ETSI TS 119 411-6 V1.1.1 (2023-08)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Trust Service Providers issuing certificates;
Part 6: Requirements for Trust Service Providers
issuing publicly trusted S/MIME certificates

Reference
DTS/ESI-0019411-6

Keywords
digital certificate, S/MIME, secure e-mail,
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 4
Foreword 4
Modal verbs terminology 4
Introduction 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 6
3 Definition of terms, symbols, abbreviations and notation 6
3.1 Terms 6
3.2 Symbols 6
3.3 Abbreviations 6
3.4 Notation 6
4 General concepts 7
4.1 General policy requirements concepts 7
4.2 Certificate Policy and Certification Practice Statement 7
4.2.1 Certification Practice Statement 7
4.2.2 Certification Policy 7
4.2.2.1 Certificate Policy General Concepts 7
4.2.2.2 ETSI Defined Policies 8
4.2.2.3 SBR Defined Policies 8
4.2.3 Terms and conditions and PKI disclosure statement 9
4.3 Certification services 9
5 General provisions on Certification Practice Statement and Certificate Policies 9
5.1 General requirements 9
5.2 Certificate Policy name and identification 9
6 Framework for the definition of other certificate policies built on the present document 10
6.1 Certificate Policy management 10
Annex A (informative): Policy identifiers for S/MIME certificates 11
A.1 ETSI Defined Certificate Policies 11
A.2 SBR Defined Certificate Policies 11
History 13

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 Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document is part 6 of a multi-part deliverable covering the policy and security requirements for Trust Service Providers issuing certificates. Full details of the entire series can be found in part 1 [2].

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

The CA/Browser Forum published "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" [1]. Those "S/MIME Baseline Requirements" (SBR) specify technologies, protocols, identity-proofing, lifecycle management, and auditing requirements for a Trust Service Provider issuing publicly-trusted S/MIME certificates used to encrypt and/or to apply electronic signatures to email messages.

The S/MIME Baseline Requirements (SBR) [1], clause 8.4 specifies the audit criteria that may be used by a Trust Service Provider to assert compliance with that standard.

The present document incorporates the policy and security requirements as specified in ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3] and adds further requirements to facilitate TSPs seeking to comply with the S/MIME Baseline Requirements (SBR) [1], clause 8.4.

1 Scope

The present document specifies policy and security requirements for the issuance, maintenance and life-cycle management of S/MIME certificates as defined in the S/MIME Baseline Requirements (SBR) [1] in the context of the ETSI *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates* series.

An S/MIME certificate for the purposes of the present document can be identified by the existence of an Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4) and the inclusion of an email address (in the form of an rfc822Name or an otherName of type id-on-SmtpUTF8Mailbox) in the subjectAltName extension.

These policy and security requirements support reference certificate policies for the issuance, maintenance and life-cycle management of S/MIME certificates issued to mailboxes (containing only an email address), natural persons (including natural persons associated with a legal person) and to legal persons, respectively.

The present document does not specify how the requirements identified can be assessed by an independent party, including requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 1: See ETSI EN 319 403-1 [i.1] for guidance on assessment of TSP's processes and services, expanded as relevant by ETSI TS 119 403-2 [i.2] for additional requirements for publicly-trusted certificates, and by ETSI TS 119 403-3 [i.3] for additional requirements for EU qualified TSPs.

NOTE 2: The present document integrates all the policy requirements of the CA/Browser Forum S/MIME Baseline Requirements (SBR) [1] with ETSI EN 319 411-1 [2] for the [LCP], [NCP], and/or [NCP+] certificate policies, and with ETSI EN 319 411-2 [3] for the [QCP-l], [QCP-n], [QCP-l-qscd], and/or [QCP-n-qscd] certificate policies.

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] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (S/MIME Baseline Requirements (SBR)).

[2] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".

[3] 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 ".

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] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.2] ETSI TS 119 403-2: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates".

[i.3] ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

3 Definition of terms, symbols, abbreviations and notation

3.1 Terms

For the purposes of the present document, the terms given in the S/MIME Baseline Requirements (SBR) [1] and ETSI EN 319 411-1 [2] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in the S/MIME Baseline Requirements (SBR) [1], ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3] apply.

3.4 Notation

The requirements identified in the present document include:

a) requirements applicable to any Certificate Policy. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) requirements applicable to the services offered under the applicable Certificate Policy. Such requirements are indicated by clauses marked by the applicable Certificate Policy as follows "[LCP]", "[NCP]", "[NCP+]", "[QCP-l]", "[QCP-n]", "[QCP-l-qscd]", and/or "[QCP-n-qscd]".

Each requirement is identified as follows:

<3 letters service component> **-** < the clause number> **-** <2 digit number – incremental>.

The service components are:

- **OVR:** General requirement (requirement applicable to more than 1 component).
- **GEN:** Certificate Generation Services.
- **REG:** Registration Services.
- **REV:** Revocation Services.
- **DIS:** Dissemination Services.
- **SDP:** Subject Device Provisioning.
- **CSS:** Certificate Status Service.

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 deleted requirements is left and completed with "Void".
- The requirement identifier for modified requirement is left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 General concepts

4.1 General policy requirements concepts

ETSI EN 319 411-1 [2], clause 4.1 applies.

4.2 Certificate Policy and Certification Practice Statement

4.2.1 Certification Practice Statement

The explanations identified in ETSI EN 319 411-1 [2], clause 4.2.1 apply.

4.2.2 Certification Policy

4.2.2.1 Certificate Policy General Concepts

The explanations identified in ETSI EN 319 411-1 [2], clause 4.2.2 apply.

The intent of the present document is to define requirements so that a TSP issuing S/MIME certificates that assert the policy identifiers described in ETSI EN 319 411-1 [2] and ETSI EN 319 411-2 [3] may also appropriately assert the policy identifiers described in the S/MIME Baseline Requirements (SBR) [1].

Clause 5.2 specifies how these policy identifiers can be combined in the certificatePolicies extension.

Clause 6 specifies a framework for other certificate policies which enhance or further constrain these policies.

4.2.2.2 ETSI Defined Policies

The present document specifies how a TSP can issue S/MIME certificates that are based on the following policy requirements specified in ETSI EN 319 411-1 [2]:

1) requirements of the Lightweight Certificate Policy (LCP);
2) requirements of the Normalized Certificate Policy (NCP); and
3) requirements of the enhanced Normalized Certificate Policy (NCP+).

In addition, the present document specifies how a TSP can issue S/MIME certificates that are based on the following policy requirements specified ETSI EN 319 411-2 [3]:

4) requirements for EU qualified certificates issued to natural persons (QCP-n);
5) requirements for EU qualified certificates issued to legal persons (QCP-l);
6) requirements for EU qualified certificates issued to natural persons where the private key related to the certified public key resides on a QSCD (QCP-n-qscd); and
7) requirements for EU qualified certificates issued to legal persons where the private key related to the certified public key resides on a QSCD (QCP-n-qscd).

4.2.2.3 SBR Defined Policies

The S/MIME Baseline Requirements (SBR) [1], clause 1.2 defines 12 S/MIME certificate policies that can be combined with the certificate policies defined in clause 4.2.2.1 of the present document:

1) requirements for Mailbox-validated - Legacy;
2) requirements for Mailbox-validated - Multipurpose;
3) requirements for Mailbox-validated - Strict;
4) requirements for Organization-validated - Legacy;
5) requirements for Organization-validated - Multipurpose;
6) requirements for Organization-validated - Strict;
7) requirements for Sponsor-validated - Legacy;
8) requirements for Sponsor-validated - Multipurpose;
9) requirements for Sponsor-validated - Strict;
10) requirements for Individual-validated - Legacy;
11) requirements for Individual-validated - Multipurpose; and
12) requirements for Individual-validated - Strict.

Use of the SBR certificate policies requires the TSP to follow the full and latest version of the SBR. As a consequence, for compliance with the SBR the TSP is required to augment the policy requirements defined in the present document with any additional requirements specific to the SBR policy.

It is recognized that further updates of the SBR may occur after the publication of the present document. In case of conflicting requirements between latest version of the SBR and the present document, it is requested that this is brought to the attention of ETSI TC ESI and the CA/Browser Forum. ETSI TC ESI will endeavour to monitor revisions to the SBR and reference the latest version within the revision cycle of the present document.

4.2.3 Terms and conditions and PKI disclosure statement

The guidelines identified in ETSI EN 319 411-1 [2], clause 4.2.3 apply.

4.3 Certification services

The guidelines identified in ETSI EN 319 411-1 [2], clause 4.3 apply.

5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

OVR-5.1-01: [LCP] or [NCP] or [NCP+]: All the applicable requirements for the certification policy supported, as identified in ETSI EN 319 411-1 [2], shall be applied.

OVR-5.1-02: [QCP-n] or [QCP-l] or [QCP-n-qscd] or [QCP-l-qscd]: All the applicable requirements for the certification policy supported, as identified in ETSI EN 319 411-2 [3], shall be applied.

OVR-5.1-03: All the applicable requirements for the certification policy supported, as identified in the S/MIME Baseline Requirements (SBR) [1], shall be applied.

OVR-5.1-04: In case of conflict between any requirement in the current version of the present document, the latest version of the SBR takes precedence, unless a requirement in ETSI EN 319 411-1 [2] or ETSI EN 319 411-2 [3] is more stringent, in which case it remains applicable.

OVR-5.1-05: [QCP-n] or [QCP-l] or [QCP-n-qscd] or [QCP-l-qscd]: In the case of Qualified certificates, the requirements of the applicable regulation shall be met.

5.2 Certificate Policy name and identification

As described in IETF RFC 3647 [i.4], clause 3.3 certificates include a Certificate Policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

Including one or more of the policy identifiers defined below in an S/MIME certificate indicates that the certificate is issued and managed according to the present document for that policy:

- The policy identifiers for [LCP], [NCP], and [NCP+] are described in ETSI EN 319 411-1 [2], clause 5.3.
- The policy identifiers for [QCP-n], [QCP-l], [QCP-n-qscd], and [QCP-l-qscd] are described in ETSI EN 319 411-2 [3], clause 5.3.
- The SBR policy identifiers are described in the S/MIME Baseline Requirements (SBR) [1], clause 7.1.6.1.

For convenience, the policy identifiers are identified in an informative Annex A to the present document.

OVR-5.2-01: The policy requirements, including policy identifiers, for the SBR Mailbox-validated policies shall only be used in combination with the [LCP] policy requirements.

OVR-5.2-02: The policy requirements, including policy identifiers, for the SBR Organization-validated policies shall only be used in combination with the [LCP] or [NCP] or [NCP+] or [QCP-l] or [QCP-l-qscd] policy requirements.

OVR-5.2-03: The policy requirements, including policy identifiers, for the SBR Sponsor-validated policies shall only be used in combination with the [LCP] or [NCP] or [NCP+] or [QCP-n] or [QCP-n-qscd] policy requirements.

OVR-5.2-04: The policy requirements, including policy identifiers, for the SBR Individual-validated policies shall only be used in combination with the [NCP] or [NCP+] or [QCP-n] or [QCP-n-qscd] policy requirements.

6 Framework for the definition of other certificate policies built on the present document

6.1 Certificate Policy management

OVR-6.1-01: [LCP] or [NCP] or [NCP+]: The requirements identified in ETSI EN 319 411-1 [2], clause 7 shall apply.

OVR-6.1-02: [QCP-n], [QCP-l], [QCP-n-qscd], and [QCP-l-qscd]: The requirements identified in ETSI EN 319 411-2 [3], clause 7 shall apply.

OVR-6.1-03: The Certificate Policy shall incorporate, or further constrain, all the requirements identified in clause 5 of the present document, as appropriate to the usage, building on the requirements of the appropriate certificate policies as referenced in the present document.

Annex A (informative): Policy identifiers for S/MIME certificates

A.1 ETSI Defined Certificate Policies

The policy identifiers for the ETSI certificate policies described in clause 5.2 of the present document are:

a) [LCP] Lightweight Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-
identifiers(1) lcp (3)
```

b) [NCP] Normalized Certificate Policy

```
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-
identifiers(1) ncp (1)
```

c) [NCP+] Normalized Certificate Policy requiring a secure cryptographic device

```
itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-
identifiers(1) ncpplus (2)
```

d) [QCP-n] Certificate Policy for EU qualified certificates issued to natural persons;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-
identifiers(1) qcp-natural (0)
```

e) [QCP-l] Certificate Policy for EU qualified certificates issued to legal persons;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-
identifiers(1) qcp-legal (1)
```

f) [QCP-n-qscd] Certificate Policy for EU qualified certificates issued to natural persons where the private key related to the certified public key reside on a QSCD;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-
identifiers(1) qcp-natural-qscd (2)
```

g) [QCP-l-qscd] Certificate Policy for EU qualified certificates issued to legal persons where the private key related to the certified public key reside on a QSCD;

```
itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-
identifiers(1) qcp-legal-qscd (3)
```

A.2 SBR Defined Certificate Policies

The policy identifiers for the SBR certificate policies described in clause 7.1.6.1 of the S/MIME Baseline Requirements (SBR) [1] are:

a) Mailbox-validated - Legacy

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) mailbox-validated (1) legacy (1)
```

b) Mailbox-validated - Multipurpose

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) mailbox-validated (1) multipurpose (2)
```

c) Mailbox-validated - Strict

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) mailbox-validated (1) strict (3)
```

d) Organization-validated - Legacy

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) organization-validated (2) legacy (1)
```

e) Organization-validated - Multipurpose

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) organization-validated (2) multipurpose (2)
```

f) Organization-validated - Strict

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) organization-validated (2) strict (3)
```

g) Sponsor-validated - Legacy

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) sponsor-validated (3) legacy (1)
```

h) Sponsor-validated - Multipurpose

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)
```

i) Sponsor-validated - Strict

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) sponsor-validated (3) strict (3)
```

j) Individual-validated - Legacy

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) individual-validated (4) legacy (1)
```

k) Individual-validated - Multipurpose

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)
```

l) Individual-validated - Strict

```
joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-
policies(1) smime-baseline(5) individual-validated (4) strict (3)
```

History

Document history		
V1.1.1	August 2023	Publication