Browser Forum Requirements [i.5] and [i.6].

d) Ensure that the identity data contained in qualified certificates for website authentication per Regulation (EU) No 910/2014 [i.4] is displayed in a user-friendly manner.

e) Authenticate the website bound to secure communications using encryption from the browser client to a server.

The present document only applies to website authentication certificates which:

a) are qualified according to Regulation (EU) No 910/2014 [i.4] and can validate to an entry included in the EU Trusted List; and

b) are issued by QTSPs whose certificates are either directly included in or validate to an entry in browser root stores.

The present document is based on a single X.509 certificate which is handled in line with both Browser Vendor objectives and Regulation (EU) No 910/2014 [i.4] requirements; alternative approaches may be added in future versions of the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.3] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.5] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.6] CA/Browser Forum: "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[i.7] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.8] ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists".

[i.9] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015.

[i.10] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.11] ETSI TS 119 403-2: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates".

[i.12] ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [i.1], ETSI EN 319 411-1 [i.2], ETSI EN 319 411-2 [i.3] and the following apply:

browser vendor root program: independent governance and security review function operated by individual Browser Vendors to manage a corresponding root store

browser vendor root store: set of root CA certificates trusted by default in the corresponding web browser

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [i.1], ETSI EN 319 411-1 [i.2], ETSI EN 319 411-2 [i.3] and the following apply:

CA/B	CA/Browser
CAB	Conformity Assessment Body
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate

NOTE: As defined in Regulation (EU) No 910/2014 [i.4].

4 Coexistence of web browser and EU trust controls for website authentication

4.1 Management of Trust in Certificate Issuers

4.1.1 Introduction

Establishing trust in a certificate's issuer is made possible through two separate processes, which can be carried out in parallel, see clauses 4.1.2 and 4.1.3.

4.1.2 Process 1 - Browser Vendor Accepted Certificate Issuer

a) A Root CA certificate is generated minimally following the requirements defined by the CA operator, the CA/B Forum Baseline Requirements [i.6], and Browser Vendor Root Program policies.

b) The CA system and its corresponding policies, processes, and operator(s) are audited against ETSI EN 319 411-1 [i.2], with an audit report prepared as in ETSI TS 119 403-2 [i.11].

c) The QTSP completes the Browser Vendor-defined process for requesting the CA certificate to be added to the Browser Vendor's Root Store. This includes submission of audit artifacts generated in a) and b), and additional artifacts to facilitate independent security reviews of the CA's policies, practices, and operations by the Browser Vendor.

d) The Browser Vendor follows its defined process to evaluate the CA's policies, practices, and operations.

- If Browser Vendor requirements are satisfied, the CA certificate will be distributed as trusted by the Browser Vendor Root Store at the Browser Vendor's discretion.

- If Browser Vendor requirements are not satisfied, the QTSP will need to follow Browser Vendor Root Program requirements for issue remediation and/or re-application.

e) The Browser Vendor can perform ongoing monitoring of the CAs in its Root Store to ensure QTSP/CA operators continue to comply with the applicable CA/B Forum Requirements and any additional Browser Vendor-specific requirements. Failure to follow the requirements defined in the CA/B Forum Baseline Requirements [i.6] or by a Browser Vendor-specific Root Program policy can result in a CA certificate's removal from the Root Store or other technical or policy restrictions at the Browser Vendor's sole discretion.

4.1.3 Process 2 - EU Qualified Certificate Issuer

a) CA certificates are generated by QTSPs which comply with QWAC issuance requirements, as specified in ETSI EN 319 411-2 [i.3] policy requirements.

b) The QTSP is audited by a Conformity Assessment Body (CAB) under ETSI EN 319 403-1 [i.10] with an audit report (i.e. Conformity Assessment Report) for the supervisory body as in ETSI TS 119 403-3 [i.12]. This process can be carried out under the same audit as auditors check on compliance to the CA/B Forum Baseline Requirements [i.6] in clause 4.1.2 item b).

c) The QTSP will have the national supervisory body under Regulation (EU) No 910/2014 [i.4] verify its Conformity Assessment Report (CAR), and is then placed on the EU Trusted List [i.8].

d) The QTSP follows its defined process for being evaluated regularly according to Regulation (EU) No 910/2014 [i.4]. The QTSP is supervised by the Member State's designated supervisory body on a regular basis. Failure to follow the Member State's designated supervisory body requirements can result in the removal of the specific service(s) from the EU Trusted List.

4.2 Validating trust in a website's certificate

4.2.1 Introduction

A browser validates a QWAC by following the process 1 in clause 4.2.2 and, if successful, the process 2 in clause 4.2.4.

4.2.2 Process 1 - Browser Vendor Certificate Validation

a) Upon attempting to establish a secure connection to a website, the browser is presented with a Qualified Website Authentication Certificate (i.e. QWAC).

b) The website's certificate is evaluated against Browser Vendor-specific security requirements.

   If the website's certificate does not satisfy Browser Vendor-specific security evaluations, the browser can present the website as untrusted without further evaluation of the CA that issued the website's certificate including validation under Regulation (EU) No 2014/910 [i.4] as in the Process 2 of clause 4.2.4. Browser Vendors can use their discretion when determining whether or not to allow users to bypass certificate validation errors due to any number of factors (for example, because a Browser Client has not fetched updated certificate status information within the Browser Vendor required timeframe).

c) The website's certificate issuer is identified and evaluated against Browser Vendor-specific security requirements, including verifying that certificate validation succeeds to an entry contained in the Browser Root Store.

   Browser Vendors are generally unable to provide updates to all Browser Users reliably and instantly, thus a stale Root Store may be in use for some users.

NOTE: Steps described in b) and c) can occur in any order.

4.2.3 Process 1 - Outcomes

If steps a), b), and c) are completed without error, the certificate will be evaluated against the requirements defined in process 2 of clause 4.2.4. If steps a), b), and c) are not completed without error, the browser can present the website as untrusted without further consideration of the EU Trusted List. As after step b), Browser Vendors can use their discretion when determining whether or not to allow users to bypass certificate validation errors due to any number of factors.

4.2.4 Process 2 - EU Qualified Certificate Validation

The browser should perform the following two actions.

a) The website's certificate is evaluated for conformance with the certificate profile requirements applicable to QWACs as specified in ETSI EN 319 411-2 [i.3], clause 6.6.1.

b) The website's certificate chain is evaluated for the presence of a certificate on the EU List of Trusted Lists as specified in ETSI TS 119 615 [i.8].

The browser may not be able to complete certificate validation if:

- it is unable to obtain up-to-date EU Trusted List information;
- website (server) settings are misconfigured (e.g. serves a certificate chain that does not build through or to a certificate on the EU Trusted List, or staples an expired OCSP response);
- QTSP misconfigurations prevent certificate path building (e.g. unavailability of Authority Information Access extension HTTP URIs) or certificate status checking (e.g. expired CRL); or
- there are multiple valid certificate chains, where at least one does not include the presence of a certificate on the EU Trusted List.

NOTE: Steps described in a) and b) can occur in any order.

4.2.5 Process 1 & 2 - Outcomes

If the process 1 in clause 4.2.2 and the process 2 in clause 4.2.4 are completed without error:

- The browser should present the website to the browser user if there are no other errors.
- The browser should indicate that the certificate is validated as being qualified as specified in Regulation (EU) No 910/2014 [i.4] using the EU Trust Mark if technically feasible. When using the EU Trust Mark the browser can provide a link to the relevant Trusted List entry.
- The identity data contained in qualified certificates for website authentication should be displayed to the browser user in a user-friendly manner if technically feasible.

If the process 1 in clause 4.2.2 is completed without error but the process 2 in clause 4.2.4 is completed with error:

- The Browser Vendor can use its discretion in presenting the website to the user, with or without warnings or bypassable errors, however it should not display a "EU Qualified Status" indicator (e.g. EU Trust Mark).

History

Document history		
V1.1.1	January 2023	Publication