ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27913—2011

用于金融服务的公钥基础设施 实施和策略框架

**Public key infrastructure for financial services—
Practices and policy framework**

(ISO 21188:2006,MOD)

2011-12-30 发布　　2012-02-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准修改采用 ISO 21188:2006《用于金融服务的公钥基础设施　实施和策略框架》(英文版)。

本标准与 ISO 21188:2006 的技术性差异为:

a) 删除第 4 章中 FIPS 缩略语;

b) 删除缩略语 PKIX,该缩略语在正文中没有出现;

c) 删除 8.3.2 中 FIPS 140-2 的引用;

d) 删除 8.4.3 中 FIPS 140-2 的引用;

e) 删除 8.4.4 中 FIPS 140-2 的引用;

f) 删除 B.7.3 中 FIPS 140-2 的引用;

g) 删除 B.7.9 中 FIPS 140-2 的引用;

h) 删除参考文献中 FIPS 的引用。

对于 ISO 21188 做了下列编辑性修改:

a) “本国际标准”改为“本标准”;

b) 删除国际标准前言。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国银行、中国工商银行、中国银联股份有限公司、中国科学院软件研究所、中国人民银行兴化中心支行。

本标准主要起草人:王平娃、陆书春、李曙光、仲志辉、张凡、贾树辉、赵志兰、景芸、刘运、冉平、王治纲、周燕媚。

引　言

随着金融服务业对互联网技术应用的不断扩大，金融行业对提供安全的、机密的和可信赖的金融交易及处理系统方面的需求不断增长，从而导致了先进安全技术与公钥密码学的结合。公钥密码学需要业务优化的技术、管理和策略基础设施（本文中定义为公钥基础设施或 PKI）来满足金融应用系统中电子标识、鉴别、报文完整性保护和授权的要求。PKI 中电子标识、鉴别和授权标准的应用进一步确保了系统安全的一致性、可预测性和电子交易的可信任性。

数字签名和 PKI 技术可用于开发金融服务业的应用。这些应用的安全和有效性部分依赖于确保基础设施整体完整性的实践。对于将个人身份与其他实体和密钥要素（如密钥）关联起来的基于授权的系统，其用户可以从标准的风险管理系统和本标准定义的可审计业务基础中受益。

国际标准化组织 TC 68 技术委员会的成员已经通过制定数字签名、密钥管理、证书管理和数据加密的技术标准和指南确定了公钥技术。ISO 15782 第 1 和第 2 部分定义了供金融业使用的证书管理系统，但没有包括证书策略和认证业务要求。本标准制定了通过证书策略、认证业务说明、控制目标和控制程序来管理 PKI 的框架，对 ISO 15782 第 1 和第 2 部分进行补充。对这些标准的实现者来说，金融交易中的实体可以依赖 PKI 标准实现的程度以及使用这些国际标准达到的 PKI 间的互操作的程度，都将部分依赖于本标准中定义的与策略和实施相关的因素。

用于金融服务的公钥基础设施 实施和策略框架

1 范围

本标准规定了通过证书策略和认证业务说明对 PKI 进行管理，以及将公钥证书用于金融服务行业的要求框架。同时也定义了风险管理的控制目标和控制程序。

本标准适用于开放、封闭和契约环境中的 PKI 系统进行区分，并且根据金融服务行业信息系统控制目标进一步定义了运行的业务。本标准的目的在于帮助实施者定义支持多证书策略的 PKI 业务，包括数字签名、远程鉴别和数字加密的使用。

本标准使得契约环境中满足金融服务行业要求且基于 PKI 控制的业务的可操作性更易于实现。尽管本标准主要针对契约环境，但并不排除将文档应用于其他环境。文档中术语“证书”是指公钥证书。属性证书不在本标准范围之内。

本标准的目标是针对不同需求的多种使用者，因此每类使用者会关注不同的内容。

业务管理者和分析者是那些需要在开展的业务中使用 PKI 技术的人员，应关注第 1～第 6 章。

技术设计者和实现者是那些编写他们的证书策略和认证业务说明的人员，应关注第 6～第 8 章，以及附录 A～附录 F。

运行管理和审计者是那些负责 PKI 系统日常运行并根据本标准进行一致性检查的人员，应关注第 6～第 8 章。

2 规范性引用文件

下列文件对于本文件的应用是比不可少的。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 13000.1 信息技术 通用多八位编码字符集(UCS) 第一部分：体系结构与基本多文种平面(GB 13000.1—1993，idt，ISO/IEC 10646-1：1993)

GB/T 14916 识别卡 物理特性(GB/T 14916—2006，ISO/IEC 7810：2003，IDT)

GB/T 15120(所有部分) 识别卡 记录技术 (GB/T 15120.1～15120.5—1994，idt，ISO 7811-1～7811-5：1985)

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 16649.1 识别卡 带触点的集成电路卡 第 1 部分：物理特性(GB/T 16649.1—2006，ISO/IEC 7816-1：1998，MOD)

GB/T 16649.2 识别卡 带触点的集成电路卡 第 2 部分：触点的尺寸和位置(GB/T 16649.2—2006，ISO/IEC 7816-2：1999，IDT)

GB/T 16649.3 识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议(GB/T 16649.3—2006，ISO/IEC 7816-3：1997，IDT)

GB/T 16649.5 识别卡 带触点的集成电路卡 第 5 部分：应用标识符的国家编号体系和注册规程(GB/T 16649.5—2002，ISO/IEC 7816-5：1994，NEQ)

GB/T 16649.6 识别卡 带触点的集成电路卡 第 6 部分：行业间数据元(GB/T 16649.6—