Indian Standard

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*