SLOVENSKI STANDARD
oSIST prEN 319 412-1 V1.5.0:2023

01-september-2023

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

Ta slovenski standard je istoveten z: **ETSI EN 319 412-1 V1.5.0 (2023-06)**

ICS:

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

oSIST prEN 319 412-1 V1.5.0:2023 **en**

Draft ETSI EN 319 412-1 V1.5.0 (2023-06)

EUROPEAN STANDARD

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

Reference

REN/ESI-0019412-1v151

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 - 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:
https://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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program: https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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.
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 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 Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

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".

The present document was previously published as ETSI TS 119 412-1 [i.14].

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

[2] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions--Part 1: Country code".

[3] ETSI TS 119 495: "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking".

[4] ISO 17442: "Financial services -- Legal Entity Identifier (LEI)".

[5] eIDAS: "SAML Attribute Profile", v1.2, 31 August 2019.

[6] IETF RFC 5912: "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)".

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.

[i.13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.14] ETSI TS 119 412-1: "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 319 401 [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

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement

3.2 Symbols

Void.

3.3 Abbreviations

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

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CRL	Certificate Revocation List

eIDAS	electronic IDentification, Authentication and trust Services
eID	electronic IDentity

NOTE: In line with eIDAS SAML Attribute Profile [5].

LEI	Legal Entity Identifier
OCSP	Online Certificate Status Protocol
OID	Object Identifier
SAML	Security Assertion Markup Language
TLS	Transport Layer Security protocol

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

TSP	Trust Service Provider
UN	United Nations

3.4 Notations

The requirements identified in the present document are preceded by a 3-letter prefix to denote the applicability to specific profiles as covered by the present multi-part deliverable.

Each requirement is identified as follows:

<3 letters profile> **-** < the clause number> **-** <2 digit number - incremental>.

The profile is identified as follows:

- **GEN:** Requirements generally applicable to certificate profiles.
- **NAT:** Requirements specifically applicable to profiles for certificates issued to natural persons.
- **LEG:** Requirements specifically applicable to profiles for certificates issued to legal persons.
- **WEB:** Requirements specifically applicable to profiles for certificates issued for specifically for website authentication.

NOTE: Such requirements can override requirements for the above classes of profiles.

- **QCS:** Requirements specifically applicable to profiles for certificates using qualified certificates statements and EU Qualified Certificates.

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for a deleted requirement is left and completed with "Void".
- The requirement identifier for a modified requirement is left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 ETSI EN 319 412 certificate profiles

4.1 General approach

All the certificate profiles specified in ETSI EN 319 412 (parts 2 [i.4], 3 [i.5], 4 [i.6], 5 [i.7] and the present document) are based upon IETF RFC 5280 [i.11] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3].