ICS 35.240.99
A 90

SZDB/Z

深 圳 市 标 准 化 指 导 性 技 术 文 件

SZDB/Z 329—2018

警务云终端系统建设与管理规范

Construction and management specification of police cloud terminal system

2018-11-02 发布　　2018-12-01 实施

深圳市市场和质量监督管理委员会　　发 布

目　次

前　言 II
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 1
4 系统组成及网络架构 2
5 公安无线虚拟专网建设规范 3
6 硬件通用规范 4
7 移动警务云平台建设规范 6
8 APP 应用开发规范 8
9 终端系统管理规范 8

前　言

本文件按照GB/T 1.1—2009给出的规则起草。

本文件由深圳市公安局视频警察支队提出。

本文件由深圳市公安局安全技术防范管理办公室归口。

本文件起草单位：深圳市中安测标准技术有限公司、中国电信股份有限公司深圳分公司、深圳市星火电子工程公司、深圳市筑泰防务智能科技有限公司、深圳市信义科技有限公司、深圳英飞拓科技股份有限公司、盛视科技股份有限公司、深圳市共济科技股份有限公司、深圳市来吉智能科技有限公司、深圳市富晋天维信息通讯技术有限公司、深圳市森讯达电子技术有限公司。

本文件主要起草人：李冉、杨学、陈世胜、倪凌、陈伟健、陈兴康、蔡建荣、董晓波、宋清东、马中旺、秦永涛、关庆佳、陈文胜、陈新朋、孙君波、蒋智勇、雷秋菊、朱伟豪。

警务云终端系统建设与管理规范

1 范围

本文件规定了警务云终端系统的网络建设规范、硬件通用规范、移动警务云平台建设规范、APP应用开发规范、终端系统管理规范。

本文件适用于深圳市公安领域的移动终端系统建设与管理。其他相关领域可参照执行。

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

GB/T 9813.1—2016 计算机通用规范 第1部分：台式微型计算机

GB 31241 便携式电子产品用锂离子电池和电池组安全要求

GA/T 818—2009 警用便携式治安管理信息采集终端通用技术要求

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1

互联网系统

移动终端连接互联网的普通操作系统，运行日常应用。

3.2

安全系统

移动终端连接公安无线虚拟专网的安全加固操作系统，运行公安业务移动应用。

3.3

双系统移动终端

同时运行“互联网系统”和“安全系统”的移动智能终端，且两个系统相互隔离。

3.4

公安信息网

公安机关开展工作使用的内部专用计算机网络，不得传输、处理、存储涉及国家秘密的信息。

3.5

公安无线虚拟专网

基于通信运营商无线网络，利用 L2TP、PPTP 隧道技术为警务工作构建的与公众互联网隔离的虚拟专用网络。用户使用移动终端通过无线 VPDN/APN 网络安全地访问公安信息网资源。

3.6 缩略语

下列缩略语适用于本文件。

AAA：认证、授权、计费（Authentication，Authorization，Accounting）

APN：接入点名称（Access Point Name）

DDoS：分布式拒绝服务（Distributed Denial of Service）

IMEI：国际移动设备身份码（International Mobile Equipment Identity）

IMSI：国际移动用户标识（International Mobile Subscriber Identification Number）

IPSec：IP安全性（IP security）

L2TP：二层隧道协议（Layer Two Tunneling Protocol）

MEID：移动设备识别码（Mobile Equipment Identifier）

PPTP：点对点隧道协议（Point to Point Tunneling Protocol）

RUIM：可移动用户识别模块（Removable User Identity Module）

UIM：用户识别模块（User Identify Module）

USIM：全球用户标识模块（Universal Subscriber Identity Module）

VPDN：虚拟拨号专用网络（Virtual Private Dialed Network）

4 系统组成及网络架构

4.1 概述

警务云终端是一部定制双系统移动终端，采用公安无线虚拟专网接入移动警务云平台，并通过安全边界实现移动警务云平台与公安信息网交换数据。

4.2 系统架构图

警务云终端系统由警务云终端、公安无线虚拟专网、移动警务云平台、边界平台、公安信息网组成，系统架构图见图1。

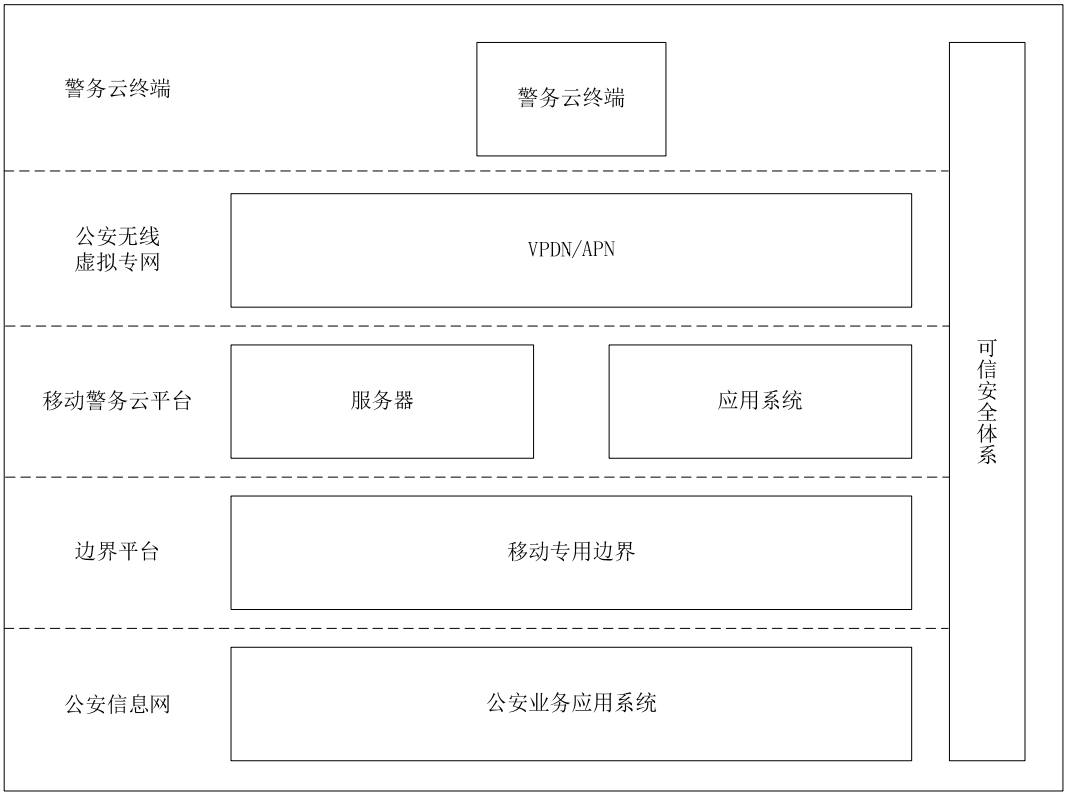

图1　警务云终端系统架构图

4.3　系统拓扑图

系统拓扑图见图2。

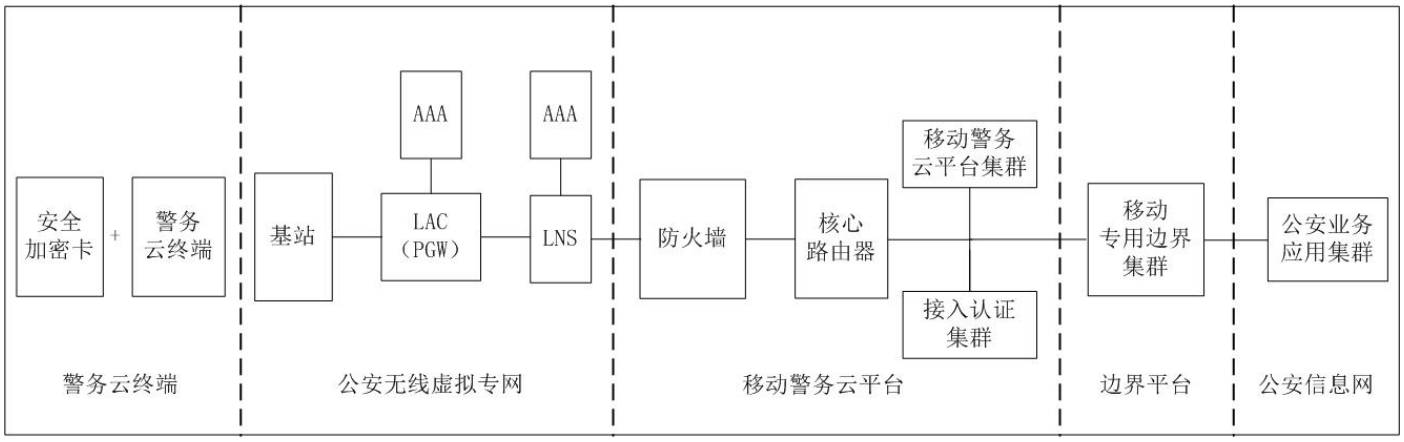

图2　警务云终端系统拓扑图

5　公安无线虚拟专网建设规范

5.1　公安无线虚拟专网应承载在通信运营商移动网络和专线链路上，通过 L2TP、PPTP 等标准隧道协议建立加密通信，其中密码加密算法符合 CHAP，数据加密算法符合 IPSec，与互联网隔离。

5.2 公安无线虚拟专网应具备二次鉴权认证机制，鉴权过程实现域名、手机号、IMSI、用户帐号、密令，终端串码、IP 等多因子捆绑认证。

5.3 通信运营商的 VPDN/APN 系统应通过国家信息安全测评，满足信息系统安全保障级二级或以上。

6 硬件通用规范

6.1 基本要求

6.1.1 设备应具有中华人民共和国工业和信息化部颁发的有效的《电信设备进网许可证》。

6.1.2 设备应为国产品牌。

6.2 外观要求

外观应符合以下要求：

a）产品表面不应有明显的凹痕、破损、划痕、变形和污染等；

b）表面涂镀层应均匀，无起泡、龟裂、脱落和磨损现象；

c）金属零部件无锈蚀及其他机械损伤。

6.3 硬件要求

硬件应符合以下要求：

a）屏幕：5.0英寸或以上（电容屏、多点触控），分辨率为1920像素×1080像素或以上；

b）CPU主频1.2GHz四核或以上，内存容量应不少于4G，存储容量应不少于64G；

c）接口配置应包括：

1）两个或以上外接 SIM 卡和 UIM 卡接口；

2）电源/USB 接口；

3）TF/SD 卡；

4）蓝牙；

5）NFC。

d）前置摄像头 500 万像素或以上；后置摄像头 1300 万像素或以上，带 LED 补光灯；

e）应具备全球定位系统（GPS）、北斗等定位及基站定位功能，卫星定位精度应在 15 米以内；

f）电池应符合 GB 31241 的规定。

6.4 设备功能及性能要求

6.4.1 操作系统：应使用经过安全加固的双系统软件，包括互联网系统和安全系统，两个操作系统同时独立运行，切换时间不应超过 3 s。

6.4.2 安全系统：应预装终端设备管理软件、接入认证安全客户端软件等必要的应用程序；不应预装与公安业务无关的应用软件。

6.4.3 视频帧率应不小于 25 帧/s。

6.4.4 屏幕最大亮度不低于 350 cd/m²，对比度应不低于 500：1。

6.4.5 设备的可靠性应符合 GB/T 9813.1—2016 的规定。设备的平均无故障工作时间（MTBF）不小于 5000h。

6.4.6 应具备电源保护措施功能。

6.4.7 功能控制要求:

a) 应提供定位、录音、拍照和摄像等功能受控机制;
b) 应支持对I/O接口屏蔽功能，防止非授权移动设备使用;
c) 扩展卡槽或外置设备仅能读取指定的安全加密卡;
d) 应具备WiFi热点扫描功能。

6.4.8 其他要求应符合 GA/T 818—2009 中 4.1 的相关规定。

6.5 通信要求

6.5.1 具备移动数据通信功能，支持 4G 并向下兼容 3G、2G。

6.5.2 支持公安无线虚拟专网通过边界平台安全接入公安信息网。

6.5.3 支持互联网系统和安全系统分别同时接入互联网和公安无线虚拟专网，且互相隔离。

6.6 安全性要求

6.6.1 电气安全性要求

6.6.1.1 抗电强度

应符合GB 4943.1—2011中5.2的相关规定。

6.6.1.2 绝缘电阻

设备的电源插头或电源引入端与外壳裸露金属部件之间的绝缘电阻,常规环境条件下应不小于100MΩ，在湿热条件下应不小于5MΩ。

6.6.1.3 泄漏电流

设备的泄漏电流应不大于 5mA（AC、峰值）。

6.6.2 信息安全要求

6.6.2.1 信息设备安全要求

应符合 GB/T 9813.1—2016 中 4.4 的相关规定，设备接入公安无线虚拟专网应遵循相应技术规范。

6.6.2.2 身份鉴别管理要求

身份鉴别鉴定管理应符合以下要求:

a) 应支持指纹或人脸等生物识别技术进行开机身份认证;
b) 在安全系统中应支持基于安全加密卡（含内置安全芯片）和 SIM/RUIM/USIM 卡相绑定的设备认证;
c) 应支持密码长度、复杂度、更换周期、最大解锁错误次数的管理;
d) 应实现终端系统弱口令检测与告警。

6.6.2.3 安全隔离要求

安全隔离应符合以下要求:

a）警务云终端安装有相互隔离的两个系统，两个系统没有主次，是并列关系，分为互联网系统和安全系统；

b）警务云终端从底层实施隔离，具备安全加固、功能裁剪及禁止 ROOT、刷机等功能；

c）警务云终端两个系统的系统数据、应用数据、用户数据完全隔离；

d）警务云终端两个系统独立运行、独立控制，互不交换数据；

e）应具备相应安全技术措施，可检测并阻断安全系统访问互联网的行为，并阻止通过互联网系统对安全系统的渗透。

6.6.2.4 访问控制要求

访问控制应符合以下要求：

a）安全系统中WLAN、蓝牙应通过移动终端管理平台进行授权网络连接和数据通信；

b）应确保安全系统仅能运行移动终端管理平台授权的应用。

6.6.2.5 数据安全要求

数据安全应符合以下要求：

a）应确保安全系统中的敏感数据加密存储；

b）应确保安全系统访问公安无线虚拟专网指定应用的数据加密传输；

c）应保证用户数据不被未授权用户查阅或修改。

6.6.2.6 安全加密卡（含内置安全芯片）要求

安全加密卡（含内置安全芯片）应符合以下要求：

a）设备应安装安全加密卡（含内置安全芯片）套件，包括安全芯片、安全卡和安全加固软件；

b）安全加密卡数据加解密、数字签名和验证、消息摘要和完整性检验等服务，应支持国产商用密码算法SM1、SM2、SM3及SM4，符合密码标准要求，配合安全平台完成数据加解密运算、数字签名验签、密钥交换和加解密、摘要值生成和完整性校验等；

c）安全加密卡应划分多个证书容器，支持多证书认证；

d）安全加密卡基于口令对用户进行认证，具有防暴力破解功能；

e）安全加密卡存储容量应不小于4G，加密速度应不低于4 Mbps。

6.6.2.7 安全和审计要求

安全和审计应符合以下要求：

a）对于可执行程序，应确保在通过防篡改检查后才能被操作系统执行；对于业务数据，应采用可信的校验机制，保证数据传输、存储过程中的完整性；

b）应能防范恶意代码的运行，实现主动防御机制，保障工作站、服务器、边界所存储和传输的数据安全性；

c）应能获取设备运行的审计日志；

d）应能获取用户操作的审计日志；

e）应支持向统一管理平台报送用户操作的审计日志。

7 移动警务云平台建设规范

7.1 概述

移动警务云平台是支撑警务云终端应用运行和管理的基本技术支撑系统，以及与其配套的标准和运

维管理体系。

7.2 移动警务云平台的功能

移动警务云平台主要包括以下功能：

a）为移动应用安全、稳定运行提供最基础的运行支撑服务，为移动应用用户提供通用便利支撑服务；

b）为移动应用全生命周期规范管理提供技术支撑服务，构建移动应用良好的管理、评价、共享、支撑机制。

7.3 移动警务云平台的构成

移动警务云平台由应用管理支撑系统和应用运行支撑系统构成。

7.4 应用管理支撑系统

7.4.1 概述

应用管理支撑系统分为开发管理和应用管理两部分。开发管理功能由应用开发资源服务子系统承担。应用管理功能由移动应用管理及发布子系统、移动互联网应用管理及发布子系统和应用部署监测子系统承担。

7.4.2 系统功能

系统功能应包括以下内容：

a）应用开发资源服务子系统：对应用开发者提供开发资源上传、检索、下载和知识库服务；

b）移动应用管理及发布子系统：提供行业移动应用的注册、审核、发布、撤销等全生命周期管理功能；提供对本地移动应用及其使用情况的汇聚功能，并按照统一标准开放接口，供应用部署监测子系统自动采集；

c）移动互联网应用管理及发布子系统：提供移动互联网应用的注册、检测、审核、发布、撤销等全生命周期管理功能；提供对移动互联网应用及其使用情况的汇聚功能，并按照统一标准开放接口，供应用部署监测子系统自动采集；

d）应用部署监测子系统：按照统一标准接口，定期从移动互联网应用管理及发布子系统和移动应用管理及发布子系统中采集移动应用及其使用情况，并具备统计分析功能。

7.5 应用运行支撑系统

7.5.1 概述

应用运行支撑系统包括统一认证授权子系统、移动信息资源服务子系统、应用监测评估子系统和实名认证子系统。

7.5.2 系统功能

系统功能应包括以下内容：

a）统一认证授权子系统：实现用户统一身份认证、应用访问授权、单点登录等功能；

b）移动信息资源服务子系统：实现统一的数据资源标准接口及数据授权访问；

c）应用监测评估子系统：实现行为审计、业务分析与综合评估等功能；

d）实名认证子系统：实现移动互联网用户实名认证功能。

8 APP 应用开发规范

8.1 概述

移动警务云平台应结合公安信息网业务系统和公安基层需求，基于警务云终端快速开发、集成各类警用功能。

8.2 APP 应用开发要求

APP应用开发应符合以下要求：

a）用户授权访问控制：应对用户进行基于角色的授权和访问控制。用户的信息访问授权应遵循“最小权限原则”和“特权分散原则”；

b）系统权限访问控制：应按照“最小权限原则”限定终端系统权限访问，不得申请开放本应用不需要的终端系统权限（如启用定位功能、打开摄像头、读取通讯录等）；

c）日志管理与安全审计：应按照统一要求，对用户登录/退出、关键数据操作等行为记录日志。应用日志应保留用户身份信息，满足历史信息可倒查要求，并按照规范提交集中管控中心；

d）应用数据加密存储：移动应用应按照规范对重要数据进行加密存储；

e）资源访问接口要求：应遵循资源提供方的技术接口及管理规范。

8.3 应用开发标准

应符合以下要求：

a）应用基本信息注册：每个新发布的应用，应在移动应用支撑平台中配置相关的应用信息；

b）应用日志信息注册：对于应用的每次访问，移动应用支撑平台应记录具体的操作内容、操作人、操作时间；

c）系统服务：基于公安信息网向独立应用提供的基于平台的接口；

d）消息服务：每个需要消息推送的应用，应配置对应的服务号，通过服务号把消息推送出去；对于服务号的配置，通过管理平台统一创建；

e）日志服务：提供查询自身应用的日志信息接口。

9 终端系统管理规范

9.1 总体要求

终端系统管理总体要求应包括以下内容：

a）统一账号及登录验证，严格授权访问，实现单点登录等；

b）详细记录操作日志，汇聚业务采集数据，深化数据挖掘分析；

c）制定完善的研发、运维、使用、安保、共享等管理制度，并实现电子化、自动化监测和控制；

d）安全管理服务应对通信网络、区域边界、计算环境的保护部件进行标记管理、策略管理、授权管理。

9.2 终端安全管理

终端安全管理应包括以下措施：

a）终端不存储数据。所有数据应存放在云端，终端仅缓存组织架构信息，不存储业务数据；终端丢失后，安全系统应有数据自动删除机制；

b）数字证书。对需与公安信息网交换数据且可能涉及公安工作秘密的警务应用，应强制实施数字证书认证，建立专用通信路径；

c）移动终端管理管控。定制研发并在安全系统预装移动终端管理工具，提供警务应用安全沙箱和加密通讯隧道，实施终端认证和访问控制，实现远程监控、远程擦除、预警锁定、手机找回、禁止运行非可信程序等；

d）应确保连续输入 10 次错误的认证信息，自动删除本机的配置信息。

9.3 专网安全管理

专网分为终端侧、运营商侧和公安机关侧三段链路。专网安全管理应包括以下内容：

a）终端安全系统侧应限制唯一网络接入点，仅限接入公安无线虚拟专网，不可接入互联网或其他网络；

b）运营商侧由 AAA 服务器对终端进行域名、手机号码、IMSI 捆绑鉴权认证；

c）公安机关自建 AAA 服务器对终端进行严格的域名、手机号、IMSI、用户名、密令、终端串码（MEID、IMEI）、IP 地址共七项信息关联验证，并在 L2TP 网络服务器部署应用层防火墙和访问控制策略，实现安全保障。

9.4 边界安全管理

边界安全管理应包括以下内容：

a）边界访问控制。采用防火墙部件等的访问控制策略，对进出安全边界的数据信息进行控制，阻止非授权访问；采用安全隔离交换部件进行强隔离，进行安全数据交换；

b）边界包过滤。通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出边界；

c）边界安全审计。进入和流出信息流进行安全检查，禁止违反系统安全策略的信息流经过边界；实施严格、精细的安全边界日志审计，做到“记录留在边界”、入口有详细日志；

d）边界完整性保护。发现和阻断违规外联，控制节点接入，实时发现并阻断入侵行为。