

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 4 ASYMMETRIC CRYPTOSYSTEMS — KEY MANAGEMENT AND LIFE CYCLE

(First Revision)

1 Scope

This part of ISO 11568 specifies techniques for the protection of symmetric and asymmetric cryptographic keys in a retail financial services environment using asymmetric cryptosystems and the life cycle management of the associated asymmetric keys. The techniques described in this part of ISO 11568 enable compliance with the principles described in ISO 11568-1. For the purposes of this document, the retail financial services environment is restricted to the interface between:

- | a card-accepting device and an acquirer;
- | an acquirer and a card issuer;
- | an ICC and a card-accepting device.

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

ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash functions*

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

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

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

(PREVIEW)

IS 15256 (Part 4) : 2013

ISO 11568-4 : 2007

ISO/IEC 14888-3, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO 15782-1:2003, *Certificate management for financial services — Part 1: Public key certificates*

ISO/IEC 15946-3:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment*

ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ANSI X9.42-2003, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*