

ICS 35.240.40

CCS A 11



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

GB/T 21077.2-2007

**Banking -- Certificate management -- Part 2: Certificate
extensions**

银行业务 证书管理 第2部分：证书扩展项

(English Translation)

Issued on: September 5, 2007

Implemented on: December 1, 2007

Issued by: Standardization Administration of China

Table of Contents

Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Extensions	
6 7 Key and policy information	
6.1 Requirements	
6.2 Certificate and CRL extensions	
7 Certificate subject and certificate issuer attributes	
7.1 Requirements	
7.2 Certificate and CRL extensions	
8 Certification Path Limited	
8.1 Requirements	
8.2 Certificate extensions	
8.3 Certification path processing program	
9 Basic CRL extensions	
20 9.1 Management Requirements	
9.2 Basic CRL and CRL entry extensions	
10 CRL distribution points and delta CRL	
22 10.1 Requirements	
10.2 Certificate extensions	
10.3 CRL and CRL entry extensions	
10.4 Match Rule	
Appendix A (informative) Examples of use of certification path defined	
References	

Foreword

GB/T 21077 "Banking Certificate management", is divided into two parts.

--- Part 1. public key certificate;

--- Part 2. Certificate extensions.

This section GB/T Part of 221,077.

The partial modification of the use of ISO 15782-2:2001 "Banking Certificate Management - Part 2. Certificate extensions" (in English).

Depending on the application, this section made the following changes.

- a) Remove ISO foreword;
- b) Taking into account the ISO 15782-1 has been published delete Chapter 2 normative references to "ISO 15782-1. banking certificate Management - Part 1. a public key certificate "provisions of footnote" forthcoming ";
- c) remove the "2 Normative references" in "FIPS-PUB140-1.1993" and so on;
- d) 8.1 chapters mentioned security related password for the device, was changed to "comply with the relevant national regulations." Appendix A of this section is an informative annex.

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

This part of the National Standardization Technical Committee centralized finance.

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

Participated in the drafting of this section. People's Bank of China, Bank of China, China Construction Bank, China Everbright Bank, China UnionPay Co. Shares Company, Beijing Venus company.

1 Scope

This section.

--- Excerpt and uses custom certificate extensions selected from the GB/T 16264.8-2005 in;

--- Certificate extensions by the provisions of the financial services industry to use the certificate extensions of additional demand.

This section will be used to finance standards bodies, including ISO 15782-1.

NOTE: ISO/IEC 8825-1 specified for ASN. ASN 1 encoding as defined in the certificate extensions. 1 Distinguished Encoding Rules (DER). By the GB/T DER rule 16264.8-2005 definition is not perfect, when certain values are encoded may lead to ambiguity.

2 Normative references

The following documents contain provisions which, through reference GB/T 21077 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 16264.2-1996 Information technology - OSI Directory - Part 2. Model (idt ISO/IEC 9594-2.

1990)

GB/T 16264.8-2005 Information technology - OSI Directory - Part 8. a public key and attribute certificate frameworks (ISO/IEC 9594-8:2001, IDT) GB/T 16284.4-1996 Information technology - Text communication - Message-oriented text interchange system - Part 4. Abstract service set Righteousness and procedures (idt ISO/IEC 10021-4:1990) Practice GB/T 17969.1-2000 Information technology - OSI OSI registration authorities - Part 1. General Regulations Cheng (eqv ISO/IEC 9834-1:1993) ISO 15782-1:2003 Banking Certificate management - Part 1. Public key certificates RFC791. 19811) Internet Protocol RFC822. 19822) ARPA Internet text message format standards RFC1035. 19873) Domain Implementation and Specification RFC1630.1994 Uniform Resource Identifiers in WWW. name and address of the World Wide Web identified targets using unified grammar

1) abolished RFC760; abolished by RFC1060.

2) repeal RFC733. by RFC987 updates; by RFC1327.

3) abolish RFC973. Abolition by RFC2136. by RFC2137 abolished; updates by RFC1348; updates by RFC1995; by RFC Update 1996; updated by RFC2065; updates by RFC2181; updates by RFC2308.

3 Terms and Definitions

The following terms and definitions apply to this section.

A characteristic of the entity.