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)

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

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 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.