ICS 35.240.99
CCS A 90

GA

中华人民共和国公共安全行业标准

GA/T 1768—2021

移动警务　身份认证技术要求

Mobile police—Technical requirements for identity authentication

2021-03-02 发布　　2021-05-01 实施

中华人民共和国公安部　　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。

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。

本文件由公安部科技信息化局提出。

本文件由公安部计算机与信息处理标准化技术委员会归口。

本文件起草单位：公安部科技信息化局、河南省公安厅、公安部第一研究所、公安部第三研究所、格尔软件股份有限公司、郑州信大捷安信息技术股份有限公司、长春吉大正元信息技术股份有限公司。

本文件主要起草人：袁艺芳、李伟强、王毅、陈巧慧、张端涛、王卓、陈骁、陈昌前、陈家明、梁松涛、韩秀德、刘兴兴、邓勇。

移动警务　身份认证技术要求

1　范围

本文件规定了移动警务身份认证的总体要求、技术要求、跨区域认证要求和跨平台认证要求。

本文件适用于移动警务身份认证系统建设、应用接入以及相关产品的设计和开发。

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 25069　信息安全技术　术语

GB/T 35678　公共安全　人脸识别应用图像技术要求

GB/T 37076　信息安全技术　指纹识别系统技术要求

GA/T 380　全国公安机关机构代码编制规则

GA/T 543(所有部分)　公安数据元

GA/T 1053　数据项标准编写要求

GA/T 1054(所有部分)　公安数据元限定词

GA/T 1561　移动警务系统　总体技术要求

GA/T 1720　移动警务　数字证书格式要求

GM/Z 0001　密码术语

GM/T 0018　密码设备应用接口规范

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

GB/T 25069、GA/T 1561 和 GM/Z 0001 界定的以及下列术语和定义适用于本文件。

3.1

移动警务数字证书　digital certificate for mobile police information system

标识移动警务系统用户、机构、设备和应用真实身份的数字证书。

3.2

统一认证　unified authentication

在移动警务系统中，采用一致的技术手段，对认证对象身份进行鉴别的过程。

3.3

票据　token

在统一认证中产生，表示认证对象访问的许可信息。

4　缩略语

下列缩略语适用于本文件。

ID:身份标识(Identity)
MAC:介质访问控制(Media Access Control)
NFC:近场通信(Near Field Communication)

5 总体要求

5.1 总体构成

移动警务身份认证部署在Ⅰ类区域、Ⅱ类区域和Ⅲ类区域中,各区域内身份认证均由对应的认证对象、认证服务和认证因子构成。移动警务平台可进行Ⅱ、Ⅲ类区域之间的跨平台认证,Ⅰ、Ⅱ、Ⅲ类区域之间可进行跨区域认证,移动警务身份认证总体构成示意图见图1。

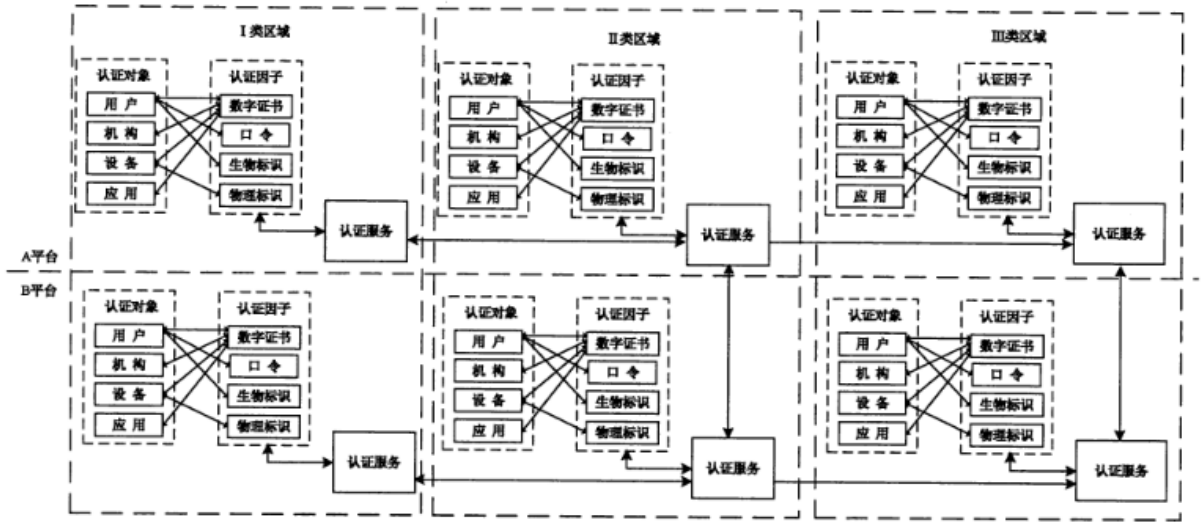

图1 移动警务身份认证总体构成示意图

5.2 技术框架

5.2.1 概述

移动警务身份认证技术框架包括认证管理、认证对象、认证服务和认证因子四部分,移动警务身份认证技术框架示意图见图2。

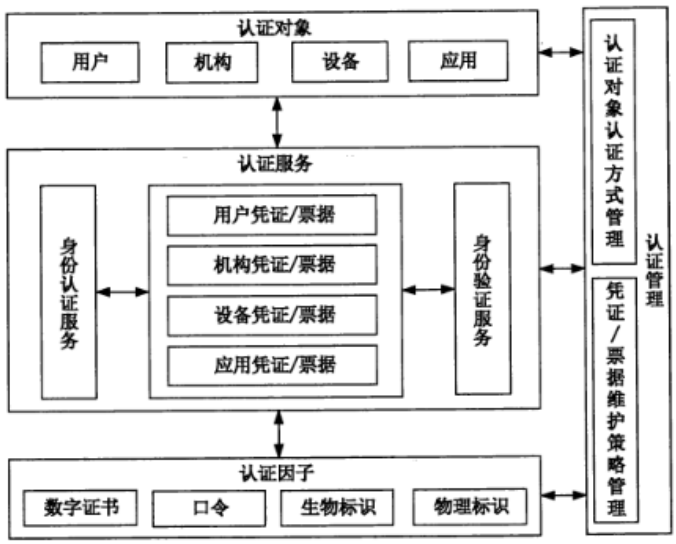

图 2　移动警务身份认证技术框架示意图

5.2.2　认证对象

认证对象包含用户、机构、设备和应用等，其中：

a）　用户包含内部用户和外部用户，内部用户包含民警和警务辅助人员，外部用户包含党政用户和企事业用户等；

b）　机构包含党政部门和企事业单位等；

c）　设备包含移动警务终端、服务器和专用设备等；

d）　应用包含应用客户端和应用服务端。

5.2.3　认证因子

认证因子包含但不限于数字证书、口令、生物标识和物理标识，其中：

a）　数字证书采用 SM2 算法并符合 GM/T 0034 的规定，证书存储方式采用硬件密码模块或软件密码模块；

b）　口令包含但不限于密码口令和短信验证码；

c）　生物标识包含但不限于人脸和指纹；

d）　物理标识包含但不限于 MAC 地址、设备 ID 等硬件唯一标识。

5.2.4　认证服务

认证服务分为Ⅰ类系统认证服务、Ⅱ类系统认证服务和Ⅲ类系统认证服务，其中：

a）　Ⅰ类系统认证服务为Ⅰ类区域用户提供实名认证，为机构、设备和应用提供统一认证服务，发放认证凭证/票据；

b）　Ⅱ类系统认证服务为Ⅱ类区域用户、机构、设备和应用提供统一认证服务，发放认证凭证/票据；

c）　Ⅲ类系统认证服务为Ⅲ类区域用户、机构、设备和应用提供统一认证服务，发放认证凭证/票据。

5.2.5 认证管理

认证管理包含但不限于认证对象认证方式管理和凭证/票据维护策略管理，其中：

a) 认证对象认证方式管理，按照Ⅰ、Ⅱ、Ⅲ类区域的安全防护要求，采用单因子、双因子或多因子认证方式；

b) 凭证/票据维护策略管理，按照Ⅰ、Ⅱ、Ⅲ类区域的安全防护要求，设置凭证/票据的有效期，更新、延期条件等。

6 技术要求

6.1 认证对象要求

6.1.1 用户认证

用户认证需满足下列要求：

a) 根据信息重要程度，Ⅰ类系统用户可采用密码口令、短信验证码、数字证书、NFC 读取二代身份证、生物标识中的一种或多种方式进行身份认证，对重要信息的访问，还应采用实名认证；

b) Ⅱ类系统用户应采用硬件密码模块或软件密码模块的移动警务数字证书进行身份认证，宜采用一种或多种其他认证标识进行辅助认证，认证场景包含人机认证和系统认证等；

c) Ⅲ类系统用户应采用硬件密码模块的移动警务数字证书进行身份认证，其他应符合Ⅱ类系统用户认证技术要求。

6.1.2 机构认证

机构认证应满足下列要求：

a) Ⅰ类系统机构采用数字证书进行认证，同时对其访问的数据、服务及应用等资源进行限定；

b) Ⅱ类系统机构采用硬件密码模块或软件密码模块的移动警务数字证书进行身份认证；

c) Ⅲ类系统机构采用硬件密码模块的移动警务数字证书进行身份认证。

6.1.3 设备认证

设备认证应满足下列要求：

a) Ⅰ类系统设备采用数字证书或基于物理标识的认证方式进行身份认证；

b) Ⅱ类系统设备采用硬件密码模块或软件密码模块的移动警务数字证书进行身份认证，设备证书应包括设备的唯一物理标识；

c) Ⅲ类系统设备采用硬件密码模块的移动警务数字证书进行身份认证，设备证书应包括设备的唯一物理标识。

6.1.4 应用认证

应用认证应满足下列要求：

a) Ⅰ类系统应用采用数字证书进行身份认证；

b) Ⅱ类系统应用采用硬件密码模块或软件密码模块的移动警务数字证书进行身份认证；

c) Ⅲ类系统应用采用硬件密码模块的移动警务数字证书进行身份认证。

6.2 认证因子要求

6.2.1 数字证书

数字证书应满足下列要求：

a) Ⅰ类系统数字证书密码算法采用国产密码算法；

b) Ⅱ、Ⅲ类系统移动警务数字证书采用签名和加密双证书机制，密码算法采用国产密码算法，认证接口符合 GM/T 0018 的规定，证书格式符合 GA/T 1720 的规定；

c) 数字证书产品需通过国家密码管理部门检测。

6.2.2 口令

口令应满足下列要求：

a) 口令由大小写字母、数字和符号组成，长度 8 位及以上，定期更换；

b) 口令进行加密存储和传输，具备防暴力破解能力；

c) 短信验证码长度 6 位及以上，设定有效期，且一次有效。

6.2.3 生物标识

生物标识应满足下列要求：

a) 生物特征信息进行加密存储和传输；

b) 人脸图像采集具备活体检测能力，采样、比对的阈值应符合 GB/T 35678 的规定；

c) 指纹识别符合 GB/T 37076 的规定。

6.2.4 物理标识

物理标识应选择硬件 ID、MAC 地址、蓝牙地址等硬件唯一标识。

7 跨区域认证要求

跨区域认证应满足下列要求：

a) Ⅰ类应用跨区域访问Ⅱ类系统信息资源时，由Ⅰ类系统服务总线向Ⅱ类系统服务总线传递凭证/票据的身份信息；

b) Ⅱ类应用跨区域访问Ⅰ类系统信息资源时，由Ⅱ类系统服务总线向Ⅰ类系统服务总线传递凭证/票据的身份信息；

c) Ⅱ类应用跨区域访问Ⅲ类系统信息资源时，由Ⅱ类系统服务总线向Ⅲ类系统服务总线传递凭证/票据的身份信息。

8 跨平台认证要求

8.1 概述

统一认证支持跨平台的身份认证与信任传递，其认证机制与流程示意图见图 3。

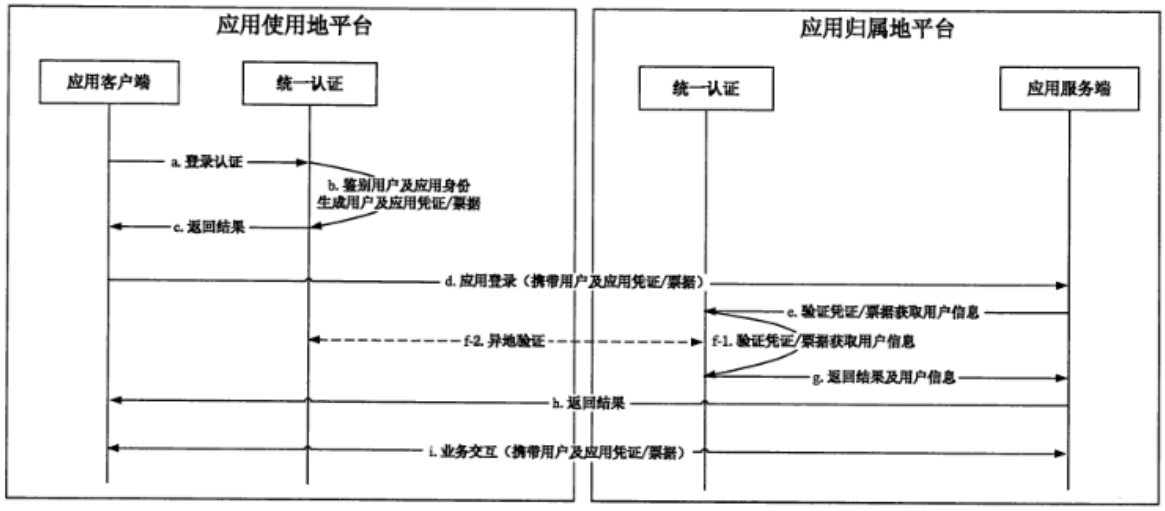

图 3　跨平台身份认证机制与流程示意图

跨平台身份认证机制由应用使用地平台和应用归属地平台联动，提供统一的身份鉴别、验证和身份信息获取等服务。应用使用地平台为当地运行的应用客户端提供服务。应用归属地平台为当地运行的应用服务端提供服务。

8.2　跨平台认证流程及要求

跨平台认证流程及要求如下：

a）　应用客户端启动时，调用统一认证客户端的身份凭证/票据获取接口，传递应用标识等参数；

b）　统一认证鉴别身份，进行鉴权，生成凭证/票据；

c）　统一认证向应用客户端返回或定向广播认证结果，应用客户端获取身份凭证/票据；

d）　应用客户端登录应用归属地平台应用服务端时，在请求报文中携带身份凭证/票据；

e）　应用服务端调用应用归属地平台的统一认证，验证身份凭证/票据，获取身份信息，进行鉴权，完成登录操作；

f）　应用归属地平台的统一认证验证应用使用地平台签发的身份凭证/票据时，可在应用归属地或应用使用地验证，在应用归属地鉴权；

g）　应用归属地统一认证向应用服务端返回验证结果及用户信息；

h）　应用服务端向应用客户端返回验证结果；

i）　在业务交互中，无会话状态维持的应用需携带凭证，有会话状态维护的应用需携带票据；

j）　跨平台认证接口符合附录 A 的规定。

附 录 A
（规范性）
跨平台认证系统接口要求

A.1 接口标识命名规则

接口标识命名规则应满足以下要求：

a) 命名格式：IF-[模块标识]-[接口类型标识]-[接口序号]；

b) 模块标识：MAM 为移动应用市场，UA 为统一认证，UPM 为统一授权，RSB 为服务总线，CCM 为级联配置管理；

c) 接口类型：SDK 为模块客户端接口，SVC 为模块网络服务接口；

d) 平台信息、应用信息、资源信息等采用符合 GA/T 543(所有部分)、GA/T 1053 和 GA/T 1054(所有部分)规定的数据元、限定词和数据项。

A.2 接口通信协议

接口通信协议应满足以下要求。

a) Android 应用 APP 接口：用于原生应用客户端调用。通信协议、接口地址格式和广播接口应满足以下要求：

1) 通信协议：采用 Android 进程间通信方式 ContentProvier 和广播方式，通过 Android 参数传递请求、返回内容；

2) 接口地址格式：对于 ContentProvider 接口，地址为 URI，格式为“content://com.ydjw.[模块].[接口]”；

3) 广播接口：地址由 Intent 封装，格式为“com.ydjw.[模块].[消息标识符参数]”。

b) H5 移动应用客户端接口：用于 H5 Web 应用调用，采用 JS、HTTP 协议。

c) 网络服务接口：用于服务端调用，通信协议和接口地址格式满足以下要求：

1) 通信协议：采用无状态 HTTP Restful 格式，基于 HTTP1.1 协议，通过 POST 方法调用，交互数据格式为 JSON，交互数据内容使用 UTF-8 编码；

2) 接口地址格式：地址为 URL，格式为：“http://[网络地址/域名]:[端口]/[上下文名称]/v[版本号]/[接口名称]”，其中“网络地址”为 IPv4 格式，“端口”为阿拉伯数字，“上下文名称”为模块名称，“版本号”为十进制阿拉伯数字。

A.3 接口版本与兼容性

接口版本与兼容性应满足以下要求：

a) 在程序中增加新版本接口时，兼容旧版本；

b) 同一网络服务接口有多个版本的，接口以列表形式上报；

c) 兼容不同版本的 Android APP 接口。

A.4 Android 应用 APP 接口参数

Android 应用 APP 接口参数应满足以下要求：

a) ContentProvider 接口参数：输入、输出参数采用 Android Bundle 封装方式，由应用进行封装；

b) 广播接口参数：广播消息标识符为大写字母表示的静态常量。

A.5 网络协议接口参数

网络协议接口参数需满足以下要求。

a) 输入(请求)参数,应包括消息头 HTTP 协议头 Header 和消息体 Body 两部分,输入(请求)参数与图 A.1 相符合,其中:

1) 请求消息头包含 XXBS(消息标识)、YYPZ(应用凭证票据)/YYPJ(应用票据)、YHPZ(用户凭证票据)/YHPJ(用户票据)、ZYBS(资源标识,可选)和 ZYGSJGBS(资源归属机构标识,与资源标识成对出现,可选)。其中,资源标识应符合 GA/T 543(所有部分)的规定,资源归属机构标识应符合 GA/T 380 的规定。

2) 请求消息体 QQXXT,直接由 HTTP 协议的 Body 体封装请求参数。

b) 输出(响应)参数:应包括消息头 HTTP 协议头 Header 和消息体 Body 两部分,输出(响应)参数与图 A.2 相符合,其中:

1) 消息头包含:XXBS(请求者提交的消息标识)、CWDM(错误代码)、CWNR(错误内容)、XYPZ(需要凭证)/XYPJ(需要票据);

2) 错误代码类别应符合表 A.1 的规定;

3) 响应消息体 XYXXT,由 HTTP 协议的 Body 体封装返回的数据;

4) 对于需要返回记录集的接口,宜在返回消息体中增加分页参数:JLZS(总记录数)、DQYM(当前页码)。

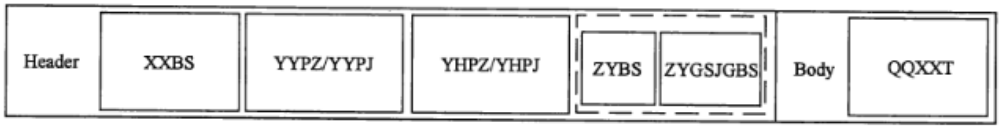

图 A.1 输入(请求)参数图

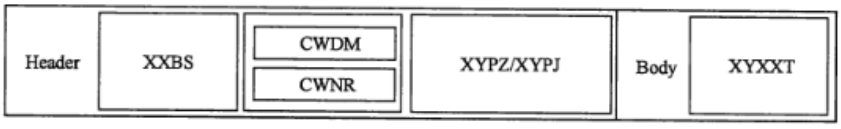

图 A.2 输出(响应)参数图

表 A.1 错误类别代码表

错误类别代码	描述
0	无错误
1	统一认证错误
2	统一授权错误
3	应用市场错误
4	移动服务总线错误
5	级联配置管理错误
6	应用开发服务错误
7	应用运行监测错误