

Banking — Key management (retail) —

Part 4: Key management techniques using public key cryptography

ICS 35.240.40

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This British Standard reproduces verbatim ISO 11568-4:1998 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Banking, Securities and other financial services, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO title page, pages ii to iv, pages 1 to 14, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 March 1999

© BSI 05-1999

ISBN 0 580 30586 4

Contents

	Page
National foreword	Inside front cover
Foreword	iii
Text of ISO 11568-4	1

INTERNATIONAL STANDARD

ISO
11568-4

First edition
1998-07-15

Banking — Key management (retail) —

Part 4:

Key management techniques using public key cryptography

Banque — Gestion de clés (services aux particuliers) —

Partie 4: Techniques de gestion de clés utilisant la cryptographie à clé publique



Contents

	Page
Foreword	iii
Introduction	1
1 Scope	1
2 Normative references	1
3 Definitions	2
4 Uses of public key cryptosystems in retail banking systems	3
4.1 Distribution of symmetric keys	3
4.1.1 Key transport	3
4.1.2 Key agreement	3
4.2 Storage and distribution of asymmetric public keys	3
4.3 Storage and transfer of asymmetric private keys	3
5 Techniques for the provision of key management services	3
5.1 Generation of an asymmetric key pair	4
5.2 Key encipherment	4
5.2.1 Encipherment of a symmetric key using an asymmetric cipher	4
5.2.2 Encipherment of an asymmetric key using an asymmetric cipher	4
5.2.3 Encipherment of an asymmetric key using a symmetric cipher	4
5.3 Key certification	4
5.4 Key separation techniques	5
5.4.1 Explicit key tagging	5
5.5 Key verification	5
6 Public Key Certificate management	5
Annex A (normative) Approved algorithms and algorithm approval procedure	6
Annex B (normative) Public Key Certificate management	7
Annex C (informative) Attribute Certificate	11
Annex D (informative) Fundamental concepts of public key cryptosystems	12
Annex E (informative) Bibliography	Inside back cover
Figure B.1	8
Table B.1	10
Table B.2	10
Table B.3	11
Table C.1	12

Descriptors: Banking, banking documents, messages, electronic messaging, information interchange, protection of information, cryptography, key management, algorithms.

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.

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.

International Standard ISO 11568-4 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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

- *Part 1: Introduction to key management;*
- *Part 2: Key management techniques for symmetric ciphers;*
- *Part 3: Key life cycle for symmetric ciphers;*
- *Part 4: Key management techniques using public key cryptography;*
- *Part 5: Key life cycle for public key cryptosystems;*
- *Part 6: Key management schemes.*

Annex A and Annex B form an integral part of this part of ISO 11568. Annex C, Annex D and Annex E are for information only.

