
**Financial transaction cards — Security
architecture of financial transaction
systems using integrated circuit cards —
Part 7:
Key management**

*Cartes de transactions financières — Architecture de sécurité des systèmes
de transactions financières utilisant des cartes à circuit intégré —*

Partie 7: Gestion de clé



Contents

1 Scope	1
2 Normative references	1
3 Definitions and abbreviations	2
3.1 Definitions	2
3.2 Abbreviations	5
4 General security principles.....	6
5 ICC systems key management requirements	6
5.1 ICC and SAM life cycle	6
5.2 Key life cycle protection.....	7
5.3 Key separation	7
5.4 Key management services.....	7
5.5 Key relationships	7
5.6 On-line transaction processing.....	8
5.7 Off-line transaction processing using a SAM	8
5.8 CDF and ADF keys.....	8
5.9 Physical security.....	9
5.10 CADs without a SAM	9
6 ICC systems cryptographic keys	9
6.1 Definition of cryptographic keys.....	9
6.2 Key hierarchy	10
7 Key life cycle	10
7.1 Key generation	11

© ISO 1998

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
Internet iso@iso.ch

Printed in Switzerland