ICS 35.240.40
CCS A 11

团　体　标　准

T/BFIA 015—2022

金融科技智能服务终端(FIST)技术要求

Technical requirements for Fintech intelligent service terminal

2022－08－16 发布　　2022－08－16 实施

北京金融科技产业联盟　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。

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。

本文件由北京金融科技产业联盟归口。

本文件起草单位：北京中新动能技术服务有限公司、北京金融科技产业联盟、北京国家金融科技认证中心有限公司、重庆国家金融科技认证中心有限责任公司、中国银联股份有限公司、北京银联金卡科技有限公司、北京立言金融与发展研究院、中国邮政储蓄银行股份有限公司、平安银行股份有限公司、拉卡拉支付股份有限公司、科大国盾量子技术股份有限公司、杭州趣链科技有限公司、赞同科技股份有限公司、西太深海量子科技（重庆）有限公司。

本文件主要起草人：张景超、蔡志军、聂丽琴、李振、冯晓文、王建新、秦逞、孙权、李定洲、陈成钱、杨波、彭乾、佟冬、李晶、朱韬武、王国栋、曾德炎、周雷、白冰、杜静漪、余雄伟、陈庆功、姜晖、冯帆。

金融科技智能服务终端（FIST）技术要求

1 范围

本文件规定了具有金融数字化资产查询、交易、支付等应用功能的金融科技智能终端（智能 POS、ATM、智能支付终端、智能自助终端）的硬件、软件、技术应用和安全要求。

本文件适用于金融科技智能服务终端的设计、生产及应用。

注：本文件称数字化资产为法定电子货币、法定数字货币、有价电子票证及其他以电子数据形式存在或表示的合法资产等。

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。

JR/T 0001—2016 银行卡销售点（POS）终端技术规范

JR/T 0089—2012（所有部分） 中国金融移动支付 安全单元

JR/T 0091—2012 中国金融移动支付 受理终端技术要求

JR/T 0120—2016（所有部分） 银行卡受理终端安全规范

JR/T 0122—2018 非银行支付机构业务设施技术要求

JR/T 0156—2017 移动终端支付可信环境技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能服务 intelligent service

通过创新技术提供满足金融综合智能化的服务。

注：服务包括货币存储、兑换、查询、支付等。

3.2

金融科技智能服务终端 fintech intelligent service terminal

通过智能化手段为用户提供多种支付功能，支持用户身份信息核验、终端健康状态监测等功能的终端设备。

注：智能化手段包括大数据、云计算、人工智能、分布式账本、TEE、量子等创新技术，支付功能包括银行卡、二维码等；金融服务需求场所包括商户个人或金融服务机构营业网点、商业服务网点等。

3.3

网络支付 network payment

依托公共网络或专用网络，在收付款人之间转移货币资金的行为。比如，扫码支付、APP/小程序支

付、网页支付等等。

4 缩略语

下列缩略语适用于本文件

4G：第四代的移动信息系统（the 4th generation mobile communication technology）

5G：第五代的移动信息系统（the 5th generation mobile communication technology）

CPU：中央处理器（Central Processing Unit / Processor）

GPS：全球定位系统（Global Positioning System）

HD:层次确定性（Hierarchical Deterministic）

HSM：硬件安全模块（hardware security module）

IPv6:互联网协议第6版（Internet Protocol Version 6）

NFC:近场通信（Near Field Communication）

RFID：射频识别（Radio Frequency Identification）

RJ45：已注册的插孔（Registered Jack）

USB：通用串行总线（Universalserial Bus）

5 终端结构

5.1 概述

金融科技智能服务终端技术架构包括操作系统、硬件、金融可信执行环境条件等，见图1。

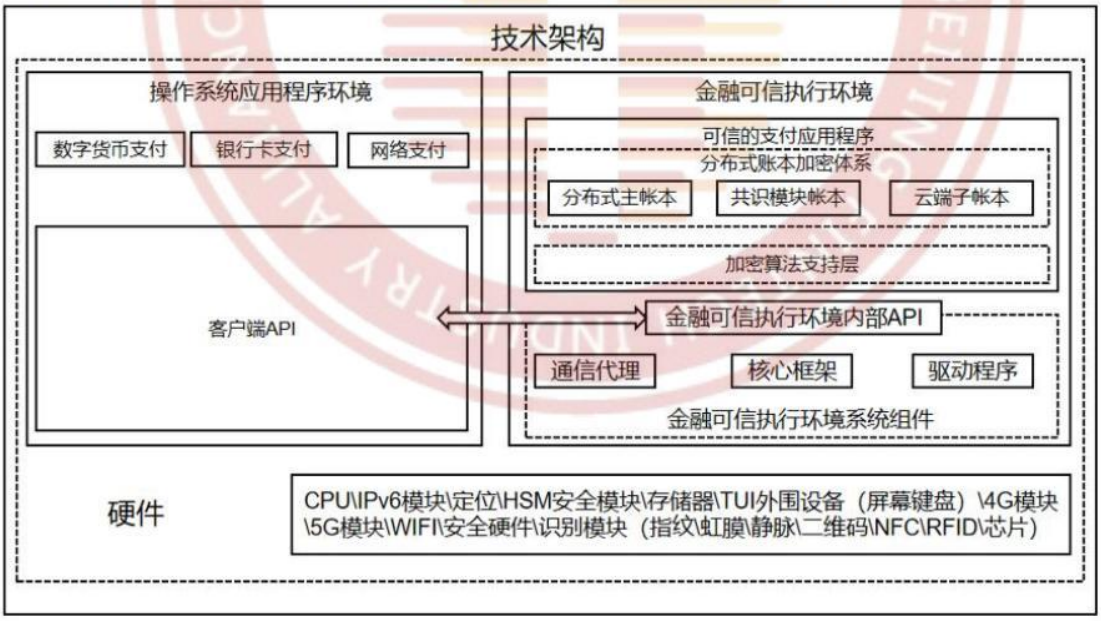

图1 终端结构

5.2 操作系统应用程序环境

支持金融行业支付、有价电子券、数字货币、票据、数字资产等应用，在富运行环境中为用户提供服务。

5.3 金融可信执行环境

金融科技智能服务终端宜提供可信应用要求的执行环境，通过专门授权，在可靠的访问控制下提供金融应用身份校验、交易授权、交易确认等需要安全保障的功能，应符合 JR/T 0156—2017 的技术要求。

对于符合高安全等级的设备，有完整的签名体系及周期自检的方式来保证合法的应用均在可信应用的范围内。

5.4 应用场景

金融科技智能服务终端所应用的场景包括金融服务网点、商业服务网点、移动端。

5.5 硬件

提供金融应用安全屏显、人脸指纹识别仪、NFC读卡器、扫描枪及其他USB外设等。

6 硬件要求

6.1 硬件设计原则

硬件设计应遵循以下原则：

——硬件系统和各模块单元的逻辑设计应尽量采用统一校验技术，并留有适当的逻辑余量；

——产品的零部件应紧固无松动；

——外形应具备人性化特点，客户操作应感到舒适方便，并应具备人文特征；

——硬件端口应具备软件激活及关闭功能。

6.2 抗破坏机制

终端遇到非操作员、非管理员非法开启或遇到暴力攻击等非正常使用时，应具备报警功能并有记录。

终端应具备软硬件电路防护机制（如防拆开关、斑马条、mesh 电路等），防止被加装非法电路或改造。

6.3 防移除机制

终端的识读等安全设备应防止恶意拆除。

6.4 防恶意窃取账户机制

终端应具备安全机制，防止有目的地保留或偷取使用人账户数据、PIN码等相关信息（比如循环攻击）。

6.5 防渗透替换机制

不允许通过条件改变、替换或修改识读设备、终端的硬件软件，达到替换或者修改磁道数据的目的。

7 软件安全要求

7.1 软件设计原则

软件设计应遵循以下原则：

——终端的软件设计应与硬件系统的硬件资源相适应；

——除应用软件外，还应配备完善的测试（诊断）软件；

——系统应具有一定的自检功能；

——对同一系列的产品，软件应遵循通用化、系列化、模块化和向下兼容的原则；
——应用软件运行和数据传输中需保密的数据，均应经过安全加密处理；
——软件的文件技术规范以及字符集中字符的编码、字型等都应符合相应的国家标准；
——可拓展性软件设计完要留有升级接口和空间，便于后续升级拓展。

7.2 系统软件

应具有系统初始化，对软件、硬件的自检及报警功能，具备断电保护功能，具有应用程序的加载和参数设定的功能。

7.3 模块化结构

支持模块化结构设计，软件应封装成几个相对独立、性能稳定的模块，供应用开发者使用。

7.4 终端监测

终端系统应支持在终端使用时进行自身健康状态监测（包括但不限于终端启动加载正常状况、终端Root 状态、CPU 及内存使用情况、网络状态等），如发现终端状态监测异常则应及时进行安全预警或阻止终端对金融 TEE 中可信应用的访问，以确保终端使用环境安全；根据终端平台的安全要求可进行运行期间定期或不定期自检。

7.5 身份验证

终端系统应实现用户身份识别验证（如支付密码、生物识别、动态令牌等）功能，并根据终端配置安全要求设置身份验证强度。

7.6 加密存储

应实现信息加密存储功能，应对存储信息真实性、完整性进行校验，阻止非授权的访问、修改等操作。

7.7 密码处理

终端应在可信环境内实现相应的密码处理操作，包括设定、修改等。

7.8 智能应用安全防护

终端应实现权限管理，对相应的应用操作及系统进行安全防护，确保应用安全。

7.9 SE 应用安全管理

应符合 JR/T 0089—2012 的技术要求。

8 金融应用支撑要求

8.1 支付应用

8.1.1 支付场景

作为线下服务终端，通过在场景中进行以终端为载体的支付交易活动，在满足交易需求和行为的基础条件下，应满足：

——支付密码、生物识别、动态令牌等身份鉴别在可信执行环境中处理；

——支付授权校验涉及的密钥或密码运算应在 SE 内存储和处理；
——为金融应用客户提供支付密码安全存储的功能，为金融应用提供安全匹配的访问控制措施；
——应用间相互调用时，提供平台级应用身份验证和应用完整性校验。

8.1.2 支付方式

终端平台应能提供 NFC、QR-code、USB-POS 等支付受理设备直接连接可信环境的功能，或者实现支付受理设备和可信环境端到端加密的功能。负责对接各类支付受理设备的支付模块应满足现有相应支付受理规范，如银行卡支付模块应满足 JR/T 0001—2016、JR/T 0120—2016、JR/T 0122—2014、JR/T 0091—2012 等相关规范。

8.1.3 身份鉴别方式

应支持 PIN 码输入、生物识别（人脸、指纹、静脉、虹膜等识别方式）、动态令牌等多种鉴别方式的数据采集，应在平台启动过程前对数据采集外设进行自检，应提供采集数据的加密传输机制。

从终端平台采集设备获取的身份鉴别信息，应直接传递到可信运行环境中，不应以明文形式在可信运行环境中处理、传输或存储身份鉴别信息。

8.2 金融分布式账本应用功能

平台实现金融分布式账本技术应用情况下，应提供账户管理(开户、销户等)、数字资产查询、数字资产交易、数字货币交易、兑换等功能的可信应用支持。

8.3 开票功能

平台实现金融电子单据服务应用情况下，应提供账单打印、电子发票申请、电子凭证、电子保单下载的可信应用支持。

8.4 监管支持功能

应提供相关交易信息监管采集接口，应支持采集定位信息记录、交易统计信息、交易视频截图、终端固件、软件更新记录等监管需要的信息接口。

8.5 可信应用管理功能

应提供对设备资源的特权访问，为授权的应用程序提供安全存储和运行环境，防止敏感应用及数据受到来自开放操作系统端恶意软件的攻击，保护应用及数据的保密性、完整性。

应支持可信应用管理功能，对终端的安全应用及硬件安全芯片中的应用进行动态部署及远程管理。

8.6 密码要求

8.6.1 密钥管理

应基于层次确定性 HD（hierarchical deterministic）密钥生成机制建立金融应用密钥体系，对于支持金融监管或审计目的的密钥，其路径或节点层次应高于金融应用密钥。

应基于 SE 提供金融密码的存储和使用服务，支持密钥全生命周期管理的要求。

8.6.2 密码服务

应基于 SE 提供金融应用密码算法服务，应提供包括 SM 系列国产密码算法在内密码运算功能。提供帐号密码保管、应用密码管理（生成、存储、使用、销毁）功能。

8.7 定位功能

应支持北斗定位与 GPS 定位系统所提供的物理位置定位，平台可信环境应提供地理位置信息校验和签名机制，终端设备应具有独立的 IPv6 地址。

8.8 通讯功能

应能够支持 4G/5G 等通信传输模块的接入，实现设备的通讯功能，同时设备应支持 USB 连接、RJ45 以太网接口通讯；设备应能够实现 WIFI 功能，宜为使用者提供网络共享功能；设备应支持 NFC 读取模块。

8.9 支持外设服务接入

宜采用边缘物理网关等技术提供统一外设接入服务，提供统一的外设配置和监控管理端，对应用的外设调用权限进行有效的控制。外设物联网关应支持 NFC、扫码、蓝牙等接入方式的管理。