

ICS 35.240.40
CCS A 11



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 21081-2007

Banking -- Key management related data element (retail)

银行业务 密钥管理相关数据(零售)

(English Translation)

Issued on: September 5, 2007

Implemented on: December 1, 2007

Issued by: Standardization Administration of China

Table of Contents

Introduction

Introduction

1 Scope

2 Normative references

3 Terms and definitions

Claim 4 Key management related data element

4.1 The concept of the 2 key set identifier

4.2 Distribution key set identifier

5 ISO 8583:1993 Realization

Applications Appendix A (informative) Key management related data transmission element

Annex B (informative) Application Example 8 key set identifier

Foreword

This standard is equivalent to international standard ISO 13492:1998 "Key management related data element (retail)" (in English).

For ease of use, for ISO 13492 made the following editorial changes.

a) Normative references to international standards in the document referenced in corresponding national standards, references to the national standards.

b) Remove the preface to international standards.

The Standard Appendix A, Appendix B is an informative annex.

The standard proposed by the People's Bank of China.

This standard by the National Standardization Technical Committee on Finance.

Introduction

This standard describes the structure and content of key management related data elements, the data elements can be in retail banking environment, through newsletters Text transmitted, to support secure key management. Wherein retail banking environment includes a card receiving device and the acquirer, and issuer Communication between the parties. Key management key and associated data elements used in the IC card does not apply to this standard.

This standard is compatible with existing bank card packet ISO standard (see ISO 8583).

GB/T 21081-2007/ISO 13492:1998 Banking - Key management related data element (retail)

1 Scope

This standard specifies the key management related data element, the data element in the transaction or transfer packets (used to protect the secret of the current transaction Key information), or transmitted in an encrypted message service (for protecting key information future transactions).

This standard describes the ISO 8583:1993 within the scope of application of key management related data element requirements, you should use the following two ISO 8583:1993 data elements. safety-related control information (53 yuan) or key management data (96 yuan). But the key management data the transfer is not limited to ISO 8583:1993 standards.

This standard applies to symmetric and asymmetric cryptography.

ISO 11568 describes the key security management processes in retail banking environment. ISO 9564 and ISO 9807, respectively, describe the security Full related data such as PIN and MAC.

2 Normative references

The following documents contain provisions which, through reference in this standard and become the standard terms. For dated references, subsequent Amendments (not including errata content) or revisions do not apply to this standard, however, encourage the parties to the agreement are based on research Whether the latest versions of these documents. For undated reference documents, the latest versions apply to this standard.

GB/T 15694.1-1995 Identification card maker identification card issuers - Part 1. Numbering System (idt ISO/IEC 7812-1:1993) ISO/IEC 7812-2:1993 Identification card issuer identification - Part 2. Application and registration procedures ISO 8583:1993 generated financial transaction card packet exchange message specification ISO 8908:1993 Banking and related financial services vocabulary and data elements ISO 9564-1:1991 management and security - Part 1 PIN. PIN protection principles and techniques ISO 9807:1991 Banking and related financial services message authentication requirements (retail) ISO 11568-1:1994 Banking - Key management (retail) - Part 1. Introduction Key Management ISO 11568-2:1994 Banking - Key management (retail) - Part 2. symmetric cryptographic key management technology ISO 11568-3:1994 Banking - Key management (retail) - Part 3. Key life cycle for symmetric ciphers ANSI X3.92. 1987 Data Encryption Algorithm

3 Terms and Definitions

ISO 8908:1993 gives the following terms and definitions apply to this standard.

Different encryption key and decryption key, the encryption key and the decryption key deduced is not feasible.

Under the control parameter called the key to achieve mutual conversion between plaintext, ciphertext set of operations.

Note: The encryption algorithm is data (plaintext) into unintelligible form (ciphertext). Decryption is the ciphertext back to the plaintext.

Predetermined set of rules to achieve data encryption and decryption process.

Note: The design of the algorithm so that it is impossible except by exhaustive search to determine the control parameters (such as keys).

GB/T 21081-2007/ISO 13492:1998