ICS 03.360;35.240.40
A 11

中华人民共和国国家标准

GB/T 27912—2011

金融服务　生物特征识别 安全框架

Financial services—Biometrics—Security framework

(ISO 19092-1:2006,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 19092-1:2006《金融服务　生物特征识别　第 1 部分:安全框架》(英文版)。

本标准与 ISO 19092-1:2006 的技术性差异如下:

a) 删除全文中涉及 ISO 19092-2 的内容(因 ISO 19092-2 提案已被 ISO 中止,且删除这些内容并不影响标准的完整性);

b) 删除原标准中的 10.1.2,因为本节中的密钥名称全部来自于已经终止的 ISO 19092-2;

c) 10.1.2(原标准 10.1.3)数字签名中"哈希算法应满足相关 ISO 标准(或者等同的国家标准)的具体要求"改为"哈希算法应满足相关国家标准的具体要求";

d) 删除 10.1.2(原标准 10.1.3)数字签名中的列项"应通过明文文本数据进行哈希运算,文本由一个或多个 BiometricHeader 和 BiometricData 类型的值组成,除了类型 BiometricHeader 和 BiometricData 值之外,还应包括一个 IntegrityBlock 类型的值";

e) 10.1.2 和 10.1.3(原标准 10.1.3 和 10.1.4)中的"密钥管理技术,如表 1 所示,应按照相关 ISO、ISO/IEC 标准(或者等同的国家标准)的具体规定执行,例如 ISO 11568,或者 ISO/IEC 11770"改为"密钥管理技术应按相关国家标准的具体规定执行";

f) 删除原标准中的表 1(其后表格的编号都减去 1);

g) 10.1.3 基于数据机密性目的的加密中"加密算法应按相关的 ISO 标准(或者等同国家标准)的具体规定执行"改为"加密算法应按相关的国家标准的具体规定执行";

h) 11.3.1 中表 12(原标准中表 13)的 147 项:"密钥产生使用密钥产生算法,具体如 ISO 标准(或者等同的国家标准)"修改为"密钥产生使用密钥产生算法,具体见相关的国家标准";

i) 附录 A.3.4 的列项 d)中的"参考模板描述(例如,生物特征 OID)"修改为"参考模板描述(例如,生物特征目标标识符)";

j) 删除 ISO 19092-1:2006 的附录 B.2,因为该处描述的个体身份识别标准不适合我国国情。

本标准还做了下列编辑性修改:

——将原文中的"本国际标准"、"ISO 19092"、"ISO 19092 的本部分"、"本部分"修改为"本标准";

——删除国际标准的前言;

——为全文统一起见,将 4.21 等错误率的定义中的"交叉率(crossover rate)"改称"交叉错误率(crossover error rate)";

——9.3.3 的列项 a)中提到的再登记的要求:"使用原始的凭证材料,而并非已经存在的生物特征模板。该方式可提供足够的保证水平,这依赖于已存在的生物特征模板和技术的可靠性和可用性"修改为"使用原始的凭证材料,而并非已经存在的生物特征模板。该方式可提供足够的保证水平,这依赖于原始的凭证材料的可靠性和可用性"(勘误);

——11.4.5 的表 22 集成电路卡(ICC)生命周期控制中的 300 项"除非 CDF 处于激活状态或者再激活状态时,否则 IC 不能用于金融交易"修改为"除非 CDF 处于激活状态或者再激活状态时,否则 ICC 不能用于金融交易"(勘误);

——C.8 中的"对单因子生物特征识别系统使用简单概率模型[20],在 N 个用户中不出现系统错误匹配的概率 Pr 为"修改为"对单因子生物特征识别系统使用简单概率模型[20],在 N 个用户中出现系统错误匹配的概率 Pr 为"(勘误)。

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:中国农业银行、中信银行、上海银晨智能识别科技有限公司、北京中科虹霸科技有限公司、北京握奇数据系统有限公司、杭州中正生物认证技术有限公司、中国人民银行兴化市中心支行、中国人民银行太原市中心支行、中国人民银行石家庄市中心支行。

本标准主要起草人:王平娃、陆书春、李曙光、刘运、赵征、林松、曾文斌、邱显超、余伟华、汪雪林、梁敏、吕瑛、仲志辉、张龙龙、李军。

引　言

随着计算机技术的引入，商业模式已经发生重大变化。电子交易替代从前的纸质交易，降低了成本，提高了效率。这些交易处于一个开放的网络环境中，存在数据被破坏的风险，金融业需求采取相应的措施应对这些风险。

生物特征识别，即“你是谁或者能做什么”的识别方式，已经出现若干年，包括如指纹识别、声音识别、眼睛扫描、脸像识别等。生物特征识别技术在可靠性不断提高的同时，成本逐步降低，使其在金融业的实施成为可能。

本标准描述了使用生物特征识别技术作为鉴别机制，保护金融业的远程电子访问或本地物理访问的机制和过程。

生物特征识别技术可用作物理或逻辑访问的人员身份鉴别。逻辑访问可包括对应用、服务或者授权的访问。本标准可促进生物特征识别在金融业内的应用，并促进生物特征识别信息的管理成为商业机构信息安全管理的组成部分。本标准通过使用生物特征识别技术，提供强度更高的鉴别方式和多因子鉴别机制，为公钥基础设施(PKI)提供更强的鉴别机制。另外，本标准允许重复确认产生数字签名的人实际上就是有权限访问私钥的人。

生物特征识别系统的广泛应用建立在一系列因素之上，已有的生物特征识别技术在这些因素上表现各异，这些因素包括：

——便利性和易用性；

——外在的安全水平；

——性能；

——非侵犯性。

本标准所讨论的鉴别机制限于封闭性用户群体，群体成员已同意使用生物特征识别技术进行身份识别。这些协议可为显性的形式(如服务协议)，或者隐性的形式(如访问某设施即表明具有执行某交易的动机)。监管不确定人员的系统不在本标准讨论的范围之内。

本标准阐述的技术用于维护生物特征信息的完整性和机密性，及提供鉴别机制。然而，本标准并不确保某项具体实现足够安全。金融机构有责任设置适当的全业务流程并进行必要的控制，以确保业务流程安全运行。此外，为验证与本标准的一致性，控制措施应包括适当的审计测试。

金融服务　生物特征识别
安全框架

1　范围

本标准规定了金融业使用生物特征识别机制鉴别人员身份的安全框架，介绍了生物特征识别技术的类型，阐述了有关应用问题。本标准也描述了实现架构，详细规定了有效管理的最小安全要求，也为专业人员提供了控制目标和使用建议。

本标准包括：

——使用生物特征识别技术，通过验证其声称的身份或识别其个体身份，对参与金融服务的人员和雇员身份进行鉴别；

——根据风险管理的要求，对用户登记时提交的凭证进行确认，以支持身份鉴别；

——在整个生命周期内，包括登记、传输、存储、身份确认、身份识别以及终止等过程，对生物特征信息进行管理；

——生物特征识别信息在其生命周期内的安全性，包括数据完整性、源鉴别和机密性；

——生物特征识别机制在逻辑和物理访问控制中的应用；

——保护金融机构及其客户的监控措施；

——在整个生物特征识别信息生命周期中所使用的物理硬件的安全性。

本标准不包括：

——个体生物特征识别信息的隐私权和所有权；

——有关数据采集、信号处理与生物特征数据匹配、以及生物特征匹配决策流程等方面的具体技术；

——生物特征识别技术在非鉴别方面的便利性应用，如语音识别、用户交互和匿名访问控制等方面的使用。

本标准适用于由于数据机密性或其他原因而对生物特征信息进行加密的强制方式。

尽管本标准并未阐述采用生物特征识别技术对业务应用系统的具体要求和限制，但其他标准可讨论这些问题。

2　符合性

如果生物特征鉴别系统的具体实现满足本标准的管理和安全要求，那么可声称其符合本标准。

采用了本标准建议的密码报文要求，且采取了适当策略、措施和操作过程的生物特征鉴别系统，就可声称其符合本标准。

通过满足本标准的第 9 章和第 10 章中的管理和安全要求，就可以满足生物特征鉴别系统很多方面的符合性要求，并且能够验证其实现方法、相关策略、操作过程是否达到第 11 章中的确认控制目标。相关机构能够使用附录 A 中规定的生物特征事件日志来记录与本标准操作方面要求的符合性。

3　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