
**Financial services — Key management
(retail) —**

Part 2:
**Symmetric ciphers, their key
management and life cycle**

Services financiers — Gestion de clés (services aux particuliers) —

*Partie 2: Algorithmes cryptographiques symétriques, leur gestion de
clés et leur cycle de vie*



This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

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

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 General environment for key management techniques	4
4.1 General	4
4.2 Functionality of a secure cryptographic device	4
4.3 Key generation	5
4.4 Key calculation (variants)	6
4.5 Key hierarchies	6
4.6 Key life cycle	7
4.7 Key storage	9
4.8 Key restoration from back-up	10
4.9 Key distribution and loading	10
4.10 Key use	11
4.11 Key cryptoperiod	11
4.12 Key replacement	12
4.13 Key destruction	12
4.14 Key deletion	12
4.15 Key archive	13
4.16 Key termination	13
5 Techniques for the provision of key management services	13
5.1 General	13
5.2 Key encipherment	13
5.3 Key variants	13
5.4 Key derivation	14
5.5 Key transformation	14
5.6 Key offsetting	15
5.7 Key notarization	16
5.8 Key tagging	16
5.9 Key verification	18
5.10 Key identification	18
5.11 Controls and audit	19
5.12 Key integrity	19
6 Symmetric key life cycle	20
6.1 General	20
6.2 Key generation	20
6.3 Key storage	20
6.4 Key restoration from back-up	21
6.5 Key distribution and loading	21
6.6 Key use	23
6.7 Key replacement	23
6.8 Key destruction, deletion, archive and termination	23
7 Key management services cross-reference	24
Annex A (normative) Notation used in this part of ISO 11568	26
Annex B (normative) Approved algorithms for symmetric key management	27
Annex C (normative) Abbreviations	28
Bibliography	29

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

This third edition cancels and replaces the second edition (ISO 11568-2:2005), which has been technically revised.

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

- *Part 1: Principles*
- *Part 2: Symmetric ciphers, their key management and life cycle*
- *Part 4: Asymmetric cryptosystems — Key management and life cycle*

Introduction

ISO 11568 is one of a series of standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment, for instance, 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 machine (ATM) transactions.

This part of ISO 11568 describes key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

- key separation;
- key substitution prevention;
- key identification;
- key synchronization;
- key integrity;
- key confidentiality;
- key compromise detection.

The key management services and corresponding key management techniques are cross-referenced in Clause 7.

This part of ISO 11568 also describes the key life cycle in the context of secure management of cryptographic keys for symmetric ciphers. 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 asymmetric ciphers, which are covered in ISO 11568-4.

In the development of ISO 11568, due consideration was given to ISO/IEC 11770; the mechanisms adopted and described in this part of ISO 11568 are those required to satisfy the needs of the financial services industry.

Financial services — Key management (retail) —

Part 2:

Symmetric ciphers, their key management and life cycle

1 Scope

This part of ISO 11568 specifies techniques for the protection of symmetric and asymmetric cryptographic keys in a retail banking environment using symmetric ciphers and the life-cycle management of the associated symmetric keys. The techniques described enable compliance with the principles described in ISO 11568-1.

The techniques described are applicable to any symmetric key management operation.

The notation used in this part of ISO 11568 is given in Annex A.

Algorithms approved for use with the techniques described in this part of ISO 11568 are given in Annex B.

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 9564-1, *Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO 11568-1:2005, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 13491-2:2005, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

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

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Abbreviations used in this part of ISO 11568 are given in Annex C.