

INTERNATIONAL STANDARD

ISO
11166-1

First edition
1994-11-15

Banking — Key management by means of asymmetric algorithms —

Part 1:

Principles, procedures and formats

*Banque — Gestion des clés au moyen d'algorithmes asymétriques —
Partie 1. Principes, procédures et formats*



Reference number
ISO 11166-1 1994(E)

Contents

	Page
Section 1 General.....	1
1.1 Scope.....	1
1.2 Normative references	1
1.3 Definitions.....	2
1.4 Abbreviations and notation.....	4
1.5 Key management facility.....	7
1.6 Key generation, storage, back-up and destruction.....	7
1.7 Keys	9
 Section 2 Key certification.....	 11
2.1 Minimum requirements for secure operation of a Key Certification Centre.....	11
 Section 3 Automatic distribution of keying material	 13
3.1 Requirements for the automated key management architecture.....	13
3.2 Automated key management architecture	13
3.3 Primitive processes.....	14
 Section 4 Cryptographic service messages.....	 22
4.1 Message formats and flows.....	22
4.2 Generation of Cryptographic Service Messages.....	33
4.3 Processing Cryptographic Service Messages	41

© ISO 1994

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 the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland