INTERNATIONAL STANDARD

ISO 13491-1

Second edition
2007-06-15

Banking — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

Banque — Dispositifs cryptographiques de sécurité (services aux particuliers) —

Partie 1: Concepts, exigences et méthodes d'évaluation

Reference number
ISO 13491-1:2007(E)

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

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 13491-1 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 13491-1:1998), which has been technically revised.

ISO 13491 consists of the following parts, under the general title *Banking — 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.

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.

Banking — Secure cryptographic devices (retail) —

Part 1:
Concepts, requirements and evaluation methods

1 Scope

This part of ISO 13491 specifies the requirements for secure cryptographic devices (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568.

This part of ISO 13491 has two primary purposes:

— to state the requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their life cycle, and

— to standardize the methodology for verifying compliance with those requirements.

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. These aim 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.

Annex A provides an informative illustration of the concepts of security levels described in this part of ISO 13491 as being applicable to SCDs.

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

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail financial services environment are contained in ISO 13491-2.

2 Normative references

The following referenced documents are indispensable for the application of this document. 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 11568-2:2005, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4, *Banking — Key management (retail) — Part 4: Key management techniques using public key cryptosystems*

ISO 13491-2, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
accreditation authority
authority responsible for the accreditation of evaluation authorities and supervision of their work in order to guarantee the reproducibility of the evaluation results

3.2
accredited evaluation authority
body accredited in accordance with a set of rules and accepted by the accreditation authority for the purpose of evaluation

NOTE An example of a set of rules is ISO/IEC 17025.

3.3
assessment checklist
list of claims, organized by device type, and contained in ISO 13491-2

3.4
assessment report
output of the assessment review body, based on the results from an assessor

3.5
assessment review body
group with responsibility for reviewing and making judgements on the results from the assessor

3.6
assessor
person who checks, assesses, reviews and evaluates compliance with an informal evaluation on behalf of the sponsor or assessment review body

3.7
attack
attempt by an adversary on the device to obtain or modify sensitive information or a service he is not authorized to obtain or modify

3.8
certification report
output of the evaluation review body, based on the results from an accredited evaluation authority

3.9
controller
entity responsible for the secure management of an SCD

3.10
deliverables
documents, equipment and any other items or information needed by the evaluators to perform an evaluation of the SCD

