SLOVENSKI STANDARD
SIST EN 319 412-1 V1.1.1:2016

01-maj-2016

Elektronski podpisi in infrastruktura (ESI) - Profili potrdil - 1. del: Pregled in skupne podatkovne strukture

Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 1: Overview and common data structures

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 319 412-1 V1.1.1:2016
https://standards.iteh.ai/catalog/standards/sist/2978d00d-b765-4746-a7ac-
9c1a9ac8880d/sist-en-319-412-1-v1-1-1-2016

Ta slovenski standard je istoveten z: **ETSI EN 319 412-1 V1.1.1 (2016-02)**

ICS:

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

SIST EN 319 412-1 V1.1.1:2016 **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI EN 319 412-1 V1.1.1 (2016-02)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 1: Overview and common data structures

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Reference
DEN/ESI-0019412-1

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

iTeh STANDARD PREVIEW

(standards.iteh.ai)

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

ETSI

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 1 of a multi-part deliverable covering the Certificate Profiles, as identified below:

Part 1:   "Overview and common data structures";

Part 2:   "Certificate profile for certificates issued to natural persons";

Part 3:   "Certificate profile for certificates issued to legal persons";

Part 4:   "Certificate profile for web site certificates";

Part 5:   "QCStatements".

iTeh STANDARD PREVIEW

(standards.iteh.ai)

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 X.509 | ISO/IEC 9594-8 [i.3] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.9] 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 Directive 1999/93/EC [i.1], superseded by the Regulation (EU) No 910/2014 [i.9], 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.

Applications need support from standardized and interoperable identity certificates profiles, in particular when applications are used for electronic signatures, authentication and secure electronic exchange in open environments and international trust scenarios, but also when certificates are used in local application contexts.

This multi-part deliverable aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.9] and in the wider international environment.

1 Scope

The present document provides an overview of the Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] based certificate profiles and the statements for EU Qualified Certificates specified in other parts of ETSI EN 319 412 [i.4] to [i.7]. It specifies common data structures that are referenced from other parts of ETSI EN 319 412 [i.4] to [i.7].

The profiles specified in this multi-part deliverable aim to support both the Regulation (EU) No 910/2014 [i.9] and use of certificates in a wider international context. Within the European context, it aims to support both EU Qualified Certificates and other forms of certificate.

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.

iTeh STANDARD PREVIEW

[1] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

(standards.iteh.ai)

[2] ISO 3166: "Codes for the representation of names of countries and their subdivisions".

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

[i.2] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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

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

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

[i.8]   IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.9]   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.10]   Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems
             Interconnection - The Directory: Selected attribute types".

[i.11]   IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation
             List (CRL) Profile".

[i.12]   Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [i.2] 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.9] or annex I of the Directive 1999/93/EC [i.1] whichever is in force at the time of
issuance

3.2   Abbreviations

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

    ASN.1   Abstract Syntax Notation 1
    CA   Certification Authority
    OID   Object Identifier
    TLS   Transport Layer Security protocol

NOTE: As specified in IETF RFC 5246 [i.8].

    TSP   Trust Service Provider
    UN   United Nations

4   ETSI EN 319 412 certificate profiles

4.1   General approach

All the certificate profiles specified in ETSI EN 319 412 are based upon IETF RFC 5280 [i.11] for generic profiling of
Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3]. The certificate profiles specify profiles for both EU Qualified
Certificates and non-qualified certificates as relevant. Reference is made to ETSI EN 319 412-5 [i.7] for requirements
relating to QCStatements.