ICS 35.240
CCS L 63

DB4403

深　圳　市　地　方　标　准

DB4403/T 128—2020

金融自助终端应用系统技术要求

Technical requirements for financial self-service terminal application system

2020-12-07 发布　　2021-01-01 实施

深圳市市场监督管理局　　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。

本文件由深圳市地方金融监督管理局提出并归口。

本文件起草单位：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。

本文件主要起草人：李绅、贺光容、朱忆军、罗振伟、赵高伦、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复杂，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。

本文件所规定的应用系统，可基于软件开发平台生成，采用零代码或低代码，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。

本文件规定的应用系统，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，其他移动金融自助终端设备可参考使用，如：平板终端（PAD）、销售点终端（POS）、手机终端等。

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。

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—2016 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。

HTTP：超文本传输协议（HyperText Transfer Protocol）

JSON：JavaScript对象简谱（JavaScript Object Notation）

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）
XML：可扩展标记语言（Extensible Markup Language）

5 总则

5.1 应用系统的设计应遵循以下原则：
a) 安全性原则：系统应保证设备正常工作和信息安全，保障金融机构和用户的财产安全；
b) 适应性原则：系统对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；
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) 开放性原则：系统应适应业务发展和变化；
f) 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；
g) 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；
h) 可扩展性原则：系统应支持业务和设备的平行扩展。
5.2 应用系统应支持国产操作系统，可在各操作系统之间平滑切换。
5.3 应用系统宜采用平台开发和业务实现分离的设计方案。
5.4 应用系统应支持组件、模板、参数配置等重用和扩展机制。
5.5 应用系统宜实现界面和业务逻辑相分离。
5.6 应用系统应支持对组件的统一管理和调度。

6 技术架构

6.1 应用系统软件架构分为中间件层、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，为用户提提供设备操作、界面交互和通信交互等功能，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架构逻辑模型，参见图 1。

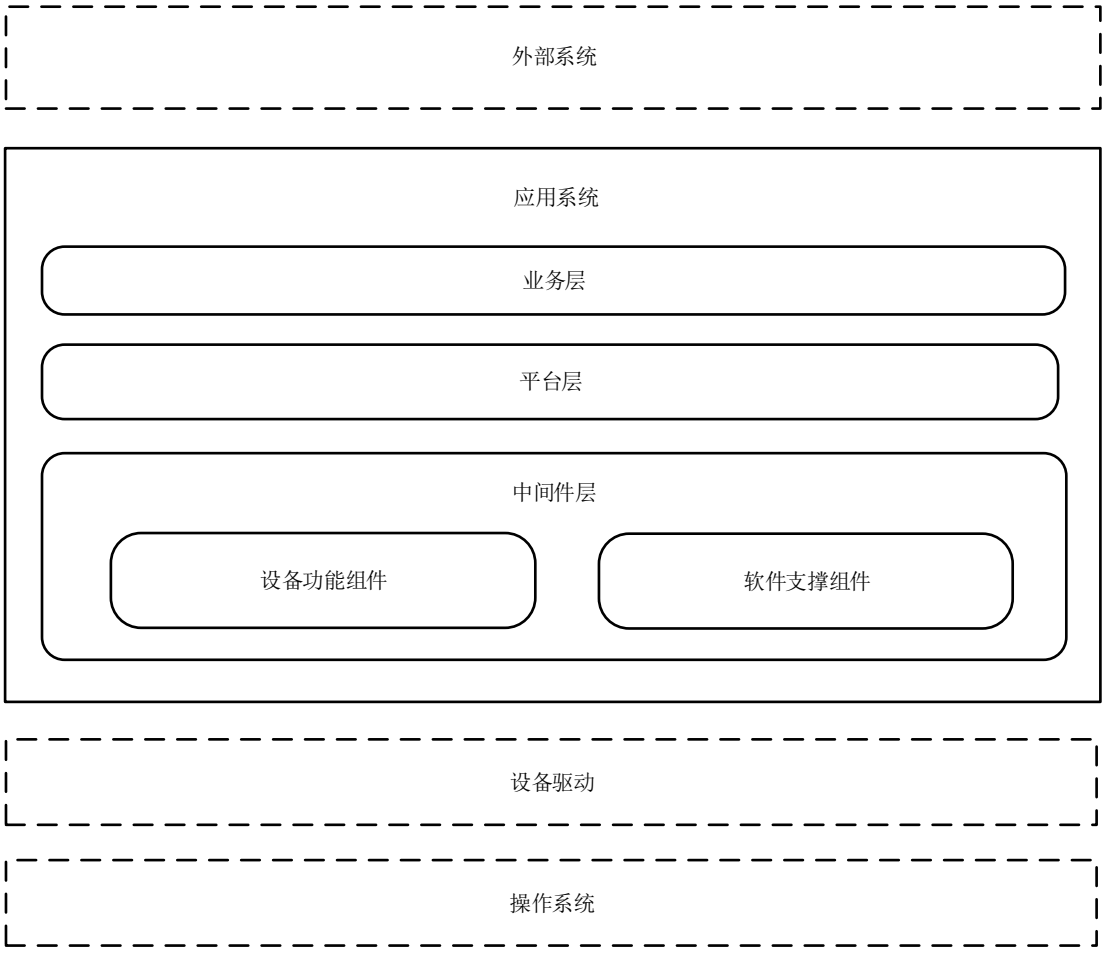

图1　金融自助终端软件架构逻辑模型

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和软件支撑组件，应满足以下要求：

a)　采用跨平台编程语言实现，可适配于多操作系统；
b)　设备功能组件和软件支撑组件相互独立；
c)　支持即插即用。

7.1.2　设备功能组件

除应满足本文件7.1.1的要求，还应满足以下要求：

a)　提供相同业务功能的设备，采用统一接口标准设计；
b)　支持对新设备的扩展。

7.1.3 软件支撑组件

7.1.3.1 宜以配置方式实现金融自助业务的需要。

7.1.3.2 宜提供各类功能组件，包括但不限于：

a) TCP/UDP/SFTP/HTTP 等网络通信协议处理组件；
b) ISO8583 报文/XML 报文/HTTP 报文/JSON 报文等金融报文协议处理组件；
c) 流程控制组件；
d) 设备通信组件；
e) 配置文件组件；
f) 数据库组件；
g) 加解密组件；
h) IC 卡组件；
i) 卡处理组件；
j) 界面组件；
k) 时间组件；
l) 文字转码组件。

7.2 平台层

宜满足以下要求：

a) 支持对业务流程完整性验证；
b) 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；
c) 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，确保数据安全；
d) 支持业务流程的可视化设计和修改，降低软件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

7.3.1.1 应定时与业务服务器进行时间同步。

7.3.1.2 宜支持远程设定终端运行参数。

7.3.1.3 应确保优先处理交易业务，监控类业务不能影响交易业务。

7.3.1.4 宜对以下关键模块进行可靠性设计：

a) 配钞算法模块；
b) 报文打包模块；
c) 报文解包模块；
d) 出钞指令处理模块。

7.3.2 初始化要求

7.3.2.1 应对运行环境的完整性和正确性进行检查，检查内容包括但不限于：

a) 关键目录/文件是否存在或被修改；
b) 关键配置项是否存在；
c) 需要操作的目录和文件是否有足够的权限；
d) 需要修改、写入、删除的文件是否为只读属性。

7.3.2.2 宜检查以下项目，不符合要求应加以修正：

a) 检测存储空间是否满足运行要求；

b) 检测界面窗口是否符合运行要求；
c) 检测配置参数的合理性和有效性。

7.3.2.3 如终端配置有存取款模块，应确保钞箱物理参数与逻辑参数一致性。

7.3.2.4 如终端配置有读卡器，应检测读卡器是否存在残留卡，有卡则执行吞卡操作。

7.3.2.5 宜先启动日志记录模块。

7.3.3 界面要求

界面应符合JR/T 0002的要求。

7.3.4 网络通信

除应满足GB/T 18789.2—2016中5.3的要求，还应满足以下要求：

a) 应支持客户机通信和服务器通信两种方式，支持长连接和短连接两种方式，宜提供文件传输功能；
b) 应采用在银行卡交换系统中普遍应用的加解密算法；
c) 应对交易响应包进行合法性检查，以防内容被篡改，检查内容包括但不限于以下项目：
   1) 终端号；
   2) 卡号；
   3) 流水号；
   4) 交易金额；
   5) 交易类型；
   6) 交易处理码。

7.3.5 业务功能处理

7.3.5.1 交易列表的生成

应获取以下各类条件可支持的交易功能，再求交集，生成用户可操作的交易列表：

a) 终端标配的交易功能；
b) 交易主机系统支持的交易功能；
c) 终端设备运行状态支持的交易功能；
d) 交易介质支持的交易功能；
e) 用户权限支持的交易功能。

7.3.5.2 现金业务

7.3.5.2.1 现金业务应满足以下要求：

a) 确保业务执行之前设备处于正常工作状态；
b) 执行完业务后，检测到纸币传送通道存在遗留纸币，应予以回收；
c) 具备验钞功能的设备，吐钞或存钞成功后，应记录冠字号信息；
d) 回收纸币应记录信息，信息宜分类记录，分类方式包括：
   1) 纸币可识别且可利用；
   2) 纸币可识别但不可利用；
   3) 纸币不可识别。
e) 按照业务外部系统要求进行冲正，不得发起冲正交易的情况包括但不限于：
   1) 发送交易报文失败；

2) 接收到需要执行吞钞的响应码；
3) 送钞后用户取钞超时；
4) 送钞过程中用户可能接触到纸币，如送钞失败、开出钞门失败；
5) 取款失败后，进入或者已完成账务结算流程。

f) 收纳现金应进行点钞和验钞，无效钞应退还给用户，并让用户确认点钞结果；
g) 如用户取消存款交易，应原钞退还给用户；
h) 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) 解包交易应答失败；
3) 比对交易应答的关键域不一致；
4) 无法识别交易应答包中的响应码。
i) 执行现金交易发生设备故障，按照以下要求处理：
1) 用户未确认点钞结果，宜退钞给用户；
2) 用户已确认点钞结果，不得退钞给用户。

7.3.5.2.2 现金业务宜满足以下要求：
a) 支持交易重发和交易冲正，减少账务纠纷；
b) 支持自动化清机；
c) 具有对账机制，支持自动化对账。

7.3.5.3 交易结果处理

应满足以下要求：
a) 正确判断和处理交易结果；
b) 严格匹配交易的请求和应答，及原始交易和关联交易。

7.3.5.4 异常处理

应满足以下要求：
a) 正确处理硬件运行机制和业务环境的变化；
b) 对业务执行时间进行计时，包括但不限于：
1) 读卡器读卡；
2) 界面显示或界面操作；
3) 用户操作键盘；
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) 界面切换。

7.3.5.5 日志记录

日志记录应满足GB/T 18789.2—2016中5.5.4的要求，且能重建整个业务流程执行过程。

7.3.6 运维支持

应满足以下要求：

a) 支持软件远程下载、更新和安装，并满足 GB/T 18789.2—2016 的要求；
b) 支持对设备进行状态检测、参数设置和维护管理；
c) 支持软件版本回滚。

7.3.7 监控支持

7.3.7.1 监控支持应支持以下功能：
a) 提供设备实时状态；
b) 提供钞箱或票箱剩余容量、钞票数量等终端实时资源信息；
c) 提供终端实时交易信息；
d) 支持设备开关机、重启应用系统、版本发布等远程控制；
e) 提供设备维修记录、交易流水、交易量等数据。

7.3.7.2 监控支持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

应满足以下要求：
a) 符合 GB/T 18789.2—2016 中 5.5、JR/T 0120.3 及 GA 1280 的相关规定；
b) 符合《信息安全等级保护管理办法》第三级的规定；
c) 支持国密算法。

8.2 设备控制安全

应满足以下要求：
a) 及时处理交易过程中出现的设备异常状态和事件，确保资金安全；
b) 执行有卡业务应确保卡信息与当前业务一致。

8.3 合法性验证

8.3.1 宜支持验证报文和指令的完整性，包括但不限于：
a) 身份验证报文；
b) 现金类指令；
c) 账务类报文。

8.3.2 宜支持生物识别进行用户或管机员身份认证，包括但不限于：
a) 人脸识别；
b) 指纹识别；
c) 声纹识别；
d) 掌静脉识别；
e) 虹膜识别；
f) 步态识别。

8.3.3 应支持校验卡信息，确保符合相关银行卡标准。

8.3.4 宜支持二维码认证。

8.3.5 应支持对终端标识唯一性的验证。

8.4 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) 密钥更新应满足 GB/T 18789.2—2016 中 5.5.1 的要求；

c) 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；

d) 支持远程密钥导入及更新。

参 考 文 献

[1]《信息安全等级保护管理办法》（公通字〔2007〕43号）