

This is a preview of "ISO 11568-4:2007". [Click here to purchase the full version from the ANSI store.](#)

Second edition
2007-07-01

Banking — Key management (retail) —

Part 4:

Asymmetric cryptosystems — Key management and life cycle

Banque — Gestion de clés (services aux particuliers) —

*Partie 4: Cryptosystèmes asymétriques — Gestion des clés et cycle
de vie*



Reference number
ISO 11568-4:2007(E)

© ISO 2007

This is a preview of "ISO 11568-4:2007". [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 2007

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 11568-4:2007". 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 Uses of asymmetric cryptosystems in retail financial services systems.....	3
4.1 General.....	3
4.2 Establishment and storage of symmetric keys	4
4.3 Storage and distribution of asymmetric public keys	4
4.4 Storage and transfer of asymmetric private keys	4
5 Techniques for the provision of key management services	4
5.1 Introduction	4
5.2 Key encipherment.....	4
5.3 Public key certification.....	5
5.4 Key separation techniques	6
5.5 Key verification	6
5.6 Key integrity techniques	7
6 Asymmetric key life cycle	8
6.1 Key life cycle phases	8
6.2 Key life cycle stages — Generation	9
6.3 Key storage	12
6.4 Public key distribution	14
6.5 Asymmetric key pair transfer	14
6.6 Authenticity prior to use	16
6.7 Use.....	17
6.8 Public key revocation	17
6.9 Replacement.....	18
6.10 Public key expiration	18
6.11 Private key destruction	18
6.12 Private key deletion	19
6.13 Public key archive.....	19
6.14 Private key termination	19
6.15 Erasure summary.....	20
6.16 Optional life cycle processes	20
Annex A (normative) Approved algorithms.....	21
Bibliography	22

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 11568-4 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, Security*.

This second edition cancels and replaces the first edition (ISO 11568-4:1998) which has been technically revised and incorporates revised text from the former part 5.

ISO 11568 consists of the following parts, under the general title *Banking — Key management (retail)*:

- *Part 1: Principles*
- *Part 2: Symmetric ciphers, their key management and life cycle*
- *Part 3: Key life cycle for symmetric ciphers (withdrawn; incorporated into Part 2)*
- *Part 4: Asymmetric cryptosystems — Key management and life cycle*
- *Part 5: Key life cycle for public key cryptosystems*
- *Part 6: Key management schemes (withdrawn)*

This is a preview of "ISO 11568-4:2007". [Click here to purchase the full version from the ANSI store.](#)

Introduction

ISO 11568 is one of a series of International Standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment; e.g. messages between an acquirer and a card acceptor, or an acquirer and a card issuer.

This part of ISO 11568 addresses the key management requirements that are applicable in the domain of retail financial services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machines (ATM) transactions.

ISO 11568-2 and ISO 11568-4 describe key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

- a) key separation;
- b) key substitution prevention;
- c) key identification;
- d) key synchronization;
- e) key integrity;
- f) key confidentiality;
- g) key compromise detection.

This part of ISO 11568 also describes the key life cycle in the context of secure management of cryptographic keys for asymmetric cryptosystems. It states both requirements and implementation methods for each step in the life of such a key, utilizing the key management principles, services and techniques described herein and in ISO 11568-1. This part of ISO 11568 does not cover the management or key life cycle for keys used in symmetric ciphers, which are covered in ISO 11568-2.

This part of ISO 11568 is one of a series that describes requirements for security in the financial services environment, as follows:

ISO 9564-1; ISO 9564-2; ISO 9564-3; ISO/TR 9564-4; ISO 11568; ISO 13491; ISO/TR 19038.