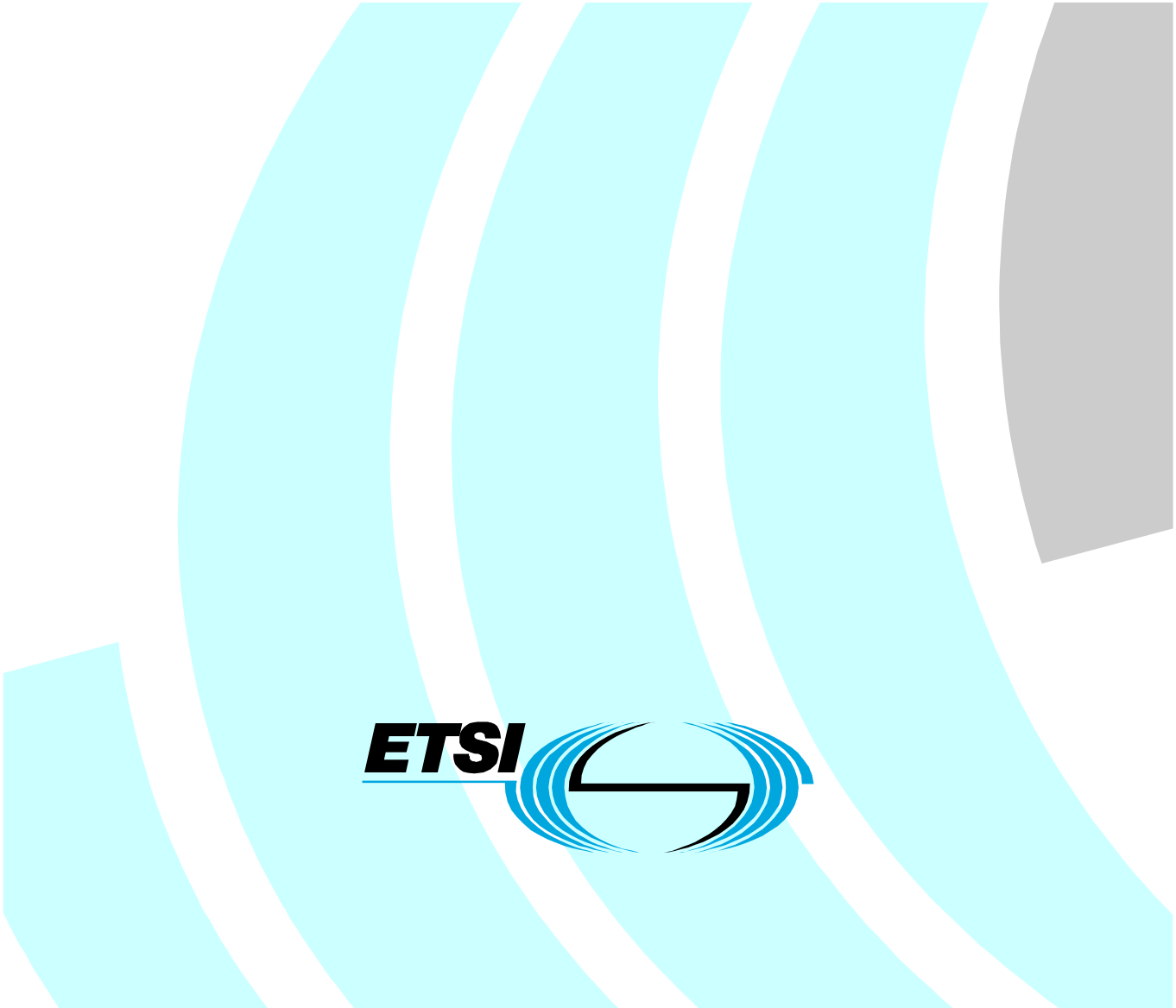
ETSI TS 102 280 V1.1.1 (2004-03)

Technical Specification

X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons



Reference
DTS/ESI-000018

Keywords
electronic signature, IP, profile, security

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Abbreviations 7
4 Document structure and terminology 7
4.1 Document structure 7
4.2 Terminology 7
5 Profile requirements 7
5.1 Generic requirements 7
5.2 Basic certificate fields 8
5.2.1 Version 8
5.2.2 Serial number 8
5.2.3 Signature 8
5.2.4 Issuer 8
5.2.5 Validity 8
5.2.6 Subject 8
5.2.7 Subject public key info 9
5.3 X.509 version 2 certificate fields 9
5.4 Standard certificate extensions 9
5.4.1 Authority key identifier 9
5.4.2 Subject key identifier 9
5.4.3 Key usage 9
5.4.4 Private key usage period 10
5.4.5 Certificate policies 10
5.4.6 Policy mappings 10
5.4.7 Subject alternative name 10
5.4.8 Issuer alternative name 10
5.4.9 Subject directory attributes 10
5.4.10 Basic constraints 10
5.4.11 Name constraints 11
5.4.12 Policy constraints 11
5.4.13 Extended key usage 11
5.4.14 CRL distribution points 11
5.4.15 Inhibit any-policy 11
5.4.16 Freshest CRL 11
5.5 RFC 3280 internet certificate extensions 11
5.5.1 Authority Information Access 11
5.5.2 Subject information access 11
5.6 RFC 3739 certificate extensions 11
5.6.1 Biometric information 11
5.6.2 Qualified certificate statement 12
Annex A (informative): Important requirements from referenced standards 13
A.1 Scope and structure 13
A.2 Basic certificate fields 13
A.2.1 Version 13
A.2.2 Serial number 13
A.2.3 Signature 13
A.2.4 Issuer 13
A.2.5 Validity 14

A.2.6 Subject 14
A.2.7 Subject public key info 14
A.3 X.509 version 2 certificate fields 14
A.4 Standard certificate extensions 14
A.4.1 Authority key identifier 14
A.4.2 Subject key identifier 15
A.4.3 KeyUsage 15
A.4.4 Private key usage period 15
A.4.5 Certificate policies 15
A.4.6 Policy mappings 15
A.4.7 Subject alternative name 16
A.4.8 Issuer alternative name 16
A.4.9 Subject directory attributes 16
A.4.10 Basic constraints 16
A.4.11 Name constraints 16
A.4.12 Policy constraints 16
A.4.13 Extended key usage 16
A.4.14 CRL distribution points 16
A.4.15 Inhibit any-policy 17
A.4.16 Freshest CRL 17
A.5 RFC 3280 internet certificate extensions 17
A.5.1 Authority information access 17
A.5.2 Subject information access 17
A.6 RFC 3739 certificate extensions 17
A.6.1 Biometric information 17
A.6.2 Qualified certificate statement 18
History 19

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://webapp.etsi.org/IPR/home.asp).

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.

Foreword

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

Introduction

The present document defines a common profile for X.509 based certificates issued to natural persons.

The Directive of the European Parliament and of the Council on a Community framework for electronic signatures (1999/93/EC [1]) defines requirements on a specific type of certificates named "Qualified Certificates". Implementation of the Directive 1999/93/EC [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 certificates 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.

1 Scope

The present document defines a common profile for ITU-T Recommendation X.509 [2] based certificates issued to natural persons. The scope of the present document is to provide a certificate profile, which will allow actual interoperability of certificates issued for the purposes of qualified electronic signatures, peer entity authentication and data authentication.

This profile depends on the Internet standards RFC 3280 [3] and RFC 3739 [4] for generic profiling of ITU-T Recommendation X.509 [2], and depends on the ETSI standard TS 101 862 [5] to define implementation of requirements defined by the Electronic Signature Directive 1999/93/EC [1] Annexes I and II.

The scope of the present document is primary limited to facilitate interoperable processing and display of certificate information in existing deployments of ITU-T Recommendation X.509 [2]. It is thus important to note that this profile deliberately has excluded support for some certificate information content options, which may 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. Guidance for implementers is provided for cases in which near term developments are affected.

This certificate profile recognizes the natural need for reasonable variations of implementation which does not negatively affect generic interoperability. This is e.g. valid for different ways to encode a certificate holder's identity.

Certain applications or protocols impose specific requirements on certificate content such as IP-sec, Network logon, S/MIME, IEEE 802.1x [12] EAP. 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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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

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

[3] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[4] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[5] ETSI TS 101 862: "Qualified Certificate profile".

[6] IETF RFC 2119: "Key words for use in RFCs to Indicate Requirement Levels".

[7] IETF RFC 3279: "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[8] ETSI SR 002 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

[9] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[10] IETF RFC 2255: "The LDAP URL Format".

[11] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[12] IEEE 802.1x: "IEEE Standard for Port Based Network Access Control".

[13] RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CRL	Certificate Revocation List
DS	Digital Signature
KEA	Key Encipherment or Agreement
NR	Non-Repudiation
OCSP	Online Certificate Status Protocol
OID	Object Identifier

4 Document structure and terminology

4.1 Document structure

The present document profiles the use of other standards.

Clause 4 contains the profiling requirements defined by the present document. This clause does not repeat the base requirements of the referenced standards.

Annex A is an informative annex which, for convenience purposes only, lists some important requirements from referenced standards that are relevant for the understanding of the present document.

4.2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in the present document are to be interpreted as described in RFC 2119 [6].

5 Profile requirements

5.1 Generic requirements

All certificate fields and extensions SHALL, where applicable, comply with RFC 3280 [3], RFC 3739 [4] and TS 101 862 [5] with the amendments specified in the present document. When "No specific requirements" is stated for a particular field or extension, this means that no specific requirements apply except for those stated by RFC 3280 [3], RFC 3739 [4] and TS 101 862 [5].

In case of discrepancies between the present specification and the named standards above, the present document is the normative one.

5.2 Basic certificate fields

5.2.1 Version

Certificates compliant with the present document SHALL be ITU-T Recommendation X.509 [2] version 3 certificates.

5.2.2 Serial number

No specific requirements.

5.2.3 Signature

Signature algorithm SHALL be specified according to RFC 3279 [7] and SR 002 176 [8].

It is strongly RECOMMENDED to use sha1WithRSAEncryption when maximum interoperability with open environment deployments is a requirement.

5.2.4 Issuer

The identity of the issuer SHALL be specified using an appropriate subset of the following attributes:

```
countryName,
organizationName,
organizationalUnitName, (multiple instances may be present)
stateOrProvinceName,
localityName,
commonName,
serialNumber, and
domainComponent.
```

Additional attributes MAY be present but they SHOULD NOT be necessary to identify the issuing organization.

The attributes `countryName` and `organizationName` SHALL be present. The `organizationName` attribute SHALL contain the full registered name of the certificate issuing organization and `countryName` SHALL contain the country within which the issuing organization is registered.

If any value of the `domainComponent` attributes contain information associated with a country, then this has no meaning beyond describing the issuer's internet domain. If a `domainComponent` attribute value indicates a different country than the `countryName` attribute value, then determination of the country of registration of the issuing organization SHALL exclusively be determined though the `countryName` attribute, disregarding any `domainComponent` attribute values.

NOTE: Use of `domainComponent` attributes in addition to the mandatory attributes `countryName` and `organizationName` is possible but it may cause conflict if the issuer name is used as distinguished name for directory entries. Implementing CAs should carefully select their issuing name in compliance with any directory infrastructure they operate within.

5.2.5 Validity

No specific requirements.

5.2.6 Subject

The subject field SHALL contain an appropriate subset of the following attributes:

```
domainComponent,
countryName,
commonName,
surname,
givenName,
serialNumber,
title,
```

```
organizationName,
organizationalUnitName,
stateOrProvinceName, and
localityName.
```

Other attributes may be present but SHALL NOT be necessary to distinguish the subject name from other subject names within the issuer domain.

The subject field SHALL include at least one of the following choice of attributes:

Choice I: `commonName`

Choice II: `givenName` and `surname`

NOTE: The use of domainComponent attributes is often used as alternative to the subject attributes countryName and organizationName. Use of domainComponent attributes in addition to these attributes is not invalid but may cause conflict if the subject name is used as distinguished name for directory entries. Implementing CAs should carefully select their subject naming in compliance with any directory infrastructure they operate within.

5.2.7 Subject public key info

The subject public key SHALL be included according to RFC 3279 [7] and SR 002 176 [8].

It is strongly RECOMMENDED to use rsaEncryption when maximum interoperability with open environment deployments is a requirement.

5.3 X.509 version 2 certificate fields

The ITU-T Recommendation X.509 [2] version 2 certificate fields Issuer and Subject Unique Identifier SHALL NOT be present.

5.4 Standard certificate extensions

5.4.1 Authority key identifier

The authority key identifier extension SHALL be present, containing a key identifier for the issuing CA's public key.

5.4.2 Subject key identifier

No specific requirements.

5.4.3 Key usage

The following key usage settings are named in this profile as type A, B, C, D and E:

Type	Non-Repudiation [NR] (Bit 1)	Digital Signature [DS] (Bit 0)	Key Encipherment or Agreement [KEA] (Bit 2 or 4)
A	X		
B	X	X	
C		X	
D		X	X
E			X

In cases where a certificate is intended to be used to validate commitment to signed content, such as electronic signatures on agreements and/or transactions, then the key usage combination SHALL be limited to type A or B. This means that the non-repudiation bit (bit 1) SHALL be set. Of these alternatives it is RECOMMENDED to use the type A setting only (see the security note below).

For all other certificates compliant with this profile, key usage settings SHALL be limited to type C, D or E.

If the certificate is declared to be a Qualified Certificate according to TS 101 862 [5] then the key usage setting SHALL be limited to type A, B or C.

NOTE: Choice of bit 2 or bit 4 for expressing [KEA] is dependent on the algorithm type specified in subject public key info (clause 5.2.7 Subject public key info). Appropriate values for RSA keys are referenced in clause A.4.3.

Security note:

Combining the non-repudiation bit (bit 1) in the keyUsage certificate extension with other keyUsage bits may have security implications depending on the security environment in which the certificate is to be used.

If the subject's environment can be fully controlled and trusted, then there are no specific security implications. For example, in cases where the subject is fully confident about exactly which data is signed or cases where the subject is fully confident about the security characteristics of the authentication protocol being used.

If the subject's environment is not fully controlled or not fully trusted, then unintentional signing of commitments is possible. Examples include the use of badly formed authentication exchanges and the use of a rogue software component.

If untrusted environments are used by a subject, these security implications can be limited through use of the following measures:

- to not combine non-repudiation key usage setting in certificates with any other key usage setting and to use the corresponding private key only with this certificate;
- to limit the use of private keys associated with certificates that have the non-repudiation key usage bit set, to environments which are considered adequately controlled and trustworthy.

5.4.4 Private key usage period

No specific requirements.

5.4.5 Certificate policies

This extension SHOULD NOT be marked critical.

5.4.6 Policy mappings

This extension is not applicable to end entity certificates addressed by the present document.

5.4.7 Subject alternative name

This extension SHALL NOT be marked critical.

5.4.8 Issuer alternative name

This extension SHALL NOT be marked critical.

5.4.9 Subject directory attributes

The subject directory attributes extension, if present, SHALL NOT be used to store any of the identification attribute listed in clause 5.2.6.

5.4.10 Basic constraints

No specific requirements.

5.4.11 Name constraints

This extension is not applicable to end entity certificates addressed by the present document.

5.4.12 Policy constraints

This extension is not applicable to end entity certificates addressed by the present document.

5.4.13 Extended key usage

This extension SHALL NOT be marked critical.

5.4.14 CRL distribution points

The CRL distribution point extension SHALL be present.

At least one reference to a publicly available CRL SHALL be present.

At least one of the present references SHALL use either http (http://) RFC 2616 [9] or ldap (ldap://) RFC 2255 [10] scheme.

The extension SHALL NOT be marked critical.

Compliant issuing CAs MAY support other certificate status checking services, such as OCSP, in addition to support of CRL through this extension.

5.4.15 Inhibit any-policy

This extension is not applicable to end entity certificates addressed by the present document.

5.4.16 Freshest CRL

No specific requirements.

5.5 RFC 3280 internet certificate extensions

5.5.1 Authority Information Access

The Authority Information Access extension SHOULD include an `accessMethod` OID, `id-ad-caIssuers`, with an `accessLocation` value specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location SHOULD use the either http (http://) RFC 2616 [9] scheme.

This recommendation MAY be ignored altogether when the issuing CA is represented by a self signed root certificate.

5.5.2 Subject information access

No specific requirements.

5.6 RFC 3739 certificate extensions

5.6.1 Biometric information

No specific requirements.

5.6.2 Qualified certificate statement

Certificates declared as Qualified Certificates SHALL comply with TS 101 862 [5] regarding use of this extension.

Annex A (informative): Important requirements from referenced standards

A.1 Scope and structure

Annex A lists important requirements and recommendations from referenced standards which are considered important for implementation of the present document.

Annex A is included for convenience in order to facilitate a better understanding of the requirements of the present document in situations where the reader does not have all referenced standards available or in situations where the reader wishes to obtain a brief understanding of the present document without having to review the complex set of referenced standards. All referenced standards in annex A are listed in clause 2 of the present document.

The list of requirements and recommendations is not exhaustive. The referenced standards are necessary to obtain full understanding of listed requirements and recommendations.

A.2 Basic certificate fields

A.2.1 Version

No specific requirement listed.

A.2.2 Serial number

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.1.2.2	Serial number of the certificate SHALL be a positive (non-negative) integer. Serial number SHALL NOT be longer than 20 octets.

A.2.3 Signature

Referenced standard	Section	Requirement or recommendation
RFC 3279 [7]	2.2.1	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

A.2.4 Issuer

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.1.2.4	All certificates issued after December 31, 2003 SHALL use the UTF8String encoding of DirectoryString.
RFC 3739 [4]	3.1.1	The issuer field SHALL identify the organization responsible for issuing the certificate. The name SHOULD be an officially registered name of the organization.

A.2.5 Validity

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.1.2.5	CAs conforming to this profile SHALL always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later SHALL be encoded as GeneralizedTime.

A.2.6 Subject

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.1.2.6	When encoding attribute values of type DirectoryString, the encoding rules for the issuer field SHALL be implemented (RFC 3280 [3] section 4.1.2.4).
RFC 3739 [4]	3.1.2	The countryName attribute value specifies a general context in which other attributes are to be understood. The country attribute does not necessarily indicate the subject's country of citizenship or country of residence, nor does it have to indicate the country of issuance. Many X.500 implementations require the presence of countryName in the DIT. In cases where the subject name, as specified in the subject field, specifies a public X.500 directory entry, the countryName attribute SHOULD always be present. It is the CA's responsibility to ensure that the serialNumber attribute is sufficient to resolve any subject name collisions.

A.2.7 Subject public key info

Referenced standard	Section	Requierement or recommendation
RFC 3279 [7]	2.3.1	The OID rsaEncryption identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}

A.3 X.509 version 2 certificate fields

No specific requirement listed.

A.4 Standard certificate extensions

A.4.1 Authority key identifier

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.1	The keyIdentifier field of the authorityKeyIdentifier extension SHALL be included in all end entity certificates. The value of the keyIdentifier field SHOULD be derived from the public key used to verify the certificate's signature or a method that generates unique values. Two common methods for generating key identifiers from the public key are described in RFC 3280 [3] (section 4.2.1.2). This extension SHALL NOT be marked critical.
RFC 3280 [3]	4.2.1.2	The value of the subject key identifier in the parent CA certificate SHALL be the value placed in the Authority Key Identifier extension of the end entity certificate.

A.4.2 Subject key identifier

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.2	Subject key identifiers SHOULD be derived from the public key or a method that generates unique values.
RFC 3280 [3]	4.2.1.2	This extension SHALL NOT be marked critical. To assist applications in identifying the appropriate end entity certificate, this extension SHOULD be included in all end entity certificates. For end entity certificates, subject key identifiers SHOULD be derived from the public key. Two common methods for generating key identifiers: 1) The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits). 2) The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey.

A.4.3 KeyUsage

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.3	The key usage extension SHALL be present.
RFC 3280 [3]	4.2.1.3	When this extension appears, it SHOULD be marked critical.
RFC 3279 [7]	3.2.1	If the keyUsage extension is present in an end entity certificate which conveys an RSA public key, any combination of the following values MAY be present: - digitalSignature; - nonRepudiation; - keyEncipherment; and - dataEncipherment.

A.4.4 Private key usage period

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.4	This extension SHOULD NOT be used within the Internet PKI. CAs conforming to this profile SHALL NOT generate certificates that include a critical private key usage period extension.

A.4.5 Certificate policies

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.5	When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }.
RFC 3739 [4]	3.2.2	The certificate policies extension SHALL contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA. The certificate policy extension MAY be marked critical.

A.4.6 Policy mappings

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.6	The policy mappings extension SHALL NOT be present in end entity certificates.

A.4.7 Subject alternative name

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.1.2.6	Conforming implementations generating new certificates with electronic mail addresses SHALL use the rfc822Name in the subject alternative name field (section 4.2.1.7) to describe such identities.
RFC 3280 [3]	4.2.1.7	When the subjectAltName extension contains an Internet mail address, the address SHALL be included as an rfc822Name.

A.4.8 Issuer alternative name

No specific requirements listed.

A.4.9 Subject directory attributes

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.9	This extension SHALL be non-critical.

A.4.10 Basic constraints

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.10	This extension MAY appear as a critical or non-critical extension in end entity certificates.

A.4.11 Name constraints

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.11	The name constraints extension SHALL NOT be present in end entity certificates.

A.4.12 Policy constraints

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.12	The policy constraints extension SHALL NOT be present in end entity certificates.

A.4.13 Extended key usage

No specific requirement listed.

A.4.14 CRL distribution points

No specific requirement listed.

A.4.15 Inhibit any-policy

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.15	The policy constraints extension SHALL NOT be present in end entity certificates.

A.4.16 Freshest CRL

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.1.16	This extension SHALL be non-critical.

A.5 RFC 3280 internet certificate extensions

A.5.1 Authority information access

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.2.1	This extension SHALL be non-critical
RFC 2560 [11]	3.1	CAs that support an OCSP service, either hosted locally or provided by an Authorized Responder, MUST provide for the inclusion of a value for a uniformResourceIndicator (URI) accessLocation and the OID value id-ad-ocsp for the accessMethod in the AccessDescription SEQUENCE.

A.5.2 Subject information access

Referenced standard	Section	Requirement or recommendation
RFC 3280 [3]	4.2.2.2	This extension SHALL be non-critical.

A.6 RFC 3739 certificate extensions

A.6.1 Biometric information

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.4	This extension SHALL NOT be marked critical.

A.6.2 Qualified certificate statement

Referenced standard	Section	Requirement or recommendation
RFC 3739 [4]	3.2.5	This extension MAY be critical or non-critical. If the extension is critical, this means that all statements included in the extension are regarded as critical.
TS 101 862 [5]	4.2.1	The indication that a certificate is issued as a Qualified Certificate is provided according to the present document either: 1) when one of the certificate policies identified in the Certificate Policies extensions, as defined in clause 4.2.1.5 from RFC 2459 [13], clearly express that the issuer intentionally has issued the certificate as a Qualified Certificate and that the issuer claims compliance with Annex I and Annex II of the Directive; or 2) when the Qualified Certificate Statements extension includes a statement, as defined in this clause.

History

Document history		
V1.1.1	March 2004	Publication