

This is a preview of "DS/ETSI EN 319 412-2...". Click here to purchase the full version from the ANSI store.

Elektroniske signaturer og infrastrukturer (ESI) – Certifikatprofiler – Del t 2: Certifikatprofiler for certifikater udstedt til fysiske personer

Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
Part 2: Certificate profile for certificates issued to natural persons

DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
dansk.standard@ds.dk
www.ds.dk

This is a preview of "DS/ETSI EN 319 412-2...". Click here to purchase the full version from the ANSI store.

DS projekt: M341994

ICS: 35.240.30

Første del af denne publikations betegnelse er:

DS/ETS, hvilket betyder, at det er en europæisk telekommunikationsstandard, der har status som dansk standard.

Denne publikations overensstemmelse er:

IDT med: ETSI EN 319 412-2 V2.2.1 (2020-07)

DS-publikationen er på engelsk.

DS-publikationstyper

Dansk Standard udgiver forskellige publikationstyper.

Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

Dansk standard

- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

DS-information

- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

DS-håndbog

- samling af standarder, eventuelt suppleret med informativt materiale

DS-hæfte

- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives

- tillæg og rettelsesblade

DS-publikationsform

Publikationstyperne udgives i forskellig form som henholdsvis

- fuldttekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publikationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

DS-betegnelse

Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandard, eller at det er indført i hovedstandard.

DS-betegnelse angives på forsiden.

Overensstemmelse med anden publikation:

Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD

- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modificeret i forhold til en given publikation.

This is a preview of "DS/ETSI EN 319 412-2...". [Click here to purchase the full version from the ANSI store.](#)



**Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 2: Certificate profile for certificates issued
to natural persons**

This is a preview of "DS/ETSI EN 319 412-2...". Click here to purchase the full version from the ANSI store.

Reference

REN/ESI-0019412-2v221

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 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/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.

© 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.

This is a preview of "DS/ETSI EN 319 412-2...". [Click here to purchase the full version from the ANSI store.](#)

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 General certificate profile requirements.....	8
4.1 Generic requirements	8
4.2 Basic certificate fields	8
4.2.1 Version.....	8
4.2.2 Signature	8
4.2.3 Issuer.....	8
4.2.3.1 Legal person issuers	8
4.2.3.2 Natural person issuers	9
4.2.4 Subject	9
4.2.5 Subject public key info	10
4.3 Standard certificate extensions	10
4.3.1 Authority key identifier	10
4.3.2 Key usage.....	10
4.3.3 Certificate policies	11
4.3.4 Policy mappings.....	11
4.3.5 Subject alternative name	11
4.3.6 Issuer alternative name	11
4.3.7 Subject directory attributes	11
4.3.8 Name constraints	11
4.3.9 Policy constraints.....	11
4.3.10 Extended key usage	11
4.3.11 CRL distribution points	11
4.3.12 Inhibit any-policy.....	12
4.4 IETF RFC 5280 internet certificate extensions	12
4.4.1 Authority Information Access.....	12
5 EU Qualified Certificate requirements.....	12
5.1 EU QCStatements.....	12
5.2 Certificate policies.....	12
Annex A (informative): Change History	13
History	14

This is a preview of "DS/ETSI EN 319 412-2...". Click here to purchase the full version from the ANSI store.

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 2 of multi-part deliverable covering the Certificate Profiles. Full details of the entire series can be found in part 1 [i.4].

The present document was previously published as ETSI TS 102 280 [i.8].

National transposition dates	
Date of adoption of this EN:	6 July 2020
Date of latest announcement of this EN (doa):	31 October 2020
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 April 2021
Date of withdrawal of any conflicting National Standard (dow):	30 April 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.

This is a preview of "DS/ETSI EN 319 412-2...". [Click here to purchase the full version from the ANSI store.](#)

INTRODUCTION

ITU and ISO issued standards for certification of public keys in Recommendation ITU-T 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.5] 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] 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 identity certificate profiles, in particular when applications are used for digital 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.5] and in the wider international environment.

This is a preview of "DS/ETSI EN 319 412-2...". Click here to purchase the full version from the ANSI store.

1 Scope

The present document specifies requirements on the content of certificates issued to natural persons. This profile builds on IETF RFC 5280 [1] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3].

This profile supports the requirements of EU Qualified Certificates as specified in the Regulation (EU) No 910/2014 [i.5] as well as other forms of certificate. The scope of the present document is primarily limited to facilitate interoperable processing and display of certificate information. This profile therefore excludes support for some certificate information content options, which can be perfectly valid in a local context but which are not regarded as relevant or suitable for use in widely deployed applications.

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.

Certain applications or protocols impose specific requirements on certificate content. The present document is based on the assumption that these requirements are adequately defined by the respective application or protocol. It is therefore outside the scope of the present document to specify such application or protocol specific certificate content.

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 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [2] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".
- [3] IETF RFC 7230 to IETF RFC 7235: "Hypertext Transfer Protocol -- HTTP/1.1".
- [4] IETF RFC 4516: "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator".
- [5] IETF RFC 2818: "HTTP Over TLS".
- [6] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".