Draft ETSI EN 319 412-4 V1.3.2 (2024-08)

Electronic Signatures and Trust Infrastructures (ESI);
Certificate Profiles;
Part 4: Certificate profile for web site certificates

Reference
REN/ESI-0019412-4v132

Keywords
electronic signature, IP, profile, 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 4
Foreword 4
Modal verbs terminology 4
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definition of terms, symbols, abbreviations and notations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
3.4 Notations 8
4 Profile requirements 8
4.1 Generic profile requirements 8
4.1.1 Certificates following DVCP, IVCP or OVCP 8
4.1.2 Certificates following EVCP or QEVCP-w 8
4.1.3 Certificates following NCP or QNCP-w-gen 8
4.1.4 Certificates following QNCP-w 9
4.2 EU Qualified Certificate statements for EU Qualified Certificates 9
4.3 Certificate policies for EU Qualified Certificates 9
Annex A (informative): Change history 10
History 11

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 draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI EN Approval Procedure.

The present document is part 4 of multi-part deliverable covering the Certificates Profiles. Full details of the entire series can be found in part 1 [i.5].

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

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

ITU and ISO issued standards for certification of public keys in Recommendation ITU X.509 | ISO/IEC 9594-8 [i.4] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.3] 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.2] defines requirements on specific types of certificates named "qualified certificates". Implementation of the Directive 1999/93/EC [i.2] and deployment of certificate infrastructures throughout Europe as well as in countries outside of Europe, have resulted in a variety of certificate implementations for use in public and closed environments, where some are declared as qualified certificates while others are not.

The CA/Browser Forum released the Extended Validation Certificate Guidelines [3] and the Baseline Requirements for the issuance and management of publicly trusted TLS/SSL certificates [2] to mitigate website spoofing attacks.

The present document aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.3] and in the wider international environment, also by meeting requirements from CA Browser Forum.

1 Scope

The present document specifies a certificate profile for web site certificates that are accessed by the TLS protocol [i.1].

The profile defined in the present document builds on the CA/Browser Forum Baseline requirements [2], Extended validation guidelines [3] and other parts of the present multi-part deliverable.

The present document focuses on requirements on certificate content. Requirements on decoding and processing rules are limited to aspects required to process certificate content defined in the present document. Further processing requirements are only specified for cases where it adds information that is necessary for the sake of interoperability.

This profile can be used for legal and natural persons. For certificates issued to legal persons, the profile builds on the CAB Forum EV Profile [3] or baseline requirements [2]. For certificates issued to natural persons, the profile builds only on CAB Forum baseline requirements [2].

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 at https://docbox.etsi.org/Reference.

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 EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

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

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

[4] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[5] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

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

[7] 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".

[8] Void.

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

NOTE: The version for reference [9] is required in WEB-4.1.3-4 to be as referenced in ETSI EN 319 411-1 for [WEB] requirements.

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] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.3] 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.4] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.5] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 412-1 [i.5] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-1 [i.5] and the following apply:

BRG	Baseline Requirements Guidelines
DVCP	Domain Validation Certificate Policy
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
IVCP	Individual Validation Certificate Policy
NCP	Normalized Certificate Policy
OVCP	Organizational Validation Certificate Policy
QEVCP-w	Policy for EU qualified website certificate issued to a legal person and linking the website to that person based on the EVCG [3]
QNCP-w	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on the BRG [2]
QNCP-w-gen	Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person based on selected requirements in BRG [9]
TLS	Transport Layer Security

3.4 Notations

For the purposes of the present document, the notations given in ETSI EN 319 412-1 [i.5] apply.

4 Profile requirements

4.1 Generic profile requirements

4.1.1 Certificates following DVCP, IVCP or OVCP

WEB-4.1.1-1: For certificates issued following the certificate policies DVCP, IVCP or OVCP, as defined in ETSI EN 319 411-1 [6], all certificate fields and extensions shall comply with requirements on subscriber certificates stated in the BRG [2].

NOTE: According to BRG [2], section 7.1.6.4 implementations systems complying to the certificate policy for domain-validated certificates 2.23.140.1.2.1 cannot contain natural person or legal person related attributes.

WEB-4.1.1-2: Certificates following IVCP or OVCP may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.1.2 Certificates following EVCP or QEVCP-w

WEB-4.1.2-1: For certificates issued following the certificate policies EVCP, as defined in ETSI EN 319 411-1 [6], or QEVCP-w, as defined in ETSI EN 319 411-2 [7], all certificate fields and extensions shall comply with requirements on subscriber certificates stated in the EVCG [3], with the amendments specified in clauses 4.2 and 4.3 of the present document for EU Qualified Certificates.

WEB-4.1.2-2: Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

WEB-4.1.2-3: If the certificate is EU Qualified, and an appropriate registration number is known to exist for the issuer, then the issuer field shall contain the attribute organizationIdentifier.

WEB-4.1.2-4: If the certificate is EU Qualified, and an appropriate registration number is known to exist for the subject, then the subject field shall contain the attribute organizationIdentifier.

WEB-4.1.2-5: If present, the issuer and subject organizationIdentifier shall have a value different from the organizationName.

WEB-4.1.2-6: Certificates may include a legal person semantic identifier as specified in clause 5.1.4 of ETSI EN 319 412-1 [i.5].

4.1.3 Certificates following NCP or QNCP-w-gen

WEB-4.1.3-1: For certificates issued following the certificate policies NCP, as defined in ETSI EN 319 411-1 [6], or QNCP-w-gen, as defined in ETSI EN 319 411-2 [7], the following requirements shall apply.

WEB-4.1.3-2: If the certificate is issued to a natural person the requirements specified in ETSI EN 319 412-2 [4] clause 4 shall apply with the exception of fields where WEB-4.1.3-4 applies.

WEB-4.1.3-3: If the certificate is issued to a legal person the requirements specified in ETSI EN 319 412-3 [5] clause 4.2 shall apply with the exception of fields where WEB-4.1.3-4 applies.

WEB-4.1.3-4: The following certificate profile requirements specified in the BRG [9] shall apply for subject certificate fields addressed by the following sub-sections of BRG [9] (the version of BRG [9] shall be as referenced in ETSI EN 319 411-1 [6] for [WEB] requirements):

a) 7.1.2.3 f) extKeyUsage.

b) 7.1.4.2.1 Subject Alternative Name.

c) 7.1.4.2.2 Subject Distinguished Name - commonName.

d) If necessary to distinguish the website identified by the subject name, the subject commonName may contain a domain name or a Wildcard Domain Name (as defined in BRG [9]) which is one of the dNSName values of the subjectAltName extension of a website authentication certificate.

WEB-4.1.3-5: The amendments specified in clauses 4.2 and 4.3 of the present document shall apply for EU Qualified Certificates.

WEB-4.1.3-6: Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.1.4 Certificates following QNCP-w

WEB-4.1.4-1: For certificates issued following the certificate policies QNCP-w, as defined in ETSI EN 319 411-2 [7], all certificate fields and extensions shall comply with requirements on subscriber certificates stated in the BRG [2].

WEB-4.1.4-2: If necessary to distinguish the website identified by the subject name, the subject commonName may contain a domain name or a Wildcard Domain Name (as defined in BRG [2]) which is one of the dNSName values of the subjectAltName extension of a website authentication certificate.

WEB-4.1.4-3: Certificates following QNCP-w may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

WEB-4.1.4-4: The amendments specified in clauses 4.2 and 4.3 of the present document shall apply for EU Qualified Certificates.

WEB-4.1.4-5: If an appropriate registration number is known to exist for the issuer, and the issuer is a legal person, then the issuer field shall contain organizationIdentifier.

WEB-4.1.4-6: If an appropriate registration number is known to exist for the subject, and the subject is a legal person, then the subject field shall contain organizationIdentifier.

WEB-4.1.4-7: If present, the issuer and subject organizationIdentifier shall have a value different from the organization name.

WEB-4.1.4-8: Certificates may include a legal person semantic identifier as specified in clause 5.1.4 of ETSI EN 319 412-1 [i.5].

4.2 EU Qualified Certificate statements for EU Qualified Certificates

QCS-4.2-1: When certificates are issued as EU Qualified Certificates, they shall include `QCStatements` as specified in clauses 4 and 5 of ETSI EN 319 412-5 [1].

4.3 Certificate policies for EU Qualified Certificates

QCS-4.3-1: When the certificates are issued as EU Qualified Certificates, they should include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.3 of ETSI EN 319 411-2 [7]. Policy identifiers included in the certificate policies extension of EU Qualified Certificates shall be consistent with the EU Qualified Certificate Statements according to clause 4.2.

Annex A (informative): Change history

Date	Version	Information about changes
July 2021	1.1.4	CR to include alternative certificate profile based on ETSI EN 319 412-3 and CABF Baseline
April 2023	1.2.5	Updated to allocate reference number to each requirement in line with ETSI EN 319 411-1 CR#1 Update to align with Web policies in ETSI EN 319 411-1 & 2
September 2023	1.3.1	Published as EN
August 2024	1.3.2	Minor editorial correction to WEB-4.1.3-2 and WEB-4.1.3-3 to reference WEB-4.1.3-4

History

Document history		
V1.0.1	July 2015	Publication as ETSI TS 119 412-4 (Withdrawn)
V1.1.1	February 2016	Publication
V1.2.1	November 2021	Publication
V1.3.1	September 2023	Publication
V1.3.2	August 2024	EN Approval Procedure AP 20241119: 2024-08-21 to 2024-11-19