



# 中华人民共和国国家标准

GB/T 27911—2011

GB/T 27911—2011

## 银行业 安全和其他金融服务 金融系统的安全框架

Banking—Security and other financial services—  
Framework for security in financial systems

(ISO/TR 17944:2002, MOD)

中华人民共和国  
国家标准  
银行业 安全和其他金融服务  
金融系统的安全框架  
GB/T 27911—2011

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100013)  
北京市西城区三里河北街16号(100045)  
网址 www.spc.net.cn  
总编室:(010)64275323 发行中心:(010)51780235  
读者服务部:(010)68523946  
中国标准出版社秦皇岛印刷厂印刷  
各地新华书店经销

\*

开本 880×1230 1/16 印张 1.25 字数 26 千字  
2012年2月第一版 2012年2月第一次印刷

\*

书号: 155066·1-44211 定价 21.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68510107



GB/T 27911—2011

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

## 参 考 文 献

[1] ISO/IEC TR 13335 (所有部分) 信息技术 信息技术安全管理指南 (Information technology—Guidelines for the management of IT Security)

---

## 目 次

前言 .....	III
1 范围 .....	1
2 标准化的领域 .....	1
2.1 概述 .....	1
2.2 身份识别和鉴别 .....	1
2.3 数据完整性 .....	3
2.4 隐私和机密性 .....	4
2.5 抗抵赖 .....	4
2.6 服务的可用性 .....	5
2.7 可追溯性和审计 .....	6
2.8 互用性 .....	7
2.9 安全管理 .....	7
2.10 加密算法 .....	9
3 ISO 空白的标准化领域 .....	10
附录 A (资料性附录) 补充信息 .....	11
参考文献 .....	12

表 9 (续)

需 求	可用的标准	标题/描述
对称	ISO 8372	信息处理 64 位块加密算法操作的模式
	ISO/IEC 10116	信息技术 安全技术 n 位分组加密操作的模式
	ISO/TR 19038:2005	银行和相关金融服务 3-DEA 操作模式 实施指南
	ANSI X9.52-1998	三重数据加密算法(T-DEA)的操作模式
	ANSI X9 TG-19	三重数据加密算法(T-DEA)的操作确认模式
	FIPS PUB 197	高级加密标准
非对称	ANSI X9.30-1	金融服务行业的公钥加密技术:第 1 部分数字签名算法
	ANSI X9.31	使用可逆公钥加密技术的数字签名
	ANSI X9.76	阈值的数字签名局部密钥更新机制
椭圆曲线	ISO/IEC 15946	信息技术 安全技术 基于椭圆曲线的加密技术 ——第 1 部分:概述 ——第 2 部分:数字签名 ——第 3 部分:密钥建立 ——第 4 部分:带报文恢复的数字签名*
	ANSI X9 TG-17	椭圆曲线算法的技术准则
	ANSI X9.62-1998	金融服务行业的公钥加密技术:椭圆曲线数字签名算法 (ECDSA)
	ANSI X9.63	金融服务行业的公钥加密技术:使用椭圆曲线加密的密钥协议和密钥传输

3 ISO 空白的标准化领域

表 10 总结了第 2 章各个表中对应“需求”列的“可用标准”是空白的或无可用 ISO 标准的一些项目。

表 10 不可用总结

需 求	可用的标准	附加备注
口令短语	无标准	
证书	无可用的 ISO 标准	ANSI X9.79 标准可用(ISO NWI 提议)
公钥基础设施(PKI)	无可用的 ISO 标准	ANSI X9.79 标准可用(ISO NWI 提议)
备份	无标准	
互用性	无可用的 ISO 标准	
非对称的加密算法	无可用的 ISO 标准	ANSI X9 标准可用
隐私和机密性	无可用的 ISO 标准	
商业实体身份标识符	无可用的 ISO 标准	
令牌	无可用的 ISO 标准	EBS 111 可用

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用重新起草法修改采用 ISO/TR 17944:2002《银行业 安全和其他金融服务 金融系统的安全框架》。

考虑到我国国情,并考虑了 2002 年以来国际上发布了一些新的与金融相关的信息安全类标准,在采用 ISO/TR 17944:2002 时做了以下修改:

- 2.2 条的表 1 中,在“生物特征识别技术”中加入了近年来新发布的一些国际标准;
- 2.3 条的表 2 中,在“报文鉴别”中加入了 ISO/IEC 19772:2009;
- 2.6 条的表 5 中,在“灾难恢复”中加入了 ISO/IEC 24762:2008;
- 2.7 条的表 6 中,在“评估标准”中加入了 ISO/IEC 18045:2008、ISO/IEC TR 19791:2006、ISO/IEC 21827:2008;
- 2.9 条的表 8 中,在“证书管理”中加入 ISO 21188;
- 2.9 条的表 8 中,在“安全管理”中加入 ISO/IEC TR 18044、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 18043:2006、ISO/IEC 27000:2009、ISO/IEC 27005:2008、ISO/IEC 27006:2007、ISO/IEC 27011:2008;
- 2.10 条的表 9 中,在“一般的”中加入了 ISO/IEC 18031:2005、ISO/IEC 18032:2005、ISO/IEC 18033-1:2005、ISO/IEC 18033-2:2006、ISO/IEC 18033-3:2005、ISO/IEC 18033-4:2005、ISO/IEC 19790:2006;
- 2.10 条的表 9 中,在“对称的”中加入了 ISO 19038;
- 第 3 章表 10 中删除生物识别、灾难恢复两行,因为在正文中加入了这两个领域的 ISO 标准,另外加入三行:“隐私和机密性”、“商业实体身份标识符”、“令牌”;
- 各表格中,被引用的有年代号的标准,如有更新版本,用最新年代号标准替换;
- 各表格中,删除已废止的国际标准。

为便于使用,本标准还做了下列编辑性修改:

- 删除 ISO 前言和引言;
- 对于已经发布的标准,删除原文中的表注“即将发布”。

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、中国工商银行、中国建设银行、交通银行、中信银行、北京银联金卡科技有限公司。

本标准主要起草人:王平娃、陆书春、李曙光、杨倩、田洁、刘运、赵志兰、邵冠军、李延、杨宝辉、贾静、李孟琰、刘志刚、仲志晖、贾树辉、景芸、张艳、马小琼。