INTERNATIONAL STANDARD

ISO 15782-2

First edition
2001-11-01

Banking — Certificate management —

Part 2: Certificate extensions

Banque — Gestion des certificats —

Partie 2: Extensions des certificats

Reference number
ISO 15782-2:2001(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO 15782 may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 15782-2 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 2, *Security management and general banking operations*.

ISO 15782 consists of the following parts, under the general title *Banking — Certificate management*:

— *Part 1: Public key certificates*

— *Part 2: Certificate extensions*

Annex A of this part of ISO 15782 is for information only.

Introduction

This part of ISO 15782 extracts and adopts selected definitions of certificate extensions from ISO 9594-8 and adds control requirements and other information required for financial institution use.

While the techniques specified in this part of ISO 15782 are designed to maintain the integrity of financial messages, the Standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application of appropriate audit tests in order to validate compliance.

The binding association between the identity of the owner of a public key and that key shall be documented in order to prove the ownership of a public key. This binding is called a “public key certificate”. Public key certificates are generated by a trusted third entity known as a Certification Authority (CA).

Banking — Certificate management —

Part 2: Certificate extensions

1 Scope

This part of ISO 15782

- extracts and adopts selected definitions of certificate extensions from ISO/IEC 9594-8;
- specifies additional requirements when certificate extensions are used by the financial services industry.

This part of ISO 15782 is to be used with financial institution standards, including ISO 15782-1.

NOTE Distinguished Encoding Rules (DER) of ASN.1 for encoding of ASN.1-defined certificate extensions are specified in ISO/IEC 8825-1. The DER rules defined by ISO/IEC 9594-8 are incomplete and can lead to ambiguities when encoding some values.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 15782. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 15782 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9594-2 | ITU-T Recommendation X.501, *Information technology — Open Systems Interconnection — The Directory: Models*

ISO/IEC 9594-8:1998 | ITU-T Recommendation X.509 (1997), *Information technology — Open Systems Interconnection — The Directory: Authentication framework*

ISO/IEC 9834-1 | CCITT Recommendation X.660 *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General procedures*

ISO/IEC 10021-4 | ITU-T Recommendation X.411, *Information technology — Message Handling Systems (MHS) — Message transfer system: Abstract service definition and procedures*

ISO 15782-1:—[1], *Banking — Certificate management — Part 1: Public key certificates*

RFC 791:1981[2], *Internet protocol*

[1] To be published.

[2] Obsoletes RFC 760; obsoleted by RFC 1060.

RFC 822:1982[3], *Standard for the format of ARPA Internet text messages*

RFC 1035:1987[4], *Domain names — Implementation and specification*

RFC 1630:1994, *Universal resource identifiers in WWW: A unifying syntax for the expression of names and addresses of objects on the network as used in the world-wide web*

FIPS-PUB 140-1:1993, *Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this part of ISO 15782, the following terms and definitions apply.

3.1
attribute
characteristic of an entity

3.2
CA certificate
certificate whose subject is a Certification Authority (CA) and whose associated private key is used to sign certificates

3.3
certificate
public key and identity of an entity together with some other information, rendered unforgeable by signing the certificate information with the private key of the certifying authority that issued that public key certificate

3.4
certificate hold
suspension of the validity of a certificate

3.5
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

EXAMPLE A particular certificate policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

NOTE 1 The certificate policy should be used by the user of the certificate to decide whether or not to accept the binding between the subject (of the certificate) and the public key. A subset of the components in the certificate policy framework are given concrete values to define a certificate policy. The certificate policy is represented by a registered object identifier in the X.509, version 3 certificate. The object owner also registers a textual description of the policy and makes it available to the relying parties.

NOTE 2 The certificate policy object identifier can be included in the following extensions in the X.509, version 3 certificates: certificate policies, policy mappings and policy constraints. The object identifier(s) may appear in none, some, or all of these fields. These object identifiers may be the same (referring to the same certificate policy) or may be different (referring to different certificate policies).

3.6
Certificate Revocation List
CRL
list of revoked certificates

[3] Obsoletes RFC 733; updated by RFC 987; updated by RFC 1327.

[4] Obsoletes RFC 973; obsoleted by RFC 2136; obsoleted by RFC 2137; updated by RFC 1348; updated by RFC 1995; updated by RFC 1996; updated by RFC 2065; updated by RFC 2181; updated by RFC 2308.

3.7
certificate-using system
implementation of those functions defined in this part of ISO 15782 that are used by a certificate user

3.8
certification
process of creating a public key or attribute certificate for an entity

3.9
Certification Authority
CA
entity trusted by one or more entities to create assign and revoke or hold public key certificates

3.10
certification path
ordered sequence of certificates of entities which, together with the public key of the initial entity in the path, can be processed to obtain the public key of the final entity in the path

3.11
Certification Practice Statement
CPS
statement of the practices which a certification authority employs in issuing certificates

3.12
compromise
violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred

3.13
CRL distribution point
directory entry or other distribution source for Certificate Revocation Lists (CRLs)

NOTE A CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

3.14
cross certification
process by which two CAs mutually certify each other’s public keys

See policy mapping (3.37).

3.15
cryptographic key
key
parameter that determines the operation of a cryptographic function

NOTE Cryptographic functions include:

- the transformation from plain text to cipher text and vice versa;
- synchronized generation of keying material;
- digital signature generation or validation.

3.16
cryptographic module
set of hardware, firmware, software or some combination thereof, that implements cryptographic logic, cryptographic processes, or both

3.17
cryptography
discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof

3.18
data integrity
property whereby data has not been altered or destroyed

3.19
delta-CRL
partial Certificate Revocation List (CRL) indicating only changes since a prior CRL issue

3.20
digital signature
signature
cryptographic transformation of data which, when associated with a data unit, provides the services of origin authentication and data integrity and may support signer non-repudiation

3.21
directory
repository
method for distributing or making available certificates or Certificate Revocation Lists (CRLs)

EXAMPLE A data base or an X.500 Directory.

3.22
distinguished name
globally unique name for an entity

NOTE Methods for determining global uniqueness are outside the scope of this part of ISO 15782. Note that an entity may be issued more than one certificate with the same distinguished name.

3.23
end certificate
last certificate considered in a certificate chain

3.24
end entity
certificate subject which uses its private key for purposes other than signing certificates

3.25
entity
legal or natural person who is a Certification Authority (CA), Registration Authority (RA) or end entity

3.26
financial message
communication containing information which has financial implications

3.27
intermediate certificates
certificate considered in a certificate chain other than the first or end certificate

3.28
key
see cryptographic key (3.15)

3.29
key agreement
method for negotiating a key value on-line without transferring the key, even in an encrypted form

EXAMPLE The Diffie-Hellman technique.

3.30
key pair
⟨public key cryptography⟩ public key and its corresponding private key

3.31
keying material
data, such as keys, certificates and initialization vectors, necessary to establish and maintain cryptographic keying relationships

3.32
key pair updating
re-certification or replacement of a CA's public/private key pair

3.33
message
data to be signed

3.34
module
see cryptographic module (3.16)

3.35
non-repudiation
service which provides proof beyond a reasonable doubt of the integrity and origin of data which can be validated by a third entity

NOTE The non-repudiation service protects against the signing entity falsely denying the action and may provide rebuttable presumption. It requires that appropriate processes and procedures (e.g., registration, audit trails, contractual arrangements, personnel, etc.) be in place.

3.36
optional
not required by this part of ISO 15782 or not required to meet an optional provision of this part of ISO 15782

NOTE Not to be confused with the ASN.1 key word “OPTIONAL”.

3.37
policy mapping
recognition that, when a Certification Authority (CA) in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain

See cross certification (3.14).

3.38
policy qualifier
policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate

3.39
private key
⟨asymmetric (public) key cryptosystem⟩ key of an entity's key pair which is known only by that entity

3.40
public key
⟨asymmetric (public) key cryptosystem⟩ key of an entity's key pair which is publicly known

3.41
Registration Authority
RA
entity that is responsible for identification and authentication of subjects of certificates, but is not a Certification Authority (CA) and hence does not sign or issue certificates

NOTE An RA may assist in the certificate application process, revocation process, or both. The RA does not need to be a separate body, but can be part of the CA.

3.42
relying party
recipient of a certificate who acts in reliance on that certificate, digital signatures verified using that certificate, or both

3.43
signature
see digital signature (3.20)

3.44
subject
entity whose public key is certified in a public key certificate

3.45
subject CA
Certification Authority (CA) that is certified by the issuing CA and hence complies with the certificate policy of the issuing CA

3.46
subject end entity
end entity that is the subject of a certificate

3.47
user
see relying party (3.42)

4 Abbreviations

The following abbreviations are used in this part of ISO 15782.

Abbreviation	Meaning
ASN.1	Abstract Syntax Notation
CA	Certification Authority
DIT	Directory Information Tree
CRL	Certificate Revocation List
ITU	International Telecommunication Union

NOTE 1 The notation used in this part of ISO 15782 is a variant of the X.509 notation for certificates, certification paths and related information.

NOTE 2 The use of a bold, sans serif font such as “**CertReqData**” or “**CRLEntry**” denotes the use of Abstract Syntax Notation (ASN.1). Where it makes sense to do so, the ASN.1 term is used in place of normal text.

5 Extensions

Version 3 certificates as defined in ISO/IEC 9594-8 provide a mechanism for CAs to append additional information about the:

- subject's public key;
- issuer's public key;
- issuer's CRLs.

This additional information is encoded in the form of extensions to certificates.

These extensions are specified in the following areas:

a) *Key and policy information*: These certificate and CRL extensions convey additional information about the keys involved, including key identifiers for subject and issuer keys, indicators of intended or restricted key usage and indicators of certificate policy.

b) *Certificate subject and issuer attributes*: These certificate and CRL extensions support alternative names, of various name forms, for a certificate subject, a certificate issuer, or a CRL issuer. These extensions can also convey additional attribute information about the certificate subject, to assist a relying party in being confident that the certificate subject is a particular person or entity.

c) *Certification path constraints*: These certificate extensions allow constraint specifications to be included in CA certificates, i.e. certificates for CAs issued by other CAs, to facilitate the automated processing of certification paths when multiple certificate policies are involved. Multiple certificate policies arise when policies vary for different applications in an environment or when interoperation with external environments occurs. The constraints may restrict the types of certificates that can be issued by the subject CA or that may occur subsequently in a certification path.

d) *Basic CRL extensions*: These CRL extensions allow a CRL to include indications of revocation reason, to provide for temporary suspension of a certificate and to include CRL-issue sequence numbers to allow relying parties to detect missing CRLs in a sequence from one CRL issuer.

e) *CRL distribution points and delta-CRLs*: These certificate and CRL extensions allow the complete set of revocation information from one CA to be partitioned into separate CRLs and allow revocation information from multiple CAs to be combined in one CRL. These extensions also support the use of partial CRLs indicating only changes since an earlier CRL issue.

Inclusion of any extension in a certificate or CRL is at the option of the authority issuing that certificate or CRL.

In a certificate or CRL, an extension is flagged as being either critical or non-critical. If an extension is flagged critical and a certificate-using system does not recognize the extension type or does not implement the semantics of the extension, then that system shall consider the certificate invalid. If an extension is flagged non-critical, a certificate-using system that does not recognize or implement that extension type may process the remainder of the certificate ignoring the extension. Extension type definitions in this part of ISO 15782 indicate if the extension is always critical, always non-critical, or if criticality can be decided by the certificate or CRL issuer. The reason for requiring some extensions to be always non-critical is to allow certificate-using implementations which do not need to use such extensions to omit support for them without jeopardizing the ability to interoperate with all certification authorities.

These extensions provide a variety of methods to increase the amount of information that the certificate conveys to facilitate automated certificate processing. The extensions are intended to allow explicit management of trust and policies corresponding to the differing needs within an organization and certification across hierarchies.