

Indian Standard

FINANCIAL SERVICES — KEY MANAGEMENT RELATED DATA ELEMENT — APPLICATION AND USAGE OF ISO 8583 DATA ELEMENTS 53 AND 96

1 Scope

This International Standard describes a key management related data element that 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.

This International Standard addresses the requirements for the use of the key management related data element within ISO 8583, using the following two ISO 8583 data elements:

security related control information (data element 53), or

key management data (data element 96).

However, these data elements can be usefully employed in other messaging formats, given that the transportation of key management related data is not limited to ISO 8583.

This International Standard is applicable to either symmetric or asymmetric cipher systems. Key management procedures for the secure management of the cryptographic keys within the financial services environment are described in ISO 11568. Security related data, such as PIN data and MACs, are described in ISO 9564 and ISO 16609, respectively.

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/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

ISO/IEC 7812-2, *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

ISO 8583-1, *Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*