

ICS 35.240.40

CCS A 11



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

GB/T 21082.4-2007

**Banking -- Key management (retail) -- Part 4: Key management
techniques using public key cryptography**

银行业务 密钥管理(零售) 第4部分: 使用公开密钥密码的密钥管理技术

(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

Use 4 retail banking system public key cryptographic system

5 Key Management Service provides technical

6 5 public key certificate management

Management Appendix A (normative) public key certificates

Annex B (informative) attribute certificate

Basic Concepts Appendix C (informative) public key cryptographic system

References

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/Part 4 T 21082 of.

The partial modification of international standard ISO 11568-4:1994 "Banking - Key management (retail) - Part 4. Publication secret Key management key password "(in English).

Taking into account China's national conditions, in the use of ISO 11568-4 doing the following modifications.

Remove the "ISO 11568-4 Annex A approved algorithms and their audit procedures" in Chapter 1 should follow the instructions of password management Relevant provisions of

the department.

For ease of use, 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.

Appendix A of this section is normative appendix, Appendix B, Appendix C is informative appendix.

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 is described in a series of key retail banking environment, standard security management process, these keys are used to protect such as that between the acquirer and the chi-square, or packets between the acquirer and the issuer. Key management for an integrated circuit card is not included in the GB/T 21082 standard.

Given the wholesale banking environment in key management is a key factor in the security exchange relatively high security environment characterized by the standard Quasi described in the field of retail banking services related to the application of key management requirements typical service types are the point of sale/point of service (POS) Debit payments, credit card payment vouchers and ATM (ATM) transactions.

This section GB/T 21082 main description applies to public-key cryptography key management techniques. When used in combination, these Technology will provide key management services as described in ISO 11568-1. These services are.

- Key separation;
- Prevent the key replacement;
- Key authentication;
- Key Sync;
- Key Integrity;

--- Key confidentiality;

--- Key leak detection.

Banking - Key management (retail) Part 4. Using public key encryption Key management technology

1 Scope

GB/T 21082 This part describes in detail the use and protection in the retail banking business environment for public-key cryptography system key technology.

It is applicable to any organization in the key lifecycle responsible for implementing key protector. This section GB/T 21082 skills described Operation in line with principles described in ISO 11568-1.

NOTE: protection details at every stage of the life cycle of the key requirements for the protection of public key cryptography are described in detail in ISO 11568-1.

Public key cryptographic system include asymmetric cryptographic digital signature and public key distribution system. While this section describes in Key management application of these systems technology, but some of these technologies also apply to security management data.

The techniques described in this section is mainly aimed at the general public key cryptography. See Appendix for the specific criteria for a particular system.

Algorithms and algorithms approval procedures and techniques described in this section should be used in conjunction with the State Password Administration comply with relevant agencies Provisions.

Appendix A provides an overview of the standardization of public key certificate management.

Appendix B describes the properties of the certificate, the technology can enhance the function of public key certificates.

Appendix C describes three public key cryptographic system mentioned above.

2 Normative references

The following documents contain provisions which, through reference GB/T 21082 in this section constitute provisions of this section. 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 15843.3-1998 Information technology - Security techniques - Entity Identification - Part 3. asymmetric signature mechanism (Idt ISO/IEC 9798-3:1993) GB/T 17964-2000 Information technology - Security techniques n-bit block cipher mode of operation (idt ISO/IEC 10116:1997) ISO/IEC 8824:1990 Information technology - OSI abstract syntax notation one (ASN.1) specification ISO/IEC 8825:1990 Information technology - OSI abstract syntax notation one (ASN.1) Specification of Basic Encoding Rules ISO 8908:1993 Banking and related financial services vocabulary and data elements ISO/IEC 9594-8:1990 Information technology - OSI Directory - Part 8. Authentication framework ISO 9807:1991 Banking and related financial services message authentication requirements (retail) ISO 11166 (all parts) banking asymmetric key management algorithms ISO 11568-1 Banking - Key management (retail) - Part 1. Introduction Key Management Key management technology symmetric ciphers. ISO 11568-2 Banking - Key management (retail) - Part 2 Mechanisms using asymmetric techniques. ISO/IEC 11770-3:1999 Information technology - Security techniques - Key management - Part 3 ISO 13491-1:1999 Banking - Secure cryptographic devices (retail) - Part 1. Concepts, requirements and evaluation methods

3 Terms and Definitions

ISO 8908:1993 is given in the following terms and definitions apply to this section.