IS 15256 (Part 1) : 2011
ISO 11568-1 : 2005

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 1 PRINCIPLES

(*First Revision*)

1 Scope

This part of ISO 11568 specifies the principles for the management of keys used in cryptosystems implemented within the retail banking environment. The retail banking environment includes the interface between

— a card accepting device and an acquirer,
— an acquirer and a card issuer,
— an ICC and a card-accepting device.

An example of this environment is described in Annex B, and threats associated with the implementation of this part of ISO 11568 in the retail banking environment are elaborated in Annex C.

This part of ISO 11568 is applicable both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the private and public keys of asymmetric cryptosystems, unless otherwise stated. The procedure for the approval of cryptographic algorithms used for key management is specified in Annex A.

The use of ciphers often involves control information other than keys, e.g. initialization vectors and key identifiers. This other information is collectively called “keying material”. Although this part of ISO 11568 specifically addresses the management of keys, the principles, services, and techniques applicable to keys may also be applicable to keying material.

This part of ISO 11568 is appropriate for use by financial institutions and other organizations engaged in the area of retail financial services, where the interchange of information requires confidentiality, integrity, or authentication. Retail financial services include but are not limited to such processes as POS debit and credit authorizations, automated dispensing machine and ATM transactions, etc.

ISO 9564 and ISO 16609 specify the use of cryptographic operations within retail financial transactions for personal identification number (PIN) encipherment and message authentication, respectively. The ISO 11568 series of standards is applicable to the management of the keys introduced by those standards. Additionally, the key management procedures may themselves require the introduction of further keys, e.g. key encipherment keys. The key management procedures are equally applicable to those keys.

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 11568-2:1994, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO 11568-4:1998, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*