ICS 03.060
A 11

# 中华人民共和国国家标准

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)

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。

# 银行业　安全和其他金融服务
# 金融系统的安全框架

## 1　范围

本标准提供了金融业所必要的安全方面的标准框架。

本标准汇总了金融行业已出现的一些关键安全问题，以及针对每一个问题的相关现有标准。

本标准适用于金融机构在实施安全策略时的标准参考。

## 2　标准化的领域

### 2.1　概述

金融行业中，信息技术安全的需求体现在令牌、设备、加密技术、密钥管理、应用程序接口（API）和协议等标准应用领域，这些不同领域可根据下面这些基础领域的基本业务需求进行分组。

多数领域已经有了各种各样可用的标准，而在其他领域，标准或正在制定或有了（新）标准需求。第2章中提及了金融机构信息安全标准化的主要领域，其中表1到表9包含了这些领域可用的（有时是必需的）的标准。表中排在前面的国际标准来自国际标准化组织，跟随在其后的有关标准来自其他标准组织[1)]。基于这些表中缺少的标准，第3章概述了ISO空白的标准化领域。

**注**：对于所提及标准的更加详细资料，可以联系参考的标准化组织（参见附录A）。

### 2.2　身份识别和鉴别

金融交易中涉及的所有实体的身份应被确定。鉴别确保一个实体的身份就是它声明的身份。金融机构应保证：只有授权的用户可以访问他们的信息技术系统。

用于身份识别和鉴别的机制建立在使用身份标识、令牌、口令短语、个人身份识别码（PIN）、生物识别技术、数字签名和证书基础之上，相关标准见表1。

**表1　身份识别和鉴别**

| 需　求 | 可用的标准 | 标题/描述 |
|---|---|---|
| 身份识别和鉴别 | ISO/IEC 9798-1 | 信息技术　安全技术　实体鉴别　第1部分：概述 |
| | ISO/IEC 9798-2 | 信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制 |
| | ISO/IEC 9798-3 | 信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制 |
| | ISO/IEC 9798-4 | 信息技术　安全技术　实体鉴别　第4部分：采用密码校验函数的机制 |
| | ISO/IEC 9798-5 | 信息技术　安全技术　实体鉴别　第5部分：使用零知识技术的机制 |
| | ISO/IEC 9594-8 | 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 |

1）　本标准中非ISO标准的引用仅用于资料目的；它们应是一个共识并且应该是被发表的或公认可用的。非ISO标准的引用并不表明ISO对这些非ISO标准的认可。