

Banking — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

ICS 35.040; 35.240.40

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

National foreword

This British Standard reproduces verbatim ISO 13491-1:1998 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Banking, Securities and other financial services, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO title page, pages ii to iv, pages 1 to 20 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 March 1999

© BSI 05-1999

ISBN 0 580 30590 2

Contents

	Page
National foreword	Inside front cover
Foreword	iv
Text of ISO 13491-1	1

INTERNATIONAL STANDARD

ISO
13491-1

First edition
1998-06-15

Banking — Secure cryptographic devices (retail) —

Part 1: Concepts, requirements and evaluation methods

*Banque — Dispositifs cryptographiques de sécurité (service aux
particuliers) —*

Partie 1: Concepts, prescriptions et méthodes d'évaluation



Contents

	Page
Foreword	iv
Introduction	1
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Secure cryptographic device concepts	3
4.1 Attack scenarios	4
4.1.1 Penetration	4
4.1.2 Monitoring	4
4.1.3 Manipulation	4
4.1.4 Modification	4
4.1.5 Substitution	4
4.2 Defence Measures	4
4.2.1 Device Characteristics	4
4.2.2 Device Management	5
4.2.3 Environment	5
5 Requirements for device characteristics	5
5.1 Introduction	5
5.2 Physical Security Requirements for SCDs	5
5.2.1 General	5
5.2.2 Tamper Evidence Requirement	6
5.2.3 Tamper Resistance Requirements	6
5.2.4 Tamper Response Requirements	6
5.3 Logical Security Requirements for SCDs	7
5.3.1 Assurance of genuine devices	7
5.3.2 Design of functions	7
5.3.3 Use of cryptographic keys	7
5.3.4 Sensitive Device States	7
5.3.5 Multiple Cryptographic Relationships	7
5.3.6 SCD Software Authentication	7
5.3.7 Minimally Tamper Resistant Devices with Tamper Evidence Characteristics	7
6 Requirements for device management	8
6.1 Life-Cycle Phases	8
6.2 Life Cycle Protection Requirements	9
6.2.1 Manufacturing and Post-Manufacturing	9
6.2.2 Pre-Use	9
6.2.3 Use	9
6.2.4 Post-Use	9
6.3 Life Cycle Protection Methods	9
6.3.1 Manufacturing	10
6.3.2 Post-Manufacturing	10
6.3.3 Pre-Use	10
6.3.4 Use	10
6.3.5 Post-Use	11
6.4 Accountability	11
6.5 Device Management Principles of Audit and Control	11
7 Evaluation method selection	13
7.1 Evaluation Methods	13
7.1.1 Informal Method	13

	Page
7.1.2 Semi-formal Method	13
7.1.3 Formal Method	13
7.2 Risk Assessment	13
7.3 Informal Evaluation Method	15
7.3.1 Manufacturer/Sponsor	15
7.3.2 Auditor	15
7.3.3 Audit Review Body	15
7.3.4 Audit Check-List	15
7.3.5 Auditor Results	15
7.3.6 Audit Report	16
7.4 Semi-Formal Evaluation Method	16
7.4.1 Manufacturer/Sponsor	16
7.4.2 Evaluation Agency	16
7.4.3 Evaluation Review Body	16
7.4.4 Evaluation Results	17
7.4.5 Evaluation Report	17
7.5 Formal Evaluation Method	17
Annex A (informative) Concepts of security levels for system security	18
Figure 1 — Evaluation Methods	14
Figure A.1	18
Figure A.2	19
Figure A.3	19
Figure A.4	20
Table 1 — Device Life-Cycle Phases	8
Table 2 — Audit and Control Principles	12
Table 3 — Risk Factors vs Evaluation Methods	14

Descriptors: Banking, banking documents, data processing, information interchange, protection of information, security techniques, cryptography, secure cryptographic devices, concepts, specifications, physical properties, characteristics, tests, conformity tests.

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 3.

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.

International Standard ISO 11568 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

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 check-lists for devices used in magnetic stripe card systems.*

Annex A of this part of ISO 13491 is for information only.

Introduction

ISO 13491 describes both the physical and logical characteristics and the management of the secure cryptographic devices (SCD's) used to protect messages, cryptographic keys and other sensitive information used in a retail banking environment, where a SCD is a physically and logically protected hardware device that provides a secure set of cryptographic services.

The security of retail electronic banking 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. While certain cryptographic equipment (e.g. host security modules) remain concentrated in the relatively high security of processing centers, a large proportion of cryptographic devices used in retail banking (e.g. PIN pads, ATM's, etc) now reside in non-secure environments. Therefore when Personal Identification Numbers (PIN's), Message Authentication Codes (MAC's), Cryptographic Keys and other sensitive data are processed in these devices, there is a risk that these devices may be tampered with or otherwise compromised to disclose or modify such data. It must be ensured that the risk of financial loss is reduced through the appropriate use of cryptographic devices that have proper characteristics and are properly managed.

1 Scope

This part of ISO 13491 specifies the requirements for Secure Cryptographic Devices which incorporate the cryptographic processes defined in ISO 9564, ISO 9807 and ISO 11568.

This part of ISO 13491 has two primary purposes:

- 1) to state the requirements concerning both the operational characteristics of SCD's and the management of such devices throughout all stages of their life cycle,
- 2) 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 practically achievable. 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 cryptographic device security. These aim for a high probability of detection of any illicit 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 secure cryptographic devices.

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

Specific requirements for the characteristics and management of specific types of SCD functionality used in the retail banking environment are contained in another part of ISO 13491.

2 Normative references

The following standards contain provisions which, through references in this text, constitute provisions of this part of ISO 13491. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreements based upon this part of ISO 13491 should apply the most recent edition of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security architecture*.

ISO 8908:1993, *Banking and related financial services — Vocabulary and data elements*.

ISO 9564-1:—, *Banking — Personal Identification Number management and security — Part 1: PIN protection principles and techniques*¹⁾.

¹⁾ To be published. (Revision of ISO 9564-1:1991)