ICS 35.240.01
CCS A90

SF

中华人民共和国司法行政行业标准

SF/T 0049—2020
代替 SF/T 0049—2019

司法行政移动执法系统技术规范

Technology specification of judicial administration mobile law enforcement system

2020－12－30 发布　　2020－12－30 实施

中华人民共和国司法部　　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。

本文件代替SF/T 0049—2019《司法行政移动执法系统技术规范》，与SF/T 0049—2019相比，除结构调整和编辑性改动外，主要技术变化如下：

——删除了规范性引用文件 GB/T 8702、GB/T 22451、YD/T 5120 和 YD/T 5160（见 2019 版的第 2 章）；

——修改了“司法行政移动执法系统、司法行政移动执法终端、执法模式、非执法模式和移动执法无线专网”术语的英文，删除了术语“执勤场景”和“押运场景”（见 3.1，2019 版的 3.1）；

——增加了缩略语“CE、DCS、eMTC、ESN、IMSI、IPSec、LTE、NB-IoT、NSA、P、PE、SA、SIP、TLS 和 XMPP”（见 3.2）；

——将“司法行政移动执法系统体系框架 1 和 2 ”修改为“司法行政移动执法系统体系框架Ⅰ型和Ⅱ型”（见 4.1.1，2019 版的 4.1.1）；

——将“终端设备层由司法行政移动执法终端组成”修改为“终端设备层由通用执法终端和专用执法终端组成”（见 4.1.2.2，2019 版的 4.1.2.2）；

——删除了功能要求中的“基本要求”（见 2019 版的 4.2）；

——修改了功能要求中终端功能和应用功能的有关内容（见 4.2.1 和 4.2.3，2019 版的 4.2.2 和 4.2.4）；

——将“工作效率”修改为“响应能力”，并修改了有关内容的表述方式（见 4.3.2.1、4.3.3.1 和 4.3.4.1，2019 版的 4.3.2.1、4.3.3.1 和 4.3.4.1）；

——修改了维护能力中有关内容的表述方式（见 4.3.4.3，2019 版的 4.3.4.3）；

——修改了网络安全的有关内容（见 4.4.3，2019 版的 4.4.3）；

——修改了电池要求中有关内容的表述方式（见 5.1.2，2019 版的 5.1.2）；

——修改了通用执法终端扩展配件的内容（见 5.1.3，2019 版的 5.1.3）；

——修改了机械环境适应性的内容（见 5.1.4，2019 版的 5.1.4）；

——修改了软件要求中操作系统的有关要求（见 5.1.5.1，2019 版的 5.1.5.1）；

——修改了操作系统安全技术中的有关要求（见 5.2.3，2019 版的 5.2.3）；

——将隔离安全技术的“包装”要求修改为“标示”要求（见 5.2.8.6，2019 版的 5.2.8.6）；

——终端应用管控中增加了“全程水印接口”要求（见 6.4.3.8）；

——组网技术要求的网络结构和内容中增加了“非法终端信号管控”的内容[见 8.1 e）]；

——在“非法终端信号管控”中增加了“基本要求”（见 8.5.1）；

——修改了非法终端信号管控“定位”的内容（见 8.5.2.4，2019 版的 8.5.1.4）；

——修改了非法终端信号管控“侦测性能”和“定位性能”的内容（见 8.5.3.2 和 8.5.3.3，2019 版的 8.5.2.2 和 8.5.2.3）；

——修改了通信制式与频率要求中的内容（见 8.5.4，2019 版的 8.5.3）；

——在安装安全要求中增加了“出厂预置”应用软件的要求（见 9.4.2.1）；

——在数据安全要求中增加了执法模式数据安全的要求[见 9.4.3 c）]；

——在即时通信功能要求中增加了禁止截屏录屏的要求[见 11.3.3 f）]。

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。

本文件由司法部信息中心提出并归口。

本文件起草单位：北京市监狱管理局、天津市监狱管理局、四川省监狱管理局、天津市公共安全大数据技术工程中心、天津大学、华为技术有限公司、电子科技大学、四川司法警官职业学院、苏州科达科技股份有限公司、浙江三维通信科技有限公司。

本文件主要起草人：王楠、姜其伟、徐平原、杜磊、袁宁、王学明、毋存杰、骆登耀、张力、余训锋、蒋涛、曹明生、欧幸宝、周宁、王纯。

本文件及其所代替文件的历次版本发布情况为：

——2019 年首次发布为 SF/T 0049—2019；

——本次为第一次修订。

司法行政移动执法系统技术规范

1 范围

本文件规定了司法行政移动执法系统的总体、终端、终端安全监控组件、网络接入安全体系、组网、应用开发、应用市场发布与级联以及即时通信软件互联的技术要求。

本文件适用于司法行政行业开展移动执法系统的设计、建设、管理和应用。

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 191 包装储运图示标志

GB/T 4208—2017 外壳防护等级(IP代码)

GB 4943.1 信息技术设备 安全 第1部分：通用要求

GB/T 18287 移动电话用锂离子蓄电池及蓄电池组总规范

GB/T 20279—2015 信息安全技术 网络和终端隔离产品安全技术要求

GB/T 21064 电子政务系统总体设计要求

GB/T 25068.1 信息技术 安全技术 网络安全 第1部分：综述和概念

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB 33473 即时通信业务HI接口总体技术要求

GB/T 34975—2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

GB/T 34976 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法

GB/T 35282 信息安全技术 电子政务移动办公系统安全技术规范

GB/T 37291—2019 基于LTE技术的宽带集群通信（B-TrunC）系统总体技术要求（第一阶段）

GA 450 居民身份证卡体技术规范

GA/T 1011 居民身份证指纹采集器通用技术要求

GM/T 0034 基于SM2密码算法的证书认证系统密码及其相关安全技术规范

SF/T 0008 全国司法行政信息化总体技术规范

SF/T 0028—2018 智慧监狱 技术规范

YD/T 2305 统一通信中即时通信及语音通信相关接口技术要求

YD/T 3409 基于LTE技术的宽带集群通信（B-TrunC）系统 终端设备技术要求（第一阶段）

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

司法行政移动执法系统 judicial administration mobile law enforcement system

面向司法行政业务领域，利用计算机网络技术、通信与自动化技术、音视频编解码技术以及图形图像处理技术，借助现代科学技术装备，围绕司法活动而支持各种移动执法的信息系统。

3.1.2

司法行政移动执法终端 judicial administration mobile law enforcement terminal

用于司法行政业务领域的便携式、可移动的智能设备。

注：包括通用执法终端和专用执法终端。

3.1.3

通用执法终端 general terminal for law enforcement

外观属于通用机形态的便携式、可移动的智能终端。

3.1.4

专用执法终端 professional terminal for law enforcement

外观属于专业机形态的便携式、可移动的三防智能终端。

3.1.5

执法模式 law enforcement mode

司法行政部门使用司法行政移动执法终端进行执法及行政办公类工作所采用的模式。

3.1.6

非执法模式 non law enforcement mode

司法行政部门使用通用执法终端（3.1.3）进行非执法工作所采用的模式。

3.1.7

移动执法无线专网 mobile law enforcement private wireless network

专用于承载司法行政移动执法系统（3.1.1）的无线网络。

3.1.8

执法模式操作系统 operation system for law enforcement

终端上支持执法模式（3.1.5）的操作系统。

3.1.9

非执法模式操作系统 operation system for non law enforcement

终端上支持非执法模式（3.1.6）的操作系统。

3.1.10

行政场景 executive scene

监狱监管区/戒毒的戒毒管理区区外，用于执法和办公的终端工作状态。

3.2 缩略语

下列缩略语适用于本文件。

ADB 安卓调试桥（Android Debug Bridge）
APN 接入点名称（Access Point Name）
CA 数字证书颁发机构（Certificate Authority）
CE 用户网络边缘路由器（Customer Edge）
CPU 中央处理器（Central Processing Unit）
DCS 数据传输系统（Data Communication System）
eMTC 增强机器类通信（Enhanced Machine Type Communication）
ESN 电子序列号（Electronic Serial Number）
HTTPS 超文本传输安全协议（Hypertext Transfer Protocol Secure）
ID 身份识别码（Identity）
IMEI 国际移动设备识别码（International Mobile Equipment Identity）
IMSI 国际移动用户识别码（International Mobile Subscriber Identity）
IP 互联网协议（Internet Protocol）
IPSec 互联网安全协议（Internet Protocol Security）
LTE 通用移动通信技术的长期演进（Long Term Evolution）
MAC 介质访问控制（Media Access Control）
MPLS 多协议标签交换（Multi-Protocol Label Switching）
NB-IoT 窄带物联网（Narrow Band Internet of Things）
NFC 近场通信（Near Field Communication）
NSA 非独立组网（Non-Stand Alone）
P 核心路由器（Provider）
PE 运营商边缘路由器（Provider Edge）
PKI 公钥基础设施（Public Key Infrastructure）
QoS 服务质量（Quality of Service）
SA 独立组网（Stand Alone）
SIM 客户识别模块（Subscriber Identification Module）
SIP 会话初始协议（Session Initiation Protocol）
SSID 服务集标识（Service Set Identifier）
SSO 单点登录（Single Sign On）
TLS 传输层安全（Transport Layer Security）
USIM 全球用户识别卡（Universal Subscriber Identity Module）
USB 通用串行总线（Universal Serial Bus）
VPN 虚拟专用网络（Virtual Private Network）
WLAN 无线局域网（Wireless Local Area Networks）
XMPP 可扩展通信与表示协议（Extensible Messaging and Presence Protocol）

4 总体技术要求

4.1 体系框架

4.1.1 基本要求

司法行政移动执法系统应符合 GB/T 21064 和 SF/T 0008 的规定。

司法行政移动执法系统应具备司法行政移动执法功能，满足司法行政单位的业务需求。

司法行政移动执法系统体系框架可根据适用对象的不同而分为Ⅰ型和Ⅱ型。

4.1.2 司法行政移动执法系统体系框架Ⅰ型

4.1.2.1 总体架构

司法行政移动执法系统体系框架Ⅰ型适用于司法体系内除监狱和戒毒所的其他相关单位。

司法行政移动执法系统体系框架Ⅰ型包括终端设备层、网络支撑层和移动应用层，其中终端设备层又包括通用执法终端和专用执法终端。在法规与标准规范和安全保障体系下，通用执法终端支持执法模式和非执法模式，在电子政务外网和互联网中，支持司法行政移动应用；专用执法终端应支持执法模式，在电子政务外网中，支持司法行政移动应用。司法行政移动执法系统体系框架Ⅰ型如图 1 所示。

图1 司法行政移动执法系统体系框架Ⅰ型

4.1.2.2 终端设备层

终端设备层由通用执法终端和专用执法终端组成。

通用执法终端具有执法模式和非执法模式两种模式，并能够互相切换；专用执法终端只具有执法模式。

4.1.2.3 网络支撑层

网络支撑层为司法行政移动执法终端提供网络支撑服务。在非执法模式下，通用执法终端由移动网络连接到互联网；在执法模式下，司法行政移动执法终端由虚拟无线专用网络连接到电子政务外网。

4.1.2.4 移动应用层

移动应用层支持司法行政移动执法终端的移动应用，包括办公移动应用、司法移动应用、行政移动应用、管理移动应用和大数据移动应用等。

4.1.3 司法行政移动执法系统体系框架Ⅱ型

4.1.3.1 总体架构

司法行政移动执法系统体系框架Ⅱ型适用于司法体系内监狱和戒毒所等单位。

司法行政移动执法系统体系框架Ⅱ型包括终端设备层、网络支撑层和移动应用层，其中终端设备层又包括通用执法终端和专用执法终端。在法规与标准规范和安全保障体系下，通用执法终端支持执法模式和非执法模式，执法模式在电子政务外网或监狱/戒毒内网工作，非执法模式在互联网工作，应符合SF/T 0028—2018 第5章的规定；专用执法终端应支持执法模式，在电子政务外网或监狱/戒毒内网工作。司法行政移动执法系统体系框架Ⅱ型如图 2 所示。

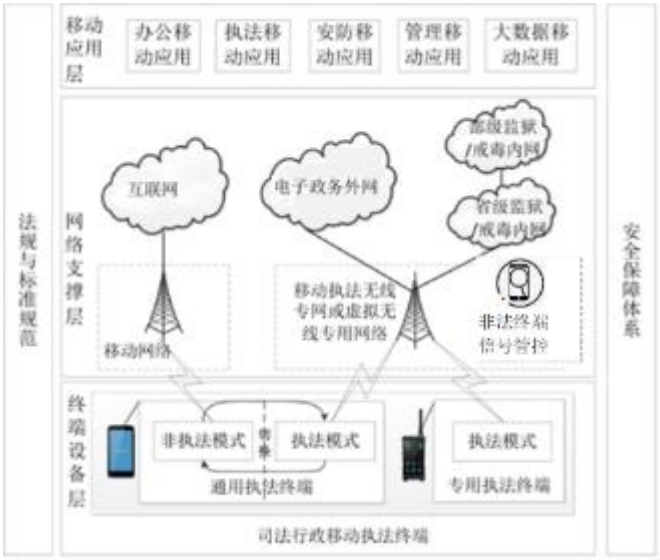

图2　司法行政移动执法系统体系框架Ⅱ型

4.1.3.2　终端设备层

终端设备层由司法行政移动执法终端组成，通用执法终端具有执法模式和非执法模式两种模式，并能够互相切换；专用执法终端应支持执法模式。

司法行政移动执法终端应纳入监狱和戒毒基础警用装备配备范围，应按在职民警全覆盖进行配备，并列入财政保障。

4.1.3.3　网络支撑层

网络支撑层为司法行政移动执法终端提供网络支撑服务。在非执法模式下，通用执法终端由移动网络连接到互联网；在执法模式下，司法行政移动执法终端由虚拟无线专用网络或移动执法无线专网连接到监狱/戒毒业务内网，可由虚拟无线专用网络或移动执法无线专网连接到电子政务外网。

4.1.3.4　移动应用层

移动应用层支持司法行政移动执法终端的移动应用，包括办公移动应用、司法移动应用、行政移动应用、管理移动应用和大数据移动应用等。

4.2　功能要求

4.2.1　终端功能

司法行政移动执法终端功能应符合但不限于以下要求：

a)　通用执法终端具备执法模式和非执法模式，并能按需定制两种模式之间的切换策略；

b)　专用执法终端具备执法模式。

4.2.2 网络功能

司法行政移动执法系统网络功能应符合但不限于以下要求：

a) 具备快速、准确、可靠和安全的传输语音、文字、图像和视频信号等功能；
b) 具备网络管控能力，包括终端管控、设备管控、通话管控和应用管控等功能。

4.2.3 应用功能

司法行政移动执法系统应根据业务需求选用但不限于以下功能：

a) 移动安防功能，包括视频监控、门禁监控、一键报警、应急预案、可视化调度、即时通信、警力部署、定位跟踪和语音对讲等功能；
b) 移动办公功能，包括文件收发、文件管理、行政申请、行政审批、协同办公和视频会议等功能；
c) 移动执法功能，包括视频执法、移动取证、执法办案、执勤值守、应急指挥、收治管理、调动调遣、外出管理、教育矫治、生活卫生和生产劳动等功能；
d) 移动执法管理功能，建立司法行政移动应用市场，形成分级统一的应用分发平台，严格审核标准，对司法行政移动执法系统应用程序进行安全管控。

4.3 性能要求

4.3.1 基本要求

移动执法系统应在响应能力、信息维护和使用能力等方面满足基本的系统整体性、协同性、可靠性、可控性、可用性和可维护性等指标和检测要求，达到预期的系统使用效果。

4.3.2 终端性能

4.3.2.1 响应能力

终端响应能力应符合但不限于以下要求：

a) 终端启动时间≤60s；
b) 终端运行模式切换时间≤30s；
c) 终端对于可用功能模块的接入时间≤30s。

4.3.2.2 访问能力

终端访问能力应符合但不限于以下要求：

a) 终端具有在不同运行模式下受控访问移动网络、专用网络或内部网络信息资源的能力；
b) 终端可访问多种受控接口，具有文字、声音、图像和视频等信息资源的采集能力。

4.3.2.3 维护能力

终端维护能力应符合但不限于以下要求：

a) 终端具备对硬件外设接口的维护、升级和扩展能力；
b) 终端具有白名单应用控制能力；
c) 系统具有终端设备接入控制能力；
d) 系统具有终端设备注销能力。

4.3.2.4 使用能力

终端使用能力应符合但不限于以下要求：

a) 终端支持系统运行模式的主动或被动切换；
b) 终端硬件性能保证至少 2 年内符合操作系统及业务系统的运行配置标准。

4.3.3 网络性能

4.3.3.1 响应能力

网络响应能力应符合但不限于以下要求：
a) 网络接入速率符合司法行政移动执法系统各场景下的网络信息通信性能需求；
b) 网络认证及模式切换响应时间满足实时性要求。

4.3.3.2 访问能力

网络访问能力应符合但不限于以下要求：
a) 网络可容纳访问的最大用户数应超过部署场景下所有可能在线的用户并发访问需求；
b) 在网络允许覆盖区域，网络接入性能符合国家及相关行业标准。

4.3.3.3 维护能力

网络维护能力应符合但不限于以下要求：
a) 保证网络信息传输过程中的数据准确性、完整性和实时性；
b) 专网及内部网络设计兼顾实用性与经济性，符合相关标准；
c) 网络制式方便扩展和升级，参数自适应调整。

4.3.3.4 使用能力

网络使用能力应符合但不限于以下要求：
a) 网络运行稳定，保证 7×24h 服务模式；
b) 专网或内部网络可容纳用户数应超过当前业务所需及未来 3 年可能融入业务的用户总数；
c) 网络通信带宽应符合各场景下的多源数据并发流转需求，符合业务系统总体通信标准。

4.3.4 应用性能

4.3.4.1 响应能力

应用系统响应能力应符合但不限于以下要求：
a) 常规应用业务系统启动时间≤10s，综合业务系统启动时间≤30s；
b) 在规定的并发用户数范围内，对于系统的一项操作请求，简单应用平均响应时间≤3s，一般应用平均响应时间≤10s，复杂应用平均响应时间≤30s，最大响应时间均≤60s；
c) 应用系统常规查询类业务平均周转时间≤30s，数据分析类业务平均周转时间≤4h，系统维护类业务平均周转时间≤12h，最大周转时间均≤24h。

4.3.4.2 访问能力

应用系统访问能力包括但不限于以下要求：
a) 应用系统支持的可并发访问的最大用户数应超过可能在线的终端用户的并发访问需求；
b) 应用系统支持的最大信息交互数应超过所有可能在线的终端用户的信息交互总体需求量。

4.3.4.3 维护能力

应用系统维护能力应符合但不限于以下要求：

a) 保证应用系统内信息流转的准确性，信息准确率≥99%；
b) 保证应用系统的信息完整性，信息完整率≥90%；
c) 保证应用系统的信息实时性，信息更新及时率≥95%；
d) 保证应用系统的日常运维管理，应用软件支持≥1 年的运维保障服务。

4.3.4.4 使用能力

使用能力应符合但不限于以下要求：
a) 应用软件系统运行稳定，保证 7×24h 服务模式，支持在线升级；
b) 应用软件系统可容纳用户数应超过当前业务所需及未来 3 年可能融入业务的用户总数；
c) 应用软件系统数据存储最小容量达到 PB 级。

4.4 安全要求

4.4.1 基本要求

司法行政移动执法系统应在终端硬件安全、软件安全和网络安全等方面满足国家相关安全指标和检测要求，符合系统使用安全规范。应符合但不限于以下要求：
a) 移动执法系统总体安全防护机制符合 GB/T 25070 的规定；
b) 移动执法系统移动办公符合 GB/T 35282 的规定；
c) 移动执法终端和网络交换设备符合国家强制性产品认证要求；
d) 信息和网络安全符合 GB/T 25068.1 的规定；
e) PKI/CA 身份认证系统符合 GM/T 0034 的规定。

4.4.2 终端安全

司法行政移动执法终端安全应符合但不限于以下要求：
a) 国家强制性产品认证及工业和信息化部设备入网要求；
b) 硬件电路设计运行自主可控；
c) 硬件功能接口安全可控；
d) 操作系统关键代码宜自主可控；
e) 具备不同工作模式的操作系统、应用程序、数据和接口的安全隔离；
f) 具备安全管控模块，支持操作权限变更、系统模块可信接入和敏感数据隔离访问等管理监控机制；
g) 具备 PKI/CA 终端存储数字证书和认证算法；
h) 具备设备生命周期管理和设备远程控制，如：远程锁定和远程擦除等功能。

4.4.3 网络安全

司法行政移动执法系统网络安全应按不低于第三级网络安全等级保护要求进行建设，包括但不限于以下要求：
a) 不同安全等级应用场景下操作系统的网络覆盖和连接应做到连续、无缝；
b) 不同安全等级的网络边界实施应符合国家标准的边界隔离技术，支持对访问终端、设备、机构和工作人员的数字证书身份认证，并支持远程或空中证书发放；
c) 应具备网络访问安全控制能力，能够管理访问者访问权限；
d) 网络数据传输宜具有加密能力。

4.4.4 应用安全

司法行政移动执法系统应用安全应符合但不限于以下要求：

a) 预装终端安全监控组件，全程后台运行；
b) 应用市场规范化准入；
c) 应用软件权限全程可控，能控制应用软件对移动终端中资源的访问；
d) 应用安全可支持数字证书，核查允许使用的数字证书，防止二次打包。

5 终端技术要求

5.1 通用技术要求

5.1.1 硬件要求

5.1.1.1 基本要求

硬件包括但不限于以下要求：

a) 通过国家相关认证和许可要求，具备工信部颁发的电信设备进网许可证、无线电发射设备型号核准证以及中国质量认证中心出具的国家强制性产品认证证书；
b) 选择国产智能终端；
c) 具备可信根，可信根具有板载独立可信芯片、密码芯片及可信执行环境结合配套固件、密码卡结合配套软件三种形态。

5.1.1.2 唯一可标识性

应具有标识硬件唯一性的标志号，如IMEI、序列号(S/N)等，且不可被更改。

5.1.1.3 硬件功能

硬件配置应保证操作系统和终端应用的正常运行，硬件宜根据实际需要选择但不限于以下功能：

a) 人机交互和显示；
b) 移动数据通信；
c) 移动语音通信；
d) 蓝牙、WLAN 和 NFC 等短距离无线通信；
e) 数据存储；
f) 拍照和摄像；
g) 通用执法终端支持生物特征识别；
h) 专用执法终端支持集群组呼（PTT）；
i) 国密 CPU 卡、IC 卡、ID 卡动态绑定，实现一卡通。
j) 一键报警；
k) 支持北斗定位。

5.1.2 电池要求

电池要求如下：

a) 安全保护性能应符合 GB/T 18287 的规定；
b) 不可拆卸电池容量≥3800mAh；
c) 最长充电时间≤4h。

5.1.3 通用执法终端扩展配件

5.1.3.1 基本要求

通用执法终端宜具备扩展配件的能力，基本要求如下：

a) 通用执法终端宜配备扫描器模块、二代身份证模块、卫星通信模块和三防模块等扩展性配件；
b) 通用执法终端扩展配件可采用独立式或背夹式。

5.1.3.2 扩展配件基本功能

扩展配件应支持终端充电功能，并具备以下基本功能：

a) 扫描器模块用于读取条码标签所包含的一维和二维等信息；
b) 二代身份证模块符合 GA 450 的规定，无需网络即可读取身份证信息；
c) 卫星通信模块支持天通卫星移动通讯网络语音和短信功能。

5.1.4 机械环境适应性（跌落性能指标）

机械环境适应性宜符合以下要求：

a) 通用执法终端六面能承受 1m 高度跌落至水泥地面的冲击，符合 GB/T 4208—2017 中的 IP65 及以上等级要求， 并通过国家级认证及实验室检测；
b) 专用执法终端能承受 1.2m 高度跌落至水泥地面的冲击，符合 GB/T 4208—2017 中的 IP67 及以上等级要求。

5.1.5 软件要求

5.1.5.1 操作系统

操作系统要求如下：

a) 通用执法终端应支持双操作系统（双域），其中执法模式操作系统支持执法模式，不可接入互联网；非执法模式操作系统支持非执法模式，可接入互联网。专用执法终端可采用单操作系统，且仅支持执法模式；
b) 通用执法终端的执法模式操作系统宜采用具有自主知识产权的国产操作系统，非执法模式操作系统不作国产化要求；
c) 通用执法终端的两个系统应独立运行，可相互切换；
d) 通用执法终端的两个系统应分别有独立的、差异化的人机交互界面，包括但不限于系统桌面、状态栏、快捷面板、锁屏和安装应用界面。

5.1.5.2 开关机

开关机应符合以下要求：

a) 具备定制开机动画的能力；
b) 执法模式操作系统具备定制桌面壁纸的能力；
c) 进入执法模式操作系统强制身份验证。

5.1.5.3 系统/场景切换

系统/场景切换要求如下：

a) 司法行政移动执法系统体系框架Ⅰ型中，通用执法终端应支持非执法模式操作系统和执法模式操作系统，执法模式操作系统仅包含行政场景。两个系统应具备手动或自动切换能力，宜具备指纹或快捷按钮切换的方式；

b) 司法行政移动执法系统体系框架Ⅱ型中，通用执法终端应支持非执法模式操作系统和执法模式操作系统，执法模式操作系统宜包含行政场景、执勤场景和押运场景。两个系统和三个场景都应具备后台和自动切换能力，自动切换能力应不受关机和重启影响。司法行政移动执法系统体系框架 Ⅱ型中通用执法终端的场景切换关系如图 3 所示；

注1：执勤场景是指监狱/戒毒监管区内，用于执法和办公的终端工作状态。

注2：押运场景是指监狱/戒毒监管区外，用于押运过程中的终端工作状态。

c) 通用执法终端应支持场景记忆功能，当终端重启后，终端自动进入重启前的场景。

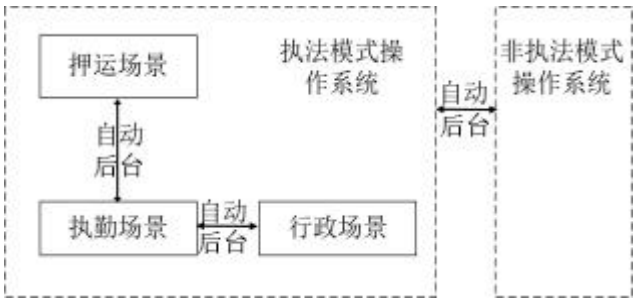

图3 司法行政移动执法系统体系框架Ⅱ中通用执法终端的场景切换关系

5.1.5.4 系统升级

系统升级应符合以下要求：

a) 系统可通过空中下载（OTA）进行升级，升级包具备合法性校验功能；

b) 司法行政移动执法终端禁止刷机成普通消费者版本。

5.1.5.5 应用管理

执法模式操作系统应支持但不限于以下功能：

a) 应用防终止、防挂起和防卸载；

b) 对应用的安装进行控制和管理；

c) 阻止或恢复指定应用运行。

5.1.5.6 通话

执法模式操作系统应具备语音电话和短信的白名单功能，禁止拨打和接听白名单外的电话，禁止收发白名单外的短信。

5.1.5.7 一键报警

执法模式应支持一键报警功能，应具备终端位置信息和周边音视频信息上报的能力。

5.1.5.8 机、卡绑定

应支持终端和SIM/USIM卡绑定使用，具备检测非法SIM/USIM 卡功能。

5.1.5.9 集群通信

专用执法终端应符合 YD/T 3409 的要求。

5.2 安全技术要求

5.2.1 安全技术体系

执法模式操作系统的安全技术体系应包括硬件安全、操作系统安全、应用层安全、外围接口安全、网络连接安全、用户数据安全和隔离安全。

非执法模式操作系统的安全技术规范应符合 GB/T 34976 的规定。

5.2.2 硬件安全技术

硬件安全技术应符合以下要求：

a) 整机硬件电路安全可控，无未知功能的部件或模块；
b) 安全启动应基于可信根对司法行政移动执法终端启动过程中涉及到的可执行实体进行静态度量，可执行实体至少覆盖引导程序、系统镜像、系统内核及关键应用；如果度量对象被篡改，则自动终止启动。

5.2.3 操作系统安全技术

操作系统安全技术应符合以下要求：

a) 防止超级管理员权限被非法获取；
b) 不存在已知高危系统漏洞；
c) 具有病毒入侵检测和防护能力；
d) 应提示网络连接状态；
e) 应提示网络数据传送状态；
f) 禁止向国外的未知和未授权服务器发送个人信息，包括但不限于：键盘或手写输入信息、用户位置信息、MAC 或 IP 地址和硬件标识信息；
g) 应支持开机和锁定的密码保护功能；
h) 不以明文的方式保存和传送口令，输入口令时应禁止明文回显；
i) 支持设备超时锁定及手动锁定功能；
j) 关键代码自主可控，包括但不限于图形子系统、多媒体子系统、电话子系统、应用管理子系统、系统核心服务、安全子系统和设备子系统；
k) 对操作系统进行可信动态度量。

5.2.4 应用层安全技术

应用层安全技术应符合以下要求：

a) 预装司法行政移动执法终端安全监控组件，不可被卸载和删除；
b) 对应用安装包或更新包进行来源检查和完整性检查；
c) 禁止安装与司法行政移动执法系统业务无关的各类应用；
d) 具备开机自启动应用的监控和配置功能；
e) 对应用进行静态度量：在应用启动时按基准值检查其完整性，若应用的完整性被破坏，则阻止其运行。

5.2.5 网络连接安全技术

网络连接安全技术应符合以下要求：

a) 执法模式操作系统下 WLAN 仅可用于采集热点信息，禁止连接无线局域网、开启热点和相互直连；
b) 具备禁止用户手动关闭数据网络连接的功能，防止脱离后台监管；

c） 通过预置 IP 访问策略，限制用户仅能访问授权的网络地址。

5.2.6 外围接口安全技术

外围接口包括但不限于蓝牙、USB 和NFC，应符合以下安全技术要求：

a） NFC 可通过管控接口配置是否开启；

b） 通过预置蓝牙连接策略或管控接口配置；

c） 通过预置 USB 接口策略或管控接口配置。

5.2.7 用户数据安全技术

用户数据安全技术应符合以下要求：

a） 保证用户数据不能被未授权用户查询、修改和删除；

b） 支持用户数据彻底删除功能，删除的数据无法再恢复；

c） 支持远程锁定司法行政移动执法终端和销毁终端上的数据；

d） 具备文件类用户数据的授权访问功能，未经用户确认未授权应用禁止访问受保护的任何文件类用户数据；

e） 执法模式操作系统切换到非执法模式操作系统时应删除执法模式操作系统内的临时文件。

5.2.8 隔离安全技术

5.2.8.1 运行隔离安全技术

运行隔离安全技术应符合以下要求：

a） 各系统分别有独立的文件系统且彼此隔离，禁止互相访问；

b） 各系统间的进程彼此隔离，不同系统中的进程互不可见；

c） 各系统下进程生成的数据彼此隔离，禁止互相访问；

d） 各系统下存储区彼此隔离、禁止互相访问；

e） 各系统使用不同加密存储密钥；

f） 各系统支持独立设置解锁方式和解锁密码；

g） 各系统的管控接口彼此隔离。

5.2.8.2 应用层隔离安全技术

应用层隔离安全技术应符合以下要求：

a） 应用在各系统独立的文件系统下安装、卸载、运行和管理；

b） 各系统下的应用及依赖的运行库相互隔离，且仅能在自身所在的系统下运行，禁止跨系统访问，仅支持执法模式操作系统向非执法模式操作系统进行单向消息提示。

5.2.8.3 网络连接隔离安全技术

网络连接隔离安全技术应符合以下要求：

a） 各系统的网络彼此隔离，禁止跨系统使用对方网络；

b） 执法模式操作系统仅能通过虚拟无线专用网络或无线专网接入司法行政移动执法系统，非执法模式操作系统仅能接入互联网。

5.2.8.4 外围接口隔离安全技术

外围接口隔离安全技术应符合以下要求：

a) 各系统下的外围接口单独管控；
b) 禁止通过蓝牙、NFC 等外围接口进行系统间数据摆渡；
c) 禁止通过外接存储设备进行系统间数据摆渡。

5.2.8.5 用户数据隔离安全技术

用户数据隔离安全技术应符合以下要求：

a) 各系统的用户数据彼此隔离，禁止互相访问，包括但不限于图片、视频、音频和文档、电话本数据、通话记录、短信数据和彩信数据；
b) 执法模式操作系统禁止写 SIM/USIM 卡联系人。

5.2.8.6 标示

标示应符合以下要求：

a) 包装盒上有产品名称和型号、制造商名称、地址、商标名称和注册商标图案等标记；
b) 包装盒内有使用说明书、检验合格证明、保修单、装箱明细单及有关的随机资料；
c) 根据产品大小选用规格合适的包装箱，包装箱上应印有产品名称和型号、制造商名称、数量、出厂日期、质量及防护要求，运输包装标志应符合 GB/T 191 的规定；
d) 采取防潮、防压、防撞和减震等措施，确保正常装卸、运输和贮存不会对司法行政移动执法终端造成损坏。

6 终端安全监控组件技术要求

6.1 运行环境

安全监控组件运行于执法终端，与服务后台构成一个封闭的终端管控平台，安全监控组件运行环境如图 4 所示。要求如下：

a) 安全监控组件：负责终端注册、终端登录、管控策略解析执行及结果上报、终端信息采集上报、安全事件监测上报和模式切换上报等；
b) 终端安全管理子系统：负责终端管控策略的制订、下发及结果展示，终端信息和安全事件的汇总展现；
c) 终端安全管控数据库：独立于终端安全管理子系统的标准信息汇总、分析及服务子系统，负责策略执行结果、安全事件、终端信息和终端安全管理子系统日志等的汇总，以及以汇总信息为基础的标准数据服务。

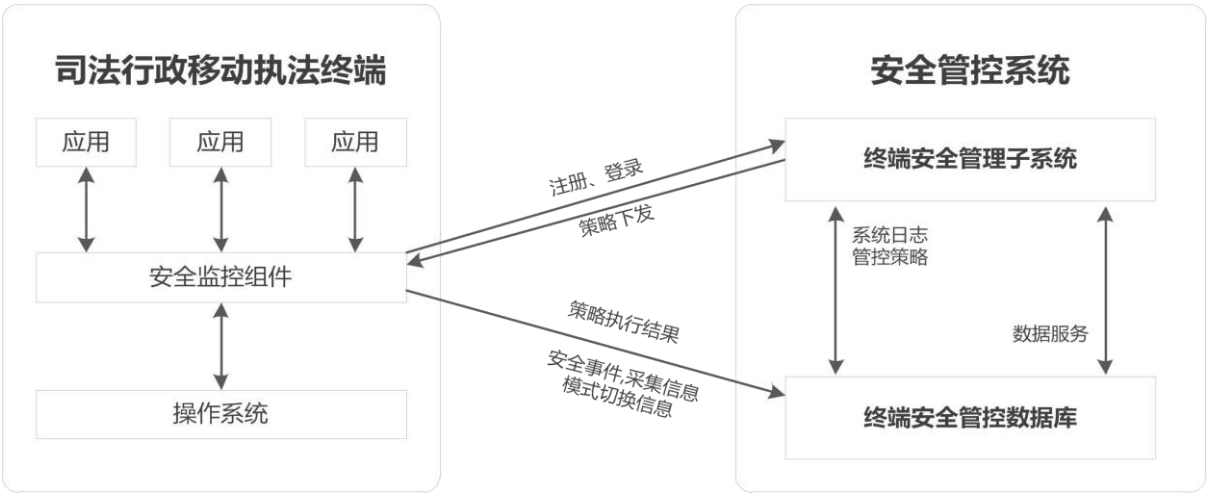

图4　安全监控组件运行环境

6.2　通用要求

6.2.1　基本要求

安全监控组件应具备管控策略来源可信的验证能力，策略执行应不受干扰而中断，策略管控应正确有效且不可被旁路。

6.2.2　传输安全

安全监控组件与终端安全管理子系统、终端安全管控数据库之间的通讯均应采用加密方式，包括但不限于使用HTTPS协议。

6.2.3　存储安全

安全监控组件如需在终端持久存储数据应采用国产密码算法对机密性和完整性进行保护，持久存储数据包括但不限于管控策略集。

6.2.4　运行保护

终端预装安全监控组件，应随终端启动而自动运行，不能被用户或其他终端应用强行终止、修改和卸载。

6.2.5　完整性保护

安全监控组件应至少在启动过程中进行必要文件的完整性检查。

6.3　功能要求

6.3.1　参数设置

注册参数应包含服务器IP地址、端口号和APN配置参数。可通过但不限于以下方式设置：

a)　安全监控组件安装包预置；

b)　安全监控组件接收包含注册参数的二维码，此二维码由终端安全管理子系统产生。

6.3.2　注册

注册应符合以下要求：

a) 能采集并提交终端软硬件信息，包括但不限于终端厂商、终端品牌、终端型号、终端标识、CPU型号、操作系统版本、组件版本、SIM 卡标识、终端密码模块编号、数字证书序列号和用户标识；
b) 能校验授权信息。

6.3.3 登录

应能采集并提交终端软硬件信息，包括但不限于终端厂商、终端品牌、终端型号、终端标识组件版本、SIM卡标识、终端密码模块编号、数字证书序列号和用户标识，验证通过则终端登录，失败则应显示原因。

6.3.4 策略更新

策略更新应符合以下要求：

a) 至少支持全量或增量两种更新方式之一；
b) 对管控策略的完整性进行校验。

6.3.5 策略解析及执行

安全监控组件应按数据包解析管控策略，并调用终端管控接口以实现管控能力。

6.3.6 执行结果反馈

安全监控组件应具备上报策略执行结果的能力。

6.4 管控要求

6.4.1 硬件模块管控

6.4.1.1 WLAN 控制

WLAN控制应支持以下方式：

a) 禁止使用：不允许终端使用 WLAN 功能；
b) 仅 WLAN 指纹扫描：仅允许终端扫描 WLAN 指纹，但无法接入 WLAN 无线网络。

6.4.1.2 移动数据网络控制

移动数据网络控制应支持以下方式：

a) 强制关闭：强制关闭终端的移动数据网络，且不允许开启；
b) 强制开启：强制开启终端的移动数据网络，且不允许关闭；
c) 不管控：允许用户自主控制终端移动数据网络的开关。

6.4.1.3 蓝牙控制

蓝牙控制应支持以下方式：

a) 禁止使用：不允许终端使用蓝牙功能；
b) 受限使用：宜支持接入指定的蓝牙设备。

6.4.1.4 NFC 控制

NFC控制应支持以下方式：

a) 禁止使用：不允许终端使用 NFC 功能；
b) 强制开启：强制开启终端的 NFC 功能，且不允许关闭；
c) 不管控：允许用户自主控制 NFC 功能的开关。

6.4.1.5 定位服务控制

定位服务控制应支持以下方式：
a) 禁止使用：禁止终端开启和使用定位服务；
b) 强制开启：强制开启终端的定位服务，且不允许关闭；
c) 不管控：允许用户自主开关和使用定位服务。

6.4.1.6 USB 工作模式控制

USB工作模式控制应支持以下方式：
a) 仅充电：仅允许充电模式，不允许使用其它模式；
b) 不管控：允许终端使用硬件所支持的所有 USB 工作模式，如媒体传输协议（MTP）模式、图片传输协议（PTP）模式和主机（HOST）模式等。

6.4.1.7 扩展存储访问控制

扩展存储包括但不限于通过USB的移动设备交换数据模式（OTG）连接的存储设备、通过Micro SD接口连接的存储卡，其访问控制宜支持以下方式：
a) 禁止使用：不允许终端对扩展存储进行读、写操作；
b) 受限使用：仅允许终端对扩展存储进行读操作；
c) 不管控：允许终端对扩展存储进行读、写操作。

6.4.1.8 摄像头控制

摄像头控制对终端所有摄像头进行统一控制，应支持以下方式：
a) 禁止使用：不允许终端使用摄像头；
b) 不管控：不对终端使用摄像头进行控制。

6.4.1.9 麦克风控制

麦克风控制宜支持以下方式：
a) 禁止使用：不允许终端使用麦克风；
b) 不管控：不对终端使用麦克风进行控制。

6.4.1.10 扬声器控制

扬声器控制宜支持以下方式：
a) 禁止使用：不允许终端使用扬声器；
b) 不管控：不对终端使用扬声器进行控制。

6.4.1.11 闪光灯控制

闪光灯控制宜支持以下方式：
a) 禁止使用：不允许终端使用闪光灯；
b) 不管控：不对终端使用闪光灯进行控制。

6.4.2 终端基本功能管控

6.4.2.1 通话功能控制

通话功能控制应支持以下方式：

a) 禁止使用：不允许终端拨打和接听电话；
b) 受限使用：只允许拨打和接听准许列表中的电话号码；
c) 不管控：不对终端拨打和接听电话进行控制。

6.4.2.2 短信（含彩信）功能控制

短信（含彩信）功能控制应支持以下方式：

a) 禁止使用：不允许终端发送和接收短信（含彩信）；
b) 受限使用：只允许发送和接收准许列表中的电话号码清单；
c) 不管控：不对终端发送和接收短信（含彩信）进行控制。

6.4.2.3 APN 管理功能控制

APN管理功能控制应支持以下方式：

a) 禁止使用：不允许用户增加、删除、修改、查看 APN 配置以及选择 APN；
b) 受限使用：仅允许用户查看 APN 配置，但不允许其他操作；
c) 不管控：不限制用户对 APN 配置的管理操作，包括增加、删除、修改、查看 APN 配置以及选择 APN。

6.4.2.4 网络访问规则控制

网络访问规则控制应支持对目标网络、主机进行访问控制，规则应对目标IP地址、网络掩码、端口、协议和是否允许访问等进行描述。

6.4.2.5 锁屏密码方式控制

锁屏密码方式控制应支持以下方式：

a) 启用混合密码方式：强制要求设置数字、字母混合的具有指定长度的解锁密码；
b) 启用纯数字密码方式：强制要求设置仅包含数字的具有指定长度的解锁密码；
c) 启用生物识别技术：强制要求开启生物识别技术，如：指纹识别、虹膜识别和人脸识别等；
d) 不管控：对锁屏密码方式不进行控制，允许用户自行选择。

6.4.2.6 恢复出厂功能控制

恢复出厂功能控制应支持以下方式：

a) 禁止使用：不允许用户通过系统菜单对终端进行恢复出厂操作；
b) 不管控：允许用户通过系统菜单对终端进行恢复出厂操作。

6.4.2.7 开发调试模式控制

开发调试模式控制应支持以下方式：

a) 禁止使用：不允许终端使用 USB 调试模式；
b) 不管控：不限制终端对 USB 调试模式的使用。

6.4.2.8 应用 ADB 方式安装/卸载功能控制

应用 ADB 方式安装/卸载功能控制宜支持以下方式：

a) 禁止使用：不允许使用 ADB 方式安装/卸载终端应用；
b) 开放使用：允许使用 ADB 方式安装/卸载终端应用。

6.4.2.9 截屏功能控制

截屏功能控制宜支持以下方式：

a) 禁止使用：不允许终端使用截屏功能；
b) 不管控：不对终端截屏功能进行控制。

6.4.2.10 网络共享功能控制

网络共享功能控制宜支持以下方式：

a) 禁止使用：不允许终端使用网络共享功能；
b) 受限使用：网络共享功能启用后，仅允许准许设备列表中指定的设备通过蓝牙接入共享网络，列表描述了接入设备的蓝牙 MAC 地址。

6.4.2.11 时间设置功能控制

时间设置功能控制宜支持以下方式：

a) 强制使用网络时间：强制同步移动通讯网络时间，不允许用户或应用修改本地时间及时间来源；
b) 不管控：允许用户或终端应用修改本地时间，或设定时间来源。

6.4.2.12 系统升级功能控制

系统升级功能控制宜支持以下方式:

a) 禁止使用：不允许用户通过系统菜单对当前系统/使用模式进行升级操作；
b) 不管控：允许用户通过系统菜单对当前系统/使用模式进行升级操作。

6.4.2.13 应用交互安装/卸载接口控制

应用交互安装/卸载接口控制宜支持以下方式：

a) 禁止使用：不允许任何终端应用调用应用交互安装/卸载接口；
b) 授权使用：仅允许授权列表中的终端应用调用应用交互安装/卸载接口，授权列表应包含但不限于被授权应用的包名和签名证书指纹值；
c) 开放使用：允许所有应用调用应用交互安装/卸载接口。

6.4.2.14 应用静默安装/卸载接口控制

应用静默安装/卸载接口控制宜支持以下方式：

a) 禁止使用：不允许任何终端应用调用应用静默安装/卸载接口；
b) 授权使用：仅允许授权列表中的终端应用调用应用静默安装/卸载接口，授权列表应包含但不限于被授权应用的包名和签名证书指纹值；
c) 开放使用：允许所有应用调用应用静默安装/卸载接口。

6.4.3 终端应用管控

6.4.3.1 应用强制安装

自动下载并静默安装列表中的终端应用，强制安装列表应包含但不限于应用包名、签名证书指纹值

和应用下载地址。

6.4.3.2 应用运行控制

应用运行控制应支持以下方式：

a) 禁止运行：不允许运行列表中的终端应用，禁止运行列表应包含但不限于应用包名和签名证书指纹值；

b) 强制运行：强制运行列表中的终端应用如已安装则强制运行，并保护其运行不被用户或其他应用中断，强制运行列表应包含但不限于应用包名、签名证书指纹值、应用组件或服务。

6.4.3.3 应用更新控制

应支持以列表形式控制应用的强制更新。对于满足列表条件的应用，应自动下载并静默更新。强制更新列表应包含但不限于应用包名和签名证书指纹值、更新包下载地址。

6.4.3.4 应用卸载控制

应用卸载控制应支持以下方式：

a) 禁止卸载：不允许卸载列表中的终端应用，禁止卸载列表应包含但不限于应用包名和签名证书指纹值；

b) 强制卸载：静默卸载列表中的终端应用，强制卸载列表应包含但不限于应用包名和签名证书指纹值。

6.4.3.5 应用安装白名单控制

应用安装白名单控制可支持以下方式：

a) 禁止安装：不允许安装列表中的终端应用，禁止安装列表应包含但不限于应用包名和签名证书指纹值；

b) 允许安装：仅允许安装列表中的终端应用，允许安装列表应包含但不限于应用包名和签名证书指纹值。

6.4.3.6 应用保活控制

处于运行状态的终端应用宜保持激活。

6.4.3.7 应用权限控制

宜支持对终端应用的权限进行统一控制，应用权限包括但不限于表1所枚举的项目，应用权限仅说明该应用对指定功能是否有权限使用，其真正使用还受限于对应功能的管控。

表1 应用权限项列表

序号	类别	权限项	描述	取值范围
1	信息获取	获取终端唯一标识（IMEI）或移动设备识别码（MEID）或计算机身份识别号码（CID）	是否允许该应用读取本机	允许/禁止/询问用户
2	应用运行	开机自启动	是否允许系统启动时调用该应用	允许/禁止/询问用户
3		应用后台运行	是否允许应用后台运行	允许/禁止/询问用户

表1（续）

4	电话	拨打电话	是否允许该应用拨打电话	允许/禁止/询问用户
5		读取通话记录	是否允许该应用读取通话记录	允许/禁止/询问用户
6		修改通话记录	是否允许该应用修改通话记录	允许/禁止/询问用户
7		删除通话记录	是否允许该应用删除通话记录	允许/禁止/询问用户
8		读取联系人数据	是否允许该应用读取联系人	允许/禁止/询问用户
9		写入联系人数据	是否允许该应用增加、删除和修改联系人	允许/禁止/询问用户
10	网络和定位	开启移动数据网络	是否允许该应用开启移动数据网络	允许/禁止/询问用户
11		访问移动数据网络	是否允许该应用使用移动数据网络	允许/禁止/询问用户
12		开启WLAN	是否允许该应用开启WLAN	允许/禁止/询问用户
13		使用WLAN	是否允许该应用使用WLAN（如WLAN指纹扫描）	允许/禁止/询问用户
14		开启蓝牙	是否允许该应用开启蓝牙	允许/禁止/询问用户
15		开启NFC	是否允许该应用开启NFC	允许/禁止/询问用户
16		获取定位	是否允许该应用获取定位信息	允许/禁止/询问用户
17	多媒体	录音	是否允许该应用进行录音	允许/禁止/询问用户
18		截屏	是否允许该应用进行截屏	允许/禁止/询问用户
19		拍照	是否允许该应用进行拍照	允许/禁止/询问用户
20		摄像	是否允许该应用进行摄像	允许/禁止/询问用户
21	应用安装信息	读取已安装应用列表	是否允许该应用读取已安装应用列表	允许/禁止/询问用户

6.4.3.8 全程水印接口

应支持配置全程水印接口，可配置全程水印的显示内容和显示位置，且全程水印一旦开启，在移动执法终端任何显示页面背景均应显示背景水印内容，包括桌面、所有系统应用和第三方应用运行时的页面显示。

6.4.4 监测采集管控

6.4.4.1 软件安装信息上报控制

应支持对终端所有应用安装信息的上报，应用安装信息包括但不限于应用名称、应用包名、应用签名证书指纹值、安装时间、当前版本和开发商等。

6.4.4.2 超级权限状态上报控制

应支持对终端超级权限状态的监测，并在发现终端被获得最高管理权限或强制管理员权限登录时，及时进行权限状态上报。

6.4.4.3 硬件合规监测控制

应支持对终端加装硬件模块的监测，加装硬件模块包括但不限于SIM/USIM卡和终端密码模块。如发现加装硬件模块变更，则进行提示、告警及合规管控处理，并作为安全事件进行上报。合规管控处理包括但不限于锁定终端、关闭终端和擦除数据。

6.4.4.4 登录失败监测控制

应支持对终端登录失败行为进行监测。如发生登录失败，则进行提示、告警及合规管控处理，合规

管控处理包括但不限于锁定终端、关闭终端和擦除数据。

6.4.4.5 互联网联通监测控制

在执法模式操作系统下，应能主动对终端与互联网的联通性进行监测。如发现联通，应主动断开对应的网络连接方式（如无线网络、移动数据网络），并形成安全事件进行上报。

6.4.4.6 终端失联监测控制

应支持对终端不同程度的失联行为进行监测及处理。当注册终端在预定期限内未进行登录时，组件应判定该终端处于相应程度的失联状态，并自动执行合规管控处理，包括但不限于提示及合规管控处理，合规管控处理包括但不限于锁定终端、关闭终端和擦除数据。

6.4.4.7 终端硬件信息上报控制

宜支持对终端硬件信息的上报，硬件信息包括但不限于终端厂商、终端型号、CPU型号、运行内存容量、内部存储容量、屏幕分辨率、支持的移动网络制式、无线网卡芯片型号、蓝牙芯片型号、NFC芯片型号和定位芯片型号等。

6.4.4.8 应用耗电量上报控制

宜支持指定应用或应用集合在指定时间范围内每个应用消耗电量的上报。

6.4.4.9 应用合规监测控制

宜支持对应用安装、运行、卸载和应用权限使用的违规行为进行监测。如发现违规行为，则进行提示、告警及合规管控处理，并作为安全事件进行上报。合规管控处理包括但不限于锁定终端、关闭终端和擦除数据。

6.4.4.10 应用流量上报控制

宜支持指定应用或应用集合在指定时间范围内每个应用网络流量的上报。

6.4.4.11 应用运行时长上报控制

宜支持指定应用或应用集合在指定时间范围内每个应用前台运行时间的上报。

6.4.4.12 应用运行异常上报控制

宜支持指定应用或应用集合在指定时间范围内每个应用运行异常次数的上报。

6.4.4.13 系统完整性监测控制

宜支持对终端系统完整性状态的监测。如通过系统接口查询发现终端系统完整性被破坏时，则进行提示、告警及合规管控处理，并作为安全事件进行上报。合规管控处理包括但不限于锁定终端、关闭终端和擦除数据。

6.4.5 场景管控

6.4.5.1 场景切换控制

场景切换控制应支持以下方式：

a) 禁止切换：不允许用户切换系统；

b） 不管控：允许用户切换系统。

6.4.5.2 场景切换

场景切换应支持以下方式：

a） 主动/被动感应近场通信媒介时，执行切换终端到对应的使用场景；
b） 感知到无线感应装置时，执行切换终端到对应的使用场景；
c） 接收到系统使用场景切换指令时，执行切换终端到指定使用场景；
d） 满足其它管控策略中围栏条件时，执行切换终端到对应的使用场景。

6.4.6 管控策略围栏

6.4.6.1 时间围栏

宜支持时间围栏。当终端处于围栏指定的时间范围之内时，自动启用围栏内控制模式。时间范围定义宜支持但不限于可重复时间段。

6.4.6.2 地理围栏

宜支持地理围栏。当终端处于围栏指定的地理范围之内时，自动启用围栏内控制模式。地理范围定义宜支持但不限于圆形地理范围。

6.4.6.3 电子围栏

宜支持WLAN、蓝牙、基站和NFC围栏。当终端扫描到围栏指定的WLAN、蓝牙或基站网络时，自动启用围栏内控制模式。WLAN无线网络的标识宜支持多组SSID和MAC地址对方式；蓝牙的标识宜支持MAC地址；基站的标识宜支持基站编号；NFC的标识宜支持唯一序列号。

6.4.6.4 默认围栏

支持默认围栏。当终端不处于其他围栏时，自动启用默认围栏所定义的控制模式。

6.4.7 远程控制和配置

6.4.7.1 终端锁定/解锁

接收到终端锁定/解锁指令时，应执行对终端的锁定或解锁操作。

6.4.7.2 数据擦除

应执行对终端的恢复出厂操作以及外部存储格式化操作。

6.4.7.3 终端重启

接收到终端重启指令时，应执行对终端的重新启动操作。

6.4.7.4 终端关机

接收到终端关机指令时，应执行对终端的关机操作。

6.4.7.5 定位信息上报

接收到定位信息上报指令时，应采集终端当前定位信息，并上报至终端安全管控数据库。

6.4.7.6 WLAN 配置推送

接收到WLAN配置推送指令时，应将指令中包含的WLAN配置更新至本机配置中。WLAN配置条目以SSID作为唯一标识。

6.4.7.7 VPN 配置推送

接收到VPN配置推送指令时，应将指令中包含的VPN配置以覆盖方式更新至终端VPN客户端。如未安装终端VPN客户端或不兼容其配置接口，则可不予以实现。

6.4.7.8 APN 配置推送

接收到APN配置推送指令时，应将指令中包含的APN配置更新至本机配置中。APN配置条目以APN名称作为唯一标识。

6.4.7.9 SSO 配置推送

接收到SSO配置推送指令时，应将指令中包含的SSO配置以覆盖方式更新至终端SSO客户端。如未安装终端SSO客户端或不兼容其配置接口，则可不予以实现。

6.4.7.10 验证证书推送

接收到验证证书推送指令时,应将指令中包含的验证证书以覆盖方式更新安全监控组件的验证证书；验证证书用于组件对自身数据完整性及数据源可信性验证。

6.4.7.11 运行状态上报

接收到运行状态上报指令时，宜采集当前运行状态，并上报至终端安全管控数据库；当前运行状态包括但不限于CPU使用率、运行内存使用率、内置存储使用率、WLAN无线网络使用率和移动数据网络使用率。

6.4.8 升级

安全监控组件的升级要求如下：

a) 宜支持具有提醒的强制升级；
b) 升级失败，应及时上报升级失败日志，内容应包括但不限于升级时间、终端品牌、终端标识、操作系统版本、当前组件版本号和待升级组件版本号。

6.5 性能要求

6.5.1 策略执行

管控策略的执行应不对系统正常运行、应用正常运行和应用数据正常使用产生影响。

6.5.2 CPU 使用率

安全监控组件在一个完整的充放电周期内平均CPU使用率应≤1%。

6.5.3 运行内存占用量

安全监控组件的运行内存占用量应≤100MB。

6.5.4 网络带宽占用量

注册、登录和策略更新过程平均网络传输速度应≤100Kbps，终端在线状态下平均网络传输速度应≤1Kbps。

6.5.5 耗电量

安全监控组件的耗电量在一个完整的充放电周期内应≤终端电量实际总耗电量的 5%。

6.5.6 策略执行时延

安全监控组件从管控策略接收完成到策略执行的时延应≤1s。

7 网络接入安全体系技术要求

7.1 体系架构

司法行政移动执法系统网络接入安全体系通过终端加固、信道加密、认证接入、接入前置设备、网闸隔离、接入控制设备和访问控制，构建包括司法行政移动执法终端、移动执法无线专网或虚拟无线专用网络、司法行政移动执法网接入区、安全边界和司法行政移动执法专网的网络接入安全体系架构。网络接入安全体系架构如图5所示。

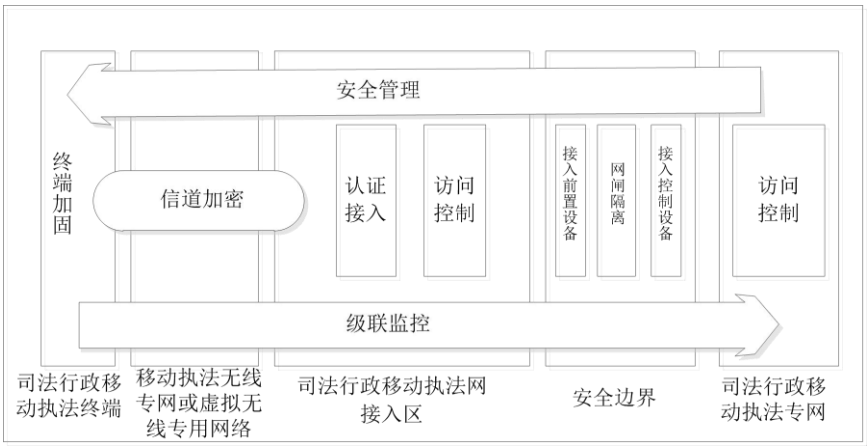

图5 网络接入安全体系架构

7.2 信道加密

信道加密应符合以下要求：

a) 具备终端与执法网接入区间端到端数据通信加密传输的能力；

b) 具备传输数据完整性的校验能力。

7.3 认证接入

认证接入应符合以下要求：

a) 支持基于数字证书端到端双向身份认证功能；

b) 具备网络接入的安全策略管理能力；

c) 具备身份数字证书的证书管理功能；

d) 基于身份认证对终端访问资源的授权管理功能；

e) 具备审计管理功能。

7.4 访问控制

访问控制应符合以下要求：

a) 具有对数字证书用户的访问控制功能；
b) 具备异常访问报警和阻断能力；
c) 具备终端远程监控和管理能力；
d) 具备鉴别终端身份合法性的验证能力。

7.5 安全边界

安全边界应包含接入前置设备、网闸设备和接入控制设备，网闸设备应符合GB/T 20279—2015第三级的要求。具体要求如下：

a) 具备基于数字证书的接入认证功能；
b) 具备基于访问接口白名单方式的控制策略功能；
c) 具备基于角色对资源进行访问控制功能；
d) 具有对交换的数据内容和格式进行检查过滤能力；
e) 具有对数据应用协议的剥离、过滤与恢复能力；
f) 具有多种传输协议的数据同步能力；
g) 具有开启、断开数据交换能力。

8 组网技术要求

8.1 网络结构和内容

司法行政移动执法系统组网从网络结构上的划分如图 6 所示。

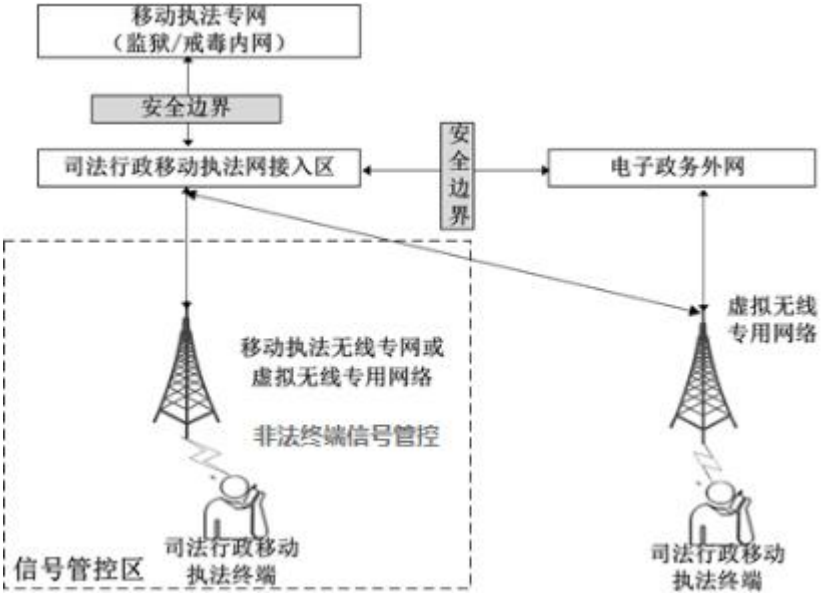

图6 司法行政移动执法系统组网

图6的网络结构内容如下：

a) 移动执法专网（监狱/戒毒内网）：各监狱/戒毒所自建或统一筹建的本地移动执法网络；

b) 司法行政移动执法网接入区：完成对接入移动执法专网的司法行政移动执法终端的审计、认证，以及电子政务外网与监狱/戒毒移动执法专网的数据隔离共享；
c) 电子政务外网：通过电子政务骨干网实现全国互联；
d) 移动执法无线专网或虚拟无线专用网络：通过移动执法无线专网或虚拟无线专用网络将司法行政移动执法终端连接到司法行政移动执法网接入区，也可通过虚拟无线专用网络将司法行政移动执法终端连接到电子政务外网；
e) 非法终端信号管控：通过在监管区内部署非法终端管控系统，对违禁移动终端实施信号屏蔽、信息与行为侦测及即时区域定位。

8.2 移动执法专网组网

8.2.1 互联互通

监狱/戒毒执法内网可租用运营商链路资源，采用MPLS VPN或其它数字专线技术组成骨干网，实现部、省两级的互联互通。

8.2.2 MPLS VPN 组网

骨干网的核心节点部署运营商核心路由器（P）设备，汇聚节点部署运营商边缘路由器（PE）设备，各监狱/戒毒移动执法专网部署用户网络边缘路由器（CE）设备。司法部及各省的监狱/戒毒移动执法专网基于IP路由组网，部署常规路由器、交换机等网络设备；在用户网络边缘设备上配置VPN策略，逻辑上实现以部为中心的星形网络连接。

8.2.3 QoS 要求

支持设置优先级、QoS带宽比例，进行带宽资源的分配，所有业务都有QoS的保障。

8.2.4 可靠性

可靠性应符合以下要求：
a) 端到端的链路可靠性：在链路故障时，能够在 200ms 内切换备用链路，支持快速重路由（FRR）、双向转发检测（BFD）等多种快速重路由切换技术；
b) 设备可靠性：路由器支持双主控冗余配置，可支持分布式结构，支持数据转发与控制分离。

8.2.5 网络管理

网络管理应符合以下要求：
a) IP 地址分配：由部、省统一规划；
b) 域名服务：在部级规划二级域名，并提供专用的域名解析服务器提供域名解析服务。内部名管理采用分级负责制，顶级域名由部级负责管理，子域由各省自行管理。

8.3 虚拟无线专用网络系统

利用移动运营商数据网络的 APN/虚拟专用拨号网（VPDN）技术实现执法终端无缝、安全接入到司法行政移动执法系统。应符合以下要求：
a) 支持空口双向认证；
b) 提供专用 APN；
c) 提供专线连接；
d) 支持接入平台认证、授权、计费（AAA）认证。

8.4 移动执法无线专网系统

8.4.1 建设模式

移动执法无线专网应按以下两种组网方式规划和实施：

a) 运营商专网模式：由运营商建设移动执法无线专网。只有移动执法终端可接入，其他公众移动通信用户无法接入网络，实现授权通信；

b) 自建专网模式：由使用单位自建专网。

8.4.2 授权通信

移动执法无线专网建设时，应通过核心网对终端进行接入鉴权，实现移动执法终端授权通信，确保移动执法终端可在管控区内正常通信，非法终端无法接入移动执法专网。

8.4.3 升级与演进

移动执法无线专网应根据业务发展预留资源，综合考虑系统升级和下一代通信系统的演进。

8.4.4 制式

移动执法无线专网建设应结合实际需要，选择时分长期演进（TD-LTE）、频分长期演进（FDD-LTE）制式或新一代演进制式。

8.4.5 频段

移动执法无线专网建网时应合理选择公众移动通信网络频段或符合GB/T 37291—2019中第7章规定的无线宽带专网频段要求。

8.4.6 网络覆盖

监管区内移动执法无线专网覆盖电平在＞-95dBm的区域应≥99%。

8.4.7 切换

通用执法终端应支持在信号管控区出入口做到精准的网络切换，保证通用执法终端进入信号管控区时切换到移动执法无线专网，出信号管控区在10m内切换到公众移动通信网络。自动切换成功率应≥99%，自动切换失败的，应后台人工切换。

8.4.8 安全性

移动执法无线专网系统设备的安全要求应符合GB 4943.1的要求。

8.5 非法终端信号管控

8.5.1 基本要求

在监狱的监管区、戒毒所的戒毒管理区和涉密会议室应建设非法终端信号管控系统。

8.5.2 功能要求

8.5.2.1 通信屏蔽

应具有对管控区域内非法终端通信屏蔽的功能，并应符合以下要求：

a) 具有屏蔽管控区域内非法终端通话的功能；

b) 具有屏蔽管控区域内非法终端发送和接收短信息功能；
c) 具有屏蔽管控区域内非法终端上网功能。

8.5.2.2 非法终端侦测

应具有对管控区域内非法终端侦测的功能，并应符合以下要求：
a) 具备实时发现进入管控区域处于开机状态的非法终端的功能；
b) 具有侦测和记录非法终端的特征码、运营商和归属地等功能；
c) 侦测到的非法终端信息包括但不限于 SIM 卡号（IMSI）、机身串号（IMEI）、电子序列号（ESN），且侦测到的终端信息具有唯一性；
d) 侦测到的非法终端信息能够查全和查准，如：中国电信终端卡内含有制式 IMSI 和 LTE 制式 IMSI。

8.5.2.3 通信行为侦测

应具有记录并统计管控区域内非法终端通信的动态状况功能，并应符合以下要求：
a) 非法终端拨打电话的记录，并记录被叫号码和时间等行为信息；
b) 非法终端发送短信的记录，并记录短信接收号码和时间等行为信息。

8.5.2.4 定位

应具有对管控区域内开机状态下的非法终端进行即时区域定位功能。

8.5.2.5 环境自适应功能

应具有搜索周围公网基站的无线环境参数和根据公网环境自动配置工作参数的功能，包括但不限于工作频点、信号强度和邻区。

8.5.2.6 通信管控客户端功能

客户端功能应符合以下要求：
a) 具有对非法终端侦测信息的管理和告警功能，包括但不限于非法终端信息、非法通信行为和开关机信息；
b) 具有数据库管理功能，包括但不限于信息存储、查询和统计；
c) 具有设备管理功能，包括但不限于设备参数设置和设备工作状态显示；
d) 具有日志管理功能，包括但不限于登录日志、操作日志和系统日志；
e) 具有权限管理功能，包括但不限于角色分配和用户权限管理。

8.5.2.7 网络功能

非法终端信号管控网络功能应符合以下要求：
a) 具有网络管理功能，包括但不限于设备告警管理和维护管理；
b) 具有安全、准确和可靠的非法终端无线管控信号的传输能力；
c) 采用光纤分布式架构独立组网；
d) 具备预留“移动执法系统警务通信”的硬件资源或模块资源的能力。

8.5.3 性能要求

8.5.3.1 覆盖性能

信号覆盖性能应符合以下要求：

a) 覆盖能力：在指定区域保证所有位置完全覆盖，无盲区；

b) 覆盖隔离：满足 10m 的隔离要求，即在覆盖区物理边界的缓冲距离＜10m。

8.5.3.2 侦测性能

非法终端侦测反应时间及成功率应符合以下要求：

a) 非法终端侦测反应时间＜30s；

b) 非法终端侦测成功率＞90%。

8.5.3.3 定位性能

即时区域定位应至少定位到楼宇，单兵定位精度应＜1m。

8.5.3.4 客户端软件操控性能

数据和日志记录时间应≥90d。

8.5.3.5 网络性能

网络性能应符合以下要求：

a) 网络运行稳定，保证 7×24h 服务模式；

b) 网络制式方便扩容和升级，参数自适应调整；

c) 保证网络信息传输过程中的数据准确性、完整性和实时性。

8.5.4 通信制式与频率要求

应支持国内运营商2G/3G/4G/5G的所有通信制式，包括码分多址（CDMA）、全球移动通信系统（GSM）、宽带码分多址（WCDMA）、时分同步码分多址（TD-SCDMA）、TD-LTE、FDD-LTE、5G独立组网（SA）和非独立组网（NSA）通信技术制式。各个制式工作频率应符合以下要求：

a) 非法终端信号管控系统对国内运营商 2G/3G/4G/5G 有效管控，并支持其他频段扩展，对管控区域内的其他警用设备（如对讲机等）无干扰；

b) 仅对下行频段或下行时隙进行干扰，不对上行频段或时隙产生任何干扰，以避免对周边公众移动通信基站的正常工作产生影响；

c) 制式包括但不限于 GSM、数据传输系统（DCS）、TD-SCDMA、CDMA 1X、CDMA2000、WCDMA、FDD-LTE、TD-LTE、窄带物联网（NB-IoT）、增强机器类通信（eMTC）、5G NSA 和 5G SA；

d) 频段包括但不限于 869MHz～880MHz、930MHz～960MHz、1805MHz～1880MHz、1885MHz～1915MHz、2010 MHz～2025MHz、2110 MHz～2170MHz、2300 MHz～2390MHz、2515 MHz～2675MHz、3300MHz～3600MHz 和 4800MHz～4900MHz。

9 应用开发技术要求

9.1 运行环境

9.1.1 客户端运行环境

客户端运行环境应符合以下要求：

a) 运行在符合安全管理要求的移动执法终端；

b) 运行在安全可靠的操作系统上，具备安全的第三方运行库；

c) 具有系统级安全增强策略；
d) 具有安全监控等功能。

9.1.2 服务端运行环境

服务端运行环境应符合以下要求：

a) 选用符合国家相关标准的服务器、应用服务器和数据库/文件系统，并对参数进行正确配置，删除或变更缺省用户/密码，关闭不必要的管理功能，优先选用国产化硬件设备和操作系统；
b) 具有用户认证、访问控制、外设控制、网络控制和行为审计等安全策略，采用数据加密、安全存储等相关安全手段；
c) 对服务器、数据库和文件系统等采用设备冗余、容量冗余等方法，提供数据安全保护策略；
d) 具备对客户端提供数据服务、计算服务、共享服务和发布服务等应用支撑服务；
e) 确保服务器使用的软件和系统部件均为相对安全的稳定版本，并安装了该版本的所有补丁。

9.2 开发要求

9.2.1 开发环境

开发环境要求如下：

a) 应用软件开发应在主流操作系统上开展，宜使用主流程序开发语言；
b) 应确保软件开发环境、使用框架和系统部件均为相对安全的稳定版本，并安装了该版本的所有补丁；
c) 应隔离开发环境和实际运行环境，并只提供给授权的开发和测试团队访问；
d) 宜使用软件变更管理系统以管理和记录在开发和产品迭代过程中代码的变更。

9.2.2 开发过程

应建立应用软件开发过程，包括以下主要活动：

a) 项目规划和监督；
b) 软件功能和性能需求分析；
c) 软件系统总体设计；
d) 软件系统详细设计；
e) 软件编码与测试；
f) 软件测试；
g) 系统集成与调试；
h) 软件安装；
i) 软件培训；
j) 软件移交。

9.2.3 开发文档

应在相应阶段完成软件文档编制，包括以下文件：

a) 软件开发计划；
b) 软件需求规格说明；
c) 软件概要设计说明；
d) 软件详细设计说明；
e) 软件接口设计说明；

f) 软件用户手册；
g) 软件测试分析报告；
h) 软件产品规格说明。

9.3 应用要求

9.3.1 基本要求

应提供符合用户需求的功能，并保证功能的完备性和准确性。

9.3.2 易用性

易用性应符合以下要求：
a) 具备可视化界面，易于操作；
b) 易于安装、更新和卸载；
c) 具备软件帮助系统。

9.3.3 维护性

维护性要求如下：
a) 应采用模块化、结构化程序设计方法；
b) 应采用统一建模语言或标准建模语言（UML）等标准的表达工具来描述算法、数据结构、接口等；
c) 应采用可维护的高级程序设计语言和主流应用（APP）开发环境；
d) 宜在软件开发过程中，进行明确的质量保证审查，包括代码规范、说明文档等。

9.3.4 易扩展性

应符合用户业务规模增加或技术发展需要的扩展和升级的需求，具有较好的灵活性和可重用性，能够实现功能重组、扩充，并保持整体稳定性。

9.4 安全要求

9.4.1 基本要求

司法行政移动执法终端应用的安全技术要求应符合GB/T 34975—2017第4章的规定。

9.4.2 安装卸载安全

9.4.2.1 安装安全

安装安全要求如下：
a) 不应在未认证的移动终端中安装和运行；
b) 应能够根据用户需求确定应用软件的安装；
c) 应能够以在线方式安装应用软件，支持自动更新升级；
d) 执法模式下，应只能出厂预置或安装司法行政移动执法系统应用市场中的应用软件；
e) 应提供应用软件安装相关信息，如程序标识、名称、版本、平台和开发商等。

9.4.2.2 卸载安全

卸载安全应符合以下要求：

a) 能够按照用户要求卸载应用软件；
b) 应用软件在卸载后，删除相关数据。

9.4.3 数据安全

数据安全应符合但不限于以下要求：
a) 执法数据和非执法数据隔离存储；
b) 非执法模式不能访问执法模式下相关应用软件使用的数据；
c) 执法模式下宜选择国密算法对数据进行加密。

9.4.4 身份鉴别

身份鉴别要求如下：
a) 应支持设置软件运行用户名/密码或利用生物特征识别等，宜具有能够防范密码猜测等攻击的手段，如足够复杂的密码、多次尝试锁定和验证码等，并在每次用户登录系统时和重新连接时进行鉴别；
b) 应禁止密码的存储、传输和明文显示及对录入密码的复制。

9.4.5 权限控制

权限控制要求如下：
a) 应对用户进行权限控制，支持在不同模式下的权限控制策略；
b) 应根据角色进行权限设置，不宜设置拥有所有权限的超级用户。

9.4.6 运行安全

运行安全要求如下：
a) 执法模式与非执法模式应只能运行本模式下的应用程序；
b) 应支持应用软件关闭后及时清除缓存页面、临时文件等剩余信息；
c) 应采用动态加载、虚拟化等技术实现客户端仅显示用户界面和传输交互数据，办公数据不在移动终端留存；
d) 应支持应用软件权限全程可控；
e) 宜根据应用需求设置会话有效期。

9.4.7 安全审计

安全审计应符合以下要求：
a) 对关键事件（用户登录/退出、敏感数据访问和敏感业务提交等）进行审计记录，包括日期和时间、事件主体身份、事件描述和是否成功等；
b) 能对审计日志进行权限设置；
c) 具有审计日志的备份、恢复等功能。

10 应用市场发布与级联技术要求

10.1 应用市场基本要求

司法行政移动执法系统应用市场的设计、部署和实施应符合GB/T 21064和SF/T 0008的规定。司法行政移动执法系统应用市场应根据建设条件和业务特点，并在司法行政移动执法系统体系框架下，进行

系统建设和运行。

10.2 应用市场级联

司法行政移动执法系统应用市场级联应符合但不限于以下要求：

a) 司法行政移动执法系统应用市场按照“部、省”两级组织机构部署管理节点，形成统一规范的管理节点级联架构；
b) 省级管理节点应与部级管理节点连通，并报备应用管理清单及监管信息；
c) 各级管理节点负责本级内部终端应用软件的审核、发布和运维等管理事项。

10.3 应用市场发布

10.3.1 发布申请

司法行政移动执法系统应用市场发布申请应符合但不限于以下要求：

a) 应用市场管理者应要求应用软件提供者提供营业执照、机构地址和联系方式等基本信息；
b) 应用市场管理者应配合终端管理机构与应用软件提供者签订协议，明确产品质量、售后服务及信息安全等方面承担的义务和责任；
c) 应用市场管理者应要求应用软件提供者提供应用软件的测试版本，并提供有效的测试帐户和登录信息，以及审核应用时所需的任何其他硬件或资源；
d) 应用市场管理者应要求应用软件提供者确保应用审核期间的可用性。

10.3.2 发布审核

司法行政移动执法系统应用市场发布审核包括但不限于以下要求：

a) 应用应符合司法行政业务需求；
b) 应用名称应使用中文或英文，且≤10 个中文字符，与现有应用不存在重名情况；
c) 应用图标应清晰，宜上传像素为 200×200，且＜2M 的图标；
d) 应用简介描述应说明应用相关信息，能够准确反映应用的核心功能。

10.3.3 发布更新

司法行政移动执法系统应用市场发布更新应符合但不限于以下要求：

a) 具备对管理范围内的所有应用软件的更新能力；
b) 具有在用户授权下的对应用软件的手动更新能力；
c) 具备在应用市场管理员授权下的应用软件强制自动更新能力。

10.4 应用市场安全

10.4.1 认证安全

司法行政移动执法系统应用市场认证安全应符合但不限于以下要求：

a) 司法行政各级应用市场接入点在完成注册后，应用市场应根据注册信息建立接入白名单，并以白名单方式控制是否允许接入；
b) 应用市场应支持应用软件和数字内容的数字版权管理功能；
c) 应用市场应具有审核应用软件提供者业务资质的机制。

10.4.2 发布安全

司法行政移动执法系统应用市场发布安全应在不带入新的安全隐患前提下，包括但不限于以下要

求：

a) 应用不应含有病毒木马等侵害用户的功能（包括代码等可疑行为）；
b) 应用不应获取无关的权限，禁止威胁用户信息安全；
c) 应用不应出现未经用户允许发送短信、拨打电话等使用隐私权限的行为；
d) 应用不应含有第三方加载可执行代码的应用或SDK（软件开发工具包）。

10.4.3 内容安全

司法行政移动执法系统应用市场不应包含以下内容：

a) 反对宪法；
b) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一；
c) 损害国家荣誉和利益；
d) 煽动民族仇恨、民族歧视，破坏民族团结；
e) 破坏国家宗教政策，宣扬邪教和封建迷信活动；
f) 散布谣言，扰乱社会秩序，破坏社会稳定；
g) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪；
h) 侮辱或者诽谤他人、侵害他人合法权益；
i) 法律、行政法规禁止的其他内容。

10.4.4 运行安全

司法行政移动执法系统应用市场运行安全包括但不限于以下要求：

a) 为终端预置软件，保持后台运行，不可被用户卸载；
b) 可在管理员授权下为终端强制安装、更新或卸载应用软件；
c) 应监管终端运行的所有应用软件，不应执行恶意行为；
d) 对应用软件的申请、审核、发布、升级更新、卸载和监管等管理行为应形成日志，由司法部管理节点集中备案。

10.4.5 信息安全

司法行政移动执法系统应用市场信息安全技术应符合GB/T 25070和GB/T 35282的规定。

11 即时通信软件互联技术要求

11.1 系统组成

11.1.1 基本要求

司法行政移动执法终端即时通信软件的接口互联及安全防护机制应符合GB 33473和YD/T 2305的规定。

司法行政移动执法终端即时通信软件应采用管理节点和应用节点的方式。其中管理节点是指负责应用节点管理维护的软件，各省按照组织机构可独立建设部署，并为接入司法部管理节点预留接口。应用节点是指在管理节点范围内部署的司法行政移动执法终端即时通信软件系统。

11.1.2 节点功能

11.1.2.1 管理节点

管理节点应符合以下要求：

a) 提供应用节点的注册、更新和注销等服务；
b) 提供应用节点的组织架构和管理信息的备份服务；
c) 提供应用节点的审计服务；
d) 提供应用节点的管理制度维护和下发服务；
e) 提供应用节点的寻址服务；
f) 提供应用节点的认证及协议转换服务。

11.1.2.2 应用节点

应用节点应符合以下要求：

a) 向本级管理节点注册、维护本应用节点；
b) 应用节点服务端提供内部所有互联终端的即时通信服务；
c) 对接管理节点的寻址服务接口，支撑用户发起的面向所有认证应用节点的会话服务；
d) 支持本地终端的文本、语音、图像和视频信息的采集及安全访问；
e) 收集本地终端用户活动和数据访问的审计日志，支撑本地应用的管理和日志采集；
f) 按照管理节点的要求，维护本地的审计规则及审计数据，并定期向管理节点上传审计数据；
g) 向管理节点上传指定数据，配合管理节点完成数据备份服务。

11.2 互联要求

11.2.1 节点互联

11.2.1.1 应用节点与管理节点间互联

应用节点与管理节点间互联应符合以下要求：

a) 应用节点向本级管理节点提出认证申请；
b) 管理节点同意后向应用节点颁发可信证书；
c) 应用节点利用可信证书与管理节点进行安全通信。

11.2.1.2 管理节点间互联

管理节点间互联应符合以下要求：

a) 管理节点间相互确认通信协议及认证方式；
b) 管理节点间相互确认管理级别及范围；
c) 管理节点相互交换应用节点认证信息。

11.2.1.3 应用节点间互联

应用节点间互联应符合以下要求：

a) 应用节点向本级管理节点提出互联申请；
b) 管理节点间进行安全认证并协商通信协议；
c) 管理节点同意后向应用节点颁发可信证书；
d) 应用节点间基于可信证书进行安全通信。

11.2.2 通信协议

11.2.2.1 基本要求

即时通信协议包括但不限于以下要求：

a) 不同应用节点可定制符合需求的即时通信应用层协议；
b) 即时通信协议可采用会话初始协议（SIP）和可扩展消息与存在协议（XMPP）等，编码效率应符合文本、音频和视频等多媒体信息交互实时性的要求；
c) 即时通信协议应考虑数据传输安全性，可采用 HTTPS 或者传输层安全（TLS）私有协议等，传输内容加密应符合国家密码主管机关相关行业标准。

11.2.2.2 通信协议互通

即时通信协议互通应符合但不限于以下要求：

a) 部署在省内的即时通信软件系统应实现全省系统内互联互通；
b) 管理节点负责不同应用节点间即时通信协议转换；
c) 即时通信系统可采用基于网关协议转换的技术实现通信协议互通要求；
d) 即时通信协议互通技术应保证转换过程中的数据传输实时性、安全性要求。

11.2.3 节点注册维护

11.2.3.1 节点注册

节点注册应符合但不限于以下要求：

a) 管理节点负责组织机构注册，全国采用统一的组织机构命名和编码规则；
b) 管理节点统一分配和管理节点 ID；
c) 应用节点应在管理节点注册后方可使用；
d) 应用节点支持按组织机构独立部署；
e) 应用节点注册信息应包括节点名、节点 ID、节点应用类型、服务器地址和服务器认证信息等。

11.2.3.2 节点维护

节点维护应符合但不限于以下要求：

a) 已建立应用节点的单位，其下的组织机构及用户信息由应用节点自行管理；
b) 未建立应用节点的单位，其在即时通信软件中的组织机构和用户信息由其上级单位的应用节点维护；
c) 各应用节点只维护本节点的组织机构和用户信息，不允许保存任何其他应用节点的组织架构和用户信息；
d) 需要查询其他应用节点的组织架构和用户信息时，向目标应用节点发起组织架构和用户信息的查询请求；
e) 各应用节点依据管理节点的要求将本节点中的组织机构和用户信息同步到管理节点；
f) 用户信息通过节点 ID 和用户 ID 进行唯一标识。

11.3 功能要求

11.3.1 基本要求

司法行政移动执法终端即时通信软件的基本功能应包括维护联系人、即时通信和应用设置等，各厂商的即时通信软件功能可与本文件所定义的不同，但应保证同一应用节点范围内部署的即时通信软件系统满足统一的标准规范。

11.3.2 联系人维护功能

维护联系人功能应符合但不限于以下要求：

a) 以单位名称为根节点，维护单位内各机构所有可见用户的信息；
b) 以任务群组名称为根节点，维护本节点所属群及其用户的信息；
c) 以好友为根节点，维护好友公开信息。

11.3.3 即时通信功能

即时通信功能包括但不限于以下要求：

a) 可在所属单位内某机构的消息对话框中进行多方通信，仅机构认证用户可以查看；
b) 可在群组消息对话框中进行多方通信，仅群组认证用户可以查看；
c) 可在好友对话框中进行一对一通信，仅通信双方可以查看；
d) 通信内容包括文本、表情、语音、文件、图片、视频和位置等多媒体消息；
e) 通信功能可以支持但不限于消息复制、转发、撤回、搜索、收藏阅后回执和阅后即焚；
f) 禁止截屏录屏。

11.3.4 应用设置功能

应用设置功能包括但不限于以下要求：

a) 可对用户头像、实名和职务等信息进行设置；
b) 可对账号、密码和验证方式等相关安全信息进行设置；
c) 可对新消息的提醒方式等设置；
d) 可对应用的语言、字体和缓存空间等进行设置；
e) 可对个人信息等公开权限进行设置。

11.4 性能要求

11.4.1 响应能力

即时通信软件系统响应能力应符合但不限于以下要求：

a) 即时通信服务系统启动时间≤30s；
b) 即时通信终端软件启动时间≤10s；
c) 即时通信应用节点服务系统在规定的并发用户数范围内，对于终端软件的一项操作请求，简单应用平均响应时间≤3s，一般应用平均响应时间≤10s，复杂应用平均响应时间≤30s，最大响应时间均≤60s。

11.4.2 访问能力

即时通信软件系统信息访问能力应符合但不限于以下要求：

a) 应用节点服务系统支持的可并发访问的最大用户数应＞可能在线的终端用户的并发访问需求；
b) 应用节点服务系统支持的最大信息交互数应符合所有可能在线的终端用户的信息交互总体需求量；
c) 管理节点服务系统支持的最大信息交互数应符合部署区域范围内所有应用节点间的信息交互总体需求量。

11.4.3 维护能力

即时通信软件系统信息维护能力应符合但不限于以下要求：

a) 保证即时通信软件系统内数据流转的准确性，数据传输准确率＞99%；

b) 保证即时通信软件系统内数据存储的完整性，保证在线可查≤1 年的数据，可调阅＞1 年的重要通信数据离线备份存储；
c) 保证即时通信软件系统的日常运维管理，应用及管理节点软件支持＞1 年的运维保障服务。

11.4.4 使用能力

即时通信软件系统使用能力应符合但不限于以下要求：
a) 即时通信软件系统运行稳定，保证 7×24h 服务模式，支持在线升级；
b) 即时通信软件应用节点服务系统可容纳的终端用户数应＞当前业务所需及未来 3 年可能融入的终端用户总数；
c) 即时通信软件应用节点服务系统数据存储最大容量＞PB 级。

11.5 安全要求

11.5.1 基本要求

即时通信软件系统总体安全目标应符合但不限于以下要求：
a) 各应用节点之间数据加密传输；
b) 各应用节点与管理节点之间数据加密传输；
c) 各应用节点之间进行数据交互时，对请求数据进行签名，签名算法应采用国密算法；
d) 各应用节点与管理节点之间进行数据交互时，对请求数据进行签名，签名算法应采用国密算法。

11.5.2 认证安全

即时通信软件系统各节点间的通信接口应采用适当的机制确保通信双方的身份认证安全，应符合但不限于以下要求：
a) 应用层应具有严格的双向认证协议机制；
b) 底层可以使用已有的双向认证协议机制；
c) 通信双方配置对方的合法地址池，只允许接收来自合法地址池的数据包；
d) 认证过程中采用的算法应符合国家商用密码管理的相关要求。

11.5.3 机密性

即时通信软件系统区域内部、跨区域的应用节点互通，分别由应用节点和管理节点按相关安全管理规定自行实施和管理，并负责信息交换的安全，具体应符合但不限于以下要求：
a) 节点间互联应符合各节点机房间数据传输的安全性；
b) 节点间接口调用采用 HTTPS 加密传输，保证业务数据安全；
c) 根据节点间整体架构方案，各节点通过 HTTPS 协议相互通信，保障业务数据的安全传输；
d) 各节点自行配置 HTTPS 加密证书，建议采用受信任的内部证书；
e) 节点数据在服务端存储备份，终端缓存数据应在离开状态时自动清空。

11.5.4 完整性

即时通信软件系统各节点间的通信接口应采用适当的机制确保递交数据内容的完整性，包括但不限于以下要求：
a) 即时通信软件应保证递交数据的准确性，接口应采用相应的机制保证传输数据的任何修改和损坏都应被立即发现；

b) 即时通信软件的数据传输完整性保护可利用现有协议的机制实现，如互联网安全协议（IPSec）等。

参 考 文 献

[1] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 30278—2013 信息安全技术 政务计算机终端核心配置规范
[4] GB/T 30850.1—2014 电子政务标准化指南 第1部分：总则
[5] GB/T 30882.1—2014 信息技术 应用软件系统技术要求 第1部分：基于B/S体系结构的应用软件系统基本要求
[6] GB/T 34980.2—2017 智能终端软件平台技术要求 第2部分：应用与服务
[7] GB/T 34990—2017 信息安全技术 信息系统安全管理平台技术要求和测试评价方法
[8] GB/T 35278—2017 信息安全技术 移动终端安全保护技术要求
[9] GA/T 1364—2017 警用数字集群(PDT)通信系统 互联技术规范
[10] SF/T 0009—2017 全国司法行政系统指挥中心建设技术规范
[11] SF/T 0012—2017 全国司法行政系统网络平台技术规范
[12] YDB 107 增值电信业务系统安全防护定级和评测实施规范 即时通信系统
[13] YDB 135—2013 移动应用软件商店 客户端技术要求
[14] YDB 136—2013 移动应用软件商店 信息安全技术要求
[15] YD/T 2587—2020 移动互联网应用商店安全防护要求
[16] YD/T 2588—2020 移动互联网应用商店安全防护检测要求