

ICS 35.240.40
CCS A 11



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

GB/T 21082.5-2007

**Banking -- Key management (retail) -- Part 5: Key life cycle for
public key cryptosystems**

银行业务 密钥管理(零售) 第5部分：公开密钥密码系统的密钥生命周期
(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

4 2 General requirements

4.1 Asymmetric key pair generation

Authenticity before using 4.2

4.3 2 public key authentication

4.4 Asymmetric key pair transmission

4.5 Key store

Foreword

GB/T 21082 "Banking - Key management (retail)" is divided into the following six sections.

- Part 1 Introduction of key management;
- Part 2 symmetric key management password;
- Part 3 symmetric cryptographic key life cycle;
- Part 4 of the use of key management public key encryption;
- The first section 5 public key cryptosystem key life cycle;
- Part 6 key management scheme.

This part of GB/T 21082 Part 5.

This section identical with the international standard ISO 11568-5:1998 "Banking - Key management (retail) - Part 5. public key cipher Code Key life cycle "(in English).

For ease of use, the ISO 11568-5:1998 in this section do 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 centralized financial management.

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, China Merchants Bank, North China Computing Technology the, Venus Limited.

Introduction

GB/T 21082 describes in retail banking environment, for the protection of such income between single-line and by chi-square, or acquirer and card issuer Packets will be between the key process safety management. Key management for an integrated circuit card is not included in GB/T 21082 standard.

Given the key management of wholesale banking transaction environment with a relatively high-security environment is characterized by the key exchange, and this standard describes Key management requirements apply to retail banking services accessible area. Such services are typically the point of sale/point of service (POS) debit, Credit authorization and ATM transactions.

GB/T 21082 This section describes the public key cryptosystem key security key lifecycle management.

Public key cryptography uses public and private keys. These keys are in GB/T 21082 in this section collectively referred to as a key pair.

Chapter 4 sets out the key to the general safety requirements at all stages of the life cycle, using the ISO 11568-1:1994 and ISO 11568-4. Key management principles described in 1998, services and technologies.

Chapter 5 provides for the related implementation methods with these general safety requirements.

Key life cycle includes three phases.

1. Activities to be stages. during the key pair is generated and can be transmitted.
2. Activities stage. During the public key is distributed to at least one or more parties for operational use.
3. After the event stage. during the key to the public key is archived, it uses the private key is terminated.

A schematic view of a private key (S) and the life cycle of a public key (P) respectively in the life cycle of FIG. 1 and FIG. 2 are given. The figure shows on How specific operation key is to change its state.

Key may be considered a single object, which may be multiple instances of a plurality of different forms in different locations. In the following You can make a clear distinction between.

--- To distribute public communication party;

--- In one of the owners can not afford to produce implementation of the key pair, to which the owner of the transmission key pair.

and.

--- Destruction of a single instance of the private key;

--- Delete the private key from a given position, that is the key to destroy all instances in this position;

Termination --- private key, the key is removed from all locations.

GB/T 21082.5-2007/ISO 11568-5:1998

Figure 1 private life cycle

GB/T 21082.5-2007/ISO 11568-5:1998

Figure 2 Public Key Lifecycle

GB/T 21082.5-2007/ISO 11568-5:1998 Banking - Key management (retail) - Part 5.

Public key cryptosystem key lifetime

1 Scope

This section details the security requirements in retail banking environment, as well as asymmetric key pair in a key private and public keys Implementation of each phase of the life cycle.

This section applies to any key management technology institutions, public key cryptographic system it manages to achieve the data protection.

2 Normative references

The following documents contain provisions which, through reference GB/T 21082 in this section and become the standard terms. For dated reference documents Member, all subsequent amendments (not including errata content) or revisions do not apply to this section, however, encouraged to reach under this section Parties to research agreement to use the latest versions of these documents. For undated reference documents, the latest versions apply to this section.

GB/T 17901.1-1999 Information technology - Security techniques - Key management - Part 1. Framework (idt ISO/IEC 11770-1.

1996)

GB/T 21082.4-2007 Banking - Key management (retail) - Part 4. Using public key encryption key management technology ISO 8908:1993 Banking and related financial services vocabulary and data elements ISO 9564-1:2002 Banking - Personal Identification Number management and security - Part 1. Personal Identification Number (PIN) to protect the original the technical and 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 Mechanisms using asymmetric techniques. ISO/IEC 11770-3:1999 Information technology - Security techniques - Key management - Part 3 ISO 13491 (all parts) banking security cryptographic devices (retail)

3 Terms and Definitions

ISO 8908:1993 standards established, and the following terms and definitions apply to this section.

Apparatus for generating secure passwords asymmetric key pair.

Receives a public key for communication with the owner of one of the public key.

Means allows entities to reverse prior to generating the certificate authentication credentials and identification documents of correctness of procedure (for example. callback, visual identification, etc.

Wait).

GB/T 21082.5-2007/ISO 11568-5:1998