
**Financial services — Secure
cryptographic devices (retail) —**

**Part 2:
Security compliance checklists for
devices used in financial transactions**

*Services financiers — Dispositifs cryptographiques de sécurité
(services aux particuliers) —*

*Partie 2: Listes de contrôle de conformité de sécurité pour les
dispositifs utilisés dans les transactions financières*

This document is a preview generated by EMS



COPYRIGHT PROTECTED DOCUMENT

© ISO 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

	Page
Foreword.....	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Use of security compliance checklists.....	2
4.1 General.....	2
4.2 Informal evaluation.....	3
4.3 Semi-formal evaluation.....	3
4.4 Strict semi-formal evaluation.....	3
4.5 Formal evaluation.....	3
Annex A (normative) Physical, logical, and device management characteristics common to all secure cryptographic devices.....	4
Annex B (normative) Devices with PIN entry functionality.....	12
Annex C (normative) Devices with PIN management functionality.....	17
Annex D (normative) Devices with message authentication functionality.....	20
Annex E (normative) Devices with key generation functionality.....	22
Annex F (normative) Devices with key transfer and loading functionality.....	27
Annex G (normative) Devices with digital signature functionality.....	33
Annex H (normative) Categorization of environments.....	35
Bibliography.....	39

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: [Foreword - Supplementary information](#)

The committee responsible for this document is ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This third edition cancels and replaces the second edition (ISO 13491-2:2005), which has been technically revised.

ISO 13491 consists of the following parts, under the general title *Financial Services — Secure cryptographic devices (retail)*:

- *Part 1: Concepts, requirements and evaluation methods*,
- *Part 2: Security compliance checklists for devices user in financial transactions*

Introduction

This part of ISO 13491 specifies both the physical and logical characteristics and the management of the secure cryptographic devices (SCDs) used to protect messages, cryptographic keys, and other sensitive information used in a retail financial services environment.

The security of retail financial services is largely dependent upon the security of these cryptographic devices.

Security requirements are based upon the premise that computer files can be accessed and manipulated, communication lines can be “tapped”, and authorized data or control inputs in a system device can be replaced with unauthorized inputs. While certain cryptographic devices (e.g. host security modules) reside in relatively high-security processing centres, a large proportion of cryptographic devices used in retail financial services (e.g. PIN entry devices, etc.) now reside in non-secure environments. Therefore, when PINs, MACs, cryptographic keys, and other sensitive data are processed in these devices, there is a risk that the devices may be tampered with, or otherwise, compromised to disclose or modify such data.

It is to be ensured that the risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper physical and logical security characteristics and are properly managed. To ensure that SCDs have the proper physical and logical security, they require evaluation.

This part of ISO 13491 provides the security compliance checklists for evaluating SCDs used in financial services systems in accordance with ISO 13491-1. Other evaluation frameworks exist and may be appropriate for formal security evaluations, e.g. ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 19790, and are outside the scope of this part of ISO 13491.

Appropriate device characteristics are necessary to ensure that the device has the proper operational capabilities and provides adequate protection for the data it contains. Appropriate device management is necessary to ensure that the device is legitimate, that it has not been modified in an unauthorized manner, e.g. by “bugging”, and that any sensitive data placed within the device (e.g. cryptographic keys) have not been subject to disclosure or change.

Absolute security is not practically achievable. Cryptographic security depends upon each life cycle phase of the SCD and the complementary combination of appropriate device management procedures and secure cryptographic characteristics. These management procedures implement preventive measures to reduce the opportunity for a breach of cryptographic device security. These measures aim for a high probability of detection of any illicit access to sensitive or confidential data in the event that device characteristics fail to prevent or detect the security compromise.

Financial services — Secure cryptographic devices (retail) —

Part 2: Security compliance checklists for devices used in financial transactions

1 Scope

This part of ISO 13491 specifies checklists to be used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes as specified in [H.5](#), ISO 9564-2, ISO 16609, ISO 11568-1, ISO 11568-2, and ISO 11568-4 in the financial services environment. IC payment cards are subject to the requirements identified in this part of ISO 13491 up until the time of issue after which they are to be regarded as a “personal” device and outside of the scope of this part of ISO 13491.

This part of ISO 13491 does not address issues arising from the denial of service of an SCD.

In the checklists given in [Annexes A to H](#), the term “not feasible” is intended to convey the notion that although a particular attack might be technically possible, it would not be economically viable since carrying out the attack would cost more than any benefits obtained from a successful attack. In addition to attacks for purely economic gain, malicious attacks directed toward loss of reputation need to be considered.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

ISO 13491-1, *Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13491-1 and the following apply.

3.1

auditor

one who has the appropriate skills to check, assess, review, and evaluate compliance with an informal evaluation on behalf of the sponsor or audit review body