INTERNATIONAL STANDARD

ISO 13492

Second edition
2007-12-15

Financial services — Key management related data element — Application and usage of ISO 8583 data elements 53 and 96

Services financiers — Élément de données lié à la gestion des clés — Application et utilisation des éléments de données 53 et 96 de l'ISO 8583

Reference number
ISO 13492:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 2
5 Data representation 3
6 Requirements for key management related data element 4
6.1 Introduction 4
6.2 Data element structure 4
6.3 Key-set identifier concepts 5
7 Security related control information usage (data element 53) 5
7.1 Format 5
7.2 Assignment of key-set identifiers 9
8 Key management data (data element 96) 9
Bibliography 10

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 13492 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 13492:1998), which has been technically revised.

Introduction

This International Standard describes the structure and contents of a key management related data element that can be conveyed in electronically transmitted messages within the financial services environment to support the secure management of cryptographic keys, where the financial services 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).

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 8583-1 and the following apply.

3.1
asymmetric cipher
cipher in which the encipherment key and the decipherment key are different and it is computationally infeasible to deduce the (private) decipherment key from the (public) encipherment key

3.2
cipher
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
set of rules for the transformation of data using a cryptographic key

EXAMPLE The transformation of plaintext to ciphertext and vice versa (i.e. a cipher); generation of keying material; digital signature computation or validation.

3.4
cryptographic key
key
parameter that determines the operation of a cryptographic algorithm

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

3.6
derived unique key per transaction
key management method which uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction-originating TRSM

NOTE The unique Transaction Keys are derived from a base derivation key using only non-secret data transmitted as part of each transaction.

3.7
primary key
key for a transaction from which other keys for the transaction are produced

NOTE This can be done by means of variants or transformations.

3.8
symmetric cipher
cryptographic algorithm using the same secret cryptographic key for both encipherment and decipherment

3.9
transaction message
message used to convey information related to a financial transaction

4 Abbreviated terms

AES Advanced Encryption Standard

BCD Binary Coded Decimal

CAID Card Acceptor Identifier

CBC Cipher Block Chaining

DEA Data Encryption Algorithm

DID Device Identifier

DUKPT Derived Unique Key per Transaction

ECB Electronic Code Book

ECIES Elliptic Curve Integrated Encryption Scheme

GID Group Identifier

IIC Institution Identification Code

IIN Issuer Identification Number

KSN Key Serial Number

MAC Message Authentication Code

PIN Personal Identification Number

RSA The Rivest, Shamir and Adleman Public Key Cryptosystem

TC Transaction Counter

TDEA Triple Data Encryption Algorithm

TRSM Tamper Resistant Security Module

5 Data representation

Data fields described in this International Standard are represented as shown in Table 1.

Table 1 — Data representation

Abbreviation	Definition
a	Alphabetic data elements contain a single character per byte. The permitted characters are alphabetic only (a to z and A to Z, upper and lower case).
an	Alphanumeric data elements contain a single character per byte. The permitted characters are alphabetic (a to z and A to Z, upper and lowercase) and numeric (0 to 9).
ans	Alphanumeric special data elements contain a single character per byte.
b	These data elements consist of either unsigned binary numbers or bit combinations that are defined elsewhere in the specification. Example: a field defined as “b 2” has a length of two bytes such that a value of 19 is stored as Hex '00 13'.
LL	Length of variable data element that follows, 01 through 99.
LLL	Length of variable data element that follows, 001 through 999.
n	Numeric data elements consist of two numeric digits (having values in the range Hex '0' – '9') per byte. These digits are right justified and padded with leading hexadecimal zeroes. Other specifications sometimes refer to this data format as Binary Coded Decimal (“BCD”) or unsigned packed. Example: a field defined as “n 12” has a length of six bytes such that a value of 12345 is stored as Hex '00 00 00 01 23 45'.

6 Requirements for key management related data element

6.1 Introduction

The key management related data element is constructed from the concatenation of two ISO 8583-1 message elements, data element 53 — Security related control information, and data element 96 — Key management data. It conveys information about the associated transaction's cryptographic key(s) and is divided into subfields including a control field, a key-set identifier and additional optional information.

The control field identifies the key management scheme and associated structure of the remainder of the data element. The use of key-set identifiers provides a standardized way to uniquely identify the institution and key-set for a given operation. For key management messages, the key-set identifier specifies the key-set that will be affected by the current operation (e.g. load key-set 2 with key contained in data element 96). For financial transaction messages containing encrypted data, the key-set identifier specifies the key-set that was used.

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 need not be explicitly identified in the key management related data element 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;

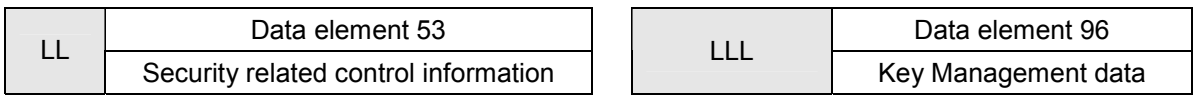
— number of different keys used with the transaction and the purpose of each such key.

6.2 Data element structure

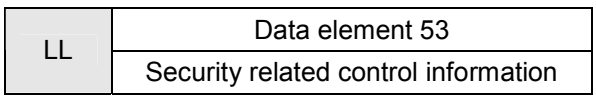
The key management related data element has two possible forms, as illustrated in Figure 1:

— Form 1, e.g. key change [see Figure 1 a)];

— Form 2, e.g. key selection [see Figure 1 b)].



a) Form 1



b) Form 2

Figure 1 — Possible forms of data element structure

In the construction in Figure 1 a), data element 53 is used to convey control information for the key data contained in data element 96.

In the construction in Figure 1 b), data element 53 is used to convey selection information regarding the keys used to protect the current financial transaction message (of which this data element forms a part).

6.3 Key-set identifier concepts

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 those listed below.

— 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 (are) to be used with that transaction, and how each such key is to be used.

7 Security related control information usage (data element 53)

7.1 Format

7.1.1 General

Data Element 53 is used to indicate which of the possible key-sets are to be used or affected by the key management message. As an option, this field may also include information concerning the algorithm and mode of operation used in the encryption of the associated key management data field. The defined values for these subfields are shown in the following tables.

The construction of this data element is dependant upon the key management scheme in which the data element is used. Two formats are illustrated:

— in Table 2, format A as used for fixed and master/session key, and

— in Table 3, format B for Derived Unique Key Per Transaction (DUKPT) key management scheme, as defined in ANSI X9.24-1.

Table 2 — Data element 53 — Structure format A

Length bytes	Field name	Description	Encoding	Required
1	Control	Identifies the key management scheme and associated structure of the remainder of the data element as defined in 7.1.2.	b 1	mandatory
4	Key-set identifier	Key-set identifier as defined in 7.1.3.	n 8	mandatory
1	Algorithm	Selects the encryption algorithm used to encipher the keys contained in the associated key management data element as defined in 7.1.5.	n 2	optional
2	Key length	Key length of the enciphered key as defined in 7.1.6.	n 4	optional
1	Protection	Mechanism used to provide key confidentiality and integrity as defined in 7.1.7.	n 2	optional
2	Reserved national	Reserved for national use.	n 4	optional
1	Reserved private	Reserved for private use.	n 2	optional

Table 3 — Data element 53 — Structure format B

Length bytes	Field name	Description	Encoding	Required
1	Control	Identifies the key management scheme and associated structure of the remainder of the data element as defined in 7.1.2.	b 1	mandatory
5	Key-set identifier	Key-set identifier as defined in 7.1.4.	n 10	mandatory
5	Device ID and Transaction Counter	Contains the 19-bit device ID and the 21-bit transaction counter as defined in 7.1.4.5 and 7.1.4.6.	b 5	mandatory

7.1.2 Control field format

Table 4 shows the control field values for the two structure formats.

Table 4 — Control field values

Value	Field contents	Definition	Structure
0	00	Default	A
1	01	Fixed key	A
2	02	Master/session	A
3	03	Reserved	undefined
4	04	DEA, DUKPT	B
5	05	TDEA, DUKPT	B

7.1.3 Key-set identifiers, format A

Table 5 shows the key-set identifier for format A values.

Table 5 — Key-set identifier — Format A values

Value	Field contents	Definition
0	00000000'	Use default key-set
nnnnnn01	nnnnnn01'	Use key-set 1 associated with institution nnnnnn[a]
nnnnnn02	nnnnnn02	Use key-set 2 associated with institution nnnnnn[a]
. . .		
nnnnnn99	nnnnnn99	Use key-set 99 associated with institution nnnnnn[a]
[a] Where nnnnnn is the IIN or IIC as specified in 7.1.4.3.		

7.1.4 Key-set identifiers, format B

7.1.4.1 General

Format B key-set identifiers as defined herein are used with DUKPT key management exclusively. The key-set identifier uniquely identifies the device and transaction as shown in Figure 2.

NOTE Some implementations replace the IIN/IIC and CAID fields with a single field to identify the Base Derivation Key.

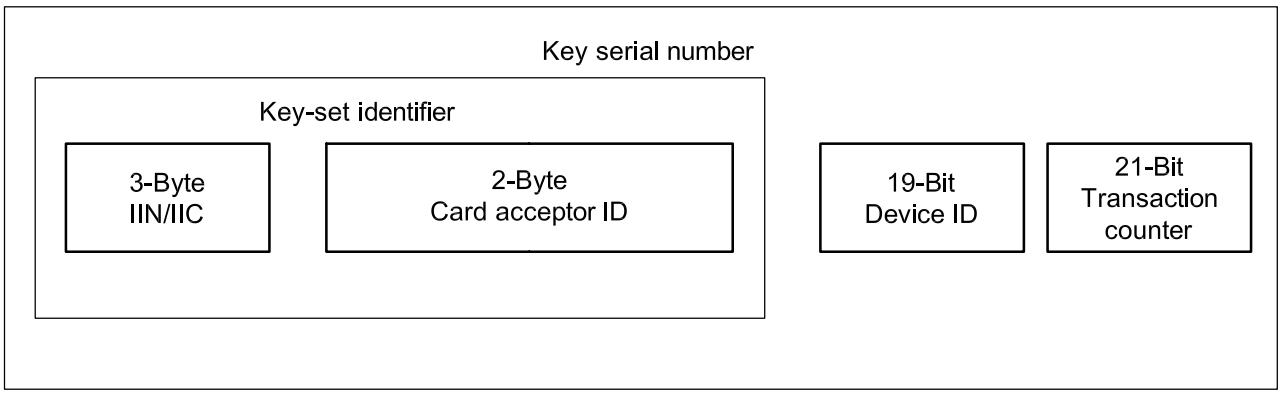


Figure 2 — Format B key-set identifier and related fields

7.1.4.2 Key Serial Number (KSN)

The key serial number uniquely identifies a DUKPT transaction. It is comprised of the 3-byte IIN/IIC, the 1-byte Merchant ID, the 1-byte Group ID, the 19-bit Device ID and the 21-bit transaction counter. The KSN is illustrated in Figure 2.

7.1.4.3 Issuer Identification Number (IIN)/Institution Identification Code (IIC) — 3 Bytes

The IIN/IIC is a unique 6-digit number, which can be obtained as described in 7.2. Use of this number will ensure the uniqueness of the KSN.

7.1.4.4 Card Acceptor ID (CAID) — 2 Byte

The CAID can be used by an acquirer or their agent to segregate merchants from each other, e.g. an acquirer might have a chain of hardware stores (e.g. Smith's Hardware Stores) and perhaps a chain of clothing stores (e.g. Wide Body Men's shops). The acquirer might assign CAID=0014 to devices issued to Wide Body Men's Shops and CAID=0026 to devices deployed to Smith's Hardware Stores. The CAID can provide a method to quickly and easily determine to which merchant a device had been issued.

7.1.4.5 Device ID (DID) — 19 Bits

The right-most 5 bytes of the KSN is divided into two fields. The left-most 19 bits constitute the Device ID field and the right-most 21 bits constitute the Transaction Counter field described below. The DID is used to designate an individual device identification within a specific GID.

7.1.4.6 Transaction Counter (TC) — 21 Bits

The right-most 21 bits of the KSN define a transaction counter under the control of the secure DUKPT firmware. The value of the counter is controlled by the firmware and changes to the value of the counter as supplied by the firmware will produce inconsistent and meaningless results.

7.1.5 Algorithm field

The algorithm field (see Table 6) defines the algorithm used to encipher the keys being transported in data element 96.

Table 6 — Algorithm

Value	Field contents	Definition
0	00	default
1	01	DEA
2	02	RSA
3	03	TDEA
4	04	ECIES
5	05	AES
6-99		as defined by the key management scheme
NOTE For definitions of the algorithms listed in this table, see ISO/IEC 18033.		

7.1.6 Key length (in bytes) field

The key length field specifies the length of the keys being transported in data element 96.

Table 7 gives examples of key length.

NOTE The key length field does not specify the length of the key used to provide the encryption of data element 96.

Table 7 — Key length examples

Value	Field contents	Definition
0	0000	default
8	0008	56 bit key with parity (i.e. DEA key)
16	0016	112-bit key with parity (i.e. a 2-key TDEA key) or 128-bit AES key

7.1.7 Key protection field

Table 8 gives examples of key protection.

Table 8 — Key protection

Value	Field contents	Definition
0	00	default
1	01	ECB enciphered key(s)[a]
3	03	CBC enciphered key(s)[a]
4	04	ANSI XR TR-31 key block
[a] Key integrity to be provided by other means.		

7.2 Assignment of key-set identifiers

To prevent institutions from assigning duplicate key-set identifiers, the leading digits of the key-set identifiers shall be assigned using either the six-digit Issuer Identification Numbers (IINs) as defined in ISO/IEC 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.

8 Key management data (data element 96)

This data element is used to transport the enciphered keys, typically in a key-change operation. As the number of keys is key management scheme dependant, so is the format of this field (see Figure 3). Examples of possible structures include single or multiple enciphered keys that may be contained in integrity-protected key blocks, such as that specified in ANSI X9 TR-31.

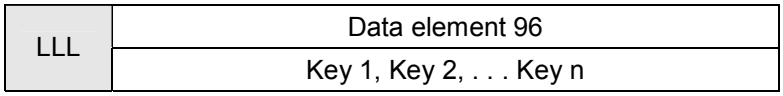


Figure 3 — Key management data — Data element 96

Bibliography

[1] ISO 9564-1, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

[2] ISO 9564-3, *Banking — Personal Identification Number management and security — Part 3: Requirements for offline PIN handling in ATM and POS systems*

[3] ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

[4] ISO 11568-2, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

[5] ISO 11568-4, *Banking — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle*

[6] ISO 16609, *Banking — Requirements for message authentication using symmetric techniques*

[7] ISO/IEC 18033 (all parts), *Information technology — Security techniques — Encryption algorithms*

[8] ANSI X9 TR-31:2005, *Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*

[9] ANSI X9.24-1:2004, *Retail Financial Services Symmetric Key Management — Part 1: Using Symmetric Techniques*

ICS 35.240.40
Price based on 10 pages