INTERNATIONAL ISO

Third edition
2016-03-15

Financial services — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

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

Partie 1: Concepts, exigences et méthodes d'évaluation

Reference number
ISO 13491-1:2016(E)

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 ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **5**

5 Secure cryptographic device concepts ... **5**
5.1 General ... 5
5.2 Attack scenarios ... 6
5.2.1 General ... 6
5.2.2 Penetration ... 6
5.2.3 Monitoring ... 6
5.2.4 Manipulation ... 6
5.2.5 Modification ... 6
5.2.6 Substitution ... 6
5.3 Defence measures ... 7
5.3.1 General ... 7
5.3.2 Device characteristics ... 7
5.3.3 Device management ... 8
5.3.4 Environment ... 8

6 Requirements for device security characteristics ... **8**
6.1 General ... 8
6.2 Physical security requirements for SCDs ... 9
6.2.1 General ... 9
6.3 Tamper evident requirements ... 9
6.3.1 General ... 9
6.4 Tamper resistant requirements ... 10
6.4.1 General ... 10
6.5 Tamper responsive requirements ... 10
6.5.1 General ... 10
6.6 Logical security requirements for SCDs ... 11
6.6.1 Dual control ... 11
6.6.2 Unique key per device ... 11
6.6.3 Assurance of genuine device ... 11
6.6.4 Design of functions ... 11
6.6.5 Use of cryptographic keys ... 12
6.6.6 Sensitive device states ... 12
6.6.7 Multiple cryptographic relationships ... 12
6.6.8 SCD software authentication ... 12

7 Requirements for device management ... **12**
7.1 General ... 12
7.2 Life cycle phases ... 13
7.3 Life cycle protection requirements ... 14
7.3.1 General ... 14
7.3.2 Manufacturing phase ... 14
7.3.3 Post-manufacturing phase ... 15
7.3.4 Commissioning (initial financial key loading) phase ... 15
7.3.5 Inactive operational phase ... 15
7.3.6 Active operational phase (use) ... 16
7.3.7 Decommissioning (post-use) phase ... 16
7.3.8 Repair phase ... 16
7.3.9 Destruction phase ... 17

7.4 Life cycle protection methods 17
7.4.1 Manufacturing 17
7.4.2 Post manufacturing phase 17
7.4.3 Commissioning (initial financial key loading) phase 17
7.4.4 Inactive Operational Phase 18
7.4.5 Active operational (use) phase 18
7.4.6 Decommissioning phase 18
7.4.7 Repair 19
7.4.8 Destruction 19
7.5 Accountability 19
7.6 Device management principles of audit and control 20
Annex A (informative) **Evaluation methods** **23**
Bibliography **33**

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 13491-1:2007), 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 used in financial transactions*

Introduction

ISO 13491 describes 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.

This part of ISO 13491 contains the security requirements for SCDs. ISO 13491-2 is a tool for measuring compliance against these requirements. It provides a checklist of

— characteristics that a device has to possess,

— how devices have to be managed, and

— characteristics of the operational environments.

The security of retail electronic payment systems is largely dependent upon the security of these cryptographic devices. This security is based upon the premise that computer files can be accessed and manipulated, communications lines can be "tapped", and authorized data or control inputs into system equipment can be replaced with unauthorized inputs. When personal identification numbers (PINs), message authentication codes (MACs), cryptographic keys, and other sensitive data are processed, there is a risk of tampering or other compromise to disclose or modify such data. The risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

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) has not been subject to disclosure or change.

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

