ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 21077.2—2007

银行业务　证书管理
第2部分：证书扩展项

Banking—Certificate management—Part 2：Certificate extensions

（ISO 15782-2：2001，MOD）

2007-09-05 发布　　2007-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 21077《银行业务　证书管理》，分为两个部分：

——第1部分：公钥证书；

——第2部分：证书扩展项。

本部分为GB/T 21077的第2部分。

本部分修改采用ISO 15782-2：2001《银行业务　证书管理　第2部分：证书扩展项》(英文版)。

根据实际应用情况，本部分做了下列修改：

a) 删除ISO前言；

b) 考虑到ISO 15782-1已经出版，删除第2章规范性引用文件对“ISO 15782-1：银行业务　证书管理　第1部分：公钥证书”的条文脚注“即将出版”；

c) 在“2　规范性引用文件”中删除“FIPS-PUB 140-1：1993”等内容；

d) 8.1章节提到有关密码设备的安全性，修改为“遵从国家相关规定”。

本部分的附录A为资料性附录。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会归口。

本部分负责起草单位：中国金融电子化公司。

本部分参加起草单位：中国人民银行、中国银行、中国建设银行、中国光大银行、中国银联股份有限公司、北京启明星辰公司。

本部分主要起草人：谭国安、杨竑、陆书春、李曙光、刘运、杜宁、刘志军、张艳、张德栋、戴宏、张晓东、马云、李红建、王威、王沁、孙卫东、李春欢。

本部分为首次制定。

银行业务　证书管理
第2部分:证书扩展项

1　范围

本部分:

——摘录和采用了从GB/T 16264.8—2005中选择的证书扩展项的定义;

——规定了证书扩展项由金融服务行业使用证书扩展项的附加需求。

本部分将用于金融机构标准,包括ISO 15782-1。

注:ISO/IEC 8825-1中规定了为ASN.1编码所定义的证书扩展项的ASN.1的特异编码规则(DER)。由GB/T 16264.8—2005定义的DER规则不够完善,在对某些值进行编码时可能导致歧义。

2　规范性引用文件

下列文件中的条款通过GB/T 21077的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 16264.2—1996　信息技术　开放系统互连　目录　第2部分:模型(idt ISO/IEC 9594-2:1990)

GB/T 16264.8—2005　信息技术　开放系统互连　目录　第8部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

GB/T 16284.4—1996　信息技术　文本通信　面向信报的文本交换系统　第4部分:抽象服务定义和规程(idt ISO/IEC 10021-4:1990)

GB/T 17969.1—2000　信息技术　开放系统互连　OSI登记机构的操作规程　第1部分:一般规程(eqv ISO/IEC 9834-1:1993)

ISO 15782-1:2003　银行业务　证书管理　第1部分:公钥证书

RFC 791:1981[1)]　网际协议

RFC 822:1982[2)]　ARPA互联网文本报文格式标准

RFC 1035:1987[3)]　域名　实现和规范

RFC 1630:1994　在WWW中统一资源标识符:万维网中标识网络目标的名称和地址使用的统一语法

3　术语和定义

下列术语和定义适用于本部分。

3.1

属性　attribute

一个实体的特性。

1) 废止RFC 760;通过RFC 1060废止。

2) 废止RFC 733:通过RFC 987更新;通过RFC 1327更新。

3) 废止RFC 973:通过RFC 2136废止;通过RFC 2137废止;通过RFC 1348更新;通过RFC 1995更新;通过RFC 1996更新;通过RFC 2065更新;通过RFC 2181更新;通过RFC 2308更新。