

ICS 35.240.40

CCS A 11



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

GB/T 27909.3-2011

**Banking -- Key management (retail) -- Part 3: Asymmetric
cryptosystems -- Key management and life cycle**

银行业务 密钥管理(零售) 第3部分：非对称密码系统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

4 Retail financial services system using asymmetrical cryptography

4.1 Overview

Creating and storing 4.2 symmetric key

4.3 Asymmetric public key storage and distribution

4.4 Asymmetric private key storage and transport

5 Key Management Service provides technical

5.1 Overview

4 5.2 Key Encryption

5.3 Public Key Authentication

5.4 Key separation technologies

6 5.5 Key Authentication

6 5.6 Key Integrity Technology

6 Asymmetric key life cycle

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 3.

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

The partial modification of international standard ISO 11568-4:2005 "Banking - Key management section (retail) 4. asymmetric cryptography System and its key management and life cycle "(in English).

When adopting ISO 11568-4 made the following changes.

--- Remove the "ISO 11568-4 Annex A approved algorithm." 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 technology GB/T 27909 sections describe the combination can provide key management in GB/T 27909.1 described service.

These services include.

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

This section describes the use of asymmetric cryptographic mechanisms, security key management involved in key life cycle. According to the standard Part 1 and this part of the key management principles, services and technologies described in this section also sets

out the various stages of the life of the key requirements and implementations law. This section does not involve a symmetric cryptographic key management mechanism or life cycle, the contents of this aspect see GB/T 27909.2.

This part of GB/T 27909, GB/T 21078.1, GB/T 20547, ISO 9564-2, ISO 9564-3, ISO 9564-4, ISO/T R19038 safety requirements, etc. One of the criteria described in the financial services sector.

Banking - Key management (retail) Part 3. asymmetric cryptosystem and Key management and life cycle

1 Scope

This section provides retail financial services environment using asymmetric cryptographic mechanisms to protect technical symmetric and asymmetric keys, also described Associated with the asymmetric key lifecycle management. This section applies to technology in line with the principles GB/T 27909.1 described.

This part of the retail financial services environment is limited to the interface between the following entities.

- Card acceptance device and the acquirer;
- Acquirer and card issuer;
- Integrated Circuit Card (ICC) and the card acceptance device.

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 Banking - Key management (retail) - Part 1. General principles (GB/T 27909.1-2011, ISO 11568-1:2005, MOD) GB/T 27909.2 Banking - Key management (retail) - Part 2. Symmetric ciphers and key management and life cycle (GB/T 27909.2-2011, ISO 11568-2:2005, MOD) GB/T 17964-2000 Information security technology block cipher mode of operation (ISO/IEC 10116:1997, IDT) GB/T 20547.2 Banking Secure cryptographic devices (retail) - Part 2. Secure financial transactions for compliance could detect clear Single (GB/T 20547.2-2006, ISO 13491-2:2005, MOD) GB/T 21078.1 Banking Personal Identification Number management and security - Part 1. ATM and POS systems online PIN the basic principles and requirements for processing (GB/T 21078.1-2007, 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) ISO/IEC 9796-2:2002 Information technology - Security technology message recovery signature scheme ISO/IEC 10118 (all parts), Information technology - Security

techniques hash function Mechanisms using asymmetric techniques. ISO/IEC 11770-3
Information technology - Security techniques - Key management - Part 3 Signatures - Part
3 ISO/IEC 14888-3 Information technology - Security techniques - Appendix. the discrete
logarithm based mechanisms ISO 15782-1:2003 Banking Certificate management - Part 1.
Public key certificates ISO/IEC 15946-3:2002 Information technology - Security techniques
- Cryptographic techniques based on elliptic curves - Part 3. Key generate ISO 16609:2004
Banking. using symmetric techniques packets certification requirements ISO/IEC 18033-2
Information technology - Security techniques - Encryption algorithms - Part 2. asymmetric
cryptography Public key cryptography ANSI X9.42-2003 financial business use discrete
logarithm password symmetric key agreement