

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures (ETSI EN 319 412-1 V1.4.1 (2020-06))

Medieninhaber und Hersteller:

ÖVE Österreichischer Verband für Elektrotechnik
Austrian Standards Institute

Copyright © ÖVE/Austrian Standards Institute – 2020.

Alle Rechte vorbehalten! Nachdruck oder Vervielfältigung,
Aufnahme auf oder in sonstige Medien oder Datenträger nur
mit Zustimmung gestattet!

**Verkauf von in- und ausländischen Normen und
technischen Regelwerken durch**

Austrian Standards Institute
Heinestraße 38, 1020 Wien
E-Mail: sales@austrian-standards.at
Internet: www.austrian-standards.at
Webshop: www.austrian-standards.at/webshop
Tel.: +43 1 213 00-300
Fax: +43 1 213 00-818

Alle Regelwerke für die Elektrotechnik auch erhältlich bei
ÖVE Österreichischer Verband für Elektrotechnik
Eschenbachgasse 9, 1010 Wien
E-Mail: verkauf@ove.at
Internet: www.ove.at
Webshop: www.ove.at/shop
Tel.: +43 1 587 63 73

ICS 35.040; 35.240.60

Ident (IDT) mit ETSI EN 319 412-1 V1.4.1 (2020-06)

Ersatz für siehe nationales Vorwort

zuständig ÖVE/Komitee
TK IT-EG
Informationstechnologie, Telekommunikation und
Elektronik

Nationales Vorwort

Diese Europäische Norm EN 319 412-1 V1.4.1:2020 hat sowohl den Status einer nationalen elektrotechnischen Norm gemäß ETG 1992 als auch den einer nationalen Norm gemäß NormG 2016. Bei ihrer Anwendung ist dieses Nationale Vorwort zu berücksichtigen.

Für den Fall einer undatierten normativen Verweisung (Verweisung auf einen Standard ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste Ausgabe dieses Standards.

Für den Fall einer datierten normativen Verweisung bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Standards.

Der Rechtsstatus dieser nationalen (elektrotechnischen) Norm ist den jeweils geltenden Verordnungen zum Elektrotechnikgesetz zu entnehmen.

Bei mittels Verordnungen zum Elektrotechnikgesetz verbindlich erklärten nationalen (elektrotechnischen) Normen ist zu beachten:

- Hinweise auf Veröffentlichungen beziehen sich, sofern nicht anders angegeben, auf den Stand zum Zeitpunkt der Herausgabe dieser nationalen (elektrotechnischen) Norm. Zum Zeitpunkt der Anwendung dieser nationalen (elektrotechnischen) Norm ist der durch die Verordnungen zum Elektrotechnikgesetz oder gegebenenfalls auf andere Weise festgelegte aktuelle Stand zu berücksichtigen.
- Informative Anhänge und Fußnoten sowie normative Verweise und Hinweise auf Fundstellen in anderen, nicht verbindlichen Texten werden von der Verbindlicherklärung nicht erfasst.

Europäische Normen (EN) von ETSI werden gemäß den „Gemeinsamen Regeln“ von CEN/CENELEC durch Veröffentlichung eines identen Titels und Textes in das Gesamtwerk der nationalen (elektrotechnischen) Normen übernommen, wobei der Nummerierung der Zusatz ÖVE/ÖNORM vorangestellt wird.

Der von ETSI übermittelte Normentext wird in englischer Sprache veröffentlicht, da davon ausgegangen werden kann, dass die Anwender der Norm über ausreichende englische Sprachkenntnisse verfügen.

Erläuterung zum Ersatzvermerk

Gemäß Vorwort zur EN wird das späteste Datum, zu dem nationale (elektrotechnische) Normen, die der vorliegenden Norm entgegenstehen, zurückgezogen werden müssen, mit dow (date of withdrawal) festgelegt. Bis zum Zurückziehungsdatum (dow) 2021-03-31 ist somit die Anwendung folgender Norm(en) noch erlaubt:

ÖVE/ÖNORM EN 319 412-1 V1.1.1:2016-05-01.

ETSI EN 319 412-1 V1.4.1 (2020-06)



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

ReferenceREN/ESI-0019412-1v121

Keywordse-commerce, electronic signature, security,
trust services

ETSI650 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 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>

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.

© ETSI 2020.

All rights reserved.

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.

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.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 ETSI EN 319 412 certificate profiles	8
4.1 General approach.....	8
4.2 Overview of other parts of ETSI EN 319 412	8
4.2.1 ETSI EN 319 412-2	8
4.2.2 ETSI EN 319 412-3	8
4.2.3 ETSI EN 319 412-4	8
4.2.4 ETSI EN 319 412-5	9
5 Common data structures.....	9
5.1 Semantics identifiers	9
5.1.1 General.....	9
5.1.2 ASN.1 module	10
5.1.3 Natural person semantics identifier	10
5.1.4 Legal person semantics identifier	11
5.1.5 eIDAS Natural person semantics identifier	12
5.1.6 eIDAS Legal person semantics identifier	12
5.2 Certificate Extensions regarding Validity Assured Certificate.....	12
5.2.1 Validity Assured General.....	12
5.2.2 Validity Assured - Short Term.....	13
5.2.3 ASN.1 Module.....	13
Annex A (informative): Change History	14
History	15

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

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.

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".

National transposition dates	
Date of adoption of this EN:	18 June 2020
Date of latest announcement of this EN (doa):	30 September 2020
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2021
Date of withdrawal of any conflicting National Standard (dow):	31 March 2021

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 [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: "Codes for the representation of names of countries and their subdivisions".
- [3] ETSI TS 119 495: "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366".
- [4] ISO 17442: "Financial services - Legal Entity Identifier (LEI)".
- [5] eIDAS: "SAML Attribute Profile v1.2", 31 August 2019.

NOTE: available at <https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2>.

- [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.