

This is a preview of "ISO 15782-1:2009". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "ISO 15782-1:2009". [Click here to purchase the full version from the ANSI store.](#)

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.



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

This is a preview of "ISO 15782-1:2009". [Click here to purchase the full version from the ANSI store.](#)

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Symbols and abbreviations.....	8
5 Public key infrastructure	8
5.1 Overview.....	8
5.2 Public key management infrastructure process flow	9
5.3 Certification Authority (CA)	9
5.4 Registration Authority (RA)	10
5.5 End entities	10
6 Certification Authority systems	10
6.1 General	10
6.2 Responsibilities in CA systems	12
6.3 Certificate life cycle requirements	15
6.4 Security quality assurance and audit requirements	29
6.5 Business continuity planning	30
7 Data elements and relationships	30
8 Public key certificate and Certificate Revocation List extensions.....	30
Annex A (normative) Certification Authority audit journal contents and use	31
Annex B (informative) Alternative trust models.....	34
Annex C (informative) Suggested requirements for the acceptance of certificate request data	40
Annex D (informative) Multiple algorithm certificate validation example	42
Annex E (informative) Certification Authority techniques for disaster recovery	44
Annex F (informative) Distribution of certificates and Certificate Revocation Lists	47
Bibliography.....	48

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 is a preview of "ISO 15782-1:2009". [Click here to purchase the full version from the ANSI store.](#)

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).