INTERNATIONAL STANDARD

ISO
13492

First edition
1998-05-15

Banking — Key management related data element (retail)

Banque — Élément de données lié à la gestion des clés (services aux particuliers)

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 13492 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

Annexes A and B of this International Standard are for information only.

Introduction

This International Standard describes the structure and contents of a key management related data element that may be conveyed in electronically transmitted messages within the retail banking environment to support the secure management of cryptographic keys, where the retail banking environment involves the communications between a card-accepting device and an acquirer, and between an acquirer and a card issuer. Key management of keys used in an Integrated Circuit Card (ICC) and the related data elements are not covered in this International Standard.

This International Standard provides compatibility with the existing ISO standard on bank card originated messages (see ISO 8583).

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO 13492:1998
https://standards.iteh.ai/catalog/standards/sist/87e4dde2-c174-42ee-9a79-
b26e534d6d45/iso-13492-1998

Banking — Key management related data element (retail)

1 Scope

This International Standard describes a key management related data element that may 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 (bit 53) or Key Management Data (bit 96). However, 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 retail banking environment are described in ISO 11568. Security related data, such as PIN data and MACs, are described in ISO 9564 and ISO 9807, respectively.

2 Normative references

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

ISO/IEC 7812-1:1993, *Identification cards — Identification of issuers — Part 1: Numbering system.*

ISO/IEC 7812-2:1993, *Identification cards — Identification of issuers — Part 2: Application and registration procedures.*

ISO 8583:1993, *Financial transaction card originated messages — Interchange message specifications.*

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

ISO 9564-1:1991, *Personal Identification Number management and security — Part 1: PIN protection principles and techniques.*

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail).*

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

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*.

ANSI X3.92:1987, *Data Encryption Algorithm.*

3 Definitions

For the purposes of this International Standard, the definitions given in ISO 8908 and the following definitions apply.

3.1
asymmetric cipher
a cipher in which the encipherment and decipherment keys are different and it is computationally infeasible to deduce the decipherment key from the encipherment key

3.2
cipher
a pair of operations that effect transformations between plaintext and ciphertext under the control of a parameter called a key

NOTE   The encipherment operation transforms data (plaintext) into an unintelligible form (ciphertext). The decipherment operation restores the original text.

3.3
cryptographic algorithm
a set of rules specifying the procedures required to perform encipherment and decipherment of data

NOTE   The algorithm is designed so that it is not possible to determine the control parameters (e.g. keys) except by exhaustive search.

3.4
cryptographic key; key
the control parameter of a cryptographic algorithm that cannot be deduced from the input and output data except by exhaustive search

3.5
cryptographic service message
a message for transporting keys or related information used to control a keying relationship

3.6
primary key
that key for a transaction from which other keys for the transaction are produced (e.g. by means of variants or transformations)

3.7
symmetric cipher
a cryptographic method using the same secret cryptographic key both for encipherment and decipherment

3.8
transaction message
a message used to convey information related to a financial transaction

4 Requirements for key management related data element

A key management related data element that conveys information about the associated transaction's key(s) is normally divided into sub-fields. This data element may be transmitted in a transaction where the nature of the sub-fields are implicitly known to the communicating parties. In environments where such transactions are exchanged, the parties may use the key management related data element as a private-use field and define its sub-fields in any mutually agreeable way. In other environments, transactions are exchanged where the nature of the sub-fields

are not implicitly known and therefore must be structured using a standardized representation to support interoperability. However, other environments, both types of transactions may be exchanged.

To distinguish between those transactions where the key management related data element must have a standardized representation and those transactions where it is used for private use, the first byte of the key management related data element shall be structured as a "control byte", where the control byte is defined as follows:

00-9F: The first sub-field of the key management related data element is a variable-length "key set identifier," as defined in 4.1 and 4.2.

A0-FF: The key management related data element is a private-use field, where the nature of the sub-fields are implicitly known to both communicating parties.

The use of key set identifiers provides a standardized way to convey any type of key management related information associated with a key management system. This approach eliminates the need to recognize specific key management techniques and to specify specific sub-fields to meet the needs of each such technique.

When the key management related data element begins with a key set identifier, the remainder of the data element contains whatever type of information is required to determine the key(s) needed to cryptographically process the transaction. Thus, there is no specified structure to the sub-fields contained in the remainder of the data element. Any information that may vary on a per transaction basis is conveyed following the key set identifier. This information normally includes the identity of a particular key(s) within a key set.

Key management related information that does not change from one transaction to the next need not be conveyed with every transaction. Rather, it may be implicitly known, or it may be installed concurrent with, and stored in association with, the corresponding key. Examples of information that may be implicitly known include the following:

— Key management technique used for the transaction's keys (e.g. static key, unique key per transaction).

— Format of enciphered or authenticated data (e.g. PIN block format).

— Encipherment algorithm used.

— Number of different keys used with the transaction and the purpose of each such key.

In some key management schemes, it may not be necessary to transmit a key management related data element in transaction messages. The need to transmit such a data element is discussed in annex A.

4.1 Concept of key set identifiers

A key set identifier is a number that uniquely identifies a key set, where a key set is a group of related keys that are all different but have certain characteristics in common, most notably:

— All are managed using the same key management method.

— The same high level key is used to encipher (for database storage) or derive all keys of the set.

— The remainder of the key management related data element (beyond the key set identifier) is identically structured for all keys of the set and is interpreted using the same logic.

Associated with any given key set is logic (e.g. computer software) at the acquiring host that may interpret the key management related data element to determine what key(s) is to be used with that transaction and how each such key is to be used.

Multiple key sets, with different key set identifiers, may use the exact same logic, differing only, for example, in the key encipherment key or the derivation key used to decipher or derive the key for the associated transaction.

The first byte of the key set identifier is the control byte (00-9F). Key set identifiers are assigned as described in 4.2. Key set identifiers are of variable length and do not have a specified maximum length. The length of the key set identifier is implicit. Therefore, the key management related data element shall not contain a "length" sub-field preceding the key set identifier that indicates the length of the key set identifier. Similarly, it is unnecessary for the key set identifier to be followed by a specified delimiter. (Note that if the key management related data element is transmitted in a variable length field, the key management related data element itself may be preceded by a length sub-field indicating the length of the entire data element, as is required in ISO 8583 for data elements Security Related Control Information and Key Management Data.)

Since key set identifiers are of variable length and the length is implicit, the acquiring host should store in the table of the key set identifiers that it recognizes the length of each key set identifier. When a host receives a transaction from, e.g. a POS terminal, the host should attempt to match the key set identifier in each such table entry with as many leftmost key management related data element digits as are specified for the particular table entry. Such a match indicates that this table entry holds the key set identifier that applies to the just-received key management related data element.

4.2 Assignment of key set identifiers

To prevent institutions from assigning duplicate key set identifiers, key set identifiers shall be assigned using either the six-digit Issuer Identification Numbers (IINs) as defined in ISO 7812 or the six-digit Institution Identification Codes (IICs) as defined in ISO 8583. The ISO Registration Authority assigns IINs to institutions that issue cards and IICs to institutions that do not issue cards. Since IINs and IICs are unique to the institution to which they are assigned and these two sets of numbers do not overlap, this ensures that, if two cryptographic environments are combined, key set identifiers that were unique in each separate environment will be unique in the combined environment.

An organization that wishes to obtain a key set identifier but has not been assigned an IIN or IIC may also obtain such an identifier from an institution that has been assigned an IIN or IIC. Such an institution shall ensure that it never assigns duplicate key set identifiers.

An institution may use an IIN or IIC directly as a key set identifier provided it will never need more key set identifiers than the quantity of IINs or IICs it has been assigned. If the institution requires additional key set identifiers, it shall concatenate one or more hexadecimal digits to the right of an IIN or IIC and in this way obtain multiple key set identifiers from a single IIN or IIC.

The institution allocating key set identifiers should choose how many digits (if any) to concatenate with its IIN or IIC to obtain its key set identifiers, prior to allocating any key set identifiers based on the IIN or IIC. For example, if an institution chooses to use seven-digit key set identifiers by concatenating a single digit with an IIN or IIC, it may not, after having used all 16 such seven-digit numbers, subsequently add an eighth digit to obtain additional key set identifiers. Such an eight-digit key set identifier would match, in the first seven digits, a key set identifier already assigned. For example, if the key set identifier seven-digit "1362047" already exists, the key set identifier eight-digit "13620475" is not allowed, and vice versa, because the one key set identifier is totally included within the other key set identifier. For an example of the usage of key set identifiers, see annex B.

5 Implementation in ISO 8583

When the key management related data element described in clause 4 is used with ISO 8583 to convey key management information for the current transaction message, the contents of the key management related data element shall be transmitted using ISO 8583 Security Related Control Information, which is a variable-length binary data element up to 48 bytes.

NOTE 1   Examples of ISO 8583 messages in which Security Related Control Information may be transmitted are an authorization or financial request that contains the Personal Identification Number (PIN) Data (bit 52) or a file action or network management message that contains the Message Authentication Code Field (bit 64 or 128).

When the key management related data element is used with ISO 8583 in cryptographic service messages to convey keying information for future use, the contents of the key management related data element shall be transmitted using ISO 8583 Key Management Data, which is a variable length binary data element up to 999 bytes.

NOTE 2   Examples of ISO 8583 messages in which Key Management Data may be transmitted are a network management request or request response either for confirming the synchronization of current keys or for exchanging future keys.

iTeh STANDARD PREVIEW

(standards.iteh.ai)