INTERNATIONAL STANDARD

ISO 15782-1

Second edition
2009-10-15

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 15782-1:2009(E)

© ISO 2009

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.

This document is a preview generated by EVS

COPYRIGHT PROTECTED DOCUMENT

© ISO 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

 © ISO 2009 – All rights reserved

Contents

Page

This document is a preview generated by EVS

© ISO 2009 – All rights reserved

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, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 15782-1:2003), which has been technically revised.

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*

This document is a preview generated by EVS

 © ISO 2009 – All rights reserved

Introduction

This part of ISO 15782 adopts ISO/IEC 9594-8 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 is intended 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).

This document is a preview generated by EVS

© ISO 2009 – All rights reserved

Certificate management for financial services —

Part 1:
Public key certificates

This document is a preview generated by EVS

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, and

— revocation and recovery procedures.

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, 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 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 ISO 15782-2. ISO 15782-2 can also be referred to for a financial services profile of certificate and CRL extensions.

ISO 21188 provides additional information for implementers on Certificate Policies, Certification Practice Statements, and PKI controls. ISO 21188 sets out a framework of requirements to manage a PKI through Certificate Policies and Certification Practice Statements and to enable the use of public key certificates in the financial services industry. It also defines control objectives and supporting procedures to manage risks.

NOTE 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. Refer to ISO 15782-2 for related ASN.1 modules.

© ISO 2009 – All rights reserved

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, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8824-2, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2*

ISO/IEC 8824-3, *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification — Part 3*

ISO/IEC 8824-4, *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications — Part 4*

ISO/IEC 8825-1, *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, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

ISO/IEC 9594-8, *Information Technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

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

ISO 16609, *Banking — Requirements for message authentication using symmetric techniques*

ISO 21188:2006, *Public key infrastructure for financial services — Practices and policy framework*

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

This document is a preview generated by EVS

 © ISO 2009 – All rights reserved