INTERNATIONAL STANDARD

ISO 13492

Third edition
2019-10

Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption

Reference number
ISO 13492:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This third edition cancels and replaces the second edition (ISO 13492:2007), which has been technically revised.

The main changes compared to the previous edition are as follows:

— introduction of the support of the AES encryption algorithm, resulting in a complete restructuring and editing of the previous edition.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document describes the structure and contents of a data element related to key management which 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 document. 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 Personal Identification Number (PIN) data and MACs, are described in ISO 9564 and ISO 16609, respectively.

This document provides key management information, including that related to the use and application of ISO 8583-1, i.e. the interchange messages used in processing card transactions, which are referenced in ISO 8583-1. However, the data elements assigned in ISO 8583-1 were built to accommodate earlier encryption technologies (e.g. data encryption standard, triple data encryption standard) and they are not long enough to accommodate the advanced encryption standard (AES) and/or other encryption methods for encrypting sensitive payment card data, which require longer data fields. Accordingly, in order to facilitate the use of AES for key management purposes related to ISO 8583-1, it has been proposed to expand the relevant data element fields in ISO 8583-1.

Although ISO 8583-1 is the most recent standard, in practice, many card processing parties still use older documents, either ISO 8583:1987 or ISO 8583:1993. Both of these documents have been withdrawn and replaced by the ISO 8583 series.

This document accommodates data encryption algorithm (DEA), triple data encryption algorithm (TDEA) and AES as encryption technologies. For DEA and TDEA, fields 52, 53 and 96 are used. For AES, depending on the key management and data encryption processes, fields 110, 111 or 50 can be used.

This document provides compatibility with the existing ISO standard on bank card originated messages (ISO 8583-1).

Financial services — Key-management-related data element — Application and usage of ISO 8583-1 data elements for encryption

1 Scope

This document describes a data element related to key management which 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 document addresses the requirements for the use of the data element related to key management within ISO 8583-1, using the following two ISO 8583-1 data elements for DEA and TDEA:

— security related control information (data element 53);

— key management data (data element 96).

The data element related to key management for DEA and TDEA 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. For AES implementations, the data elements are summarized in one field.

This document is applicable to either symmetric or asymmetric cipher systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 8583-1,*Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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 1 to entry: 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
DUKPT
key management method which uses a unique key for each transaction and prevents the disclosure of any past key used by the transaction-originating secure cryptographic device (SCD)

Note 1 to entry: The receiving SCD can derive the unique transaction keys from a base derivation key using only non-secret data transmitted as part of each transaction.

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

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

4 Abbreviated terms

AES advanced encryption standard

BCD binary coded decimal

CBC cipher block chaining

DEA data encryption algorithm

ECB electronic code book

ECIES elliptic curve integrated encryption scheme

IIN issuer identification number

MAC message authentication code

PIN personal identification number

RSA The Rivest, Shamir and Adleman public key cryptosystem

SCD secure cryptographic device

TDEA triple data encryption algorithm

TLV tag length value

UKPT unique key per transaction

5 Data representation

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

Table 1 — Data representation

Abbreviation	Definition
a	The alphabetic data element contains a single character per byte. The permitted characters are alphabetic only (a to z and A to Z, uppercase and lowercase).
an	The alphanumeric data element contains a single character per byte. The permitted characters are alphabetic (a to z and A to Z, uppercase and lowercase) and numeric (0 to 9).
ans	The alphanumeric special data element contains a single character per byte.
ansb	The alphanumeric special data element consists of binary.
b	The data element consists 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	The length of variable data element follows, 01 to 99. This length format is specific to bitmap usage.
LLL	The length of variable data element follows, 001 to 999. This length format is specific to bitmap usage.
LLLL	The length of variable data element follows, 0001 to 9999. This length format is specific to bitmap usage.
n	Numeric data elements. The permitted values are numeric only (0 to 9). In the case of tag length value (TLV) structure, numeric values have to be implemented in binary coded decimal (BCD), which consists 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 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'. For bitmap structure it is up to the implementer to use either standard numeric or BCD.

6 Requirements for key-management-related data element

6.1 Introduction

The data element related to key management for DEA and TDEA 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 structure for all these fields will utilize data set, TLV or bitmap structure, (referred to as composite data element in ISO 8583-1:2003, 5.4.4).

Regardless of algorithm used, 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 (UKPT)];

— 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.

Table 2 describes usages of the fields relevant for key management and data encryption.

Table 2 — Field usage

Field	Data element name	Usage
50 (see ISO 8583-1)	Encryption data	Includes PIN encryption Data, MAC security related information, sensitive encryption data and key management encryption data.
52	PIN data	Is not used if field 110, 111, or 50 is used instead.
53	Security related control information	Is not used if field 110, 111, or 50 is used instead.
64	MAC	Contains the MAC value. Security related control information will be within new proposed field 110, 111 or 50. The length would be maintained to 8 bytes even for AES encryption as the 16 bytes length will be truncated to the leftmost 8 bytes.
96	Key management data	Is not used if field 110, 111, or 50 is used instead.
110[a]	Encryption data	Includes PIN encryption data, MAC security related information, sensitive encryption data and key management encryption data.
111[a]	Encryption data	Includes PIN encryption data, MAC security related information, sensitive encryption data and key management encryption data.
128	MAC	Contains the MAC value. Security related control information will be within new proposed field 110, 111 or 50. The length would be maintained to 8 bytes even for AES encryption as the 16 bytes length will be truncated to the leftmost 8 bytes.

[a] Format for Field 110 (see ISO 8583:1987) and Field 111 (see ISO 8583:1993) has been changed from LLLVAR...999 to LLLLVAR...ansb 9999.

6.2 Data element structure

6.2.1 Data element structure for field 53 and 96

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

— Form 1, for example key change [see Figure 1 a)];

— Form 2, for example key selection [see Figure 1 b)].

LL	Data element 53
	Security related control information

LLL	Data element 96
	Key management data

a) Form 1

LL	Data element 53
	Security related control information

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).

When data element 53 is used to indicate which of the possible key-sets are to be used or affected by the key management message, this section applies. 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 Tables 3 and 4.

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

— in Table 3, format A as used for fixed and master/session key;

— in Table 4, format B for derived unique key per transaction (DUKPT) key management scheme, as defined in ANSI X9.24-3.

Table 3 — Data element 53 — Structure format A

Length bytes	**Field name**	**Description**	**Encoding**	**Required**
1	Control	Control identifies the key management scheme and associated structure of the remainder of the data element as defined in 7.1.	b 1	Mandatory
4	Key-set identifier	Key-set identifier is as defined in 7.2.	n 8	Mandatory
1	Algorithm	Algorithm selects the encryption algorithm used to encipher the keys contained in the associated key management data element as defined in 7.3.	n 2	Optional
2	Key length	Key length of the enciphered key is as defined in 7.4.	n 4	Optional
1	Protection	Protection is a mechanism used to provide key confidentiality and integrity as defined in 7.5.	n 2	Optional
2	Reserved national	Reserved for national use.	n 4	Optional
1	Reserved private	Reserved for private use.	n 2	Optional

Table 4 — Data element 53 — Structure format B

Length bytes	Field name	Description	Encoding	Required
1	Control	Control identifies the key management scheme and associated structure of the remainder of the data element as defined in 7.1.	b 1	Mandatory
5	Key-set identifier	Key-set identifier is as defined in 7.2.2.	n 10	Mandatory
5	Device ID and transaction counter	Device ID and transaction counter are as described in 7.2.2.	b 5	Mandatory

Data element 96 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 2). Examples of possible structures include single or multiple enciphered keys that may be contained in integrity-protected key blocks, such as that specified in ISO 20038. In KSN compatibility mode of AES DUKPT the control field contains the value associated with AES DUKPT according to Table 9.

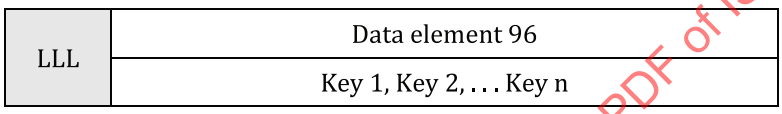

Figure 2 — Key management data — Data element 96

6.2.2 Data element structure for field 50, 110, 111

This subclause describes data sets for PIN encryption (Table 5), message authentication coding (Table 6), data encryption (Table 7) and key exchange (Table 8). A single message may include multiple data sets including multiple instances of the same type for data encryption and key exchange.

The length fields in the TLV coding of sub-elements shall be coded according to ISO/IEC 8825-1, if the TLV coded version of a data set is used, while the length of the data set itself is always coded as a 2-byte binary value.

Table 5 — Data set 01/71 — PIN encryption

Data set 01 TAG	Data set 71 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
80	2	65	Control	Control identifies the key management scheme and associated structure of the remainder of the data element.	b 1	Mandatory
81	3	LLVAR	Key-set identifier	Key-set identifier is as defined in 7.2.	b 8, b 10, b 16 or b 32	Mandatory
82	4	LLVAR	Derived information or Device ID and transaction counter (control contains TDEA, DUKPT)	Derived information is a random number or counter in order to have a UKPT, e.g. UKPT PIN encryption. or Device ID and transaction counter contains the transaction counter.	b 5, b 8, b 16 or b 32	Optional

Table 5 *(continued)*

Data set 01 TAG	Data set 71 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
83	5		Algorithm	Algorithm selects the encryption algorithm used to encipher the keys contained in the associated key management data element as defined in 7.3.	n 2	Optional
84	6		Key length in bytes	Key length of the enciphered key. See 7.4.	n 4	Optional
85	7		Key protection	Key protection is a mechanism used to provide key confidentiality and integrity. See 7.5.	n 2	Optional
86	8	LLVAR	Key index	Key index is used when multiple keys are identified with the same key-set identifier, e.g. key rotation.	n 2 or n 5	Optional
87	9		PIN block format	PIN block format is as defined in ISO 9564-1.	n 2	Mandatory
88	10	LLVAR	Encrypted PIN block	Encrypted PIN block is as defined in ISO 9564-1.	b 8 or b 16	Mandatory
89	11	LLVAR	Additional encrypted PIN block	Additional encrypted PIN block is used for PIN change.	b 8 or b 16	Optional

Table 6 — Data set 02/72 — MAC

Data set 02 TAG	Data set 72 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
80	2		Control	Control identifies the key management scheme and associated structure of the remainder of the data element.	b 1	Mandatory
81	3	LLVAR	Key-set identifier	Key-set identifier as defined in 7.2.	b 8, b 10, b 16 or b 32	Mandatory
82	4	LLVAR	Derived information or Device ID and transaction counter (control contains TDEA, DUKPT)	Derived information is a random number or counter in order to have a UKPT e.g. UKPT PIN encryption. or Device ID and transaction counter contain the transaction counter.	b 5, b 8, b 16 or b 32	Optional
83	5		Algorithm	Algorithm selects the encryption algorithm used to encipher the keys contained in the associated key management data element. See 7.3.	n 2	Optional

Table 6 *(continued)*

Data set 02 TAG	Data set 72 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
84	6		Key length in bytes	Key length is of the enciphered key. See 7.4	n 4	Optional
85	7		Key protection	Key protection is a mechanism used to provide key confidentiality and integrity. See 7.5.	n 2	Optional
86	8	LLVAR	Key index	Key index is used when multiple keys are identified with the same key-set identifier, e.g. key rotation.	n 2 or n 5	Optional
87	9		Padding method	See 7.6	n 2	Optional
88	10	LLVAR	Initialisation vector for cipher block chaining (CBC)	Initialisation vector.	b 8, b 16 or b 32	Optional

Table 7 — Data set 03/73 — Data encryption

Data set 03 TAG	Data set 73 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
80	2		Control	Control identifies the key management scheme and associated structure of the remainder of the data element.	b 1	Mandatory
81	3	LLVAR	Key-set identifier	Key-set identifier as defined in 7.2.	b 8, b 10, b 16 or b 32	Mandatory
82	4	LLVAR	Derived information or Device ID and transaction counter (control contains TDEA, DUKPT)	Derived information is a random number or counter in order to have a UKPT, e.g. UKPT PIN encryption or Device ID and transaction counter contain the transaction counter.	b 5, b 8, b 16 or b 32	Optional
83	5		Algorithm	Algorithm selects the encryption algorithm used to encipher the keys contained in the associated key management data element. See 7.3.	n 2	Optional
84	6		Key length in bytes	Key length is of the enciphered key. See 7.4.	n 4	Optional
85	7		Key protection	Key protection is a mechanism used to provide key confidentiality and integrity. See 7.5.	n 2	Optional
NOTE Additional data elements to be encrypted are defined as corresponding external code set, see https://www.iso20022.org/external_code_list.page.						

Table 7 *(continued)*

Data set 03 TAG	Data set 73 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
86	8	LLVAR	Key index	Key index is used when multiple keys are identified with the same key-set identifier, e.g. key rotation.	n 2 or n 5	Optional
87	9		Padding method	See 7.6.	n 2	Optional
88	10	LLVAR	Encrypted data format	Encrypted data format describes the content and coding of the encrypted data before encryption. See 7.7.	ans	Optional
89	11	LLLLVAR	Encrypted data	Encrypted data uses a structure within it prior to encryption to identify the data. Permits the encryption of multiple data elements together.	b 8 up to b 9999	Optional
8A	12	LLVAR	Encrypted PAN		b	Optional
8B	13	LLVAR	Encrypted card sequence number		b 8 or b 16	Optional
8C	14	LLVAR	Encrypted track 1 data		b 8 up to b 80	Optional
8D	15	LLVAR	Encrypted track 2 data		b 8 up to b 74	Optional
8E	16	LLLVAR	Encrypted track 3 data		b 8 up to b 112	Optional
8F	17	LLVAR	Encrypted card verification data	Card verification data.	b 8 or b 16	Optional
90	18	LLVAR	Encrypted expiration date		b 8 or b 16	Optional

NOTE Additional data elements to be encrypted are defined as corresponding external code set, see https://www.iso20022.org/external_code_list.page.

Table 8 — Data set 04/74 — Key exchange

Data set 04 TAG	Data set 74 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
80	2		Control	Control identifies the key management scheme and associated structure of the remainder of the data element.	b 1	Mandatory
81	3	LLVAR	Key-set identifier	Key-set identifier as defined in 7.2.	b 8, b 10, b 16 or b 32	Mandatory

Table 8 *(continued)*

Data set 04 TAG	Data set 74 BITMAP		Field name	Description	Representation	Required
	Bit	Length				
82	4	LLVAR	Derived information or Device ID and transaction counter (control contains TDEA, DUKPT)	Derived information is a random number or counter in order to have a UKPT, e.g. UKPT PIN encryption or contains the transaction counter.	b 5, b 8, b 16 or b 32	Optional
83	5		Algorithm	Algorithm selects the encryption algorithm used to encipher the keys contained in the associated key management data element. See 7.3.	n 2	Optional
84	6		Key length in bytes	Key length is of the enciphered key. See 7.4.	n 4	Optional
85	7		Key protection	Key protection is a mechanism used to provide key confidentiality and integrity. See 7.5.	n 2	Optional
86	8	LLVAR	Key index	Key index is used when multiple keys are identified with the same key-set identifier, e.g. key rotation.	n 2 or n 5	Optional
87	9	LLLLVAR	Encrypted data	Encrypted data uses a structure within it prior to encryption to identify the data.	b 8 up to b 9999	Optional
88	10	LLLLVAR	Key checksum value	Key checksum value contains a value used to verify a conveyed key. Length depends on algorithm used (see 7.3).	b 8 up to b 9999	Optional

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 the following:

— 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 format

7.1 Control field format

Table 9 shows the control field values for the two structure formats.

Table 9 — Control field values

Value	Field content	Definition	Format
0	00	Default	A
1	01	Fixed key	A
2	02	Master/session	A
3	03	UKPT	A
4	04	DEA, DUKPT	B
5	05	TDEA, DUKPT	B
6	06	AES, DUKPT	B

7.2 Key-set identifier

7.2.1 Format A

Format A is used primarily for master-session and UKPT key management as a means of distinguishing between several master keys. Table 10 is one example of a key-set identifier for format A values. Note that this table uses six-digit identifiers for the institution. With the extension of issuer identification numbers (IINs) from six to eight digits, the institution identification may need to increase correspondingly.

Table 10 — Key-set identifier — Format A values

Value	Field content	Definition
0	00000000	Use default key-set
xxxxxx01	xxxxxx01	Use key-set 1 associated with institution xxxxxx
xxxxxx02	xxxxxx02	Use key-set 2 associated with institution xxxxxx
. . .		
xxxxxx99	xxxxxx99	Use key-set 99 associated with institution xxxxxx

Another example is provided in ISO 20038:2017, Table A.1.

7.2.2 Format B

Format B key-set identifiers as defined herein are used with DUKPT key management exclusively. The key-set identifier uniquely identifies the base derivation key as defined in ANSI X9.24-3.

7.3 Algorithm field

The algorithm field (see Table 11) defines the algorithm used.

Table 11 — Algorithm

Field value	Definition
00	Default
01	DEA as defined in ISO/IEC 18033-3
NOTE Modes of operation of block ciphers are not specified but left to mutual agreement by participants.	