![SIST logo]

SLOVENSKI STANDARD
oSIST prEN 319 412-4 V1.2.0:2021

01-oktober-2021

Elektronski podpisi in infrastruktura (ESI) - Profili potrdil - 4. del: Profil potrdila za potrdila za spletna mesta

Electronic Signatures and Infrastructures (ESI) - Certificate Profiles - Part 4: Certificate profile for web site certificates

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: ~~oSIST prEN 319 412-4 V1.2.0:2021~~ **ETSI EN 319 412-4 V1.2.0 (2021-08)**

<u>**ICS:**</u>

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

oSIST prEN 319 412-4 V1.2.0:2021   **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Draft ETSI EN 319 412-4 V1.2.0 (2021-08)

EUROPEAN STANDARD

Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 4: Certificate profile for web site certificates

Reference

REN/ESI-0019412-4v121

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 - 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:
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

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.

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 4 of multi-part deliverable covering the Certificates Profiles. Full details of the entire series can be found in part 1 [i.5].

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 ITU X.509 | ISO/IEC 9594-8 [i.4] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.3] 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 the Directive 1999/93/EC [i.2] 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.

The CA/Browser Forum released the Extended Validation Certificate Guidelines [3] and the Baseline Requirements for the issuance and management of publicly trusted TLS/SSL certificates [2] to mitigate website spoofing attacks.

The present document aims to maximize the interoperability of systems issuing and using certificates both in the European context under the Regulation (EU) No 910/2014 [i.3] and in the wider international environment, also by meeting requirements from CA Browser Forum.

1 Scope

The present document specifies a certificate profile for web site certificates that are accessed by the TLS protocol [i.1].

The profile defined in the present document builds on the CA/Browser Forum Baseline requirements [2], Extended validation guidelines [3] and other parts of the present multipart deliverable.

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.

This profile can be used for legal and natural persons. For certificates issued to legal persons, the profile builds on the CAB Forum EV Profile [3] or baseline requirements [2]. For certificates issued to natural persons, the profile builds only on CAB Forum baseline requirements [2].

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

[2]   CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[3]   CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

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

[5]   ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

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

[7]   ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

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

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

[i.2]   Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.3]   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.4]   Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.5]   ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

3   Definition of terms, symbols and abbreviations

3.1   Terms

For the purposes of the present document, the terms given in ETSI EN 319 412-1 [i.5] apply.

3.2   Symbols

Void.

3.3   Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-1 [i.5] and the following apply:

TLS   Transport Layer Security

4   Profile requirements

4.1   Generic profile requirements

4.1.1   Certificates following DVCP, IVCP or OVCP

For certificates issued following the certificate policies DVCP, IVCP or OVCP, as defined in ETSI EN 319 411-1 [6], all certificate fields and extensions shall comply with requirements on subscriber certificates stated in the BRG [2].

NOTE: According to BRG [2], section 7.1.6.4 implementations systems complying to the certificate policy for domain-validated certificates 2.23.140.1.2.1 cannot contain natural person or legal person related attributes.

Certificates following IVCP or OVCP may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.1.2　　Certificates following EVCP or QEVCP-w

For certificates issued following the certificate policies EVCP, as defined in ETSI EN 319 411-1 [6], or QEVCP-w, as defined in ETSI EN 319 411-2 [7], all certificate fields and extensions shall comply with requirements on subscriber certificates stated in the EVCG [3], with the amendments specified in clauses 4.2 and 4.3 of the present document for EU Qualified Certificates.

Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.5] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.1.3　　Certificates following NCP or QNCP-w

For certificates issued following the certificate policies NCP, as defined in ETSI EN 319 411-1 [6], or QNCP-w, as defined in ETSI EN 319 411-2 [7], the following requirements apply:

NCP-w-1: If the certificate is issued to a natural person the requirements specified in ETSI EN 319 412-2 [4] clause 4.2 shall apply.

NCP-w-2: If the certificate is issued to a legal person the requirements specified in ETSI EN 319 412-3 [5] clause 4.2 shall apply.

NCP-w-3: The following certificate profile requirements specified in the BRG [2], section 7.1 shall apply:

a) 7.1.1: version number

b) 7.1.2.3: Subscriber Certificate profile: excluding requirement that the certificatePolicies:policyIdentifier "indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these [BRG] Requirements"

c) 7.1.2.4: All certificates: except that the size limits specified in IETF RFC 5280 [8] may be relaxed as specified in ETSI EN 319 412-2 [4] and ETSI EN 319 412-3 [5]

d) 7.1.4.2: Subject Information - Subscriber Certificates

e) 7.1.6.1: Reserved Certificate Policy Identifiers

NCP-w-4: The amendments specified in clauses 4.2 and 4.3 of the present document apply for EU Qualified Certificates.

NCP-w-5: Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1 [i.4] to provide relevant semantics definitions to determine the identity of the subject of the certificate.

4.2　　EU Qualified Certificate statements for Certificates following QEVCP-w or QNCP-w

When certificates are issued as EU Qualified Certificates, they shall include `QCStatements` as specified in clauses 4 and 5 of ETSI EN 319 412-5 [1].

4.3　　Certificate policies for Certificates following QEVCP-w or QNCP-w

When the certificates are issued as EU Qualified Certificates, they should include, in the certificate policies extension, one of the certificate policy identifiers defined in clause 5.3 of ETSI EN 319 411-2 [7]. Policy identifiers included in the certificate policies extension of EU Qualified Certificates shall be consistent with the EU Qualified Certificate Statements according to clause 4.2.