SWEDISH STANDARDS INSTITUTE

SVENSK STANDARD
SS-ISO 13491-1:2007

Fastställd 2007-08-27
Utgåva 1

Banksystem – Utrustning för säker krypto-hantering –
Del 1: Begrepp, krav och metoder för evaluering (ISO 13491-1:2007, IDT)

Banking – Secure cryptographic devices (retail) –
Part 1: Concepts, requirements and evaluation methods (ISO 13491-1:2007, IDT)

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

ICS 35.240.40
Språk: engelska
Publicerad: oktober 2007
© Copyright SIS. Reproduction in any form without permission is prohibited.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

Den internationella standarden ISO 13491-1:2007 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO 13491-1:2007.

The International Standard ISO 13491-1:2007 has the status of a Swedish Standard. This document contains the official English version of ISO 13491-1:2007.

Upplysningar om **sakinnehållet** i standarden lämnas av SIS, Swedish Standards Institute,
telefon 08 - 555 520 00.

Standarder kan beställas hos SIS Förlag AB som även lämnar **allmänna upplysningar** om svensk och utländsk standard.
Postadress: SIS Förlag AB, 118 80 STOCKHOLM
Telefon: 08 - 555 523 10. *Telefax*: 08 - 555 523 11
E-post: sis.sales@sis.se. *Internet*: www.sis.se

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

Contents

Page

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

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*

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

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.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

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*

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

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

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

3.11
device compromise
successful defeat of the physical or logical protections provided by the SCD, resulting in the potential disclosure of sensitive information or unauthorized use of the SCD

3.12
device security
security of the SCD related to its characteristics only, without reference to a specific operational environment

3.13
environment-dependent security
security of an SCD as part of an operational environment

3.14
evaluation agency
organization trusted by the design, manufacturing and sponsoring authorities, which evaluates the SCD (using specialist skills and tools) in accordance with this part of ISO 13491

3.15
evaluation report
output of the evaluation review body, based on the results from an evaluation agency or auditor

3.16
evaluation review body
group with responsibility for reviewing, and making judgements on, the results of the evaluation agency

3.17
formal claim
statement about the characteristics and functions of an SCD

3.18
logical security
ability of a device to withstand attacks through its functional interface

3.19
operational environment
environment in which the SCD is operated, i.e. the system of which it is part, the location where it is placed, the persons operating and using it and the entities communicating with it

3.20
physical security
ability of a device to withstand attacks against its physical construction, including physical characteristics such as electromagnetic emissions and power fluctuations, the analysis of which can lead to side channel attacks

3.21
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage (e.g. PIN entry device or hardware security module), and which may be integrated into a larger system, such as an automated teller machine (ATM) or point of sale (POS) terminal

3.22
sensitive data
sensitive information
data, status information, cryptographic keys, etc., which need to be protected against unauthorized disclosure, alteration, or destruction

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

3.23
sensitive state
device condition that provides access to the secure operator interface, such that it can only be entered when the device is under dual or multiple control

3.24
sponsoring authority
sponsor
individual, company or organization that requires the SCD to undergo evaluation

3.25
tamper evident characteristic
characteristic that provides evidence that an attack has been attempted

3.26
tamper resistant characteristic
characteristic that provides passive physical protection against an attack

3.27
tamper response characteristic
characteristic that provides an active response to the detection of an attack

4 Abbreviated terms

ATM	automated teller machine
MAC	message authentication code
PIN	Personal Identification Number
POS	point of sale
SCD	secure cryptographic device

5 Secure cryptographic device concepts

5.1 General

Cryptography is used in retail financial services to help ensure the following objectives:

a) the integrity and authenticity of sensitive data, e.g. by MAC-ing transaction details;

b) the confidentiality of secret information, e.g. by encrypting customer PINs;

c) the confidentiality, integrity and authenticity of cryptographic keys;

d) the security of other sensitive operations, e.g. PIN verification.

To ensure that the above objectives are met, the following threats to the security of the cryptographic processing shall be countered:

— disclosure or modification of cryptographic keys and other sensitive information;

— unauthorized use of cryptographic keys and services.

This preview is downloaded from www.sis.se. Buy the entire standard via https://www.sis.se/std-62900

A secure cryptographic device (SCD) is a physically and logically secure hardware device providing a defined set of cryptographic functions, access controls and secure key storage. SCDs are employed to protect against these threats. The requirements of this part of ISO 13491 pertain to the SCD and not the system in which the SCD may be integrated. However, it is important to analyse the interfaces between the SCD and the remainder of the system to ensure that the SCD may not be compromised.

Since absolute security is not achievable in practical terms, it is not realistic to describe an SCD as being “tamper proof” or “physically secure”. With enough cost, effort and skill, virtually any security scheme can be defeated. Furthermore, as technology continues to evolve, new techniques may be developed to attack a security scheme that was previously believed to be immune to feasible attack. Therefore, it is more realistic to categorize an SCD as possessing a degree of tamper protection, where an acceptable degree is one that is deemed adequate to deter any attack envisaged as feasible during the operational life of the device, taking into account the equipment, skills and other costs to the adversary in mounting a successful attack and the financial benefits that the adversary could realize from such an attack.

Security of retail payment systems includes the physical and logical aspects of device security, the security of the operational environment and management of the device. These factors establish jointly the security of the devices and the applications in which they are used. The security needs are derived from an assessment of the risks arising from the intended applications.

The required security characteristics will depend on the intended application and operational environment, and on the attack types that need to be considered. A risk assessment should be made as an aid to selecting the most appropriate method of evaluating the security of the device. The results are then assessed in order to accept the devices for a certain application and environment. Evaluation methods are given in Clause 8.

5.2 Attack scenarios

5.2.1 General

SCDs are subject to the following five primary classes of attack, which may be used in combination:

— penetration;

— monitoring;

— manipulation;

— modification;

— substitution.

These attacks are described below.

NOTE These attack scenarios do not form an exhaustive list, but are an indication of the main areas of concern.

5.2.2 Penetration

Penetration is an attack which involves the physical perforation or unauthorized opening of the device to ascertain sensitive data contained within it, e.g. cryptographic keys.

5.2.3 Monitoring

Monitoring is an attack which may involve the monitoring of electromagnetic radiation, power consumption differentials, timing differentials, etc. for the purposes of discovering sensitive information contained within the device. Alternatively, it may involve the visual, aural or electronic monitoring of secret data being entered into the device.