ICS 35.240.40
CCS A 11

中华人民共和国国家标准

GB/T 27913—2022
代替 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 21188:2018,MOD）

2022-04-15 发布　　2022-04-15 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 27913—2011《用于金融服务的公钥基础设施　实施和策略框架》，与GB/T 27913—2011 相比，除编辑性改动外，主要技术变化如下：

——删除了“业务持续性考虑遵照 ISO 15782-1：2003 的附录 J”（见 2011 年版的 D.4）；

——修改 “应由授权人执行”为“由授权人员启动的过程来执行”（见 7.4.1，2011 年版 8.4.1）；

——增加了关于“两个或多个 CA 可以加入用于相互识别的公共方案”（见 5.4）；

——增加了关于“CA 的负责管理人员应能够证明信息安全策略得到实施和遵守”和“宜存在并执行考虑业务与技术因素的风险评估的规程，以识别、分析、评价可信服务风险。风险评估的结果应传达给负责信息安全和风险管理的管理组或委员会”部分内容（见 7.2.2）。

本文件修改采用 ISO 21188：2018《用于金融服务的公钥基础设施　实施和策略框架》。

本文件与 ISO 21188：2018 的技术性差异及其原因如下：

——删除了全文中 FIPS（美国联邦信息处理标准）的相关术语和涉及 FIPS 140-2 的引用，选择使用 ISO 19790，以适应我国密码管理的要求。

——增加了第 2 章中对 GB/T 16649.1～GB/T 16649.12、GB/T 16649.15、GB/T 18336.1—2015、GB/T 18336.2—2015、GB/T 18336.3—2015 的引用。

——删除了第 4 章中的 SAN（storage area network，存储区域网络），该词汇在 ISO 21188：2018 中未出现。

——增加了第 4 章中 SAN（主体替换名称）和 EV（扩展型验证），这些词汇在本文件中出现。

——更改了 5.7.1 中提及的“如 5.7.3 及 5.7.6 所示”为“如 5.7.2 及 5.7.6 所示”，ISO 21188：2018 中引用错误。

——删除了附录 D 的 D.3 中出现的“（见 0）”，ISO 21188：2018 中引用错误。

本文件做了下列编辑性修改：

——删除了 5.10 中涉及 DOD（美国国防部）的有关示例。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行、中金金融认证中心有限公司、重庆工商大学、山东财经大学、北京国家金融标准化研究院有限责任公司、中国科学院信息工程研究所。

本文件主要起草人：李伟、胡莹、杨富玉、李达、曲维民、甄杰、董坤祥、冯蕾、谢宗晓、马春旺、赵改侠、王自冲、曹剑锋、李家琪、谢彦丽、薄舜添、贺宇、熊刚、苟高鹏。

本文件及其所代替文件的历次版本发布情况为：

——2011 年首次发布为 GB/T 27913—2011；

——本次为第一次修订。

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（本文件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。

在我国，数字签名和 PKI 技术可用于开发金融服务业的应用。这些应用的安全性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文件定义的可审计业务基础中受益。

本文件制定了通过证书策略、认证业务说明、控制目标和控制规程来管理 PKI 的框架。对这些标准的实现者来说，我国金融交易中的实体可以依赖本文件实现的程度以及使用本文件达到的 PKI 间的互操作的程度，都将依赖于本文件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

本文件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规程。虽然本文件可能用于处理数字签名或密钥建立的公钥证书的生成，但它不会用于处理身份验证方法、不可否认性要求或密钥管理协议。

本文件适用于对开放、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。本文件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、密钥交换和数据加密的使用。

本文件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。尽管本文件主要针对契约环境，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。属性证书不在本文件范围之内。

本文件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（例如，电子商务），见第1章～第6章。

技术设计者和实现者是那些编写证书策略和认证业务说明的人员，见第6章～第7章，以及附录A～附录G。

运行管理和审计者是那些负责PKI系统日常运行并根据本文件进行一致性检查的人员，见第6章～第7章。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 14916—2006 识别卡 物理特性（ISO/IEC 7810:2003，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 16649.2 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 16649.3 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 16649.4 识别卡 集成电路卡 第4部分：用于交换的结构、安全和命令

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 16649.6 识别卡 带触点的集成电路卡 第6部分：行业间数据元

GB/T 16649.7 识别卡 带触点的集成电路卡 第7部分：用于结构化卡查询语言（SCQL）的行业间命令

GB/T 16649.8 识别卡 带触点的集成电路卡 第8部分：与安全相关的行业间命令

GB/T 16649.9 识别卡 集成电路卡 第9部分：用于卡管理的命令