



SLOVENSKI STANDARD

SIST EN 319 412-5 V2.1.1:2016

01-maj-2016

Elektronski podpisi in infrastruktura (ESI) - Profili potrdil - 5. del: Izjave QC

Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 5:
QCStatements

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: **ETSI EN 319 412-5 V2.1.1 (2016-02)**

SIST EN 319 412-5 V2.1.1:2016
<https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016>

ICS:

03.080.99	Druge storitve	Other services
35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST EN 319 412-5 V2.1.1:2016 **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 412-5 V2.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016>

ETSI EN 319 412-5 V2.1.1 (2016-02)



Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

[SIST EN 319 412-5 V2.1.1:2016
https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016](https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016)

Reference

REN/ESI-0019412-5v211

Keywords

e-commerce, electronic signature, 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 412-5 V2.1.1:2016

<https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351240/EN-319-412-5-v2-1-1-2016>
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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.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 2016.

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	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	7
4 Qualified certificate statements.....	8
4.1 General requirements	8
4.2 QCStatements claiming compliance with the EU legislation	8
4.2.1 QCStatement claiming that the certificate is a EU qualified certificate.....	8
4.2.2 QCStatement claiming that the private key related to the certified public key resides in a QSCD.....	8
4.2.3 QCStatement claiming that the certificate is a EU qualified certificate of a particular type.....	9
4.3 Generic QCStatements.....	9
4.3.1 Introduction.....	9
4.3.2 QCStatement regarding limits on the value of transactions	9
4.3.3 QCStatement indicating the duration of the retention period of material information.....	10
4.3.4 QCStatement regarding location of PKI Disclosure Statements (PDS).....	10
5 Requirements on QCStatements in EU qualified certificates.....	11
Annex A (informative): Relationship with the Regulation (EU) No 910/2014	12
A.1 EU qualified certificates for electronic signatures	12
A.2 EU qualified certificates for electronic seals.....	13
A.3 EU qualified certificates for website authentication	14
Annex B (normative): ASN.1 declarations.....	15
History	17

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 (<https://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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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

The present document was previously published as ETSI TS 101 862 [i.4].

National transposition dates	
Date of adoption of this EN:	22 February 2016
Date of latest announcement of this EN (doa):	31 May 2016
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2016
Date of withdrawal of any conflicting National Standard (dow):	30 June 2017

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-T X.509 | ISO/IEC 9594-8 [i.7] which are used for the security of communications and data for a wide range of electronic applications.

The IETF qualified certificate profile, IETF RFC 3739 [2] defines an extension to X.509 certificates, the `qcStatements` extension, which can include statements relevant for qualified certificates. IETF RFC 3739 [2] defines qualified certificates in a general context as "a certificate whose primary purpose is to identify a person with a high level of assurance, where the certificate meets some qualification requirements defined by an applicable legal framework". The use of IETF RFC 3739 [2] `qcStatements` in the present document goes beyond the scope of the RFC which is directed at natural persons only.

The `qcStatements` certificate extension can contain any statement by the certificate issuer that can be useful to the relying party in determining the applicability of the certificate for an intended usage. Such statement can be a declaration that the certificate fulfils specific legal requirements for qualified certificates according to a defined legal framework.

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.8] Annexes I, III and IV.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN 319 412-5 V2.1.1:2016](https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/f922e686-1133-405c-9160-02cf67351210/sist-en-319-412-5-v2-1-1-2016>

1 Scope

The present document defines specific QCStatement for the qcStatements extension as defined in IETF RFC 3739 [2], clause 3.2.6, including requirements for their use in EU qualified certificates. Some of these QCStatements can be used for other forms of certificate.

The QCStatements defined in the present document can be used in combination with any certificate profile, either defined in ETSI EN 319 412-2 [i.2], ETSI EN 319 412-3 [i.5] and ETSI EN 319 412-4 [i.6], or defined elsewhere.

The QCStatements defined in clause 4.3 may be applied to regulatory environments outside the EU. Other requirements specified in clause 4 are specific to Regulation (EU) No 910/2014 [i.8] but may be adapted for other regulatory environments.

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] ISO 639-1:2002: "Codes for the representation of names of languages -- Part 1: Alpha-2 code".
- [2] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".
- [3] Recommendation ITU-T X.680-X.699: "Information technology - Abstract Syntax Notation One (ASN.1)".
- [4] ISO 4217: "Codes for the representation of currencies and funds".
- [5] IETF RFC 2818: "HTTP Over TLS".

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 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
- [i.2] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons".
- [i.3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [i.4] ETSI TS 101 862: "Qualified Certificate profile".

- [i.5] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons".
- [i.6] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".
- [i.7] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".
- [i.8] 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 and repealing Directive 1999/93/EC.
- [i.9] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [i.10] 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.11] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".
- [i.12] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

3 Definitions and abbreviations

3.1 Definitions

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

EU qualified certificate: qualified certificate that is stated to be in accordance with Annex I, III or IV of the Regulation (EU) No 910/2014 [i.8] or Annex I of the Directive 1999/93/EC [i.3] whichever is in force at the time of issuance

QCStatement: statement for inclusion in a qcStatements certificates extension as specified in IETF RFC 3739 [2]

qualified electronic signature/seal creation device: As specified in Regulation (EU) No 910/2014 [i.8].

secure signature creation device: As specified in Directive 1999/93 [i.3].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CRL	Certificate Revocation List
EC	European Commission
EU	European Union
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
PDS	PKI Disclosure Statements
PKI	Public Key Infrastructure
QC	Qualified Certificate
QSCD	Qualified electronic Signature/Seal Creation Device
RFC	Request For Comments
URL	Uniform Resource Locator