BS ISO 13492:2019

BSI Standards Publication

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

National foreword

This British Standard is the UK implementation of ISO 13492:2019. It supersedes BS ISO 13492:2007, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2019

ISBN 978 0 580 99441 8

ICS 35.240.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2019.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO 13492:2019

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)

COPYRIGHT PROTECTED DOCUMENT

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 ..... **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 **3**
6.1 Introduction 3
6.2 Data element structure 4
6.2.1 Data element structure for field 53 and 96 4
6.2.2 Data element structure for field 50, 110, 111 6
6.3 Key-set identifier concepts 10
7 Security related control information usage format **11**
7.1 Control field format 11
7.2 Key-set identifier 11
7.2.1 Format A 11
7.2.2 Format B 11
7.3 Algorithm field 11
7.4 Key length (in bytes) field 12
7.5 Key protection field 12
7.6 Padding method field 12
7.7 Encrypted data format field 13
Bibliography **14**

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).

INTERNATIONAL STANDARD **ISO 13492:2019(E)**

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