INTERNATIONAL STANDARD

ISO 15782-1

First edition
2003-06-01

Certificate management for financial services —

Part 1: Public key certificates

Gestion de certificats pour les services financiers —
Partie 1: Certificats de clé publique

Reference number
ISO 15782-1:2003(E)

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.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 2.

The main task of technical committees is to prepare International Standards. 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 document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 15782-1 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 *Certificate management for financial services*:

— *Part 1: Public key certificates*

— *Part 2: Certificate extensions*

Introduction

This part of ISO 15782 adopts ISO/IEC 9594-8 | ITU-T Recommendation X.509 for the financial services industry and defines certificate management procedures and data elements.

Detailed requirements for the financial industry for the individual extensions are given in ISO 15782-2.

While the techniques specified in this part of ISO 15782 are designed to maintain the integrity of financial messages and support the service of non-repudiation, this part of ISO 15782 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, with these controls including 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 is documented in order to prove the ownership of the corresponding private key. This binding is called a *public key certificate*. Public key certificates are generated by a trusted entity known as a Certification Authority (CA).

The proper implementation of this part of ISO 15782 ought to provide assurances of the binding of the identity of an entity to the key used by that entity to sign documents, including wire transfers and contracts.

This part of ISO 15782 defines a certificate management framework for authentication, including the authentication of keys for encryption. The techniques specified by this part of ISO 15782 can be used when initiating a business relationship between legal entities (entities).

Certificate management for financial services —

Part 1:
Public key certificates

1 Scope

This part of ISO 15782 defines a certificate management system for financial industry use for legal and natural persons that includes

— credentials and certificate contents,

— certification authority systems, including certificates for digital signatures and for encryption key management,

— certificate generation, distribution, validation and renewal,

— authentication structure and certification paths,

— revocation and recovery procedures, and

— extensions to the definitions of public key certificates and certificate revocation lists.

This part of ISO 15782 also recommends some useful operational procedures (e.g. distribution mechanisms, acceptance criteria for submitted credentials).

Implementation of this part of ISO 15782 will also be based on business risks and legal requirements.

This part of ISO 15782 does not include

— the protocol messages used between the participants in the certificate management process,

— requirements for notary and time stamping,

— certificate policy and certification practices requirements,

— requirements for trusted third parties, or

— Attribute Certificates.

While this part of ISO 15782 provides for the generation of certificates that could include a public key used for encryption key management, it does not address the generation or transport of keys used for encryption.

Implementers wishing to comply with ISO/IEC 9594-8 | ITU-T Recommendation X.509 can utilize the certificate structures defined by that International Standard. Those wishing to implement compatible certificate and certificate revocation structures but without the overhead associated with the X.500 series can utilize the ASN.1 structures defined in Annex A.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8824-1 | ITU-T Recommendation X.680 (1997), *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8824-2:1998 | ITU-T Recommendation X.681 (1997), *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2*

ISO/IEC 8824-3 | ITU-T Recommendation X.682 (1997), *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification — Part 3*

ISO/IEC 8824-4 | ITU-T Recommendation X.683 (1997), *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications — Part 4*

ISO/IEC 8825-1 | ITU-T Recommendation X.690 (1997), *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 8825-2 | ITU-T Recommendation X.691 (1997), *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO/IEC 9594-2 | ITU-T Recommendation X.501 (1997), *Information technology — Open Systems Interconnection — The Directory: Models — Part 2*

ISO/IEC 9594-6 | ITU-T Recommendation X.520 (1997), *Information technology — Open Systems Interconnection — The Directory: Selected attribute types — Part 6*

ISO/IEC 9594-8 | ITU-T Recommendation X.509 (1997), *Information Technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail)*

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

ISO/IEC 15408 (all parts), *Common Criteria for Information Security Evaluation*

ISO 15782-2:2001, *Banking — Certificate Management — Part 2: Certificate extensions*

ANS X9.30-1, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)*

ANS X9.31-1, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, Part 1: The RSA Signature Algorithm*

ANS X9.62, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
ASN.1 module
identifiable collection of ASN.1 types and values

3.2
attribute
characteristic of an entity

3.3
audit journal
chronological record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results

3.4
authorization
granting of rights

3.5
CA-certificate
certificate whose subject is a CA, and whose associated private key is used to sign certificates

3.6
(certificate) hold
suspension of the validity of a certificate

3.7
certificate information
information in a certificate which is signed

3.8
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. Some of the components in the certificate policy framework are given concrete values and 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).

3.9
certificate policy framework
comprehensive set of security and liability related components that can be used to define a certificate policy

NOTE A subset of the components in the certificate policy framework are given concrete values to define a certificate policy.

3.10
certificate request data
credentials
signed information in a certificate request, including the entity's public key, entity identity and other information included in the certificate

3.11
certificate revocation list
CRL
list of revoked certificates

3.12
certificate-using system
implementation of those functions defined in this part of ISO 15782 that are used by a certificate user

3.13
certification
process of creating a public key certificate for an entity

3.14
certification authority
CA
entity trusted by one or more entities to create, assign, and revoke or hold public key certificates

3.15
certification authority system
set of entities, including a CA, that manages certificates throughout the life of the certificate

NOTE The entities are responsible for

— generation,
— submission,
— registration,
— certification,
— distribution,
— use,
— renewal,
— revocation or hold, and
— expiry.

3.16
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

3.17
certification practice statement
CPS
statement of the practices which a certification authority employs in issuing certificates

3.18
compromise
violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred

3.19
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.20
CRL distribution point
directory entry or other distribution source for 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.

3.21
cross certification
process by which two CAs mutually certify each other's public keys

cf. **policy mapping** (3.48)

3.22
(cryptographic) key
parameter that determines the operation of a cryptographic function

NOTE Cryptographic functions include the following:

— the transformation from plain text to cipher text and vice versa;

— synchronized generation of keying material;

— digital signature generation or validation.

3.23
cryptographic module
device wherein cryptographic functions (e.g. encryption, authentication, key generation) are performed

3.24
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

3.25
cryptoperiod
time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect

3.26
data integrity
property whereby data has not been altered or destroyed

3.27
delta-CRL
partial CRL indicating only changes since a prior CRL issue

3.28
(digital) 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

3.29
directory
repository
method for distributing or making available certificates or CRLs

EXAMPLE A data base or an X.500 Directory.

3.30
distinguished name
globally unique name for an entity

NOTE 1 Methods for determining global uniqueness are outside the scope of this part of ISO 15782.

NOTE 2 An entity may be issued more than one certificate with the same distinguished name.

3.31
dual control
process of utilizing two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information

NOTE 1 Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is able to access or to utilize the materials (e.g. cryptographic key).

NOTE 2 For manual key and certificate generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of key among the entities. Also see split knowledge.

3.32
end certificate
final certificate considered in a certificate chain

3.33
end entity
certificate subject, other than a CA, which uses its private key for purposes other than signing certificates

3.34
entity
legal (e.g. a corporation, labour union, state or nation) or natural person

EXAMPLE CA, RA or end entity.

3.35
financial message
communication containing information which has financial implications

3.36
hash
(mathematical) function which maps values from a large (possibly very large) domain into a smaller (fixed) range and satisfies the following properties:

— it is computationally infeasible to find any input which maps to a pre-specified output;

— it is computationally infeasible to find any two distinct inputs which map to the same output

3.37
key agreement
method for negotiating a key value on-line without transferring the key, even in an encrypted form

EXAMPLE The Diffie-Hellman technique.

3.38
key fragment
part of a private key which has been divided into pieces (also called shares) that are distributed amongst entities such that the pooled fragments of specific subsets of entities can generate digital signatures of the original private key

3.39
key management
generation, storage, secure distribution, and application of keying material in accordance with a security policy

3.40
key pair
⟨public key cryptography⟩ public key and its corresponding private key

3.41
keying material
data, such as keys, certificates and initialization vectors, necessary to establish and maintain cryptographic keying relationships

3.42
keying relationship
state existing between a communicating pair or between members of a group (logical entity) during which time they share keying material

3.43
message
data to be signed

3.44
non-repudiation
service which provides proof of the integrity and origin of data which can be verified by a third party

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

3.45
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”.

3.46
out-of-band notification
notification using a communication means independent of the primary communications means

3.47
policy mapping
recognition that, when a 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

cf. **cross certification** (3.21)

3.48
policy qualifier
policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate

3.49
private key
⟨asymmetric (public) key cryptosystem⟩ key of an entity’s key pair which is known only by that entity

3.50
public key
⟨asymmetric (public) key cryptosystem⟩ key of an entity’s key pair which is publicly known

3.51
public key 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

3.52
public key validation
PKV
process that does arithmetic tests on a candidate public key to provide assurance that it conforms to the specifications of the standard

NOTE 1 Since attacks may be possible on the owner and/or user if using a non-conforming public key.

NOTE 2 Public key validation can include arithmetic property tests (range, order, primality, etc.), canonical generation tests and consistency tests between components of a public key. Methods for public key validation are typically found in financial industry signature standards (e.g. ANS X9.62).

3.53
registration authority
RA
entity that is responsible for identification and authentication of subjects of certificates, but is not a CA and hence does not sign or issue certificates

NOTE An RA may assist in the certificate application process, revocation process or both.

3.54
relying party
user
recipient of a certificate who acts in reliance on that certificate

3.55
split knowledge
condition under which two or more entities separately have key fragments which, individually, convey no knowledge of the resultant cryptographic key

3.56
subject
entity whose public key is certified in a public key certificate

3.57
subject CA
CA that is certified by the issuing CA

3.58
trusted CA public key
public key used to validate the first certificate in a chain of certificates as a part of certification path processing

EXAMPLE The root key in a centralized trust model or a local CA key in a decentralized trust model (see Annex G).

NOTE If an end entity validates a chain of certificates from a trusted CA public key to the end certificate, then the end certificate is considered valid.

3.59
zeroize
active destruction of electronically stored data such as by degaussing, erasing or overwriting

4 Abbreviations and symbols

Abbreviation	Meaning
ASN.1	Abstract syntax notation
BER	Basic encoding rules
CA	Certification authority
CPS	Certification practice statement
CRL	Certificate revocation list
DER	Distinguished encoding rules
DSA	Digital signature algorithm
ECDSA	Elliptic curve digital signature algorithm
ITU-T	International Telecommunication Union telecommunications standardization sector
PKI	Public key infrastructure
RA	Registration authority
RSA	Rivest Shamir Adleman algorithm
SHA-1	Secure hash algorithm-1
URI	Uniform resource identifier

Symbols	Meaning
X{information}	Signing of "information" by X
X_p	X's public key. (e.g. X_{1p} is X_1's public key)
X_s	X's private key
$X_1«X_2»$	X_2's certificate issued by the CA, X_1
$X_1«X_2»X_2«X_3»X_{n-1}«X_n»$	Certificate path. Each item in the path is the certificate for the CA which produced the next item. This path is of arbitrary length and is functionally equivalent to $X_1«X_n»$. Possession of X_{1p} allows a user to extract the authenticated public key of X_n.
$X_{1p}·X_1«X_2»$	Unwrapping of a certificate or path. The public key of the leftmost CA (X_1) is used to extract the authenticated public key of the rightmost certificate ($X_1«X_2»$) by working through the path of intervening certificates. This example extracts X_{2p}.

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), as defined in ISO/IEC 8824-1 to ISO/IEC 8824-4 and ISO/IEC 8825-1 and ISO/IEC 8825-2. Where it makes sense to do so, the ASN.1 term is used in place of normal text.

5 Public key infrastructure

5.1 Overview

Public key infrastructure (PKI) is a term used to describe the technical, legal and commercial infrastructure that enables the wide deployment of public key technology.

Public key technology is used for creating digital signatures and for managing symmetric keys. With public key cryptography, two keys are used: one is kept private with the user, the other is made publicly available. That