
**Financial transaction cards — Security
architecture of financial transaction
systems using integrated circuit cards —**

Part 5:
Use of algorithms

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

Partie 5: Utilisation des algorithmes



Contents

1 Scope	1
2 Normative references	1
3 Definitions	2
4 Notations	5
4.1 Values and entities	5
4.2 Processes	5
4.3 Optionlist	5
4.4 Functions	6
4.5 Digital signatures	6
4.6 Security message format	6
5 Mapping security functions to process types	7
6 Process specifications	9
6.1 Process 1: Key Exchange (KE)	9
6.1.1 KE-symmetric-symmetric	9
6.1.2 KE-symmetric-symmetric-mutual-timeliness	10
6.1.3 KE-symmetric-asymmetric	11
6.1.4 KE-asymmetric-symmetric	12
6.1.5 KE-asymmetric-symmetric-mutual	13
6.1.6 KE-asymmetric-symmetric-mutual-timeliness	14
6.1.7 KE-asymmetric-asymmetric	15
6.2 Process 2: Entity Authentication (EA)	16
6.2.1 EA-symmetric-timeliness	17
6.2.2 EA-symmetric-timeliness-mutual	18

© 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