



COMPENDIUM OF
INDIAN STANDARDS
ON

SECURITY IN FINANCIAL SERVICES

Prepared by:

**SERVICE SECTOR
DEPARTMENT**



BUREAU OF INDIAN STANDARDS

NEW DELHI

INTRODUCTION

This compendium is a collection of Indian standards published by Bureau of Indian Standard in the field of Banking and Financial Securities Services, developed and published by the Banking and Financial Services Sectional Committee, SSD 03, of Bureau of Indian Standards.

The information contained in this compendium can be beneficial to the stakeholders providing services in the field of banks and financial institutions, Fin-Tech companies and Regulators and compliance offices service providers.

1. IS/ISO 5158:2023 — Mobile financial services — Customer identification guidelines

The standard covers the guidelines for customer identification in mobile financial services (MFS), covering a general identification framework, evaluation of identity assurance levels (ALs), and related security and privacy considerations. The guidelines apply to various MFS providers, such as banks and third-party payment services, and focus on identifying natural persons.

2. IS 15042 (Part 1):2021/ISO 9564-1:2017 — Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems

The standard specifies the basic principles and techniques which provide the minimum security measures required for effective international PIN management. These measures are applicable to those institutions responsible for implementing techniques for the management and protection of PINs during their creation, issuance, usage and deactivation.

3. IS 15042 (Part 2):2017/ISO 9564-2: 2014 — Financial services — Personal Identification Number (PIN) management and security — Part 2: Approved algorithms for PIN encipherment

The standard specifies the approved cryptographic algorithms for enciphering Personal Identification Numbers (PINs) in card-based systems, ensuring that PINs are securely protected throughout their lifecycle.

4. IS 15042 (Part 4):2019/ISO 9564-4: 2016 — Financial services — Personal Identification Number (PIN) management and security — Part 4: Requirements for PIN handling in e Commerce for Payment Transactions

The standard specifies the requirements for the use and management of cardholder PINs in e-Commerce transactions involving card-based verification, such as ATM, POS terminals, fuel dispensers, and vending machines. It applies to organizations managing PIN verification in these contexts.

5. IS 15256:2024/ISO 11568: 2023 — Financial services — Key management (retail)

The standard describes the management of symmetric and asymmetric cryptographic keys that can be used to protect sensitive information in financial services related to retail payments. The document covers all aspects of retail financial services, including connections between a card-accepting device and an acquirer, between an acquirer and a card issuer.

6. IS 16005 (Part 1):2019/ISO 13491-1: 2016 — Financial services — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods

The standard defines the security characteristics for Secure Cryptographic Devices (SCDs) and specifies the operational and management requirements throughout the device lifecycle.

7. IS 16005 (Part 2):2023/ISO 13491-2:2023 — Financial services — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions

The Standard provides security compliance checklists for evaluating Secure Cryptographic Devices (SCDs) used to protect sensitive information in financial transactions.

8. IS 16007: 2021/ISO 13492: 2019 — Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption

The standard describes a data element related to key management which can be transmitted either in transaction messages to convey information about cryptographic keys used to secure the current transaction, or in cryptographic service messages to convey information about cryptographic keys to be used to secure future transactions.

9. IS 15899:2023/ISO 16609:2022 — Financial services — Requirements for message authentication using symmetric techniques

The standard outlines the procedures for ensuring the authenticity and integrity of financial messages using symmetric encryption techniques and applies to both stored data and transmitted messages and aims to protect against unauthorized modification and ensure message authenticity.

10. IS/ISO/TR 19038: 2005 — Banking and related financial services — Triple DEA— Modes of operation — Implementation guidelines

The standard provides the technical support and implementation guidelines for the **Triple Data Encryption Algorithm (TDEA)** modes of operation, ensuring enhanced cryptographic protection of digital data in financial applications.

11. IS/ISO 20038: 2017 Banking and related financial services — Key wrap using AES

The guidelines provided in this standard are crucial for financial institutions to implement secure key management practices. By defining standardized methods for key wrapping, derivation, and validation, the standard ensures the protection of sensitive cryptographic keys, fostering trust and security across banking and related financial services.

12. IS/ISO 21188: 2018 Public key infrastructure for financial services — Practices and policy framework

This standard provides essential guidelines for financial institutions and regulatory bodies to implement and maintain secure PKI systems. By defining clear processes for certificate management, security controls, and trust models, it ensures the reliability, integrity, and interoperability of digital financial transactions.

13. IS/ISO 23195: 2021 Security objectives of information systems of third- party payment services

This standard specifies terminology for third-party payment (TPP) services, defines two logical models to identify protected assets, and outlines security objectives to counter threats specific to TPP-based payment flows.

*For further details of these Indian Standards, please visit **KNOW YOUR STANDARD** section of BIS website using the following link:*

https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/nowyourstandards/indian_standards/isdetails