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

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'.

