ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27928.1—2011

金融业务　证书管理
第1部分:公钥证书

**Certificate management for financial services—
Part 1:Public key certificates**

(ISO 15782-1:2003,MOD)

2011-12-30 发布　　2012-05-01 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 27928 在总标题“银行业务 证书管理”下，包括以下 2 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 27928 的第 1 部分。

本部分修改采用 ISO 15782-1：2003《银行业务　证书管理　第 1 部分：公钥证书》(英文版)。

本部分根据 ISO 15782-1：2003 重新起草，与 ISO 15782-1：2003 的技术性差异及原因为：

a) 删去“2 规范性引用文件”中对下列文件的引用：

ANS X9.30-1　金融服务业　使用不可逆算法的公钥密码　第 1 部分：数字签名算法(DSA)；

ANS X9.31-1　金融服务业　使用可逆算法的公钥密码　第 1 部分：RSA 签名算法；

ANS X9.62　金融服务业　公钥密码：椭圆曲线数字签名算法(ECDSA)。

b) 6.2.1.2d)中：“宜使用标准化(ISO 或国家的)密码技术和密码模块，用于符合金融业使用要求的 4 级安全模块。”修改为：“宜使用国家的密码技术和密码模块，用于符合金融业使用要求的 4 级安全模块”。

c) 删去原英文标准中“6.3.5 CA 公钥分发”中如下文字：

对高风险应用，应使用 ISO 9807：1991，附录 C 中定义的 3DES MAC，或者单 DES MAC，单 DES MAC 使用不同密钥对每一个数据库或缓冲区的条目进行签名。对中低风险应用，使用任何核准的 TC68 密钥管理标准的单 DES MAC 就足够了。并删去本节最后一段中“如 DSA 和 RSA”。

d) 把 6.4.2 最后一段中原文“自动化的审计日志应保护以防止修改或替换。哈希和数字签名的使用可遵循 ANS X9.30，ANS X9.31 和 ANS X9.62 中规定”修改为“自动化的审计日志应保护以防止修改或替换。哈希和数字签名的使用应遵循我国密码管理部门的规定。”

e) 删去附录 B 标题的注释：3)对慎重的基于日志的算法如：Diffie-HelIman，DSA 和 ECDSA；删除附录 B.3 示例，因为该示例用了 DSA 和 RSA 的例子。

f) 将附录 E 的脚注“4)即将发布(ISO 8824-2：1998 的修订版)”，因为其对应的国家标准 GB/T 16262.2—2006 已经发布。

g) 删去附录 I(资料性附录)，因为其中引用了 DSA 等例子。

h) 删除 5.5，因为与 3.33 重复。

为便于使用，本部分还做了下列编辑性修改：

a) 对规范性引用文件中所引用的国际标准，有相应国家标准的，改为引用国家标准；

b) 删除 ISO 前言。

附录 A～附录 F 为规范性附录。附录 G～附录 J 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(SAC/TC 180)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、中国工商银行、中国农业银行、中国建设银行、交通银行、中国银联股份有限公司、华北计算技术研究所、北京工商大学。

本部分主要起草人：王平娃、陆书春、李曙光、吕毅、杨颖莉、刘运、林中、张启瑞、仲志晖、景芸、周亦鹏、钱湘隆、赵金波、曹文中、李劲松、刘先。

引　言

GB/T 27928 的本部分在金融服务业方面采纳了 GB/T 16264.8 部分，定义了证书管理的过程和数据元。

ISO 15782-2(即将转化我国国家标准)给出了金融业对独立扩展项的详细需求。

虽然本部分所描述的技术是用于保证金融报文的完整性和支持不可否认服务，但本部分不能保证一个特定的执行是安全的。金融机构有责任在全过程的适当位置加入必要的控制以确保这些过程被安全地执行。这些控制包括为了验证符合性而应用适当的审计测试。

证明公钥拥有者的身份和公钥的绑定是为了证实对应私钥的所有权。该绑定称作公钥证书。公钥证书由可信实体——认证机构(CA)生成。

本部分的正确执行应以保证绑定了实体用于文件(包括电汇和合同)签名的密钥和实体身份为前提。

本部分定义了用于鉴别的证书管理框架，包括鉴别加密密钥。

本部分所描述的技术能应用于合法实体(实体)之间发起的业务关系。

金融业务　证书管理
第1部分:公钥证书

1　范围

GB/T 27928的本部分定义了用于法人和自然人的金融业证书管理系统,包括:

——凭证和证书内容;

——证书授权系统,包括用于数字签名和加密密钥管理的证书;

——证书的生成、分发、验证和更新;

——鉴别结构和认证路径;

——撤销和恢复程序;

——公钥证书和证书撤销列表的定义扩展项。

本标准适用于金融行业中公钥证书的管理。

GB/T 27928的本部分也推荐了一些有用的操作程序(例如,分发机制,对所提交凭证的接受标准)。

GB/T 27928的本部分的执行也将基于业务风险和法律要求。

GB/T 27928的本部分不包括以下内容:

——在证书管理过程中各参与方之间使用的协议报文;

——对公证人和时间戳的要求;

——证书策略和认证行为的要求;

——可信第三方的要求;

——属性证书。

虽然本部分规定了证书(可包括用于加密密钥的公钥管理)生成的相关方面,但并未说明加密密钥的生成与传输。

希望遵守GB/T 16264.8的实施者可以采用该标准定义的证书结构。希望实现兼容证书和证书撤销结构而没有X.500系列相关的头字段的实施者可以采用附录A中所定义的ASN.1结构。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16262.1　信息技术　抽象语法记法一(ASN.1)第1部分:基本记法规范(GB/T 16262.1—2006,ISO/IEC 8824-1:2002,IDT)

GB/T 16262.2—2006　信息技术　抽象语法记法一(ASN.1)第2部分:信息客体规范(ISO/IEC 8824-2:2002,IDT)

GB/T 16262.3　信息技术　抽象语法记法一(ASN.1)　第3部分:约束规范(GB/T 16262.3—2006,ISO/IEC 8824-3:2002,IDT)

GB/T 16262.4　信息技术　抽象语法记法一(ASN.1)　第4部分:ASN.1规范的参数化(GB/T 16262.4—2006,ISO/IEC 8824-4:2002,IDT)

GB/T 16263.1　信息技术　ASN.1编码规则　第1部分:基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范(GB/T 16263.1—2006,ISO/IEC 8825-1:2002,IDT)