

Banking — Key management (retail) —

Part 5: Key life cycle for public key cryptosystems

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 11568-5:1998 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 13 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.

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 30587 2

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	iii
Text of ISO 11568-5	1

INTERNATIONAL STANDARD

ISO
11568-5

First edition
1998-07-15

Banking — Key management (retail) — **Part 5:** **Key life cycle for public key cryptosystems**

Banque — Gestion de clés (services aux particuliers) —

Partie 5: Cycle de vie des clés pour les systèmes cryptographiques à clé publique



Contents

	Page
Foreword	iii
Introduction	1
1 Scope	3
2 Normative references	3
3 Terms and definitions	4
4 General requirements	4
4.1 Asymmetric key pair generation	4
4.2 Authenticity prior to use	5
4.3 Public key certification	5
4.4 Asymmetric key pair transfer	5
4.5 Key storage	5
4.6 Key retrieval	6
4.7 Public key distribution	6
4.8 Public key certificate verification	7
4.9 Key use	7
4.10 Public key registration	7
4.11 Public key revocation	7
4.12 Key replacement	7
4.13 Private key destruction	8
4.14 Private key deletion	8
4.15 Private key termination	8
4.16 Public key archive	8
4.17 Key pair recovery	8
5 Implementation requirements	8
5.1 Asymmetric key pair generation	8
5.2 Authenticity prior to use	9
5.3 Public key certification	9
5.4 Asymmetric key pair transfer	9
5.5 Key storage	10
5.6 Key retrieval	11
5.7 Public key distribution	11
5.8 Public key verification	11
5.9 Key use	11
5.10 Public key registration	11
5.11 Public key revocation	12
5.12 Key replacement	12
5.13 Private key destruction	12
5.14 Private key deletion	12
5.15 Private key termination	12
5.16 Public key archive	12
5.17 Key pair recovery	12
Figure 1 — Private key life cycle	2
Figure 2 — Public key life cycle	3
Table 1 — Permissible methods for transfer of an asymmetric key pair (P: public key, S: private key)	9

Descriptors: Banking, banking documents, messages, identification cards, credit cards, data processing, information interchange, protection of information, cryptography, key management, life cycle.

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.

International Standard ISO 11568 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Subcommittee SC 6, *Financial transaction cards, related media and operations*.