

ICS 35.240.40
CCS A 11



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

GB/T 27909.1-2011

Banking -- Key management (retail) -- Part 1: Principles

银行业务 密钥管理(零售) 第1部分：一般原则

(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 Key Management	
4.1 Safety Goal	
4.2 Security Level	
4.3 Key Management Goal	
5 Key Management Principles	
Cryptography 4	
6.1 Summary	
6.2 Cryptography	
6.3 Asymmetric cryptosystem	
6.4 Asymmetric cryptosystem	
6.5 Other cryptosystem	

Foreword

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

- 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 1.

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

The partial modification of international standard ISO 11568-1:2005 "Banking - Key management (retail) - Part 1. General principles" (In English).

When adopting ISO 11568-1 made the following changes.

Remove the "ISO 11568-1 Annex A cryptographic algorithm approval process" described in Chapter 1, the key management for cryptographic algorithms 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 documents referenced, corresponding to the national standard 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 in retail financial services environment key safety management processes, 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.

Key management is authorized to provide the key to the communicating parties, and before the key is destroyed, so the key is under continuous process control security process.

Data security depends on preventing leakage of keys and unauthorized modifications, substitutions, insertions or termination, therefore, it relates to key management Key generation, storage, distribution, use and destruction of each program. Through standardization of these procedures, but also for the development of audit trail norms laid the foundation.

This section does not provide the same key distinction between an entity approach. Final Rule requires key management process by the communication related parties Negotiated decisions and should agree on the identity of the individual and their responsibilities, communication parties to this rule bear the corresponding responsibilities. GB/T 27909 Ben Body does not relate to the allocation of individual responsibility, which is a key management implementations need to be considered.

Banking - Key management (retail) Part 1. General principles

1 Scope

This section sets out the key principles of password management system in the retail financial services environment implementation should follow. This part of the retail financial it means a service environment interfaces between entities.

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

Appendix A shows an example of the environment, Appendix B describes the implementation of this part of the subject-related threats.

This section can also apply to the symmetric key cryptography and asymmetric cryptographic system of private and public keys. In symmetric cryptosystems , The sender and recipient use the same key. Cryptographic algorithms used for key management should comply with the relevant provisions of the state password administration.

In addition to involving the use of a password key, and often it involves control information, e.g., as an initialization vector key identifier. The information referred to the "key element." Although this section specifically describes the key management, but it is the principle of service and technology is also applicable to the key elements.

This section applies to financial institutions and other organizations in the field of retail financial services. In these areas, the exchange of information requires confidentiality , Completeness or authenticity. Retail Financial Services, including but not limited to POS lending remember authorization, such as vending machines and automated teller machines (ATM) transactions and other services.

In ISO 9564 and ISO 16609 standards, describe the retail financial transactions a personal identification number (PIN) encryption as well as in the newspaper Message authentication password used by the operation. GB/T 27909 also apply to the management of these standards introduced key. In addition, key management Processing procedure itself requires the introduction of a deeper level of key, e.g., key-encrypting key. Key management process is equally applicable to these keys.

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 20547.2-2006 Banking Secure cryptographic devices (retail) - Part 2. financial transactions comply with safety equipment Detection list (ISO 13491-2:2005, MOD) GB/T

27909.2 Banking - Key management (retail) - Part 2. Symmetric ciphers and key management and life cycle (ISO 11568-2:2005, MOD) GB/T 27909.4 Banking - Key management (retail) - Part 4. asymmetric cryptography and key management and life cycle Period (ISO 11568-4:2007, MOD)

3 Terms and Definitions

The following terms and definitions apply to this document.

Asymmetric key pair Generated and used in a public key cryptosystem public key and its associated private key.