ICS 03.080.99, 35.020, 35.040 SLOVENSKÁ TECHNICKÁ NORMA Október 2025

STN	**Elektronické podpisy a dôveryhodné infraštruktúry (ESI) Profily certifikátu Časť 1: Prehľad a spoločné dátové štruktúry**	**STN EN 319 412-1 V1.6.1** 87 9412

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

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 09/25

Obsahuje: EN 319 412-1 V1.6.1:2025

141054

ETSI EN 319 412-1 V1.6.1 (2025-06)

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

Reference
REN/ESI-0019412-1v161

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

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Trust 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".

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

National transposition dates	
Date of adoption of this EN:	12 June 2025
Date of latest announcement of this EN (doa):	30 September 2025
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 March 2026
Date of withdrawal of any conflicting National Standard (dow):	31 March 2026

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.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 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 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 Regulation (EU) No 910/2014 [i.9] and the 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 in the ETSI docbox.

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 Trust 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)".

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

[8] EUID CIR: "Commission Implementing Regulation (EU) 2021/1042 of 18 June 2021 laying down rules for the application of Directive (EU) 2017/1132 of the European Parliament and of the Council as regards technical specifications and procedures for the system of interconnection of registers and repealing Commission Implementing Regulation (EU) 2020/2244 (EUID)".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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 Trust 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 Trust 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 Trust Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates".

[i.7] ETSI EN 319 412-5: "Electronic Signatures and Trust 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".

[i.15] EPREL CIR: "Commission Implementing Regulation (EU) 2024/994 of 2 April 2024 laying down operational details of the product database established under Regulation (EU) 2017/1369 of the European Parliament and of the Council".

[i.16] Council Directive 2020/1756 of 20 November 2020 amending Directive 2006/112/EC on the common system of value added tax as regards the identification of taxable persons in Northern Ireland.

[i.17] ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".