



**Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 4: Certificate profile for web site certificates
issued to organizations**

ReferenceRTS/ESI-0019412-4-TS

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
<http://www.etsi.org/standards-search>

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:
<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2015.
All rights reserved.

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

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references.....	5
3 Definitions and abbreviations.....	6
3.1 Definitions.....	6
3.2 Abbreviations	6
4 Profile requirements	6
4.1 Generic profile requirements	6
4.2 EU qualified certificate statements.....	6
4.3 Certificate policies.....	6
History	7

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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

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

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 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 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.

Through the use of the multipart ETSI TS 119 412 standard, trust service providers (TSPs) can issue certificates, in the context of the Regulation (EU) No 910/2014 [i.3] or where similar requirements are present, in a way which will maximize interoperability of (qualified) certificates issued to natural person, to legal person or to organizations as web site certificate, for the purposes of (qualified) electronic signatures, (qualified) electronic seals, peer entity authentication, data authentication, data integrity, as well as data confidentiality.

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.3] and those from CA Browser Forum.

1 Scope

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

The profile defined in the present document builds on the CAB Baseline requirements and Extended validation guidelines.

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.

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 <http://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 TS 119 412-5: "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".

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 TS 119 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
- [i.6] ETSI TS 119 411-2: "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".
-

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 119 412-1 [i.5] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 119 412-1 [i.5] and the following apply:

TLS	Transport Layer Security
-----	--------------------------

4 Profile requirements

4.1 Generic profile requirements

All certificate fields and extensions shall comply with requirements on subscriber certificates stated in the Certificate Content and Profile (clause 9 and appendix B) of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [2], or extended validation certificates [3], with the amendments specified in clauses 4.2 and 4.3 for qualified certificates.

Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI TS 119 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.2 EU qualified certificate statements

Certificates issued as EU qualified certificates shall include `QCStatements` as specified in clauses 4 and 5 of ETSI TS 119 412-5 [1].

4.3 Certificate policies

EU qualified certificates should include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.2 of ETSI TS 119 411-2 [i.6]. 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.

History

Document history		
V1.0.0	June 2015	EN Approval Procedure AP 20151016: 2015-06-18 to 2015-10-16
V1.0.1	July 2015	Publication (same technical content as ETSI EN 319 412-4 V1.0.0)