ICS 35.240.99
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1561—2019

移动警务系统　总体技术要求

Mobile police information system—General technical requirements

2019-04-19 发布　　2019-04-19 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部科技信息化局提出。

本标准由公安部通信标准化技术委员会归口。

本标准起草单位：公安部科技信息化局、天津市公安局、公安部第一研究所、广西壮族自治区公安厅、郑州信大捷安信息技术股份有限公司、公安部第三研究所、华为技术有限公司、北京明朝万达科技股份有限公司、北京安荣科技有限公司、大唐移动通信设备有限公司、北京可信华泰信息技术有限公司。

本标准主要起草人：陈昌前、李雁、袁艺芳、陈玉东、韩秀德、佟学俭、李习睿、喻波、陈家明、夏元松、席新、闫锐、安鹏、陈绪、顾流、王忠利、田健生、王春雪、曹磊、郝志伟、崔松。

移动警务系统　总体技术要求

1　范围

本标准规定了移动警务系统组成与分类、移动警务终端、无线接入网络、移动警务服务平台、移动警务应用和安全与集中管控的技术要求。

本标准适用于移动警务系统的规划、设计、建设、验收等。

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/T 21061　国家电子政务网络技术和运行管理规范

GB/T 25070　信息安全技术　信息系统等级保护安全设计技术要求

GB/T 29828　信息安全技术　可信计算规范　可信连接架构

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

3　术语和定义、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

移动警务系统　mobile police information system

利用移动终端通过无线网络处理警务信息的系统。

3.1.2

移动警务服务平台　mobile police service platform

为移动警务应用提供运行服务的支撑环境。

3.1.3

移动警务终端　mobile police terminal

在移动警务系统中处理警务信息的无线终端设备。

3.1.4

增强受控终端　advanced controlled mobile police terminal

从硬件和操作系统进行安全控制的移动警务终端。

3.1.5

一般受控终端　general controlled mobile police terminal

从操作系统的应用层进行安全控制的移动警务终端。

3.1.6

个人普通终端　personal common mobile police terminal

不进行特殊安全控制的移动警务终端。

3.1.7

移动服务总线　service bus for mobile police application

为移动警务应用提供资源服务并对资源进行统一管控的中间件。

3.1.8

集中管控中心　centralized management and control center

对移动警务系统进行统一管理、集中监测、安全管控的信息系统。

3.1.9

安全管控系统　security management and control system

对移动警务系统用户、终端、网络、应用、数据等要素的安全进行综合管控的信息系统。

3.1.10

终端安全监控组件　mobile terminal security monitoring software

运行于移动警务终端，具有监测信息上报、安全策略配置和管控指令执行等安全监控功能的软件。

3.2　缩略语

下列缩略语适用于本文件。

IPSec：互联网安全协议(Internet Protocol Security)

PKI：公钥基础设施(Public Key Infrastructure)

VPN：虚拟专用网络(Virtual Private Network)

4　系统组成与分类

4.1　系统组成

移动警务系统由移动警务终端、无线接入网络、移动警务服务平台、移动警务应用和安全与集中管控组成，如图1所示。

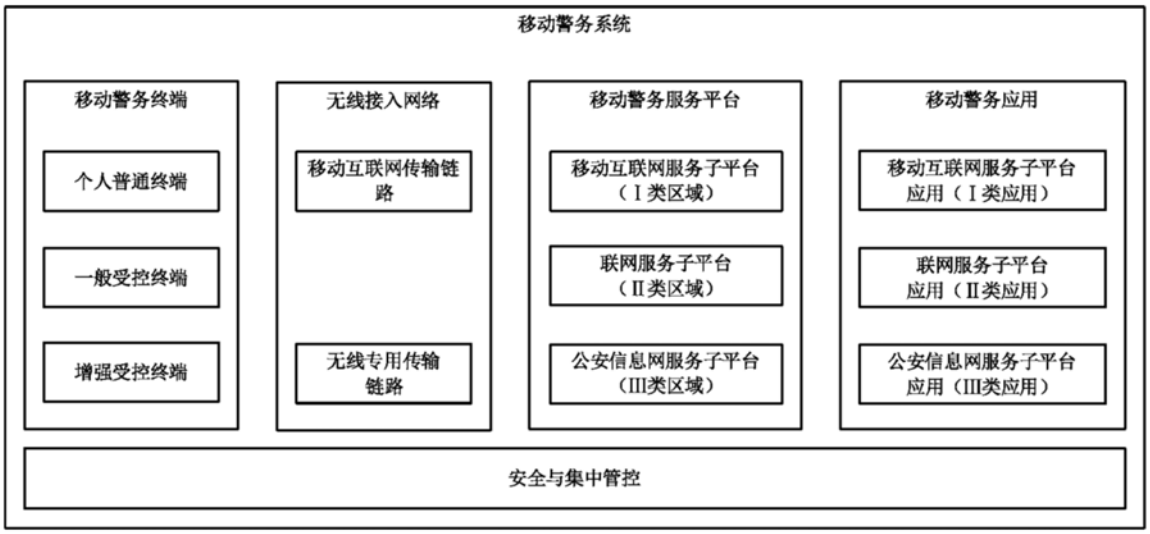

图1　移动警务系统组成

其中：

a)　移动警务终端可分为个人普通终端、一般受控终端和增强受控终端；

b)　无线接入网络可分为移动互联网传输链路和无线专用传输链路；

c) 移动警务服务平台可分为移动互联网服务子平台(Ⅰ类区域)、联网服务子平台(Ⅱ类区域)和公安信息网服务子平台(Ⅲ类区域);
d) 移动警务应用可分为基于移动互联网服务子平台的移动警务应用(Ⅰ类应用)、基于联网服务子平台的移动警务应用(Ⅱ类应用)和基于公安信息网服务子平台的移动警务应用(Ⅲ类应用);
e) 安全与集中管控包括密码使用、跨区域安全防护、数据安全、安全管控系统和集中管控中心。

4.2 系统分类

4.2.1 Ⅰ类系统

Ⅰ类系统由个人普通终端、移动互联网传输链路、Ⅰ类区域、Ⅰ类应用和相应的安全与集中管控措施组成。

4.2.2 Ⅱ类系统

Ⅱ类系统由一般受控终端/增强受控终端、无线专用传输链路、Ⅱ类区域、Ⅱ类应用和相应的安全与集中管控措施组成。

4.2.3 Ⅲ类系统

Ⅲ类系统由增强受控终端、无线专用传输链路、Ⅱ类区域的接入控制、Ⅲ类区域、Ⅲ类应用和相应的安全与集中管控措施组成。

5 技术要求

5.1 移动警务终端

5.1.1 个人普通终端

个人普通终端应满足下列要求:
a) 接入Ⅰ类区域,禁止接入Ⅱ类区域、Ⅲ类区域;
b) 终端操作系统、应用软件、应用数据具备安全防护能力。

5.1.2 一般受控终端

一般受控终端满足下列要求:
a) 应接入Ⅱ类区域,禁止接入Ⅰ类区域、Ⅲ类区域;
b) 应对终端操作系统、应用、网络连接、外围接口、用户数据进行安全增强;
c) 应安装终端安全监控组件等安全软件;
d) 应安装软/硬介质的密码模块;
e) 宜通过人机认证等方式将人员和使用的证书进行自动关联。

5.1.3 增强受控终端

增强受控终端满足下列要求:
a) 可接入Ⅱ类区域或Ⅲ类区域,禁止接入Ⅰ类区域使用;
b) 应对终端硬件、操作系统、应用、网络连接、外围接口、用户数据进行安全增强;
c) 应预装终端安全监控组件等安全软件;
d) 应安装硬介质的密码模块;
e) 应通过人机认证等方式将人员和使用的证书进行自动关联;

f) 终端硬件、操作系统应具备可信计算环境。

5.2 无线接入网络

5.2.1 移动互联网传输链路

移动互联网传输链路应满足下列要求：

a) 为个人普通终端访问Ⅰ类区域提供网络通道；
b) 为Ⅰ类区域获取互联网资源提供网络通道。

5.2.2 无线专用传输链路

无线专用传输链路应满足下列要求：

a) 为一般受控终端访问Ⅱ类区域提供网络通道；
b) 为增强受控终端访问Ⅲ类区域提供网络通道；
c) 采用虚拟专网或物理专网方式进行网络隔离。

5.3 移动警务服务平台

5.3.1 通用要求

移动警务服务平台满足下列要求：

a) 为移动警务终端提供接入、安全保护及安全管控服务；
b) 具备基础信息标识功能，包括但不限于开发资源、应用、用户、机构、终端、服务等；
c) 具备应用管理发布，包括但不限于注册、发布、更新、下载、安装、卸载等；
d) 具备移动服务总线，对资源和服务提供注册、发布、下线、调度等功能，不同移动警务平台间及同一移动警务平台不同区域间应通过移动服务总线进行数据交换，移动服务总线间应采用数字证书或等效措施进行认证；
e) 具备认证服务，为用户、机构、设备、应用提供认证功能，Ⅰ类区域认证服务采用的认证技术可包括但不限于数字身份证书、口令、生物特征认证等；Ⅱ类区域、Ⅲ类区域认证服务采用的认证技术应基于移动警务 PKI 数字身份证书，并辅以口令、生物特征认证等；
f) 具备授权服务，为用户、应用、资源提供授权管理及鉴权功能；
g) 具备应用监测服务，为移动应用提供应用行为监测、使用评估功能。

5.3.2 移动互联网服务子平台

移动互联网服务子平台(Ⅰ类区域)应提供终端接入、互联网边界防护、Ⅰ类区域应用支撑、Ⅰ类区域安全管控等功能。

5.3.3 联网服务子平台

联网服务子平台(Ⅱ类区域)应满足下列要求：

a) 提供终端接入控制、密码基础服务、Ⅱ类区域应用支撑、Ⅱ类区域安全管控等功能；
b) 联网服务子平台之间基于国家电子政务外网或专线使用 IPsecVPN 技术实现互联，采用身份认证、访问控制、信道加密等措施保护安全，并满足 GB/T 21061 相关技术要求；
c) 禁止为同一终端同时提供Ⅱ类区域和Ⅲ类区域的访问通道；
d) 与其他网络资源共享时采用访问控制和隔离交换等保护措施。

5.3.4 公安信息网服务子平台

公安信息网服务子平台(Ⅲ类区域)应提供移动安全接入、密码基础服务、Ⅲ类区域应用支撑、Ⅲ类

区域安全管控、集中管控等功能，移动安全接入提供终端接入控制、信道加密、访问控制、隔离交换等功能。

5.4 移动警务应用

移动警务应用满足下列要求：

a) 同一应用仅属于Ⅰ类应用、Ⅱ类应用、Ⅲ类应用中的一种；

b) 禁止跨系统部署，Ⅰ类应用应部署于Ⅰ类系统；Ⅱ类应用应部署于Ⅱ类系统；Ⅲ类应用应部署于Ⅲ类系统；

c) 应使用移动警务服务平台定义的统一标识，包括但不限于资源、应用、用户、机构、终端、服务等；

d) 应使用认证和授权服务，实现用户身份认证、单点登录和应用鉴权；

e) 应通过移动服务总线访问跨平台、跨区域资源；

f) 宜通过移动服务总线访问本区域资源。

5.5 安全与集中管控

5.5.1 基本要求

满足下列要求：

a) Ⅰ类系统、Ⅱ类系统应符合 GB/T 25070 中二级技术要求，Ⅲ类系统应符合 GB/T 25070 中三级技术要求；

b) 安全保护宜符合 GB/T 29828 可信计算技术要求；

c) 各类系统应具备表 1 所示的安全防护功能；

d) 集中管控中心应支持分级管控和级联；

e) 安全管控系统应部署于Ⅰ类区域、Ⅱ类区域、Ⅲ类区域，集中管控中心部署于Ⅲ类区域；

f) 各区域安全管控系统与本级集中管控中心应通过移动服务总线对接。

表 1 安全防护功能

序号	安全功能			Ⅰ类系统	Ⅱ类系统	Ⅲ类系统
1	移动警务终端计算环境	可信防御		○	○	●
2		密码模块	软介质	○	◎	—
3			硬介质	○	◎	●
4		防刷机		○	○	●
5		防破解		○	○	●
6		统一认证		○	●	●
7		统一授权		○	●	●
8		应用防护		●	●	●
9		存储加密		○	○	○
11		防泄漏检查		○	●	●
12		数据隔离		○	●	●

表 1（续）

序号	安全功能		Ⅰ类系统	Ⅱ类系统	Ⅲ类系统
13	服务端计算环境	可信防御	○	○	●
14		可信验证	○	○	●
15		存储加密	○	○	○
17		防泄漏检查	○	●	●
18	区域边界	恶意代码防范	●	●	●
19	通信网络	网络隔离	●	●	●
20		协议加密	●	●	●
21		数据加密	○	●	●
22	安全管控	策略联动	●	●	●
23		数据防篡改	●	●	●
注：—表示不涉及，○表示建议采用，● 表示强制要求，◎ 表示必选其一。					

5.5.2 密码使用要求

密码使用应满足下列要求：

a） 具备密钥管理、证书管理功能；

b） 采用国产商用密码算法，构建移动警务系统 PKI 证书体系，进行加解密保护，并符合 GM/T 0034 相关技术要求；

c） 使用移动警务系统根证书，由公安信息网根证书按统一格式签发；

d） 采用国产商用密码算法的专用硬件密码设备，对系统关键信息节点进行保护。

5.5.3 跨区域安全防护要求

跨区域安全防护应满足下列要求：

a） 在Ⅰ类区域与Ⅱ类区域之间，具备网络隔离、数据安全交换和应用访问控制等功能；

b） 在Ⅱ类区域之间，具备数据安全传输、互联边界防护等功能；

c） 在Ⅱ类区域与Ⅲ类区域之间，具备设备安全接入、网络隔离、数据安全交换、应用访问控制等功能，禁止未脱敏降级的敏感数据出公安信息网；

d） 在Ⅱ类区域与其他专网之间，具备网络隔离、数据安全交换、应用访问控制等功能；

e） 在各类区域之间，禁止旁路跨区域安全防护功能。

5.5.4 数据安全要求

移动警务系统自身产生和通过移动警务系统使用的数据，应满足下列要求：

a） 进行移动警务数据分类分级安全保护；

b） 跨系统的数据交换满足高安全等级系统的安全要求；

c） 从高安全等级向低安全等级系统数据交换时进行脱敏降级。

5.5.5 安全管控系统要求

安全管控系统应满足下列要求：

a） 管控对象包括但不限于用户、终端、网络、应用和数据；

b） 具备数据采集和上报、策略接收和下发等功能。

5.5.6 集中管控中心要求

集中管控中心应满足下列要求：

a） 具备资产管理、日志审计、关联分析、策略管理、安全管理等功能；

b） 将监测信息报送到上级集中管控中心，并从上级集中管控中心接收并执行安全策略与指令。

中华人民共和国公共安全
行业标准
移动警务系统　总体技术要求
GA/T 1561—2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年8月第一版
*
书号:155066·2-34502

GA/T 1561-2019