ICS 35.240
CCS L 79

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXXX—XXXX

政务服务自助服务终端一体化技术规范 第7部分：安全规范

Integration of self-service Terminal in Shenzhen Government Service

Part 7: specification for security

（送审稿）

xxxx-xx-xx 发布　　xxxx-xx-xx 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。

DB4403/T XXXX-XXXX《政务服务自助服务终端一体化技术规范》分为7个部分：

——第1部分：总体规范；

——第2部分：业务规范；

——第3部分：设备及兼容规范；

——第4部分：用户体验设计规范；

——第5部分：部署实施规范；

——第6部分：运维规范；

——第7部分：安全规范。

本文件为DB4403/T XXXX-XXXX的第7部分。

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。

本文件由深圳市政务服务数据主管部门提出并归口。

本文件起草单位：

本文件主要起草人：

政务服务自助服务终端一体化技术规范

第 7 部分：安全规范

1 范围

本文件规定了政务服务自助服务终端一体化技术规范的物理安全、软件安全、数据安全、网络安全和安全管理要求。

本文件适用于深圳市政务服务自助终端的安全体系设计、建设和管理。

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 9254.2-2021 信息技术设备、多媒体设备和接收机 电磁兼容 第2部分：抗扰度要求

GB/T 17618--2015 信息技术设备 抗扰度 限值和测量方法

GB/T 17799.1-2017 电磁兼容 通用标准 居住、商业和轻工业环境中的抗扰度

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 36951-2018 信息安全技术 物联网感知终端应用安全技术要求

3 缩略语

下列缩略语适用于本文件。

USB 通用串行总线（Universal Serial Bus）

TF 一种极细小的快闪存储器卡（Trans-flash Card）

ID 身份标识号码（Identity document）

4 总体要求

政务服务自助终端应在安全的网络条件下接入，安装部署环境应符合安全要求，日常管理和故障维修等应遵循安全管理要求。

5 物理安全要求

5.1 外观及结构要求

设备外观及结构安全要求如下：

a) 具备物理安全防护措施，外观完好且不易被破坏，防止被恶意破坏或暴力破解；

b) 具备清晰可辨的设备归属字样和标识，产品表面说明功能的文字、符号、标志应清晰、端正、牢固；

c) 具备摄像头，支持开机即启动，支持远程控制，支持正面拍摄使用者；

d) 按键安装平整，操作灵活可靠，零部件紧固无松动。

5.2 场地安全要求

部署场地安全要求如下：

a) 具备雷电防护措施；

b) 应具有良好的接地系统，逻辑地和保护地必须与交流地分开；

c) 具备安全防控措施，配备现场安防管理人员，防止设备损坏及盗窃等行为。

5.3 电磁兼容要求

应符合[GB/T 17799.1—2017电磁兼容 通用标准]，满足在居住、商业和轻工业环境中相应的静电放电、射频辐射电磁场、电快速瞬变脉冲群、浪涌（冲击）、射频场感应的传导骚扰及电压暂降、短时中断和电压变化等抗扰度测试要求。

5.4 外设和通信接口

设备外设和通信接口安全要求如下：

a) 应使用文字或图案标记来说明已有外设和通信接口用途，未经允许，不得随意接入非自助服务终端专用外设；

b) 不应具有除以太网网口以外的其他任何网络通信接口，包括WIFI、蓝牙、无线拨号模块等；

c) 宜去除板载调试接口或将接口封闭在产品外壳内；

d) 机箱端口抗扰度，机箱端口抗扰度符合GB/T 9254.2-2021 信息技术设备、多媒体设备和接收机电磁兼容 第2部分：抗扰度要求；

e) 电源输入端口抗扰度，电源输入端口抗扰度符合GB/T 9254.2-2021 信息技术设备、多媒体设备和接收机电磁兼容 第2部分：抗扰度要求。

5.5 终端部件更换要求

不得随意更换终端的部件，如遇损坏，需维修、报废的，应向主管部门报备后，脱网处理更换硬件。

6 软件安全要求

6.1 基本要求

软件安全要求如下：

a) 设备软件应支持读取唯一ID识别码、信息摘要或设备信息的功能；

b) 服务器平台软件应具备安全事件审计日志功能。

c) 服务器平台系统及服务应定期开展漏洞扫描、渗透测试等安全风险评估工作。

6.2 接入认证要求

接入认证要求如下：

a)应支持唯一ID识别、IP/MAC地址绑定符合GB/T 36951-2018感知终端接入标准和数字证书方式的接入认证；

b)接入政务外网和互联网，应通过开通相应的业务端口和防火墙策略等方式实现安全接入；

c)应对网络交互的地址和端口协议等进行检查，实时监控数据包进出；

d)应优化访问控制列表，保证访问控制规则数量最小化。

6.3 入侵防护要求

入侵防护要求如下：

a)应安装经过安全认证的恶意代码扫描软件，支持对恶意代码入侵报警和处理;

b)应支持攻击行为的检测并发出预警提示,记录攻击行为信息,在发生严重入侵事件时应提供报警;

c)应在关键网络节点处支持恶意代码的检测和清除，并维护清除恶意代码防护机制的升级和更新;

6.4 操作系统要求

设备操作系统安全要求如下：

a) 安装正版操作系统；

b) 应有定期更新升级补丁计划；

c) 应限制未授权接口和端口的使用；

d) 定期清除用户缓存信息，避免信息泄漏。

6.5 信息安全等级保护定级要求

政务服务自助终端服务平台软件信息安全等级保护要求如下：

a) 根据GB/T 22239-2019标准等级保护要求，安全等级应执行二级等保或以上标准。

b) 除政务云平台提供的安全保障外，还应满足应用系统安全设计、数据安全设计的要求。

7 数据安全要求

7.1 数据完整

数据应符合完整性要求，采用校验或密码等技术保证重要数据在传输及存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

7.2 数据保密

数据保密要求如下：

a)重要数据在传输及存储过程中，应使用密码技术加密，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b)自助终端设备应仅采集与保存业务办理时必需的用户个人信息;应禁止未授权访问和非法使用用户个人信息；

c)自助终端展示个人重要信息时，应数据脱敏后展示，对于代办业务的，系统应只对代办人显示主干信息，对个人隐私信息做好保护；

d)自助终端仅允许用户查看自己授权的相关信息,并在除信息录入环节外的其他界面对数据做脱敏处理，用户敏感数据不完整展示。

7.3 数据使用安全保护

任何个人或组织的关键数据（关键、敏感或重要数据）需要通过访问控制、安全、保密等手段，提供个人或组织的数据安全保护和隐私保护。

7.4 数据存储安全设计

数据存储安全设计要求如下：

a)办事人员在办理业务时坚持不存储用户隐私数据的原则，通过实人认证授权后，系统才可调用外部系统获取数据；业务办理完毕后，及时清除内存或缓存中的用户隐私数据。

b)应提供重要数据的本地数据备份与恢复功能；

c)应提供线上异地实时备份功能，对重要数据实时备份至专设备份服务器。

7.4.1 后端数据储存设计

应使用分布式数据库系统进行系统数据存储。对办事人员上传的信息、照片的处理，应遵循按需获取、用后清除的原则；对办事人员的敏感信息，坚持不保存、不落地原则。

7.4.2 支持数据序列化处理技术

应对数据进行数据结构序列化、反序列化，以实现高效的压缩、存储。

7.5 关键数据加密

应对关键、敏感或重要数据实行分级加密存储，支持字段级、记录级、文件级加密存储。系统对于办事人员关键数据，应在数据库中进行序列化处理，采用国产密码算法加密等措施防止用户关键数据泄漏。

7.6 数据访问日志记录

数据库操作应有日志审计记录，防止数据库文件被损坏导致用户数据泄漏或丢失。

系统应记录用户访问系统、办理业务过程中的系统日志，供系统审计使用。系统应记录业务逻辑的关键路径以及出错信息，方便线上排错。

8 网络安全要求

8.1 网络环境

政务服务自助终端服务应部署在政务外网或专线网络，不应部署在互联网环境。

8.2 专机专网专用

应采用统一分配且固定的IP地址资源，采用屏蔽线接入固定接入点，确保专机专网专用，禁止私自更改IP地址或接入其他网络、网段。

8.3 网络安全加固

应部署并配置基于国产密码算法的信道加密、基于多因素的安全授权和准入访问等安全设备和策略。

9 安全管理要求

9.1 日志审计

应对终端访问后端服务进行日志审计，内容应包括事件类型、结果、内容描述、日期/时间等。公安业务办理日志需对接公安内网安全审计平台。

9.2 权限管理

应为不同的管理员用户提供不同的访问权限，禁止非授权用户查询或配置自助终端功能属性。

9.3 视频监控

政务服务自助终端应部署在具备视频监控能力的环境，保障终端部署区域范围的监控视频清晰可见，无监控盲区。

9.4 身份认证

政务服务自助终端部署在24小时自助服务区的，需具备安防视频监控，还需支持刷身份证或者扫码进入自助服务区。

9.5 违规外联告警

政务服务自助终端若发生违规外联情况，应及时发出违规告警，并作出提示。

9.6 日常巡检保障

应对政务服务自助终端所属环境进行周期性的日常巡检，避免在强磁场、温度高、灰尘多和潮湿的环境工作，并做好记录。

9.7 安全使用

政务服务自助终端安全使用应符合以下要求：

a) 政务服务自助终端实行部署网点保管责任制，设备部署网点主管单位的主要领导是保管的第一责任人，设备部署所在网点的业务负责人是保管和使用的直接责任人。相关人员应严格履行保管职责，做到妥善保管，正确使用。
b) 政务服务自助终端仅限于规定的区域内使用，不得私自转移使用，非经过授权许可，严禁使用政务服务自助终端为其他第三方业务系统提供各类信息数据，严禁从政务服务自助终端上拷贝日志等任何数据。
c) 政务服务自助终端是特殊设备，设备部署网点所属单位应每日进行巡检并做好记录，保持终端设备安全、可靠运行。
d) 政务服务自助终端服务软件、事项须在主管部门的指导下安装和卸载，不得随意卸载、更改终端软件及关键配置参数。
e) 严禁在政务服务自助终端上储存、处理国家秘密信息，或与涉及国家秘密信息的设备及载体连接。