ETSI TS 119 411-5 V2.1.1 (2025-02)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Implementation of qualified certificates for website authentication as in amended Regulation 910/2014

Reference

RTS/ESI-0019411-5v211

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

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

The present document is part 5 of a multi-part deliverable covering policy requirements for Trust Service Providers issuing certificates. Full details of the entire series can be found in part 1 [i.2].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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

Regulation (EU) No 910/2014 [i.7] amended by Regulation (EU) No 2024/1183 [i.3] sets the security requirements for the European Digital Single Market and the European Trust Space. Under Regulation (EU) No 910/2014 [i.7], EU Commission and EU member states operate a trust scheme for the approval of trust services, including issuers of Qualified certificates for Website Authentication (QWACs), with requirements for certificates specified in Annex IV of the regulation. Trusted issuers of website certificates are listed in EU Trusted Lists according to EU Commission Implementing Decision 2015/1505 [i.9].

The present document defines two approaches for deploying and consuming qualified certificates for website authentication. The first approach (1-QWACs) is backwards compatible with existing standards for QWACs and describes how web browsers can establish secure TLS connections with websites using the QWAC as a TLS certificate, directly authenticating website identity information.

The second approach (2-QWACs) describes how web browsers can establish secure TLS connections with websites without using the QWAC as a TLS certificate, whilst indirectly authenticating the website through a binding between the authenticated website identity information included in the QWAC and the TLS certificate used to establish the secure connection to the website.

1 Scope

The present document defines two approaches for issuing qualified certificates for website authentication, deploying them to websites, and their consumption by web browsers.

Objectives of Approach #1 (i.e. "1-QWAC Approach")

1-QWACs:

a) Support coexistence of trust controls based upon meeting requirements from both the Web Browser Vendor within the meaning of Recital 65 of the Regulation (EU) 2024/1183 [i.3] and EU Trusted Lists with ETSI standards aimed at supporting EU trust controls.

b) Include requirements for TLS certificates based on CA/Browser Forum Requirements [i.4] and [i.5] as applied in ETSI standards [4].

c) Authenticate the website directly by using the QWAC to establish a TLS connection between the web browser and the server.

NOTE: TLS uses encryption to secure data transmitted over a network providing confidentiality, integrity, and authentication.

Objectives of Approach #2 (i.e. "2-QWAC with Certificate Binding Validation Approach")

2-QWACs with Certificate Binding Validation:

- Support trust controls based upon EU Trusted Lists with ETSI standards aimed at supporting EU trust controls for a QWAC, which is used to bind the identity in the QWAC to the TLS certificate(s) to be used by the web browser to establish a TLS connection between the web browser and the server.
- Support trust controls based upon Web Browser Vendor Root Stores for the TLS certificate which is used to establish a TLS connection between the web browser and the server.

All approaches:

- aim to meet the requirements of Article 45, Article 45a, and Recital 65 of Regulation (EU) 2024/1183 [i.3];
- include requirements of qualified certificates for website authentication as specified in Regulation (EU) 2024/1183 [i.3]; and
- enable the display of identity data contained in qualified certificates for website authentication and validated by the EU trust schemes in a user-friendly manner.

Clause 4 specifies Trust Service Provider requirements for issuing QWACs.

Clause 5 provides website operator guidance for using QWACs.

Clause 6 specifies web browser requirements for consuming QWACs.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

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

[2] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[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".

[4] ETSI EN 319 412-4: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

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

[6] IETF RFC 8288: "Web Linking".

[7] ETSI TS 119 182-1: "Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[8] ETSI TS 119 312: "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

[9] IETF RFC 7519: "JSON Web Token (JWT)".

[10] IETF RFC 7515: "JSON Web Signature (JWS)".

[11] Recommendation ITU-T X.680 (2008): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

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 Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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

[i.3] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.4] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.5] CA/Browser Forum: "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[i.6] ETSI EN 301 549: "Accessibility requirements suitable for public procurement of ICT products and services in Europe".

[i.7] 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 transaction.

[i.8] IETF RFC 7518: "JSON Web Algorithms (JWA)".

[i.9] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

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 [3] and the following apply:

1-QWAC: qualified certificate for website authentication based on Approach #1 in clause 1 of the present document

2-QWAC: qualified certificate for website authentication based on Approach #2 in clause 1 of the present document

Transport Layer Security: protocol standardized by the IETF RFC 8446 [5] which is used by web browsers to establish encrypted connections to websites

Transport Layer Security Certificate: X.509 public key certificate with an extended key usage extension that contains the id-kp-serverAuth KeyPurposeId, used to authenticate a website in accordance with a transport layer security protocol

web browser: software application that acts on behalf of a user to retrieve, render, and interact with websites

web browser vendor: legal entity who provides a web browser

web browser vendor root store: set of transport layer security root certificates that transport layer security certificates have to chain up to in order to be trusted by the web browser

web browser vendor root store policy: policy defining the individual rules on the issuers of the transport layer security root certificates in the root store by the web browser vendor

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 [3] and the following apply:

HTTP	Hypertext Transfer Protocol
TLS	Transport Layer Security
QTSP	Qualified Trust Service Provider
QWAC	Qualified Website Authentication Certificate

NOTE: QWAC is termed qualified certificate for website authentication in Regulation (EU) 2024/1183 [i.3].

4 Trust Service Provider Requirements for issuing Qualified Certificates for Website Authentication

4.1 1-QWAC Approach

4.1.1 Policy Requirements

The 1-QWAC certificate shall be issued in accordance with one of the following certificate policies as specified in ETSI EN 319 411-2 [3]:

a) QEVCP-w; or

b) QNCP-w.

4.1.2 Certificate Profile Requirements

The 1-QWAC certificate shall be issued in accordance with ETSI EN 319 412-4 [4] for the relevant certificate policy as identified in clause 4.1.1 of the present document.

4.2 2-QWAC Approach

4.2.1 Policy Requirements

The 2-QWAC certificate shall be issued in accordance with the QNCP-w-gen certificate policy as specified in ETSI EN 319 411-2 [3].

4.2.2 Certificate Profile Requirements

The 2-QWAC certificate shall be issued in accordance with ETSI EN 319 412-4 [4] for the relevant certificate policy as identified in clause 4.2.1 of the present document, except as described below:

- the extKeyUsage value shall only assert the extendedKeyUsage purpose of id-kp-tls-binding as specified in Annex A.

5 Website Operator Guidance for using Qualified Certificates for Website Authentication

5.1 Usage of 1-QWACs

The website operator requests a 1-QWAC from a QTSP as defined in clause 4.1 of the present document and configures its use (e.g. provisions the 1-QWAC on a TLS terminator).

5.2 Usage of 2-QWACs

The website operator requests:

- a Qualified Website Authentication Certificate (i.e. 2-QWAC) from a QTSP; and
- a TLS certificate from a TLS Certificate issuer (e.g. TSP or Certification Authority) whose corresponding root CA certificate is included in the desired Web Browser Vendor Root Store(s).

When using a 2-QWAC, website operators shall:

1) Enumerate the TLS certificate(s) they wish relying parties to use to establish secure connections with their website;

2) Produce a TLS Certificate Binding over their selected TLS certificate(s) with their 2-QWAC as described in Annex B and place it on their website; and

3) Configure their website to serve:

   a) an HTTP 'Link' response header (as defined in IETF RFC 8288 [6]) with a relative reference to the TLS Certificate Binding, and a `rel` value of `tls-certificate-binding`; and

   b) the TLS certificate(s).

Website operators should deploy the appropriate HTTP caching directives for their TLS Certificate Binding file. The cache lifetime should not extend beyond the lifetime of the TLS Certificate Binding, in order to ensure consistent behaviour for relying parties, but there are no security implications if the caching directives are incorrectly set. Website operators may choose to rely upon a unique binding filename or location to reduce the potential of cache errors.

Periodically, website operators will receive new QWACs and TLS certificates. When the operator wishes to roll over from an existing QWAC to a new QWAC, it produces a fresh TLS Certificate Binding and deploys it using the ordinary mechanism. Website operators should also remove no-longer-used TLS certificates from the TLS Certificate Binding to optimize certificate validation.

6 Web Browser Requirements for consuming Qualified Certificates for Website Authentication

6.1 General Procedures

6.1.1 Determining Usage

If a certificate is received as part of the TLS Handshake protocol which has QCStatements indicating that it is a QWAC, it shall be processed under procedures for 1-QWAC.

If a certificate is received as part of the TLS Certificate Binding which has QCStatements indicating that it is a QWAC, it shall be processed under procedures for 2-QWAC.

6.1.2 Validation of QWACs

For 1-QWACs and 2-QWACs, validation shall include:

1) that the QWAC includes QCStatements as specified in clause 4.2 of ETSI EN 319 412-4 [4] and the appropriate Policy OID specified in ETSI EN 319 411-2 [3];

2) that the QWAC chains back through appropriate & valid digital signatures to an issuer on the EU Trusted List which is authorized to issue Qualified Certificates for Website Authentication as specified in ETSI TS 119 615 [1];

3) that the QWAC's validity period covers the current date and time;

4) that the website domain name in question appears in the QWAC's subject alternative name(s); and

5) that the QWAC's certificate profile conforms with:

   a) For a 1-QWAC, clause 4.1.2 of the present document; or

   b) For a 2-QWAC, clause 4.2.2 of the present document.

The web browser may also perform further checks on the security and authenticity of the QWAC as appropriate (e.g. for checking revocation status).

6.2 Usage of QWACs

6.2.1 Usage of 1-QWACs (i.e. "Approach #1")

When using 1-QWACs for the establishment of secure TLS connections with websites authenticated with identity information, web browsers shall:

1) Establish a secure TLS connection with the site using the web browsers' procedures and configuration, and evaluate the presented TLS Certificate with the security requirements of the web browser vendor and their policies for web security, domain authentication and the encryption of web traffic as outlined in Recital 65 of the Regulation (EU) 2024/1183 [i.3].

   - If this step fails, the procedure finishes negatively.

2) Evaluate the presented TLS certificate with the validation criteria laid out in clause 6.1.2 of the present document to establish if it is considered a 1-QWAC.

   - If this step fails for any reason, the procedure finishes negatively.

3) Display the outcome as specified in clause 6.3 of the present document.

6.2.2 Usage of 2-QWACs with TLS Certificate Binding (i.e. "Approach #2")

When using 2-QWACs with secure TLS connections to websites, web browsers shall:

1) Establish a secure TLS connection with the site using the web browsers' procedures and configuration, and evaluate the presented TLS Certificate with the security requirements of the web browser vendor and their policies for web security, domain authentication and the encryption of web traffic as outlined in Recital 65 of the Regulation (EU) 2024/1183 [i.3].

   - If this step fails, the procedure finishes negatively.

2) Examine the HTTP headers included in any main frame navigation response from the server (relating to navigation by the web browser to the address as displayed in the address bar) for a HTTP 'Link' response header (as defined in IETF RFC 8288 [6]) with a `rel` value of `tls-certificate-binding`.

   - If this step is absent, the procedure finishes negatively.

3) Fetch the resource located at this link and evaluate it for conformance with the profile laid out in Annex B.

   - If this step fails or the resource is non-conformant, the procedure finishes negatively.

4) Examine the QWAC presented in the binding with the validation criteria laid out in clause 6.1.2 of the present document.

   - If this step fails or the certificate is not considered a '2-QWAC' under clause 6.1.2 of the present document, the procedure finishes negatively.

5) Validate the JAdES signature on the TLS Certificate binding according to ETSI EN 319 102-1 [2].

   - If this step fails or the TLS Certificate binding is not considered valid, the procedure finishes negatively.

6) Validate that the TLS Certificate used to establish this connection in Step 1 appears in the list contained in the validated binding.

   - If this step fails or the list does not contain the certificate, the procedure finishes negatively.

7) Display the outcome as specified in clause 6.3 of the present document.

6.3 Validation outcomes

Regardless of how the QWAC was delivered (i.e. as a 1-QWAC or 2-QWAC), if the applicable procedure described in clause 6.2 of the present document finishes:

- **successfully (with a valid QWAC)**, the web browser:
  - shall indicate that the QWAC is validated as being qualified as specified in Regulation (EU) 2024/1183 [i.3] using the EU Trust Mark if technically feasible. When using the EU Trust Mark the web browser may provide a link to the relevant Trusted List entry.
  - shall display the identity data contained in qualified certificates for website authentication to the web browser user in a user-friendly manner. The web browser should take the accessibility requirements defined in ETSI EN 301 549 [i.6] into account.
- **negatively (without a valid QWAC)**, the web browser:
  - may use its discretion in presenting the website to the user, with or without warnings or bypassable errors, however it shall not display a "EU Qualified Status" indicator (e.g. EU Trust Mark).
  - may include a warning that a QWAC failed to validate.

Annex A (normative): id-kp-tlsBinding EKU specification

The following ASN.1 module shall be interpreted using the syntax defined in Recommendation ITU-T X.680 [11]. It defines the KeyPurposeID id-kp-tls-binding.

```
TLSBindingMod  { itu-t(0) identified-organization(4) etsi(0)
    id-qwacImplementation(194115) id-mod(0) id-mod-tlsbinding(1) v1(0) }
DEFINITIONS EXPLICIT TAGS ::=
BEGIN
  -- EXPORTS ALL
  -- IMPORTS NOTHING
  -- Object Identifier arc for extended Key Usage purpose id-kp-tls-binding
  id-tlsBinding OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
      etsi(0) id-qwacImplementation(194115) tls-binding (1) }
  id-kp-tls-binding OBJECT IDENTIFIER ::= { id-tlsBinding id-kp-tls-binding(0) }
END
```

Annex B (normative):
TLS Certificate Binding Profile

A website operator can use a public key certificate to produce a binding to one or multiple TLS certificates as specified in this annex. This binding is produced by generating a JAdES signature over the fields described below using the certificate private key corresponding to the QWAC and according to ETSI TS 119 182-1 [7]. Only header parameters specified in this profile may be present in the header of the generated JAdES signature. The JAdES signatures shall be serialized using JWS Compact Serialization as specified in IETF RFC 7515 [10].

Table B.1: Signed header parameters

Header Parameter	Description
`alg`	Specifies the cryptographic algorithm used for signing the binding. This field shall not conflict with the type of public key in the signing certificate.
`kid`	Identifies the key used for signing the binding.
`cty`	This field identifies the purpose of the JAdES signature and ensures context separation. It shall be "TLS-Certificate-Binding-v1".
`x5t#S256`	The SHA-256 hash of the DER encoding of the X.509 certificate that corresponds with the private key used for signing the binding.
`x5c`	The signing certificate and Certificate Chain (Base64 encoded). The Chain shall be ordered as described in IETF RFC 7515 [10] and shall finish in a trust anchor on the EU Trusted List which is authorized to issue QWACs (ETSI TS 119 615 [1]).
`iat`	This field contains the claimed signing time. The value shall be encoded as specified in IETF RFC 7519 [9].
`exp`	This field contains the expiry date of the binding. The maximum effective expiry time is whichever is soonest of this field, the longest-lived TLS certificate identified in the sigD member payload (below), or the notAfter time of the signing certificate. The value shall be encoded as specified in IETF RFC 7519 [9].

`sigD`	Includes a data object following the format below:
	
	`{`
	`    "mId":   "http://uri.etsi.org/19182/ObjectIdByURIHash",`
	`    "pars":  [A comma-separated list of TLS certificate file names.],`
	`    "hashM": [The string identifying one of the approved hashing`
	`algorithms`
	`             identified by ETSI TS 119 312 [8] for JAdES. This hashing`
	`             algorithm is used to calculate the hashes described in the`
	`             "hashV" member below.],`
	`    "hashV": [A comma-separated list of TLS certificate file hashes.`
	`Each`
	`             hash is produced by taking the corresponding X.509`
	`             certificate, computing its base64url encoding, and`
	`             calculating its hash using the algorithm identified in the`
	`             "hashM" member above.]`
	`}`

NOTE: At the time of publication of the present document, in line with the hash algorithms required as part of the digital signature algorithms in IETF RFC 7518 [i.8] and the requirements for AdES formats listed in the latest version of ETSI TS 119 312 [8] V1.5.1, Annex A, it is required that SHA-256, SHA-384, and SHA-512 are supported, and it is assumed that strings identifying them are S256, S384, and S512 respectively.	

Signature: Produced by the signing certificate private key over the fields above, according to ETSI TS 119 182-1 [7].

Future versions of the present document may use a different format or hash function and will be distinguished by a different type in the cty field.

Annex C (informative): Web Browser Recommendations

C.1 General Web Browser Recommendations

a) Web browsers should support both 1-QWAC and 2-QWAC as defined in the present document.

b) Web browser vendors should make available to issuers of 1-QWACs any requirements in addition to those required under clause 4.1 of the present document (TSP policy and certificate profile requirements).

c) When adding requirements relevant to issuers of 1-QWACs, as in b) above, Web browser vendors should substantiate the positive impact of those additions to user security and privacy.

C.2 Basic Recommendations on Web Browser Vendor Root Store Policies for TLS certificates

When a web browser vendor runs a web browser vendor root store for TLS certificates, it should publish and maintain a web browser vendor root store policy which defines the rules that apply to the root store. If instead, a web browser vendor relies on either the operating system's root store or a root store run by an upstream web browser vendor, it should publicly disclose the location of the corresponding root store policy. The following conditions define the basic requirements on web browser vendor root store policies for TLS certificates so that the web browser vendor and its root store are in compliance with the present document. Additional requirements of the root store policy should not weaken the CA/Browser Forum Requirements [i.5] or reduce its effect.

C.3 Content of the Root Store Policy

When a web browser vendor runs a web browser vendor root store for TLS certificates, its web browser vendor root store policy should contain at least the following content:

1) Scope of the root store policy

2) Contact address and means of contact

3) Revisions

4) A non-exhaustive list of requirements to be included in the root store

5) A non-exhaustive list of requirements to remain in the root store

6) A non-exhaustive list of requirements to be excluded from the root store

7) Description of the application process to be added to the root store and its processing time

8) Description of the removal process from the root store and its processing time

9) Description of the updating process of the root store policy and ways of participation

The web browser vendor may publish interpretation guidelines and examples that support a better understanding of its root store policy.

C.4 Application of a Root Store Policy

When there is a root store policy that complies with the present document, the TLS certificate issuer should fully comply with that root store policy.

Web browser vendors should respond to general inquiries or questions from TSPs related to their stated policies within 14 calendar days.

Annex D (informative):
Change history

Date	Version	Information about changes
June 2024	v1.1.2	Initial draft
September 2024	v1.1.3	Update after call on July 11
October 2024	v1.1.4	Update after call on October 22
November 20224	v1.1.5	Update after ESI#84
November 2024	v1.1.6	Update for RC
December 2024	v1.1.7	Update after comments on RC
January 2025	v1.1.8	Update after comments from public review
February 2025	v1.1.9	Update after comments on v1.1.8

History

Document history		
V1.1.1	January 2023	Publication as ETSI TR 119 411-5
V2.1.1	February 2025	Publication