



中华人民共和国国家标准

GB/T 27912—2026

代替 GB/T 27912—2011

金融服务 生物特征识别 安全框架

Financial services—Biometrics—Security framework

(ISO 19092:2023, MOD)

2026-09-28 发布

2027-04-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 2

4 缩略语 7

5 金融服务背景下的生物特征识别技术 8

 5.1 概述 8

 5.2 通用的安全注意事项 9

 5.3 个人设备漏洞及控制策略 9

 5.4 生物特征验证与生物特征辨识 9

6 生物特征模态和核心系统 10

 6.1 概述 10

 6.2 生物特征模态 10

 6.3 生物特征识别系统及其配套系统 12

7 金融生物特征认证系统——可用性考量 18

 7.1 概述 18

 7.2 生物特征模态的特性 18

 7.3 生物特征识别系统的性能与评估 18

8 金融生物特征认证系统——架构 20

 8.1 概述 20

 8.2 概念性业务架构 21

 8.3 技术架构 21

 8.4 注册架构 22

 8.5 PBP 设备和相关的生物特征认证架构 22

9 金融生物特征认证系统——威胁和漏洞 28

 9.1 通用威胁考量 28

 9.2 生物特征呈现漏洞 29

 9.3 比对、决策和存储子系统漏洞 30

10 金融生物特征认证系统——安全要求 31

 10.1 通则 31

 10.2 通用的安全要求 31

 10.3 身份注册 32

 10.4 呈现 33

 10.5 数据的存储和处理 33

10.6 比对与决策 34

10.7 登记 34

10.8 再登记 35

10.9 细化 35

10.10 验证 35

10.11 辨识 36

10.12 终止 36

10.13 中止和重新激活 37

10.14 存档 37

10.15 安全符合性验证 37

附录 A（资料性） 生物特征识别应用场景 39

 A.1 概述 39

 A.2 卡片 PBP 39

 A.3 互联网的卡片 PBP 40

 A.4 移动支付设备 41

 A.5 移动支付终端 43

附录 B（资料性） 生物特征识别环境的威胁和漏洞 45

 B.1 卡的漏洞和缓解措施 45

 B.2 移动设备的漏洞和缓解措施 45

附录 C（规范性） 生物特征识别安全控制清单 47

 C.1 概述 47

 C.2 通用安全控制 47

 C.3 生物特征基准数据生命周期控制 48

附录 D（资料性） 技术差异及其原因一览表 51

参考文献 53

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 27912—2011《金融服务 生物特征识别 安全框架》，与 GB/T 27912—2011 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加、更改和删除了部分术语(见第 3 章,2011 年版的第 4 章)；
- b) 增加和删除了部分缩略语(见第 4 章,2011 年版的第 5 章)；
- c) 增加了金融服务背景下的生物特征识别技术(见第 5 章)；
- d) 更改了生物特征模态和核心系统(见第 6 章,2011 年版的第 6 章、第 8 章)；
- e) 增加了金融生物特征认证系统的可用性考量、架构、威胁和漏洞、安全要求(见第 7～10 章)；
- f) 增加了生物特征识别安全控制清单(见附录 C)；
- g) 删除了技术方面的考虑(见 2011 年版的第 7 章)；
- h) 删除了管理和安全要求(见 2011 年版的第 9 章)；
- i) 删除了安全基础设施(见 2011 年版的第 10 章)；
- j) 删除了生物特征身份确认的控制目标(见 2011 年版的第 11 章)；
- k) 删除了生物特征登记(见 2011 年版的附录 B)；
- l) 删除了安全考虑(见 2011 年版的附录 C)；
- m) 删除了生物特征识别设备的安全要求(见 2011 年版的附录 D)；
- n) 删除了现有的应用(见 2011 年版的附录 E)。

本文件修改采用 ISO 19092:2023《金融服务 生物特征识别 安全框架》。

本文件与 ISO 19092:2023 相比，存在较多技术差异，在所涉及的条款的外侧页边空白位置用垂直单线(|)进行了标识。这些技术差异及其原因一览表见附录 D。

本文件做了下列编辑性改动：

- 在 3.14 生物特征样本的定义下增加示例：包含指纹图像的记录是生物特征样本；
- 增加部分缩略语；
- 10.6.2 a) 后增加示例；
- 调整附录 A、附录 B 的顺序，与正文中的引用顺序保持一致；
- 附录 C 表 C.2 中，删除第一个编号 29 条款以及该行之上的 Control criteria 行。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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：北京国家金融标准化研究院有限责任公司、中国人民银行福建省分行、中国人民银行湖北省分行、中国人民银行甘肃省分行、紫光数字影像科技(广东)有限公司、中国银联股份有限公司、中国人民银行武威市分行、北京银联金卡科技有限公司、中国工商银行股份有限公司、中国人民银行三明市分行、中国人民银行龙岩市分行、中国人民银行吉林省分行、中国人民银行吉林市分行、中国人民银行张掖市分行、中国人民银行白银市分行、中国人民银行云南省分行、中国农业银行股份有限公司、交通银行股份有限公司、招商银行股份有限公司、中信银行股份有限公司、中金金融认证中心有限公司、北京数字认证股份有限公司、北京中科虹霸科技有限公司、金电信息科技(北京)有限责任公司、甘肃银行股份有限公司、杭州银行股份有限公司、徽商银行股份有限公司、广东南粤银行股份有限公司、武汉农村商业银行股份有限公司、重庆农村商业银行股份有限公司、广州银行电子结算中心、蚂蚁科技集团股

份有限公司、浙江中正智能科技有限公司、中关村智联软件服务业质量创新联盟。

本文件主要起草人：韩竺吾、刘运、林羽、刘晓、段国建、乔梁、汤洋、彭秋蕾、李沐阳、周刚、李远、赵海、李恩达、邵淼、饶宇熹、邱显超、彭晓圆、李伟强、周庆斌、丁一、马小琼、邓琳莹、韩博、李瓚、陈欢、王益萱、唐云霞、袁凡、钱菲、顾幸男、张腾腾、张洪鹏、许晓亮、李川、华夏、周亮、李喆、方彧、胡元瑞、王娟娟、陆碧波、梁敏、黄群。

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 27912—2011；

——本次为第一次修订。

引 言

零售电子交易的安全认证历来以基于卡及 PIN 的技术为核心保障机制。然而,随着新技术的涌现和传统技术的发展,采用个人生物特征识别技术作为交易认证的替代或补充方法已成为可能。

生物特征识别是一种识别个体身份的机制,包括使用指纹、虹膜和面部图像等识别方式。

生物特征识别系统在公众中的广泛应用取决于多重因素:

- 便利性和易用性;
- 适当的安全水平;
- 性能;
- 非入侵性。

本文件为金融业零售支付领域生物特征识别技术的整合应用提供安全指南,涵盖从组件到系统层面的基于卡或其他技术的实施方案,同时包含兼容性验证的相关建议。需要说明的是,本文件中的指南并不能保证某一特定的实施方案能够抵御所有威胁。部署此类技术的金融机构有责任根据机构自身安全风险管理体系,采取适当的控制措施以有效应对相关威胁。

金融服务 生物特征识别 安全框架

1 范围

本文件规定了在金融服务(主要针对零售支付场景)中使用生物特征识别技术对客户进行身份认证的安全框架,并介绍了最常见的生物特征识别技术类型和相关应用问题。本文件还描述了实现生物特征认证的典型架构和相关的控制目标。

本文件的适用范围包括:

- 基于以下目的的生物特征识别技术应用:
 - 对声称身份的验证;
 - 个体身份辨识;
 - 生物特征认证威胁、漏洞和控制措施;
 - 支持身份认证的登记凭证验证;
 - 生物特征信息的全生命周期管理,包括登记、传输和存储、验证、识别和销毁过程;
 - 与生物特征采集和生物特征数据处理配套使用的硬件安全要求;
 - 生物特征认证架构和相关安全要求。
- 本文件的适用范围不包括:
- 生物特征数据采集、特征提取与比对、识别决策流程的详细技术规范;
 - 生物特征识别技术在非金融交易场景中的应用,例如物理或逻辑的系统访问控制。

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 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

ISO 11568 金融服务 密钥管理(零售)[Financial services—Key management(etail)]

- 注: GB/T 27909.1—2011 银行业务 密钥管理(零售) 第1部分:一般原则(ISO 11568-1:2005,MOD)
- GB/T 27909.2—2011 银行业务 密钥管理(零售) 第2部分:对称密码及其密钥管理和生命周期(ISO 11568-2:2005,MOD)
- GB/T 27909.3—2011 银行业务 密钥管理(零售) 第3部分:非对称密码系统及其密钥管理和生命周期(ISO 11568-4:2007,MOD)
- GB/T 21082.4—2007 银行业务 密钥管理(零售) 第4部分:使用公开密钥密码的密钥管理技术(ISO 11568-4:1998,MOD)

ISO 13491-1 金融服务 安全加密设备(零售) 第1部分:概念和要求[Financial services—Secure cryptographic devices(etail)—Part 1:Concepts and requirements]

注: GB/T 21079.1—2022 金融服务 安全加密设备(零售) 第1部分:概念、要求和评估方法(ISO 13491-1:2016,MOD)

ISO 13491-2 金融服务 安全加密设备(零售) 第2部分:金融交易中设备安全符合性检测清单[Financial services—Secure cryptographic devices(etail)—Part 2: Security compliance checklists for devices used in financial transactions]