ICS 35.240
L 63

DB4403

深　　圳　　市　　地　　方　　标　　准

DB 4403/T XXXXX—2020

金融自助终端应用系统技术要求

Technical requirements for financial self-service terminal application system

点击此处添加与国际标准一致性程度的标识

（送审稿）

2019 年 4 月 30 日

2020－XX－XX 发布　　2020－XX－XX 实施

深圳市市场监督管理局　　发 布

目　　次

前　言

本标准按照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。

本标准由深圳市地方金融监督管理局提出并归口。

本标准主要起草单位：深圳市金融科技协会、深圳怡化电脑股份有限公司、深圳合众金融设备服务有限公司。

本标准主要起草人：李绅、贺光容、朱忆军、罗振伟、陈盘中、王庆华、张媛。

引　言

近年来，随着金融自助设备的飞速增长和金融机构转型创新的不断升级，我国金融自助终端软件的国产化技术也取得了快速发展，国产化金融自助终端软件系统的市场份额逐渐加大。

当前金融自助终端应用系统产品化存在诸多问题，阻碍了金融机构终端业务快速创新和推广。如：

a) 应用系统产品化开发和运维过程复杂、难度大，对开发人员的要求高，需要专业级别的编码人员。

b) 软件更新和版本升级日益加快，导致应用系统代码版本呈几何级数增长。软件升级与运维代码版本的控制问题难以解决，软件运维代价大。

c) 无法平滑过渡到国产操作系统平台，不能满足当前金融软件国产化的发展要求。

d) 银行业务数量增加造成平台组件日趋臃肿，难以维护，最终导致平台功能退化。

e) 不同设备的兼容性问题难以解决。

本标准所规定的应用系统，可基于软件开发平台生成，采用非编码或极少编码，以图形化、可视化的方式，让复杂的应用系统开发简单化，且能控制软件版本数量，方便后期维护。

本标准规定的应用系统，可有效解决当前应用系统产品化存在的问题，提高应用系统的设计质量和技术水平，节约应用系统的开发设计成本和维护成本，降低应用系统的开发和运维的技术门槛，为金融自助终端软件的生命周期提供技术保障。

金融自助终端应用系统技术要求

1 范围

本文件提供了金融自助终端应用系统（以下简称应用系统）的总则、技术架构、技术要求及安全性要求。

本文件适用于金融自助终端应用系统的设计、测试、维护和验收，包括现金交易设备、票据及智能柜台等非现金设备，其他自助设备终端应用系统可参考使用。

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 18789.1 信息技术 自动柜员机通用规范 第 1 部分:设备

GB/T 18789.2 信息技术 自动柜员机通用规范 第 2 部分:安全

GA 1280 自动柜员机安全性要求

JR/T 0002 银行卡自动柜员机（ATM）终端技术规范

JR/T 0120.3 银行卡受理终端安全规范 第3部分：自助终端

3 术语和定义

GB/T 18789.1、JR/T 0002界定的以及下列术语和定义适用于本文件。

3.1

金融自助终端 financial self-service terminal

由用户直接操作的具有金融业务功能的设备。

3.2

金融自助终端应用系统 financial self-service terminal application system

通过控制管理终端模块、与操作人员人机交互、与业务主机交互协作，完成金融终端业务的应用软件系统。

4 缩略语

下列缩略语适用于本文件。

B/S	浏览器/服务器模式	（Browser/Server）
C/S	客户端/服务器模式	（Client/Server）
HTTP	超文本传输协议	（HyperText Transfer Protocol）
SFTP	安全文件传输协议	（Secure File Transfer Protocol）
TCP	传输控制协议	（Transmission Control Protocol）

UDP　用户数据报协议　（User Datagram Protocol）

5 总则

5.1 系统的设计应遵循以下原则：

a) 适应性原则：系统对所在环境应具有良好的适应性，具有抗干扰、能容错、安全可靠和多渠道灵活接入的能力。

b) 安全性原则：系统应保证设备正常工作和信息安全，保障用户的财产安全。

c) 稳定性原则：系统应支持 7×24 小时服务，当设备或网络发生异常时，所有不涉及该设备或网络操作的业务应不受影响，当设备或网络故障消除时，系统应能自动恢复到正常状态下运行。

d) 完整性原则：系统应按序准确完整地执行业务流程的各项功能，出现内部异常或外部干扰时，应执行规定的异常处理流程。

e) 经济性原则：系统架构和设计应尽可能地降低工程实施和软件运维成本。

f) 前瞻性原则：系统设计应充分考虑未来业务发展和管理的变化。

g) 可扩展性原则：系统应支持新业务和新需求的平行扩展。

5.2 系统应支持国产操作系统，宜实现在各操作系统之间平滑切换。

5.3 系统宜支持 C/S、B/S 以及 C/S+B/S 混合模式。

5.4 系统应采用平台开发和和业务实现分离的设计方案。

5.5 系统应支持组件、模板、参数配置等重用和扩展机制。

5.6 系统宜实现界面和业务逻辑相分离。

5.7 系统应支持对组件的统一管理和调度，宜采用插件技术实现业务功能。

5.8 系统应支持通过参数配置方式连接外部系统。

5.9 系统日志应即时记录相关重要数据信息，日志内容应能还原整个业务流程执行过程。

6 技术架构

6.1 应用系统参考技术架构分为中间件层、平台层和业务层三个层次，各层次描述如下：

a) 中间件层：为平台层提供用于业务开发和运行的组件，包括设备功能组件和软件支撑组件。

b) 平台层：提供各类金融业务开发和运行环境，包括组件管理、数据管理、流程执行等功能。

c) 业务层：根据金融终端业务功能和维护管理需求，为用户提供设备操作、界面交互和通信交互，执行业务流程，实现相应的金融终端服务和维护管理服务。

6.2 应用系统、设备驱动与操作系统共同构建成金融自助终端软件技术参考模型，参见图 1　。

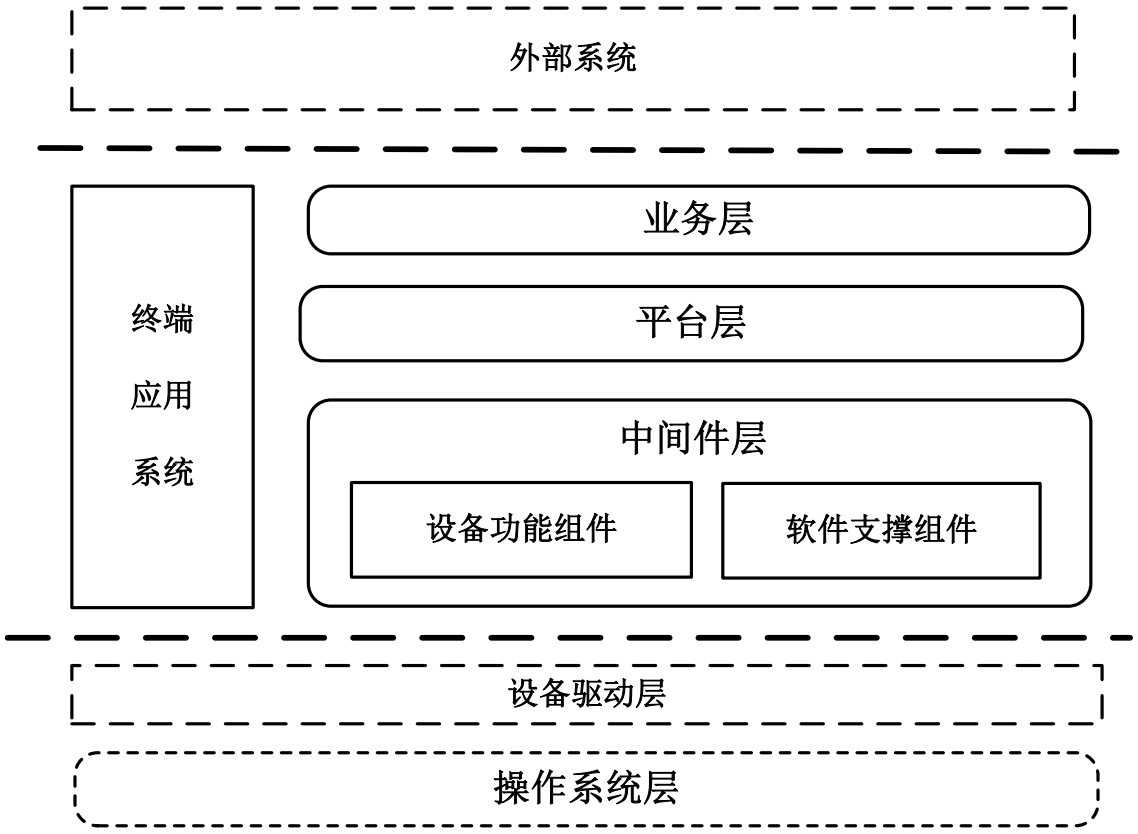

图1　金融自助终端软件技术参考架构

6.3　基于实际业务和终端自身需求，前置系统、监控系统等外部系统可通过多渠道网络方式接入终端应用系统，共同完成相关业务或服务。

7　应用系统技术要求

7.1　中间件层

7.1.1　一般要求

中间件层包括设备功能组件及软件支撑组件，应满足以下要求：

a)　宜采用 C++等跨平台编程语言实现，满足适配多操作系统的要求；
b)　设备功能组件和软件支撑组件相互独立，可单独升级，不影响其它模块；
c)　支持即插即用。

7.1.2　设备功能组件

应满足以下要求：

a)　提供相同业务功能的设备，应归于同一类设备设计统一接口；
b)　接口应不涉及和具体硬件特性相关的参数或配置；
c)　应支持对新设备的扩展。

7.1.3　软件支撑组件

应满足以配置方式实现国内金融自助业务的需要，提供各类功能组件，包括：TCP/UDP/SFTP/HTTP各类网络通信协议操作、流程节点模板操作、金融报文协议操作、设备通信操作、配置文件操作、文字转码操作、数据库操作、加解密操作、超时判断操作、IC卡操作、卡表操作、屏幕页面操作等。

7.2 平台层

应满足以下要求：

a) 应提供不受具体业务流程内容约束的业务执行环境；
b) 可支持对业务流程合法性和完整性验证；
c) 宜以统一接口与通信协议，调用中间件层的各类设备或软件组件；
d) 宜采用统一的数据管理与调用机制，防止非法增加、修改、丢失和泄露数据，确保数据的安全性；
e) 宜支持业务流程的可视化设计和修改，降低工程实施和系统运维的技术门槛。

7.3 业务层

7.3.1 一般要求

业务层应满足以下要求：

a) 应定时与前置系统或服务主机进行时间同步；
b) 宜对以下关键模块进行冗余设计：
    1) 配钞算法模块；
    2) 报文打包模块；
    3) 报文解包模块；
    4) 出钞指令处理模块。
c) 应支持自动下载或远程设定相关运行参数及交易参数；
d) 应确保交易业务优先处理，监控类业务不能影响交易业务，在有用户交易或管理员操作时，不允许处理关机停机、重启机器、暂停服务、开启服务等管理命令。

7.3.2 系统初始化要求

应满足以下要求：

a) 系统初始化时，应对系统运行环境的完整性和正确性进行检查，检查的内容应包括：
    1) 关键目录/文件是否存在/被修改；
    2) 关键配置项是否存在；
    3) 需要操作的目录和文件是否有足够的权限；
    4) 需要修改、写入、删除的文件是否为只读属性。
b) 系统初始化或运行过程中时，可检查以下项目，不符合要求的应采取对应处理措施或修正：
    1) 检测剩余磁盘空间是否满足运行要求，不满足要求则根据预设策略释放出足够硬盘空间；
    2) 检测屏幕分辨率是否正确，不符合要求则调整屏幕分辨率；
    3) 检测界面窗口是否符合运行要求，如窗口最大化要求、置顶显示要求；
    4) 检测界面指针和光标是否满足运行，如需要屏蔽时则屏蔽鼠标指针和光标；
    5) 需要加载配置检测对配置参数的合理性和有效性。
c) 系统初始化时，宜先启动日志记录模块；
d) 系统初始化时，可对设备进行身份验证，确保设备授权运行和提供服务；

e) 如终端配置有存取款模块，初始化时应确保钞箱当前的物理参数，与配置文件设定的参数是否一致，若不一致应屏蔽钞箱的出钞功能；
f) 如终端配置有读卡器，初始化时应对其中的残留卡执行吞卡操作。

7.3.3 系统运行要求

宜满足以下要求：
a) 定时记录主要进程的中央处理器使用率、内存使用、句柄数等信息；
b) 支持多中央处理器环境，将相关进程绑定到指定中央处理器。

7.3.4 人机交互要求

界面应符合JR/T 0002的要求。

7.3.5 网络通信

应满足以下要求：
a) 宜支持以下一种或多种类型的报文：8583 报文、类 8583 报文、结构体定长报文、XML 报文、SOAP 报文、HTTP 报文、JSON 报文；
b) 应按照外部系统提供的固定 IP 地址和端口进行通信，宜提供固定 IP 地址和端口供外部系统进行远程控管；
c) 应支持客户机通讯和服务器通讯两种方式，支持长连接和短连接两种方式，宜提供文件传输功能；
d) 应按照前置系统要求进行联网，并具备严格的安全保密机制，保障网络传输信息处理系统的安全、稳定和可靠，满足以下要求：
   1) 应采用在银行卡交换系统中普遍采用的加密算法；
   2) 密钥应存贮在硬件加密设备中，交易信息的加密/解密优选在硬件加密设备中进行；
   3) 应遵循国家标准和行业标准中相关的数据安全保密规定。
e) 应对交易响应包内容逐项进行合法性检查，检查项目包括：交易类型、交易处理码、流水号、卡号、交易金额、终端号。
f) 系统应利用所有的关键信息域，严格匹配交易的请求和应答，匹配原始交易和关联交易，如请求和应答的关键信息域不匹配或者未识别，应将该笔交易视为不成功交易进行处理。

7.3.6 业务功能处理

7.3.6.1 交易功能的匹配

系统应按以下流程进行逐级匹配，产生可支持的交易功能：
a) 终端可支持的全部交易功能；
b) 由主机工作参数产生的允许终端可执行的交易功能；
c) 终端当前的软硬件状态可支持的交易功能；
d) 当前网络状态可支持的交易功能；
e) 交易介质可支持的交易功能；
f) 用户权限可支持的交易。

7.3.6.2 合法性检查

应满足以下要求：

a) 应支持对卡信息进行校验运算，确认是否符合相关银行卡标准；
b) 应支持对涉及硬件特性或业务规约的配置项进行合法性校验，如单次最大存款张数、最大吞卡张数等，不符规定的应给出错误信息或采用默认值。

7.3.6.3 现金业务

应满足以下要求：

a) 在处理现金业务前，应确认同时满足以下条件：
   1) 设备处于正常状态；
   2) 设备不会有中止业务的隐患；
   3) 已回收遗留纸币；
   4) 有足够满足本次业务的可用资源，如纸币、打印纸、钞箱空间、回收箱/废钞箱空间等。
b) 以下情况应检测纸币传送通道是否存在遗留纸币，发现遗留纸币应予以回收：
   1) 存取款模块初始化时；
   2) 系统进行工作模式切换时；
   3) 现金交易处理完成后；
   4) 清机加钞处理前。
c) 吐钞或存钞成功后，应记录冠字号信息；
d) 应在日志中详细记录每笔交易信息，如金额、账号、通讯信息、存钞信息、拒钞信息、配钞信息、回收纸币信息等，其中回收纸币信息宜按以下纸币分类方式记录：
   1) 可识别，且可利用的；
   2) 可识别，且不可利用的；
   3) 不可识别的。

7.3.6.4 交易结果处理

应满足以下要求：

a) 系统应能正确判断和处理交易结果；
b) 如交易结果不明确，系统应提示用户查询发卡行、查询余额；
c) 如转账、无卡存款、缴费类，系统应提示通知用户查询发卡行；
d) 如交易接收超时，系统应提示交易结果不确定，提示用户查询发卡行。

7.3.6.5 清机与对账

系统宜支持自动化清机。

系统应具有对账机制，宜实现对账自动化与无纸化。

7.3.6.6 异常处理

应满足以下要求：

a) 系统检测到钞箱发生插拔事件或钞箱硬件传感器产生误报时，应能自动正确处理钞箱参数变化；
b) 系统应对以下操作或流程进行计时，如操作超时，应中止当前业务，并采取相应措施保障账务安全：
   1) 读卡器读卡；
   2) 界面显示或界面操作；
   3) 按键；

4） 网络响应；
5） 存款时等待放钞；
6） 存款时等待取走拒钞；
7） 取款时等待取走纸币；
8） 退卡时等待取走卡；
9） 空闲时状态报文发送监控服务器间隔时间；
10） 界面切换。

c） 系统应支持防设陷取现或设陷转账，保障账户资金安全和设备资产安全。

7.3.6.7 冲正处理

应用系统应具备冲正机制。冲正交易应满足以下要求：

a） 冲正交易应按照业务主机或前置系统的要求进行；
b） 系统接收到冲正应答后，应记录异常交易明细，包括原始交易的交易类型、流水号、交易时间、交易卡号、交易金额、发起冲正的原因、冲正次数、冲正交易结果；
c） 以下情况不得发起冲正交易：
1） 连网络物理连接失败；
2） 交易报文发送失败；
3） 收到主机需要吞钞处理的响应码；
4） 送钞后用户超时未取钞；
5） 用户可能接触到纸币，如送钞失败、开出钞门失败；
6） 取款失败后，进入或者已完成账务结算流程。

7.3.6.8 打印

应满足以下要求：

a） 对涉及现金和账户变化的异常情况，宜将相关信息醒目打印在交易凭证上。
b） 交易凭证上的卡号，除被吞卡和转账交易的转入卡外，宜隐去卡号校验位前 4 位数字，可用星号代替。

7.3.6.9 信息数据记录

应满足以下要求：

a） 应及时存储异常交易信息，避免被后续交易覆盖；
b） 不应记录客户敏感信息；
c） 除冲正交易外，交易完成后应及时清空如账户信息、交易金额、用户密码、卡信息、流水号、内部跟踪号等数据。

7.3.7 账务处理

应满足以下要求：

a） 执行涉及现金收纳的业务，应进行点钞和验钞，无效钞应及时退还给用户，并显示点钞结果让用户确认，如用户取消交易，或由于票据、证券、零钞等资源不足导致交易失败，或业务主机或前置系统明确应答本次交易失败，应原钞退还；
b） 对于异常交易，应根据前置系统要求处理，可采取交易重发、交易冲正等方法进行处理，实现账务平衡减少交易纠纷；
c） 执行涉及现金收纳的交易，发生以下情况应做吞钞处理，不得退钞给用户：

1） 接收交易响应包超时；
2） 主机发来的交易应答包解包失败，或关键域检验不一致；
3） 主机发来的交易应答包中的响应码无法识别。

d） 执行涉及现金收纳的交易，发生设备故障，应按照以下要求处理：
1） 如设备故障发生时用户尚未确认点钞结果，应将现金退还给用户，提示故障；
2） 如设备故障发生时用户已确认点钞结果且成功上账，其他设备能够正确完成后续交易流程时，应继续处理后续流程直至交易成功并打印凭条；其他设备无法继续完成后续交易流程时，应执行业务返回和交易冲正；
3） 如设备故障发生时用户已确认点钞结果但上账失败，应回收现金并退卡，同时提示用户进行账务查询并联系业务提供方处理。

7.3.8 运维支持

应满足以下要求：

a） 系统宜支持动态加载或移除硬件模块；
b） 系统应支持维修签到签退，支持对设备维修过程的监控；
c） 系统应支持自动化远程下载和安装硬件设备的介质程序和驱动程序的功能；
d） 系统应支持管理员对设备进行日常管理、参数设置、设备模块的管理和检测等；
e） 系统自动升级或远程升级失败，应根据前置系统或者系统配置要求，判断是否进行版本滚回。

7.3.9 监控支持

应满足以下要求：

a） 系统应提供以下监控服务：
1） 实时提供终端运行状态；
2） 提供终端交易业务信息；
3） 提供设备状态、凭证箱、钞箱状态、交易流水等信息；
4） 支持设备逻辑开关机、重启系统、版本发布等远程控制；
5） 提供设备台账数据、维修记录、交易量等数据。

b） 系统应优先执行交易服务，执行监控服务不得影响交易服务的执行。

8 应用系统安全性要求

8.1 一般要求

应用系统的安全性应满足GB/T 18789.2、JR/T 0120.3及GA 1280的要求。

8.2 设备控制安全

应满足以下要求：

a） 系统执行业务，应及时发现和处理涉及业务安全的设备状态/事件，保障交易安全和用户信息安全；
b） 系统在等待进卡时，如检测到进卡口闸门开应停止有卡服务，在进卡口闸门恢复正常之前如检测到有卡插入，应锁住卡片防止卡片被强行拉走；
c） 系统执行有卡业务，宜确保业务过程中读卡器中有卡且卡信息与当前业务完全一致；
d） 系统发送以下指令或报文前，宜验证指令或报文的完整性和合法性：

1） 交易合同报文；
2） 用户身份验证报文；
3） 出钞指令；
4） 存款报文；
5） 取款报文；
6） 转账报文；
7） 其他可能导致账户资金数量变化的报文。

8.3 硬盘读写安全

系统应保证磁盘读写安全，防止对硬盘频繁读写。

8.4 业务流程安全

应满足以下要求：

a） 系统切换至密码输入页面，宜有保护密码的宣传画面及语音提示；
b） 系统应能检测到长按键，并按照客户要求处理事件。

8.5 密钥安全

应满足以下要求：

a） 密钥管理应满足 JR/T 0120.3 的要求；
b） 系统应支持远程密钥导入及更新；
c） 系统应按照前置系统或业务主机要求，定期更换密钥或重新申请密钥。