IS 15042 (Part 2) : 2007
ISO 9564-2 : 2005

Indian Standard

BANKING — PERSONAL IDENTIFICATION NUMBER MANAGEMENT AND SECURITY

PART 2 APPROVED ALGORITHMS FOR PIN ENCIPHERMENT

(*First Revision*)

1 Scope

This part of ISO 9564 specifies algorithms for the encipherment of Personal Identification Numbers (PINs). These algorithms, based on the approval processes established in ISO 9564-1, are the data encryption algorithm (DEA) and the RSA encryption algorithm.

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 9564-3, *Banking — Personal identification Number management and security — Part 3: Requirements for offline P/N handling in ATM and POS systems*

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

ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric Ciphers*

EMV 2000, *Integrated Circuit Card Specifications for Payment Systems, Book 2: Security and Key Management')*

ANSI INCITS 92-1981, *Data Encryption Algorithm* [formerly ANSI X3.92-1981 (R1998)][2)]

ANSI X9.52-1 998, *Triple Data Encryption Algorithm Modes of Operation*[2)]

AS 2805.5.3-1992, *Electronic funds transfer — Requirements for interfaces — Ciphers — Data encipherment algorithm 2 (DEA 2)* [3)]

---

1) EMV Europay, Mastercard, VISA.
2) American National Standards Institute standard
3) Standards Australia standard.