INTERNATIONAL STANDARD

ISO 8732

First edition
1988-11-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Banking — Key management (wholesale)

Banque — Gestion de clés

Reference number
ISO 8732 : 1988 (E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 8732 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services.*

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Printed in Switzerland

Contents

Figures

Tables

Introduction

This International Standard describes procedures for the secure management of the secret cryptographic keys used to protect messages in a wholesale banking environment, for instance messages between banks, or between a bank and a corporate customer, or a bank and a government.

Key management is the process whereby cryptographic keys and initialisation vectors (keying material) are provided for use by two parties and continue to be subject to secure handling procedures until they have been destroyed. The security of the data enciphered by means of keying material is dependent upon the prevention of unauthorised disclosure, modification, substitution, insertion or deletion of keys or initialisation vectors (IVs). If these are compromised the security of the related data can no longer be ensured. Thus, key management is concerned with the generation, distribution, storage, custody, monitoring, destruction, and back-up procedures for keying material. Also, by the formalisation of such procedures provision is made for audit trails to be established.

Automated key distribution is the electronic transmission of cryptographic keys (and, where needed, IVs) via a communication channel. Automated key distribution utilises two types of keys:

1) Key Enciphering Keys: used to encipher and decipher other keys.

2) Data keys: used to encipher and decipher initialisation vectors (IVs), to authenticate Cryptographic Service Messages, and to encipher/decipher or authenticate data.

Since key management facility(s) can be designed to replace electronically distributed Key Enciphering Keys and data keys automatically, manual intervention is kept to a minimum. Key Enciphering Keys generally have longer cryptoperiods than data keys.

The level of security to be achieved needs to be related to a number of factors, including the sensitivity of the data concerned and the likelihood that it will be intercepted, the practicality of any envisaged encipherment process, and the cost of providing, and breaking, a particular means of providing security. It is therefore necessary for each communicating pair to agree the extent and detail of security and key management procedures. Absolute security is not practically achievable so key management procedures need not only to aim to reduce the opportunity for a breach of security but also to aim for a 'high' probability of detection of any illicit access or change to keying material that may occur despite any preventative measures. This applies at all stages of the generation, exchange and use of keying material, including those processes that occur in cryptographic equipment and those related to communication of cryptographic keys and initialisation vectors between communicating pairs or key centres. Thus, whilst wherever possible this International Standard has specified requirements in absolute terms, in some instances a level of subjectivity cannot be practically avoided. For instance, defining the frequency of key change is beyond the scope of this standard, and will be dependent upon the degree of risk associated with the factors listed above.

This International Standard has been divided into sections, as follows:

One: General
Two: Manual distribution of keying material
Three: Automatic distribution of keying material

The final details of the key management procedures need to be agreed between the communicating pair(s) concerned and will thus remain the responsibility of the communicating pair(s). An aspect of the detail to be agreed will be the identity and duties of particular individuals. This International Standard does not concern itself with allocation of individual responsibilities as this needs to be considered uniquely for each key management implementation.

Annex A gives an example of the implementation of the requirements for manual distribution of keying material.

This page intentionally left blank

Banking — Key management (wholesale)

Section 1 : General

1 Scope and field of application

This International Standard specifies methods for the management of keying material used for the encipherment, decipherment and authentication of messages exchanged in the course of wholesale financial transactions. It specifies requirements for

i) the control during its life of keying material to prevent unauthorised disclosure, modification, substitution, and replay;

ii) the manual or automatic distribution of keying material, to permit interoperability between cryptographic equipment or facilities using the same algorithm;

iii) ensuring the integrity of keying material during all phases of its life, including its generation, distribution, storage, entry, use, archival and destruction;

iv) recovery in the event of failure of the key management process or when the integrity of the keying material is questioned.

It thus provides a means whereby an audit trail can be identified for all keying material.

This International Standard is designed for the use of symmetric algorithms for key distribution, where originator and recipient use the same key. It is designed for messages formatted and transmitted in coded character sets. It is intended that provision will, in due course, be made to cover the use of asymmetric algorithms for key distribution.

This standard does not provide a means to distinguish cryptographically between two physical parties when they share a common key.

The procedures specified are appropriate for use by financial institutions and by their corporate and government customers, and in other relationships where the interchange of information requires confidentiality, protection and authentication.

2 References

ISO 646, *Information processing — ISO 7-bit coded character set for information processing interchange.*

ISO 7982-1, *Bank telecommunications — Funds transfer messages — Part 1: Vocabulary and data elements.*

ISO 8372, *Information processing — Modes of operation for a 64-bit block cipher algorithm.*

ISO 8730, *Banking — Requirements for message authentication (wholesale).*

ISO 8731, *Banking — Approved algorithms for message authentication.*

ANSI X3.92, *1981 Data Encryption Algorithm.*

3 Definitions

For the purpose of this International Standard the following definitions apply.

3.1 audit trail: see *security audit trail.*

3.2 authentication: A process used, between a sender and a receiver, to ensure *data integrity* and to provide *data origin authentication.*

3.3 bias: The condition where, during the generation of random or pseudo-random numbers, the occurrence of some numbers is more likely than others.

3.4 ciphertext: Enciphered information.

3.5 code: A symbol representing data, typically to facilitate automated processing.

3.6 communicating pair: Two *logical parties* who have previously agreed to exchange data.

NOTE — A party and a Key Distribution Centre or Key Translation Centre exchanging Cryptographic Service Messages do not constitute a communicating pair.

3.7 Co-ordinated Universal Time: The time scale maintained by the Bureau International de l'Heure (International Time Bureau) that forms the basis of a co-ordinated dissemination of standard frequencies and time signals.

NOTE — May alternatively be described as Greenwich Mean Time (GMT).

3.8 counter: An incrementing count used between two parties to control successive key distributions under a particular *Key Enciphering Key.*

3.9 cryptographic equipment: Equipment in which cryptographic functions (eg *encipherment, authentication,* key generation) are performed.

3.10 cryptographic key; key: A parameter used in conjunction with an algorithm for the purpose of *validation, authentication, encipherment* or *decipherment.*

3.11 cryptographic keying material: see *keying material.*

3.12 cryptography: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.

NOTE — Cryptography determines the methods used in *encipherment* and *decipherment*. An attack on a cryptographic principle, means or method is cryptanalysis.

3.13 cryptoperiod: A defined period of time during which a specific *cryptographic key* is authorised for use, or during which time the *cryptographic keys* for a given system may remain in effect.

3.14 data integrity: The property that data has not been altered or destroyed in an unauthorised manner.

3.15 data key: A *cryptographic key* used for the *encipherment, decipherment* or *authentication* of data.

3.16 data origin authentication: The corroboration that the source of data received is as claimed.

3.17 decipherment: The reversal of a corresponding reversible *encipherment.*

3.18 decryption: see *decipherment.*

3.19 dual control: A process of utilising two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilise the materials, eg *cryptographic key.*

3.20 encipherment: The cryptographic transformation of data (see *cryptography*) to produce *ciphertext.*

3.21 encryption: see *encipherment.*

3.22 exclusive-or: see *modulo-2 addition.*

3.23 field tag: A unique string of characters used in formatted messages that identifies the meaning and location of the associated data field.

3.24 financial message: A message containing information which has financial implications.

3.25 hexadecimal digit: A single character in the range 0-9, A-F (upper case), representing a four bit string.

3.26 initialisation vector (IV): A number used as a starting point for *encipherment* of a data sequence. It increases security, by introducing additional cryptographic variance, and also facilitates the synchronisation of *cryptographic equipment.*

3.27 interoperability: The ability to exchange *cryptographic keys*, whether manually or in an automated environment, with any other party.

3.28 key: see *cryptographic key.*

3.29 key component: One of at least two parameters having the format of a *cryptographic key* that is combined with one or more like parameters by means of *modulo-2 addition* to form a *cryptographic key.*

3.30 Key Distribution Centre: A facility which generates and returns *cryptographic keys* for distribution.

3.31 Key Enciphering Key: A *cryptographic key* used for the *encipherment* and *decipherment* of *cryptographic keys.*

3.32 key generator: A type of *cryptographic equipment* used for generating *cryptographic keys* and, where needed, *initialisation vectors.*

3.33 key loader: An electronic, self-contained unit which is capable of storing at least one *cryptographic key* and transferring that *cryptographic key*, upon request, into *cryptographic equipment.*

3.34 key management facility: A protected enclosure (eg room or *cryptographic equipment*) and its contents where cryptographic elements reside.

3.35 key offset; offset: The result of adding a *counter* to a *cryptographic key* using *modulo-2 addition.*

3.36 Key Translation Centre: A facility which transforms and returns *cryptographic keys* for distribution.

3.37 keying material; cryptographic keying material: The data (eg keys and IVs) necessary to establish and maintain a *keying relationship.*

3.38 keying relationship: The state existing between a *communicating pair* during which time they share at least one *data key* or *Key Enciphering Key.*

3.39 logical party: One or more physical parties forming one member of a *communicating pair.*

3.40 Message Authentication Code (MAC): A *code* in a message between a sender and a receiver used to validate the source and part or all of the text of a message. The *code* is the result of an agreed calculation.

3.41 modulo-2 addition; exclusive-or: A binary addition with no carry, giving the following values:-

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

3.42 notarisation: A method of modifying a *Key Enciphering Key* in order to authenticate the identities of the *originator* and the ultimate *recipient.*

3.43 notarising key: A *cryptographic key* used for *notarisation.*

3.44 notary seal: A value created from the identities of the *logical parties* of a *communicating pair*, and used in the creation of a *notarising key* (pair).

3.45 offset: See *key offset.*

3.46 originator: The party (logical or other) that is responsible for originating a Cryptographic Service Message.

3.47 plaintext: Unenciphered information.

3.48 recipient: The party (logical or other) that is responsible for receiving a Cryptographic Service Message.

3.49 security audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures and to recommend any indicated changes in control, policy and procedures.

3.50 security audit trail: Data collected and potentially used to facilitate a *security audit*.

3.51 security life: The time span over which cryptographically protected data has value.

3.52 split knowledge: A condition under which two or more parties separately and confidentially have custody of the constituent parts of a single key that, individually, convey no knowledge of the resultant *cryptographic key*.

3.53 validation: The process of checking the *data integrity* of a message, or selected parts of a message.

3.54 zeroisation: A method of erasing or overwriting electronically stored data.

4 Abbreviations

The following abbreviations are used in this International Standard:

The notation used in clauses 12 to 15 is described in annex B.

Abbreviation	Meaning	Description (see also table 2)
CKD	Key Distribution Centre	A facility which generates and returns cryptographic keys for distribution.
CKT	Key Translation Centre	A facility which transforms and returns keys for distribution.
CSM	Cryptographic Service Message	A message for transporting keys or related information used to control a keying relationship.
CTA	Counter A	Counter used between a CKD or CKT and party "A".
CTB	Counter B	Counter used between a CKD or CKT and party "B".
CTP	Counter P	Counter used in a Point-to-Point keying relationship.
CTR	Counter R	The value of the counter found to be in error.
DEA	Data Encryption Algorithm	—
DSM	Disconnect Service Message	A message type used to discontinue one or more keys or to terminate a keying relationship.
ECB	Electronic Code Book	A mode of implementing the encipherment algorithm.
EDC	Error Detection Code	A code in a Cryptographic Service Message used to validate the data integrity of the message.
EDK	Effective Date of Key	Date and Co-ordinated Universal Time on which the data key is activated.
ERF	Error Field	The identification of error conditions detected in a prior Cryptographic Service Message.
ERS	Error Recovery Service	A message type used to recover from count or other errors in a Key Distribution Centre or Key Translation Centre environment.
ESM	Error Service Message	A message type used to give a negative acknowledgement on receipt of any Cryptographic Service Message other than an ESM and to give the recipient data with which to recover.
IDA	Identifier of Authentication Key	Identifies the key to be used to authenticate a Disconnect Service Message.The identified key is discontinued.
IDC	Identifier of Key Distribution Centre or Key Translation Centre	—
IDD	Identifier of Key to be Discontinued	—
IDK1	Key Identifier	Identifier of the key being transmitted in a Cryptographic Service Message.

Abbreviation	Meaning	Description
IDK2	Key Enciphering Key Identifier	Identifier (name) of the Key Enciphering Key or key pair used to encipher the key being transmitted in a Cryptographic Service Message.
IDU	Identity of Ultimate Recipient	The identity of the intended final recipient of a Cryptographic Service Message sent within a Key Distribution Centre or a Key Translation Centre environment.
IV	Initialisation Vector	—
KD	Data Key	A key used to encipher/decipher, or authenticate data.
KDU	Notarised Data Key	A data key enciphered under a notarising key (pair).
KDX	Fixed Data Key	A data key with fixed value used in the computation of an Error Detection Code.
KK	Key Enciphering Key	A cryptographic key used for the encipherment and decipherment of cryptographic keys.
*KK[1)]	Key Enciphering Key Pair	A pair of keys used for the encipherment and decipherment of keys.
KKM	Master Key Enciphering Key	The highest level Key Enciphering Key in a multi-layer key management architecture.
KKU	Notarised Key Enciphering Key	A Key Enciphering Key enciphered under a notarising key.
*KKU[1)]	Notarised Key Enciphering Key Pair	A Key Enciphering Key Pair enciphered under a notarising key pair.
KN	Notarising Key	A cryptographic key used for notarisation.
KSM	Key Service Message	A message type used to transfer keys between communicating pairs.
MAC	Message Authentication Code	—
MCL	Message Type	The tag for the field that defines the type of Cryptographic Service Message.
NOS	Notarisation Indicator	A tag that, when present, indicates that notarisation was used.
NS	Notary Seal	A value used for notarisation purposes.
ORG	Originator	Originator of CSM.
P	Key Parity	Indicates that the plaintext key conforms to the specification for odd parity.
RCV	Recipient	Recipient of CSM.
RFS	Request For Service Message	Used to request translation of keys by a Key Translation Centre for retransmission to another party.
RSI	Request Service Initiation Message	Used to request keys from another party.
RSM	Response Service Message	Used to provide an authenticated acknowledgement.
RTR	Response To Request Service Message	Used to send keys from a Key Distribution Centre or from a Key Translation Centre.
SVR	Service Request	Specifies type of service requested.

1) The asterisk* indicates that a pair of keys is involved. Where the use of a pair of keys is an option, in the main text the asterisk is enclosed in parentheses.

5 Key management facility

5.1 General

A key management facility shall provide means of access control whereby its contents are protected from unauthorised disclosure, modification, substitution, replay, insertion or deletion.

NOTE — To achieve such control, action needs to be taken to either preclude access or to ensure that attempts to gain access have a high probability of being detected and reported.

5.2 Contents of key management facility

All cryptographic equipment, including key generation equipment, shall be located within a key management facility.

NOTE — Cryptographic equipment may itself act as the key management facility, and so provide all the required functions.

6 Requirements of cryptographic equipment

6.1 Generation of keys and initialisation vectors (IVs)

6.1.1 General

Key and IV generation procedures shall be under dual control.

The generation of keys and initialisation vectors shall be by means of a process that ensures that all keys and initialisation vectors are random or pseudo-random. The design of this generation process shall be such that no cryptographic advantage is gained by attacking the key generation process rather than the encipherment process.

The output from a key generator shall be automatically checked for generation failure (eg the repeated output of the same key). Operation of the key generator shall stop immediately if any failure is detected.

Keys shall not be available in plaintext form from cryptographic equipment, even upon failure of the equipment, other than at the time of initial generation of a key.

A means shall be provided for the manual zeroisation of plaintext keys (see annex F).

6.1.2 Keys and IVs for manual distribution

All key generation, distribution and storage resources (eg copies, ribbons, etc) shall be protected from unauthorised use, alteration, replacement, destruction or exposure. Waste products shall be destroyed under dual control. The key generation process shall take place in an area where unauthorised viewing is prevented.

Where keys or IVs are printed, provision shall be made to protect them from unauthorised disclosure or replacement.

NOTE — Such protection may include uniquely identified key books with numbered pages protected by tamper resistant packaging so that page substitution is not possible.

Where a specially designed device containing electronically protected memory is used, safety devices shall be built into the software procedures or hardware to prevent unauthorised access. Any attempts to gain unauthorised access into the protected memory shall result in the stored plaintext key being automatically erased, or otherwise rendered unintelligible. There shall be no external display, control or means of extracting the stored key without the linking or insertion of the device containing electronically protected memory into a secure receiver.

Where distribution of a key involves split knowledge, to ensure security, each key component shall be produced on a separate printed form or storage medium.

6.1.3 Keys and IVs for automated distribution

Where cryptographic equipment is used to generate keys and IVs automatically it shall be physically protected to prevent:

1) the disclosure, modification and replacement of the keys

2) the modification or replacement of the IVs

3) the modification or replacement of the key generation algorithm, or device.

6.2 Entry of keys

6.2.1 General

Cryptographic equipment shall permit, at either the system level or the device level, the entry of keys having a format complying with this standard. Access to key entry controls or systems shall be limited by physical or logical means, or both.

6.2.2 Manual entry of keys

A means shall be provided for the manual entry of keys or key components. A means of correcting individual errors or of re-entering the entire key shall be provided. If any plaintext key component is displayed it shall be visible only to authorised personnel and shall be cleared immediately after the key entry process is completed.

NOTE — Re-entry of an entire key may also be used as a means of verifying a previously entered key.

6.2.3 Automated entry of keys

Where a means is provided for automated entry of keys there shall be no display of the key during key entry. Keys retained on special devices such as key loaders shall be entered under dual control.

6.2.4 Parity checking

Where parity checking is available, the parity of plaintext keys or key components shall be verified during entry in order to preclude unintentional single bit modification of the key.

6.2.5 Storage of plaintext keys

Any intermediate storage of plaintext keys that is utilised during key entry shall be zeroised once the transfer of the key to another location is complete.

6.2.6 Retention of electronically stored keys

A short term power failure shall not result in the loss of a key.

6.2.7 Electromagnetic interference

Protection shall be provided against compromise of keys as a result of radiation or conduction of electromagnetic interference from cryptographic equipment or key loaders.

6.2.8 Functional test

Immediately prior to manual key entry and system initialisation, the cryptographic equipment shall be subject to a test to check that it is operating correctly. This test shall include the operation of all control functions.

6.2.9 Operational error or failure

A means shall be provided to indicate the failure or incorrect operation of the cryptographic equipment (see also 6.1.1). A manual or automatic process shall be provided for the reporting and documentation of all such errors or failures.

6.3 Counter checking

Where keys are associated with counters (see 12.2) the cryptographic equipment shall provide a means for detecting and reporting the erasure, loss or lowering of a counter.

7 Keying material

7.1 Transportation and storage of keying material

Keying material shall be transported and stored in such a manner as to protect it against modification or substitution, and to prevent disclosure of plaintext keys before, during or after the period in which the keys are active.

Access to storage, including the movement of any keying material to or from storage, shall be under dual control. When keying material is entered or removed, the physical access shall be specifically authorised, physically or logically constrained, and fully documented.

7.2 Keys

7.2.1 Custody of keys

Dual control shall be maintained over keys at all times. Keys stored on a computer shall be enciphered or otherwise not be capable of being disclosed.

Lists of staff designated to hold or access keys shall be kept. These lists shall not contain any details of the content of keys.

7.2.2 Validity of keys

Keys shall normally be allocated a unique identifier or an effective date, and the communicating pair shall agree upon the cryptoperiod for each key.

Data keys may be exchanged on the basis that they are for immediate or for future use (see 7.2.4). No key shall be operational until an authenticated acknowledgement has been received from the recipient. Where a key has not been specifically identified (eg by number or effective date) it shall be the only such key and shall be put into service by the communicating pair immediately after the recipient's acknowledgement is received by the originator.

Where it is suspected or known that a key has been compromised it shall no longer be considered to be valid and shall be withdrawn from current use.

7.2.3 Key changes

Keys shall be changed:

a) at the end of the cryptoperiod; or

b) with the agreement of both members of the communicating pair; or

c) immediately after it is known or suspected that a key has been compromised.

All key changes shall be acknowledged. Where the cryptoperiods of an existing and a new key overlap, an explicit date (or other implicit time reference) shall be specified whereupon the old key is no longer current. During this changeover period both keys shall be held under the same level of security.

Keys withdrawn from use shall not be knowingly or intentionally re-used except for the purpose of reconstructing a key/message pair (see 7.2.5).

7.2.4 Reserve keys

Where keys are stored in reserve, to facilitate planned or unexpected key changes, they shall be subject to the same level of security control as keys in current use.

7.2.5 Archiving of keys

Where the continued storage (archiving) of a key after the expiration of its cryptoperiod, or compromise, is required each such key shall be uniquely identified, or converted into a different form or format so that there is no ambiguity that it is archived and obsolete. All archived keys shall be enciphered under a key designated for that purpose. It shall not be possible to use archived keying material other than for the reconstruction of a key/message pair.

NOTE — The detailed procedures for the archiving of keys are application dependent and are not defined in this standard.

7.2.6 Back-up of keys

When a printed key is exchanged, the original printed form shall be retained for back-up. Where keys are exchanged automatically a protected copy shall be kept in storage. All back-up copies of active keys shall be subject to the same level of security control as keys in current use.

7.2.7 Destruction of keys (see also annex F)

All copies of keys that are no longer required shall be destroyed under dual control. Printed keys shall be destroyed by means of incineration, cross-cut shredding, or pulping, or other secure method.

Keys stored on magnetic media shall either be zeroised, under password control, or the magnetic media shall be destroyed as for printed keys.

A detailed record of withdrawal from service and destruction shall be retained, for audit trail purpose.

Section 2 : Manual distribution of keying material

An example of manual key distribution and control procedures appears in annex A.

8 Despatch of manually distributed keying material

All documents accompanying manually distributed keying material shall be prepared prior to the generation of the keying material. This documentation shall include:

a) A receipt for the keying material for signature by the recipient.

b) Details of the recipient.

c) Details of any passwords required for access to material distributed on magnetic storage media or other secure storage devices (eg key loaders).

d) Where a courier service is used, a receipt for signature by the courier.

e) Details of the date of generation of keying material, together with details of the issuer and the issue date.

All such documentation shall be signed by authorised signatories.

Once keying material has been generated (see 6.1), access to key components shall be controlled by the processes of dual control and split knowledge. Each key component shall be placed in a separate envelope which is sealed in such a manner that any subsequent unauthorised interference can be detected. Each envelope shall be marked to indicate its contents and the address of the appropriate function, and then placed in a second, separate, envelope that is sealed, and addressed to the recipient. The second envelope shall give no indication of its contents.

NOTE — Each package thus consists of an outer envelope with a single inner envelope containing a single key component.

The individual components of a key shall be despatched, together with a receipt using a method to ensure separate despatch, for example, on different days. Any passwords required for access to magnetic storage media or other storage devices, eg key loaders, shall be despatched separately from the medium or device.

Where keying material is transported by mail then a secure method shall be used. Where delivery is by means of courier a receipt shall be obtained from the courier by the sender. The courier shall not be aware of the nature of the contents of an envelope.

9 Receipt of manually distributed keying material

Upon receipt of a package containing a key component the recipient shall examine the innermost envelope in order to check, so far as is possible, that access to its contents has not been attempted or achieved. If it is suspected that the security of the inner envelope has been compromised the sender shall be advised immediately. The signatures on the accompanying documentation shall be checked by the recipient for authenticity. The identity of the key components, eg sequence number or effective date, shall be recorded. When the recipient of the key component is satisfied with the authenticity of the key component the receipt that accompanied it shall be signed and returned (see also 7.2.2). Keys shall be placed in secure storage immediately upon receipt. Inner envelopes (ie those containing the key components) shall be retained under appropriate control (see clause 7).

This page intentionally left blank

Section 3 : Automatic distribution of keying material

10 Requirements for the automated key management architecture

This International Standard is designed to meet the following requirements for automated key management. It is assumed that:

1) the data network is expandable.

2) either a communicating pair has a Key Enciphering Key in common or each has a Key Enciphering Key Pair in common with a Key Distribution Centre or a Key Translation Centre.

10.1 The architecture shall support the ability to have at least one data key between communicating pairs.

10.2 Any communicating pair may share more than one Key Enciphering Key.

10.3 The architecture shall support the ability to change data keys automatically between communicating pairs.

10.4 A particular data key shall be used for either encipherment/decipherment or for authentication but not for both, except when authenticating a Cryptographic Service Message.

10.5 A data key or Key Enciphering Key shared between a communicating pair shall not be disclosed to a third party (except for a Key Translation Centre (CKT) or a Key Distribution Centre (CKD)).

10.6 A key used between any communicating pair shall not intentionally be used between any other communicating pair.

10.7 The same data key shall not be knowingly or intentionally used by more than one communicating pair.

10.8 The compromise of any key shared between any communicating pair shall not compromise any third party.

10.9 The architecture shall support communicating parties that do not have a key generation capability.

10.10 The architecture shall support any party initiating a secure connection with any other party.

10.11 In a three layer architecture (see 11.1) the ability to exchange Key Enciphering Keys automatically between a communicating pair shall be provided.

11 Automated key management architecture

11.1 General

The architecture shall consist of either two or three layers of keys (see figure 1). All implementations shall have the capability of functioning in a two layer architecture.

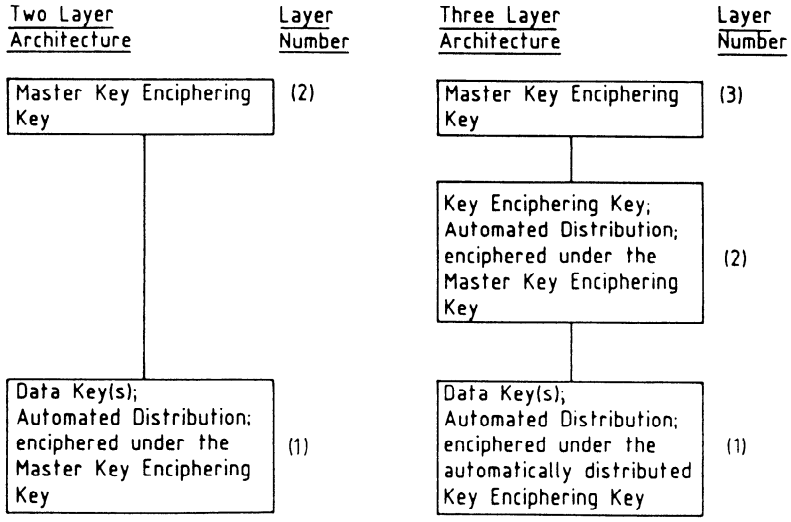

Figure 1 — Key distribution architecture