
**Identification cards — Integrated circuit
card programming interfaces —**

Part 5:
Testing procedures

*Cartes d'identification — Interfaces programmables de cartes à puce —
Partie 5: Essais*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	vi
Introduction.....	vii
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions	2
4 Symbols and abbreviated terms.....	3
5 Testing methodology	4
5.1 Terms of testing.....	4
5.1.1 Purpose of testing.....	4
5.1.2 Testing objective.....	4
5.1.3 Testing Principles.....	4
5.1.4 GCI under test:.....	6
5.1.5 SAL under test:.....	6
5.1.6 Conformance attainment.....	7
5.2 Conformance vector.....	8
5.3 Structure of tests.....	10
5.4 Test environment.....	12
5.4.1 Stack configurations.....	12
5.4.2 Card-application emulators.....	12
5.4.3 Verification and logging capability of components.....	12
5.4.4 Procedural element	12
6 Components.....	12
6.1 Service access layer API	12
6.1.1 Basic tests.....	12
6.1.2 Discoverability tests.....	12
6.2 Generic card interface.....	15
6.2.1 Basic test.....	15
6.2.2 Processing tests.....	15
6.2.3 Discoverability tests.....	17
6.2.4 Generic card interface acted on ISO/IEC 24727-2 implementation (i.e. CLA = "FF")	18
6.3 Interface device API	19
6.4 Trusted channel API.....	19
6.4.1 TC_API_Open.....	19
6.4.2 TC_API_Close.....	19
6.4.3 TC_API_Write.....	19
6.4.4 TC_API_Read.....	19
6.5 SAL on-card implementation component testing	20
7 Authentication protocols.....	20
7.1 General	20
7.2 SAL security test sequences	21
7.2.1 Cryptographic operations	22
7.2.2 Simple assertion.....	26
7.2.3 Asymmetric internal authenticate.....	27
7.2.4 Asymmetric external authenticate.....	28
7.2.5 Symmetric internal authenticate.....	30
7.2.6 Symmetric external authenticate.....	31
7.2.7 Compare	33
7.2.8 PIN compare.....	35