IS 15256 (Part 6) : 2002
ISO 11568-6 : 1998

भारतीय मानक

बैंकिंग — कुंजी प्रबंधन (खुदरा)

भाग 6 कुंजी प्रबंधन योजनाएँ

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 6 KEY MANAGEMENT SCHEMES

ICS 35.240.40

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

November 2002

Price Group 6

NATIONAL FOREWORD

This Indian Standard (Part 6) which is identical with ISO 11568-6:1998 'Banking — Key management (retail) — Part 6 : Key management schemes' issued by the International Organization for Standardization (ISO) was adopted by the Bureau of Indian Standards on the recommendation of the Banking and Financial Services Sectional Committee (MSD 7) and approval of the Management and Systems Division Council.

The text of the International Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

In this adopted standard, normative references appear to the following International Standards for which Indian Standards do not exist:

ISO 8908:1993	Banking and related financial services — Vocabulary and data elements
ISO/IEC 9796:1991	Information technology — Security techniques — Digital signature scheme giving message recovery
ISO/IEC 9798-3:1993	Information technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm
ISO/IEC 10118 (all parts)	Information technology — Security techniques — Hash functions
ISO 11166 (all parts)	Banking — Key management by means of asymmetric algorithms
ISO 11568-1:1994	Banking — Key management (retail) — Part 1 : Introduction to key management
ISO/IEC 11770-3:1999	Information technology — Security techniques — Key management — Part 3 : Mechanisms using asymmetric techniques
ISO 13491-1:1998	Banking — Secure cryptographic devices (retail) — Part 1 : Concepts, requirements and evaluation methods
ISO 13491-2 : 2000	Banking — Secure cryptographic devices (retail) — Part 2 : Security compliance checklists for devices used in magnetic stripe card systems

The International Standards ISO 8908 and ISO 11166 (all parts) have been withdrawn by the International Organization for Standardization (ISO).

In this adopted standard, informative references also appear to the following International Standards, for which no Indian Standards exist:

ISO 8732:1988	Banking — Key management (wholesale)
ISO 11568-2:1994	Banking — Key management (retail) — Part 2 : Key management techniques for symmetric ciphers
ISO 11568-3:1994	Banking — Key management (retail) — Part 3 : Key life cycle for symmetric ciphers

(*Continued on third cover*)

Introduction

ISO 11568 is one of a series of standards describing procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568 but will be addressed in another ISO standard.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard addresses the key management requirements that are applicable in the more accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machine (ATM) transactions.

ISO 11568 is a multi-part standard.

This part of ISO 11568 provides general information and criteria concerning key management schemes for use in a retail banking environment. Annex A provides a description of certain key management schemes that are considered by ISO members as suitable for implementation in the retail banking environment.

Indian Standard

BANKING — KEY MANAGEMENT (RETAIL)

PART 6 KEY MANAGEMENT SCHEMES

1 Scope

This part of ISO 11568 contains descriptions of key management schemes that have been submitted by national standards bodies of member countries as suitable for implementation in retail banking environments.

Each description is intended only to provide an overview of the key management scheme, pointing out its main characteristics, the particular techniques employed and other useful information.

More detailed information about these schemes is to be found in the documents named as reference material within each description.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11568. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11568 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8908:1993, *Banking and related financial services — Vocabulary and data elements.*

ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

ISO/IEC 9798-3:1993, *Information technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm.*

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

ISO 11166 (all parts), *Banking — Key management by means of asymmetric algorithms.*

ISO 11568-1:1994, *Banking — Key management (retail) — Part 1: Introduction to key management.*

ISO/IEC 11770:—[1)], *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.*

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

ISO 13491-2:—[1)], *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in magnetic stripe card systems.*

---

1) To be published.

3 Definitions

For the purposes of this part of ISO 11568, the definitions given in ISO 8908 apply.

4 Generic overview of retail banking key management schemes

A key management scheme is a set of rules that define how cryptographic keys in retail banking systems are to be created, distributed, used and replaced.

The objective of a key management scheme is to ensure that cryptographic keys are managed in such a way that the data that is ultimately to be protected will be safeguarded from potential compromise resulting from non-secure creation, transfer, use or replacement of cryptographic keys.

In order to accomplish this objective, key management schemes shall employ key management techniques described in ISO 11568-2 and ISO 11568-4.

Secure cryptographic devices, as described in ISO 13491, shall be used to provide the intended level of security.

The requirements and implementation of the phases of the life cycle of cryptographic keys are addressed in ISO 11568-3 and ISO 11568-5.

Key management schemes may employ symmetric, asymmetric or hybrid techniques.

A key management scheme shall conform to the key management principles set out in ISO 11568-1.

5 List of key management schemes

The following key management schemes are described in annex A of this part of ISO 11568.

— A.1 Inter-bank key management scheme (France)

— A.2 Transaction key management scheme (UK)

— A.3 Derived unique key per transaction scheme (USA)

— A.4 Telematic Base Security Standard (Switzerland)

— A.5 Terminal to Acquirer Key Management — Transaction Keys (Australia)

— A.6 Node to Node Key Management — Session Keys (Australia)

— A.7 Terminal to Acquirer Key Management — Session Keys (Australia)

— A.8 Terminal Cryptographic Unit Initialization using Asymmetric Cipher (Australia)

Annex A
(informative)

Description of key management schemes

A.1 Inter-bank key management scheme

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *Inter-Bank Key Management Scheme*
SUBMITTED BY: *AFNOR* (France)
ASSOCIATED ALGORITHM(S): *DEA*
DESCRIPTION OF SCHEME: Master Key. Connection Keys: Cryptoperiod is several years. Key encipherment keys: This is an optional layer in the key hierarchy for use in high-volume systems. Cryptoperiod is 3 times the cryptoperiod of data keys — less one day. This is 3 months at the most. Data keys (= Session keys): Automatically generated and distributed every "n" days — 31 days at the most. These keys are: — PIN Encryption key — MAC key NOTE This implementation is a variation of Master Key/Session Key.
KNOWN IMPLEMENTATIONS: Inter-bank network in France.
TECHNICAL REFERENCES: Groupement Cartes Bancaires STUR RCB.

A.2 Transaction key management scheme

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *APACS 40 TRANSACTION KEY*
SUBMITTED BY: *APACS, U.K.*
ASSOCIATED ALGORITHM(S): *DEA* (as defined in ANSI X3.92)
DESCRIPTION OF SCHEME: The scheme carries out the functions of: a) Message authentication — producing 32-bit MAC's in accordance with ANSI X9.19. b) PIN encryption — using a PIN/PAN block format in accordance with ANSI X9.8. **Key Management** Separate keys are used for the two functions. The keys are updated for each transaction using card data, a key register and a one-way function. The key register is updated at the terminal and the host using MAC residues. Messages within a transaction are linked by including the MAC residue from the previous message in the MAC calculation. End-to-end and "break forward" protection for PIN's can be acheived by omitting some of the card data from the transmitted messages. NOTE This implementation is a variation on Non-Reversibly Transformed unique key per Transaction.
KNOWN IMPLEMENTATIONS: U.K.
TECHNICAL REFERENCES: APACS Standard 40: *Acquirer Interface Requirements for Electronic Data Capture Terminals: Data Capture Terminals: Part 3, Section 3 — Security.*

A.3 Derived unique key per transaction scheme

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *Derived Unique Key per Transaction*
SUBMITTED BY: *U.S.A.*
ASSOCIATED ALGORITHM(S): *DEA*
DESCRIPTION OF SCHEME: A unique key is generated for each transaction. A Security Management Information Data element (SMID) resides in each terminal and in each acquirer security module. A SMID contains: — key set identifier (KSID) that identifies/designates base key; — tamper resistant security module (TRSM) ID that enables acquirer to compute initially; — loaded key; — transaction counter, incremented with each transaction using cryptography. Terminal derives (i.e. creates) a new transaction key from previous transaction key. Based on data in its SMID, acquirer can compute transaction key for any transaction from any terminal to which it is linked.
KNOWN IMPLEMENTATIONS: U.S.A.
TECHNICAL REFERENCES: ANSI X9.24.

A.4 Telematic Base Security Standard

RETAIL BANKING — KEY MANAGEMENT SCHEMES

(to be used in conjunction with ISO 11568-6)

NAME OF KEY MANAGEMENT SCHEME: *Telematic Base Security Standard* (TBSS)

SUBMITTED BY: *National Body of Switzerland*

ASSOCIATED ALGORITHM(S): *RSA, RIPEMD*

DESCRIPTION OF SCHEME:

The TBSS specifies services and mechanisms required to secure telebanking services. All mechanisms follow international standards (or drafts), limit the options allowed therein and specify algorithms to be used such that interoperability can be guaranteed. TBSS standardizes mechanisms and procedures for the following Security Services — Entity Authentication, Confidentiality, Non-repudiation of origin and receipt — and includes the necessary key management services and mechanisms. An outline of the relevant parts of TBSS is given below.

a) **Key Transport**

Describes the mechanisms for the secure transfer of secret keys to be used for symmetric algorithms. As key transport always has to be done in an authenticated manner, these mechanisms fulfil the aim of entity (or user) authentication at the same time. Three key transport mechanisms (which differ in the capabilities of the partners and the features) are specified:

1) **Key Transport Mechanism 1**

One pass; uses Digital Signatures and RSA encipherment together with a time-stamp or sequence number. Follows ISO/IEC 11770-3 and conforms to ISO 11166-1. Features: Mutual authentication (implicit/explicit), key determined by one party.

2) **Key Transport Mechanism 2**

Two pass; uses asymmetric encipherment (RSA) together with random numbers. Follows ISO/IEC 11770-3. Features: Unilateral authentication, key determined by one party.

3) **Key Transport Mechanism 3**

Three pass; uses asymmetric encipherment (RSA) together with random numbers. Follows ISO/IEC 11770-3. Features: Mutual authentication, key determined by both parties.

b) **Public Key Transport without certificate**

— Via authentic channel.

— With written confirmations.

— Transport of a signed message containing the Public Key; check authenticity by comparing a hash transported over a different channel (letter, registered mail).

c) **Certification and Public Key Directories** *(This section is not written yet.)*

NOTE Certain weaknesses in the RIPEMD algorithm have been identified by German cryptoanalysts.

KNOWN IMPLEMENTATIONS: Videotext telebanking: currently being developed under this standard. EDIFACT message security: planned.

TECHNICAL REFERENCES: ISO/IEC 9796, ISO/IEC 9798-3, ISO/IEC 10118, ISO 11166-1, ISO 11568-1, ISO/IEC 11770-3.

A.5 Terminal to Acquirer Key Management — Transaction Keys

RETAIL BANKING — KEY MANAGEMENT SCHEMES

(to be used in conjunction with ISO 11568-6)

NAME OF KEY MANAGEMENT SCHEME: *Terminal to Acquirer Key Management — Transaction Keys*

SUBMITTED BY: *Australian National Body — Technical Committee IT/5*

ASSOCIATED ALGORITHM(S): *DEA*

DESCRIPTION OF SCHEME:

This standard specifies key management techniques for keys used in the authentication, encryption and decryption of electronic messages relating to financial transactions using transaction keys. It may be adopted in situations where a secure terminal-acquirer dialogue is desired and the terminal devices are at least tamper-evident, as defined in clause 4.4 of AS 2805 6.1.

This key management system is based on a terminal key whose value at any time is dependent on the Message Authentication Code (MAC) residues of previous transactions. For each transaction a new set of transaction keys, including a MAC key and a PIN encryption key, is cryptographically generated using the terminal key and data read from the financial transaction card.

The scheme is intended to prevent back-tracking of previous transactions and to fulfil the requirements of a Terminal Cryptographic Unit (TCU) utilizing a 64-bit block oriented algorithm. Furthermore, the scheme provides for:

a) the encryption keys to change with every transaction;

b) different keys for PIN encryption, message authentication and privacy (data encryption);

c) a measure of end-to-end (acceptor to issuer) protection when card key information is available but not transmitted;

d) card issuer authentication by means of an Authentication Parameter (AP);

e) prevention of the use of data intercepted on the communications link from being used to derive future keys;

f) an audit trail by chaining together a successive set of transactions on the basis of the Message Authentication Code (MAC) residue key update procedures;

g) the usage of five permutations of subsets of the card data and the repeated application of a common one-way function;

h) the progressive implementation of parts of the scheme in appropriate intelligent card technology, thus providing a higher level of protection to the card holder.

NOTE This implementation is a variation on Non-Reversibly Transformed unique key per Transaction.

KNOWN IMPLEMENTATIONS: Australian EFT/POS Networks. Australian Banking Industry.

TECHNICAL REFERENCES: Australian Standard AS 2805 6.2 and others in this series.

A.6 Node to Node Key Management — Session Keys

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *Node to Node Key Management — Session Keys*
SUBMITTED BY: *Australian National Body — Technical Committee IT/5*
ASSOCIATED ALGORITHM(S): *DEA*
DESCRIPTION OF SCHEME: This standard specifies key management techniques for keys used in the authentication, encryption and decryption of electronic messages relating to financial transactions using session keys. In particular, this standard defines security interface procedures between nodes, methods of interchange of the various encryption keys used for securing transactions and ensures that messages can only be authenticated at their correct destination. The conventions may be adopted in all situations where a secure node-to-node dialogue is desired and can be used in conjunction with the terminal-to-acquirer systems, as described in another part of the standard. The objective is to provide a key management scheme for use between any two nodes in a network and divide different keys for PIN encryption, message authentication and privacy (data encryption). A key hierarchy of two levels is maintained: a) Level 1 — Key Encrypting Key (KEK); the KEK is statistically unique to each link and is used to encrypt session keys to enable secure exchange of the keys on that link. b) Level 2 — Session Keys (KS); separate KS are maintained for each function and direction of transmission. There are two privacy (data encryption) keys on a link; one for encrypting data to be sent and the other for decrypting data received. There are two MAC keys: one for computing MACs on messages to be sent and the other for verifying MACs on messages received. There shall be two PIN encryption keys for encrypting PINs on a link, one for each direction of transmission. The advantages of the system are two fold: a) the scheme is independent of the network architecture and allows for gateways to other networks, and b) the node-to-node scheme can be used in conjunction with the schemes as described in AS 2805 6.2 and AS 2805 6.4. NOTE This implementation is a variation of Master Key/Session Key.
KNOWN IMPLEMENTATIONS:Australian EFT/POS Networks. Australian Banking Industry. Interchange between Australian banks and switches.
TECHNICAL REFERENCES: Australian Standard AS 2805 6.3 and others in this series.

A.7 Terminal to Acquirer Key Management — Session Keys

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *Terminal to Acquirer Key Management — Session Keys*
SUBMITTED BY: *Australian National Body — Technical Committee IT/5*
ASSOCIATED ALGORITHM(S): *DEA*
DESCRIPTION OF SCHEME: This standard specifies key management techniques for keys used in the authentication, encryption and decryption of electronic messages relating to financial transactions using session keys. In particular, this standard defines security interface procedures between nodes, methods of interchange of the various encryption keys used for securing transactions and ensures that messages can only be authenticated at their correct destination. The objective is to provide a key management scheme for use between a terminal and an acquirer in a network. The terminal-to-acquirer mechanism provides for session keys to be generated by the acquirer and for these to be communicated to the terminal encrypted under a key encrypting key. The key encrypting keys are not like traditional master keys in that they are themselves updated by means of a one-way function from information that is not transmitted. The key update is initiated by the acquirer, who controls the update frequency. The scheme is used to prevent back-tracking of key encrypting key changes and, hence, prevents back-tracking of transactions prior to the last update of the key encrypting keys. Furthermore, the scheme divides different keys for PIN encryption, message authentication and privacy (data encryption). A key hierarchy of two levels is maintained: a) Level 1 — Key Encrypting Key (KEK); the KEK is statistically unique to each link and is used to encrypt session keys to enable secure exchange of the keys on that link. b) Level 2 — Session Keys (KS); separate KS are maintained for each function and direction of transmission. There are two privacy (data encryption) keys on a link: one for encrypting data to be sent and other for decrypting data received. There are two MAC keys: one for computing MACs on messages to be sent and the other for verifying MACs on messages received. There is one PIN encryption key for encrypting PINs on a terminal-to-acquirer link. For the terminal-to-acquirer links, these keys are dynamically created by the acquirer in such a way as to ensure statistical uniqueness and to prevent the ability to forecast any key. The advantages of the system are two-fold: a) the scheme is independent of the network architecture and allows for gateways to other networks, and b) multiple acquirers are allowed access to terminals and each is responsible for its own security; less security on the part of one acquirer does not jeopardize the security of others. Each acquirer to which a terminal can communicate has its own partitioned set of keys and data that cannot be accessed by any other acquirer.
KNOWN IMPLEMENTATIONS:Australian EFT/POS Networks. Australian Banking Industry.
TECHNICAL REFERENCES: Australian Standard AS 2805 6.4 and others in this series.

A.8 Terminal Cryptographic Unit Initialization using Asymmetric Cipher

RETAIL BANKING — KEY MANAGEMENT SCHEMES (to be used in conjunction with ISO 11568-6)
NAME OF KEY MANAGEMENT SCHEME: *Terminal Cryptographic Unit Initialization using Asymmetric Cipher*
SUBMITTED BY: *Australian National Body — Technical Committee IT/5*
ASSOCIATED ALGORITHM(S): *DEA, RSA*
DESCRIPTION OF SCHEME: The standard defines the interface and method to initialize remotely a Terminal Cryptographic Unit (TCU) and is designed to be adopted wherever secure remote terminal initialization is required and it is desired to avoid delivery via a sponsor facility for secure initialization. The term "initialization" refers only to the initial set-up of a cryptographic keying relationship between the TCU and the sponsor and acquirers. The main objective of the scheme is to remove the requirement for visits by agents of acquirers during the life of a TCU for the purpose of initialization of key management cryptographic variables and defines the technique by which terminals can be remotely initialized. Initialization is limited to cryptographic initialization of the first key of the TCU's key management scheme. Furthermore, the scheme minimizes the probability of initialization of TCUs unknown to the sponsor.
KNOWN IMPLEMENTATIONS: Australian EFT/POS Networks. Australian Banking Industry. Interchange between Australian banks and switches.
TECHNICAL REFERENCES: Australian Standard AS 2805 6.5.3 and others in this series.

Annex B
(informative)

Bibliography

[1] ISO 8732:1988, *Banking — Key management (wholesale).*

[2] ISO 11568-2:1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers.*

[3] ISO 11568-3:1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers.*

[4] ISO 11568-4:—[2)], *Banking — Key management (retail) — Part 4: Key management techniques using public key cryptography.*

[5] ISO 11568-5:—[2)], *Banking — Key management (retail) — Part 5: Key life cycle for public key cryptosystems.*

(*Continued from second cover*)

ISO 11568-4:1998	Banking — Key management (retail) — Part 4 : Key management techniques using public key cryptography
ISO 11568-5:1998	Banking — Key management (retail) — Part 5 : Key life cycle for public key cryptosystems

The Sectional Committee responsible for the preparation of this standard has reviewed the provisions of the above referred standards and has decided that they are acceptable as such for use in conjunction with this standard.

Annexes A and B of this standard are for information only.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act,* 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc : No. MSD 7 (249).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters :

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110 002
Telephones : 323 01 31, 323 33 75, 323 94 02

Telegrams : Manaksanstha
(Common to all offices)

Regional Offices :		Telephone
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110 002	323 76 17 323 38 41
Eastern	: 1/14 C.I.T. Scheme VI M, V. I. P. Road, Kankurgachi KOLKATA 700 054	337 84 99, 337 85 61 337 86 26, 337 91 20
Northern	: SCO 335-336, Sector 34-A, CHANDIGARH 160 022	60 38 43 60 20 25
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600 113	254 12 16, 254 14 42 254 25 19, 254 13 15
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400 093	832 92 95, 832 78 58 832 78 91, 832 78 92

Branches : AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. NALAGARH. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.

Printed by Dee Kay Printers.