

ICS 35.240.40
CCS A 11



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

GB/T 27909.2-2011

**Banking -- Key management (retail) -- Part 2: Symmetric ciphers
-- Key management and life cycle**

银行业务 密钥管理(零售) 第2部分：对称密码及其密钥管理和生命周期
(English Translation)

Issued on: December 30, 2011

Implemented on: February 1, 2012

Issued by: Standardization Administration of China

Table of Contents

Introduction	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
General Environmental Management Technology 4 key	
4.1 Overview	
4.2 Features password security device	
4.3 Key generation	
4.4 Key calculation (deformation)	
Key rating 4.5	
4.6 Key Lifecycle	
4.7 Key storage	
Reacquire 4.8 backup key	
4.9 Key distribution and import	

Foreword

GB/T 27909 "Banking - Key management (retail)" is divided into the following three parts.

--- Part 1. General principles;

--- Part 2. Symmetric ciphers and key management and life cycle;

--- Part 3. asymmetric cryptography and key management and life cycle.

This part of GB/T 27909 Part 2.

This section drafted in accordance with GB/T 1.1-2009 given rules.

The partial modification of international standard ISO 11568-2:2005 "Banking - Key management (retail) - Part 2. symmetric cryptosystem EC and its key management and life cycle "(in English).

When adopting ISO 11568-2 made the following changes.

Remove the "ISO 11568-2 Appendix B approved symmetric key management algorithms," explains techniques as described in this section in Chapter 1 Algorithm involved should comply with the relevant provisions of the state password administration.

This section also 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) Delete ISO foreword.

This section proposed by the People's Bank of China.

This part of the National Standardization Technical Committee on Finance (SAC/TC180) centralized.

This section is responsible for drafting units. China Financial Computerization Corporation.

Participated in the drafting of this section. People's Bank of China, Industrial and Commercial Bank of China, Agricultural Bank of China, Bank of China, Bank of Communications, China Everbright Bank of China Unionpay.

Introduction

GB/T 27909 describes a process safety management in key retail financial services environment, such as the keys used to protect the acquirer Between the parties and the acceptance packet acquirer and card issuer between.

This section describes the retail financial services sector in the applicable key management requirements, a typical type of service have sales/service points (POS) and ATM authorize borrowing record (ATM) transactions.

When using the key management GB/T 27909 sections describe the combination can provide key management in GB/T 27909.1 described Management services.

These services include.

- Key separation;
- Prevent the key replacement;
- Key authentication;
- Key Sync;
- Key Integrity;
- Key confidentiality;
- Key leak detection.

Control Key Management Service and the corresponding reference key management technologies, see Chapter 7.

This section describes the use of symmetric cryptography mechanism, key security

management involved in key life cycle. According to GB/T 27909.1 and this part of the key management principles, services and technologies described in this section also specifies the various stages of the life of the key requirements and implementations law. This section does not involve asymmetric cryptographic key management mechanism or life cycle, the contents of this aspect see GB/T 27909.3.

When this part of the development, give full consideration to the ISO/IEC 11770 standards.

This section describes the use of technology and meet the needs of the financial services industry.

Banking - Key management (retail) Part 2. Symmetric ciphers and key management and life cycle

1 Scope

This section describes the retail financial services environment, when using symmetric and asymmetric cryptographic protection mechanism asymmetric key technologies, and also describes Said the symmetric key associated with the life cycle management. The techniques described in this section in line with GB/T 27909.1 principles described.

Techniques described in this section apply to any asymmetric key management operations.

Symbols used in this section, see Appendix A.

This section describes the algorithm technology involved to comply with the relevant provisions of the state password administration.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB/T 27909.1-2011 Banking - Key management (retail) - Part 1. General principles (ISO 11568-1:2005, MOD) GB/T 20547.2-2006 Banking Secure cryptographic devices (retail) - Part 2. Financial transaction device security compliance Detection Listing (ISO 13491-2:2005, MOD) GB/T 21078.1-2007 Banking Personal Identification Number management and security - Part 1. ATM and POS systems in the United the basic principles and requirements for machine PIN processing (ISO 9564-1:2002, MOD) GB/T 21079.1 Banking Secure cryptographic devices (retail) - Part 1. Concepts, requirements and evaluation methods (GB/T 21079.1-2007, ISO 13491-1:1998, MOD) Operation ISO/IEC 10116 Information technology - Security techniques n-bit block cipher ISO 16609:2004 Banking technology using symmetric message authentication requirements ISO/IEC 18033-1 Information technology - Security techniques - Encryption algorithms - Part 1. Summary ISO/T R19038.2005 Banking and related financial services - Triple DEA

operation mode Implementation Guide ANSI X9.24 Part 1-2004 retail financial services
symmetric key management - Part 1. using symmetric techniques ANSI X9.65 Triple Data
Encryption Algorithm (3-DEA), the implementation of standards

3 Terms and Definitions

The following terms and definitions apply to this document.

Password cipher

Under the control parameter called the key to realize pair of operation between the plaintext and ciphertext conversion.

NOTE: Data encryption (plain text) into cipher text into unreadable; decryption operation ciphertext back into plaintext.