

INTERNATIONAL ISO
This is a preview of "ISO 15782-2:2001". Click here to purchase the full version from the ANSI store.

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 2001

This is a preview of "ISO 15782-2:2001". [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.

© ISO 2001

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.ch
Web www.iso.ch

Printed in Switzerland

This is a preview of "ISO 15782-2:2001". [Click here to purchase the full version from the ANSI store.](#)

Contents

Page

Foreword.....	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviations.....	6
5 Extensions.....	7
6 Key and policy information	8
6.1 Requirements.....	8
6.2 Certificate and CRL extensions	9
7 Certificate subject and certificate issuer attributes	14
7.1 Requirements.....	14
7.2 Certificate and CRL extensions	15
8 Certification path constraints.....	17
8.1 Requirements.....	17
8.2 Certificate extensions	19
8.3 Certification path processing procedure	21
9 Basic CRL extensions	24
9.1 Management requirements.....	24
9.2 Basic CRL and CRL entry extensions	25
10 CRL distribution points and delta-CRLs	27
10.1 Requirements.....	27
10.2 Certificate extensions	28
10.3 CRL and CRL entry extensions.....	29
10.4 Matching rules	31
Annex A (informative) Examples of the use of certification path constraints	36
Bibliography.....	38

This is a preview of "ISO 15782-2:2001". [Click here to purchase the full version from the ANSI store.](#)

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.

This is a preview of "ISO 15782-2:2001". [Click here to purchase the full version from the ANSI store.](#)

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).