ICS 03.240
A 90
备案号:65889—2019

YZ

中华人民共和国邮政行业标准

YZ/T 0164—2018

快递手持终端安全技术要求

Security technical specification of hand-held terminal for express

2018-11-29 发布　　2019-03-01 实施

国家邮政局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家邮政局提出。

本标准由全国邮政业标准化技术委员会(SAC/TC462)归口。

本标准起草单位:上海市快递行业协会、杭州汇创技术有限公司、北京云邮信通物联网研究院、顺丰速运有限公司。

本标准主要起草人:高镇海、孟庆国、何锦华、信雨、郭杰、老世荣、夏颐、黄旭涛。

快递手持终端安全技术要求

1 范围

本标准规定了快递手持终端的基本要求、系统安全、业务系统登录安全、应用软件安全、寄递服务用户个人信息保护和传输安全等内容。

本标准适用于收派环节快递手持终端的设计、生产、使用和检测,邮政手持终端可参照使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 4943.1—2011	信息技术设备　安全　第1部分:通用要求
YZ/T 0139—2015	邮政业安全生产设备配置规范
YZ/T 0147—2015	寄递服务用户个人信息保护指南
YZ/T 0152—2016	邮政业信息系统安全等级保护基本要求
ISO/IEC 14443(所有部分)	识别卡　无接触点集成电路卡　邻近卡(Identification cards—Contactless intergrated circuit cards—Proximity cards)

3 术语和定义

下列术语和定义适用于本文件。

3.1

快递手持终端　hand-held terminal for express

快递企业提供寄递服务所使用的,具有信息采集、处理、存储、输入和输出等功能的手持操作信息技术产品。

3.2

寄递服务用户个人信息　personal information of posting and delivery service users

用户在使用寄递服务过程中的个人信息。寄递服务用户个人信息可分为个人敏感信息和个人一般信息。

[YZ/T 0147—2015,定义3.1]

3.3

个人敏感信息　personal sensitive information

一旦遭到泄露或修改,会对标识的用户造成安全隐患或不良影响的寄递用户信息。个人敏感信息包括寄(收)件人的姓名、地址、身份证件号码、电话号码、物品名称、物品价值等。

[YZ/T 0147—2015,定义3.2]

3.4

个人一般信息　personal general information

除个人敏感信息以外的寄递用户信息。

[YZ/T 0147—2015,定义3.3]

4 缩略语

下列缩略语适用于本文件,见表1。

表1 缩 略 语

序号	缩 略 语	中 文 名 称	英 文 名 称
1	4G	第四代移动通信技术	4th Generation Mobile Communication Technology
2	IMEI	国际移动设备识别码	International Mobile Equipment Identity
3	MAC	物理地址	Media Access Control Address
4	MDM	移动设备管理	Mobile Device Management
5	NFC	近距离无线通信	Near Field Communication
6	ROOT	系统中的根用户	Root
7	RFID	射频识别	Radio Frequency IDentification
8	SD	安全数据卡	Secure Digital Card
9	SN	产品序列号	Serial Number
10	USB	通用串行总线	Universal Serial Bus
11	WiFi	无线保真网络	Wireless Fidelity

5 基本要求

5.1 快递手持终端应符合 GB 4943.1—2011、YZ/T 0139—2015 和 YZ/T 0152—2016 的要求。

5.2 快递手持终端应采用4G及以上的通信技术。通信模块应内置不可拆卸。

5.3 快递手持终端应具备卫星定位功能。卫星定位系统宜同时具备定位和短报文功能。

5.4 快递手持终端应具备 NFC 功能,可读取包括二代居民身份证在内的非接触卡。读取功能应符合 ISO/IEC 14443 的规定。

5.5 快递手持终端应能正确识读一维条码和二维条码。

6 系统安全

6.1 快递手持终端激活前应验证设备特征信息,如 SN、IMEI、MAC 等。

6.2 快递手持终端应通过 MDM 系统下发配置策略,配置策略可在快递手持终端注册完成后自动部署到终端上,也可由 MDM 系统按需推送。

6.3 快递手持终端不应关闭 MDM 系统自身进程或取消激活。

6.4 快递手持终端应限制用户对非业务所需功能的使用,按需控制设备外设及相关的功能项,如摄像头、麦克风、NFC、USB、SD、蓝牙、WiFi、截屏、USB 共享控制、数据同步等。

6.5 快递手持终端应通过 MDM 系统实现远程擦除数据、锁屏、定位等功能,并可在设备丢失或员工离职时快速实现上述操作。

6.6 快递手持终端应通过技术手段防止用户获得 ROOT 权限。

6.7 快递手持终端违规使用时,系统应提供风险告警、功能禁用、网络隔离、配置擦除、数据擦除等不同级别的处理功能。

7 业务系统登录安全

7.1 业务系统应具有专用的登录控制模块对登录用户进行身份标识和鉴别,保证系统中不存在重复的用户身份标识,确保身份鉴别信息不被冒用。
7.2 用户登录口令应设置为不易破解的口令,口令应定期更换或修改。
7.3 用户登录口令等敏感数据的输入控件应防止输入劫持,防止键盘记录。
7.4 用户登录口令应使用国家认可的加密算法加密并使用安全协议传输。
7.5 用户登录模块应使用验证码,验证码应在业务系统服务器端生成并在服务器端校验。

8 应用软件安全

8.1 快递手持终端应遵循最小安装的原则,仅安装与业务应用相关的应用软件。
8.2 MDM 系统应建立应用软件黑白名单,仅允许安装和使用白名单中的应用软件。及时清理白名单外的应用软件,并对快递手持终端安装的应用软件进行全面的安全检查。
8.3 快递手持终端应通过 MDM 系统发布和更新业务应用软件。
8.4 对具有上传功能的应用软件,应在服务器端限制上传文件的类型,并对上传的目录设置禁止脚本执行权限,防止木马、后门脚本上传。
8.5 应用软件应设置版本合规性要求,不符合版本要求的应用软件不应使用。
8.6 应用软件的用户界面应具有屏蔽用户未授权访问的功能。在服务器端应对用户访问进行权限检查,防止用户越权访问。
8.7 应用软件在上线和版本变更等关键时间节点前,应检测软件源代码中可能存在的程序缺陷和安全漏洞。

9 寄递服务用户个人信息保护

9.1 快递手持终端不应保存寄递服务用户个人信息。
9.2 快递手持终端应通过 NFC 方式读取身份证件信息,不应通过拍照方式获取寄递服务用户个人敏感信息。对不具备 NFC 读取条件的,拍照后应加密存储并在上传后及时清除相关信息。
9.3 快递手持终端应用软件中显示的寄递用户个人敏感信息应通过加入特殊字符、加密等方式进行脱敏处理。
9.4 快递手持终端不应存在泄露寄递服务用户个人信息的安全漏洞,应采取防录屏、防截屏、防输入劫持、防键盘记录等必要的安全技术,防止窃取寄递服务用户个人信息的行为发生。

10 传输安全

10.1 快递手持终端与业务系统服务器之间的数据传输过程应保证数据的安全性、完整性。
10.2 快递手持终端与业务系统服务器建立连接之前,应利用密码技术进行会话初始化验证。
10.3 快递手持终端与业务系统服务器之间的数据传输应进行路由控制,建立安全的访问路径,并使用国家认可的加密算法进行加密。