American National Standard for Financial Services

X9.97-2:2009
Identical to
ISO 13491-2:2005

Banking — Secure cryptographic devices (retail) —

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

Accredited Standards Committee X9, Incorporated
Financial Services Industry

Date Approved: 5/22/2009

American National Standards Institute

Contents

Page

Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretation should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by:

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

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 must 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. parts 1 to 3 of ISO/IEC 15408 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.

Banking — 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 parts 1 and 2 of ISO 9564, ISO 16609 and parts 1 to 6 of ISO 11568, 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 document.

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 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 9564-1:2002, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO 9564-2, *Banking — Personal Identification Number management and security — Part 2: Approved algorithms for PIN encipherment*

ISO 11568 (all parts), *Banking — Key management (retail)*

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

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

ISO 18031, *Information technology — Random number generation*

3 Terms and definitions

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