ICS 35.240.99
A 90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

移动警务 PKI 系统总体技术要求

Mobile police —— General technical requirements for PKI system

（报批稿）

（本稿完成于 2020 年 10 月 20 日）

xxxx-xx-xx 发布　　xxxx-xx-xx 实施

中华人民共和国公安部　　发　布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义、缩略语 1
4 总体架构 2
5 通用技术要求 3
6 接口要求 4
7 安全要求 5
8 管理要求 5
附录 A （规范性附录） 发证流程 6

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 PKI 系统总体技术要求

1 范围

本文件规定了移动警务 PKI 系统的总体架构、通用技术要求、接口要求、安全要求和管理要求。

本文件适用于移动警务 PKI 系统的规划、设计、建设、验收和管理等。

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 19771 信息技术 安全技术 公钥基础设施 PKI组件最小互操作规范

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25069 信息安全技术 术语

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密码算法的证书系统密码及其相关安全技术规范

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

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

空中发证 autonomous certificate issuance based on wireless mode

依托无线传输链路申请和签发数字证书的方式。

4 缩略语

下列缩略语适用于本文件。

CA：证书认证机构（Certificate Authority）

CRL：证书吊销列表（Certificate Revocation List）
KMC：密钥管理中心（Key Management Center）
LDAP：轻量级目录访问协议（Lightweight Directory Access Protocol）
LRA：本地证书注册机构（Local Registration Authority）
PKI：公钥基础设施（Public Key Infrastructure）
RA：证书注册机构（Registration Authority）

5　总体架构

5.1　系统架构

移动警务 PKI 系统包括中央系统和下级系统，中央系统为唯一根节点，包括 LDAP 和 CA，下级系统包括 LDAP、CA、RA、LRA 和 KMC。系统架构示意图见图 1。

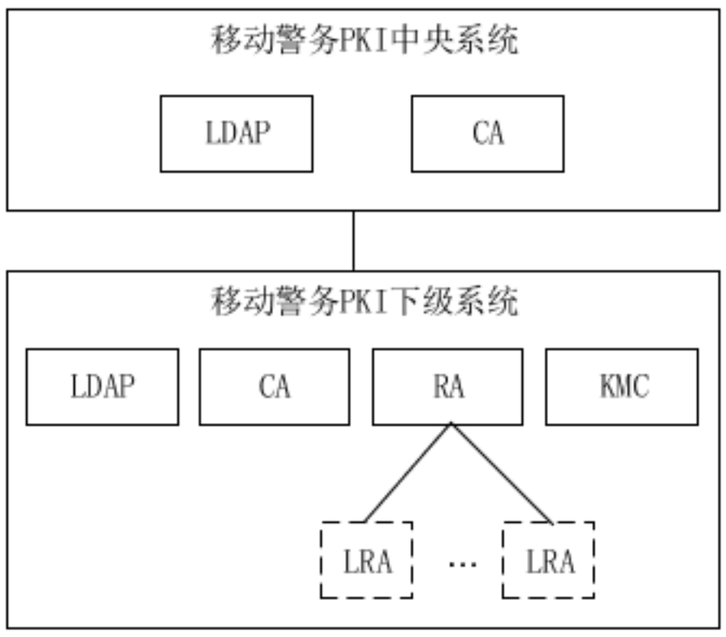

图 1 移动警务 PKI 系统架构示意图

其中：

a）　LDAP 实现移动警务证书和 CRL 的存储与发布，中央系统 LDAP 存储所有下级系统的移动警务证书和 CRL，并提供所有下级系统 LDAP 的地址服务；
b）　CA 实现移动警务数字证书的签发，中央系统 CA 签发下级系统 CA 证书，下级系统 CA 实现移动警务数字证书的签发、更新、延期、注销以及 CRL 生成等；
c）　RA 实现移动警务数字证书的注册、申请、审核和发放等；
d）　LRA 基于 RA 实现本地移动警务数字证书的注册、申请和发放等，可按需部署；
e）　KMC 为移动警务数字证书提供加密证书密钥对的生成及管理功能。

5.2 系统部署

移动警务 PKI 系统部署与图 2 相符合。

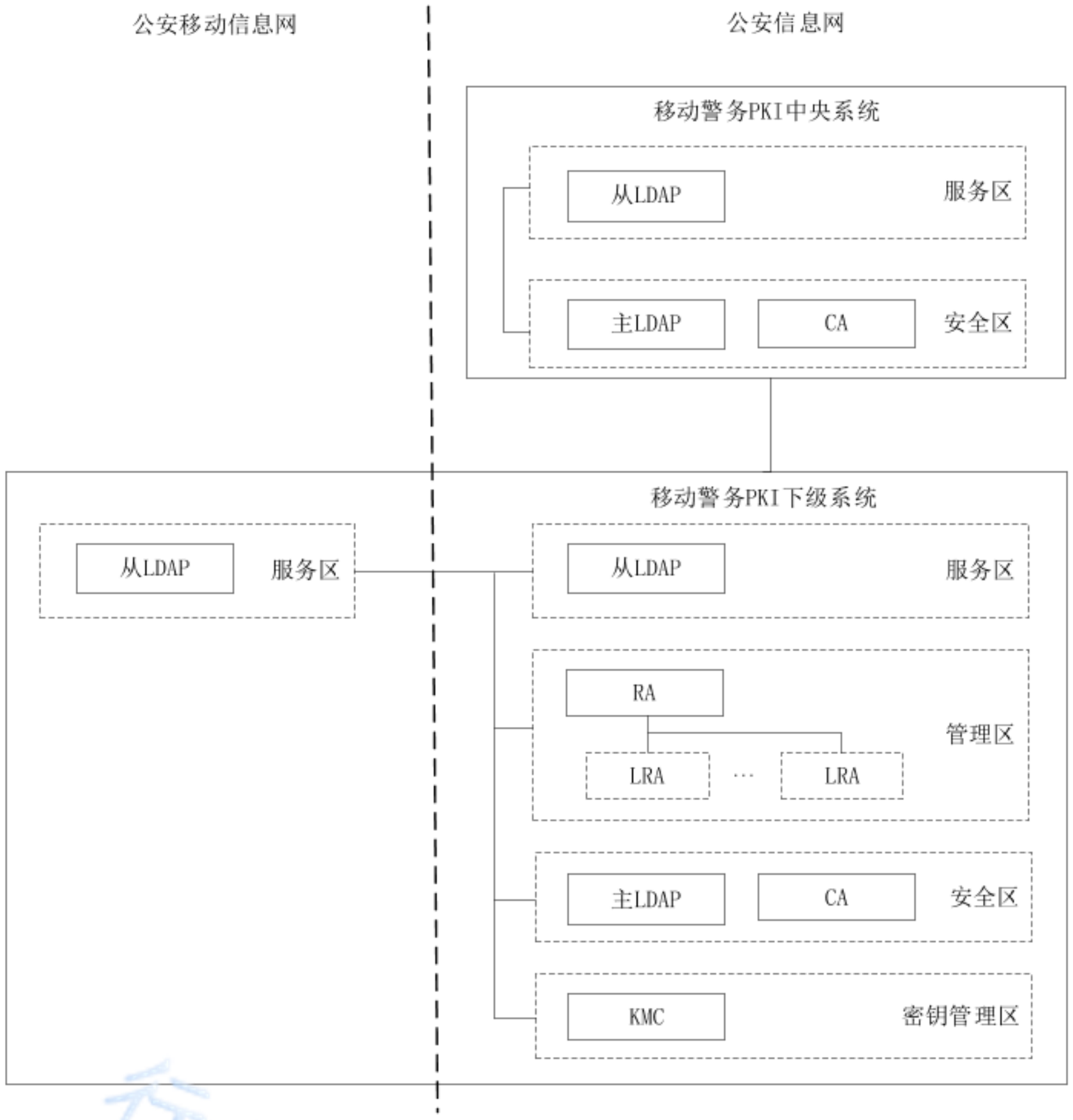

图 2 移动警务 PKI 系统部署图

其中：

a) 移动警务 PKI 中央系统部署在公安信息网中，其 LDAP 进行主从部署，从 LDAP 部署在服务区，主 LDAP 和 CA 部署在安全区；

b) 移动警务 PKI 下级系统部署在公安信息网和公安移动信息网中，其 LDAP 进行主从部署，从 LDAP 在公安信息网和公安移动信息网的服务区同时部署， RA 和 LRA 部署在公安信息网的管理区，主 LDAP 和 CA 部署在公安信息网的安全区， KMC 部署在公安信息网的密钥管理区。

6 通用技术要求

6.1 目录服务要求

目录服务应满足下列要求：

a) 主 LDAP 将移动警务数字证书及 CRL 同步到从 LDAP；

b) 部署在公安信息网的下级系统从 LDAP 与公安移动信息网的从 LDAP 建立同步机制；

c) 下级系统 LDAP 上报本级所有移动警务数字证书及 CRL；

d） 中央系统 LDAP 提供所有下级系统 LDAP 地址及目录服务。

6.2 证书发放要求

证书发放需满足下列要求：

a） Ⅰ类系统的数字证书格式宜符合 RFC 5280 的规定，数字证书的申请和发放流程应符合 GB/T 25056 的规定；

b） Ⅱ类系统移动警务数字证书应由移动警务 PKI 系统签发，证书格式应符合 GA/T 1720 的规定，介质应使用通过国家密码产品管理部门检测的硬件或软件密码模块，接口调用宜符合 GM/T 0018 的要求；

c） Ⅲ类系统移动警务数字证书应由移动警务 PKI 系统签发，证书格式应符合 GA/T 1720 的规定，介质应使用通过国家密码产品管理部门检测的硬件密码模块，接口调用应符合 GM/T 0018 的要求；

d） 移动警务数字证书的申请和发放流程应符合附录 A 的要求；

e） 支持批量证书申请和用户管理。

6.3 证书中心要求

证书中心应满足下列要求：

a） 支持同时签发加密证书和签名证书；

b） 采用国产商用密码算法；

c） 支持签发用户证书、机构证书、设备证书和应用证书；

d） 支持空中发证、有线发证和离线发证。

6.4 密钥管理要求

密钥管理应满足下列要求：

a） 支持加密证书密钥对的全生命周期管理，包括生成、注册、分发、安装、存储、使用、更新、废除、归档、撤销、注销、销毁、备份和恢复等；

b） 基于通过国家密码产品管理部门检测的硬件密码设备，实现密钥的生成及管理。

7 接口要求

7.1 接口功能

应为第三方提供移动警务数字证书的签发、撤销、更新等接口服务。

7.2 接口协议

接口协议应满足下列要求：

a） 移动警务 PKI 系统采用 HTTP 或 HTTPS 协议为第三方提供接口服务，请求报文头中“ContentType”值为“application/x-www-form-urlencoded”，请求报文体采用 URLEncode 编码；

b） 请求报文体中采用 UniqueUserKey 标识用户信息；

c） 对外提供服务的 URL 地址应为：“[http|https]://HOST:PORT/servlet/[*]JsonRpcServlet”，其中：

1） HOST 为服务端地址；

2） PORT 为服务端口，宜为 8080/8443/8043；

3） “*”为移动警务 PKI 系统服务标识。

8 安全要求

安全要求应满足下列要求：

a） 移动警务 PKI 系统自身安全符合 GA/T 1561 的规定；

b） CA 和 RA 符合 GB/T 19771 的规定，KMC 符合 GM/T 0034 的规定；

c） 服务区、管理区、安全区、密钥管理区之间，以及与外部信息网络之间的安全防护措施包括但不限于边界防护、访问控制、入侵防御。

9 管理要求

9.1 系统管理

系统管理需满足下列要求：

a) 宜对用户、机构、设备和应用等移动警务数字证书对象的基础信息进行管理；

b) 应对系统进行分级管理；

c) 应对系统按系统管理员、安全管理员和审计管理员进行权限管理；

d) 应对系统登录进行基于数字证书的双因子或多因子认证，包含且不限于口令、生物标识、物理标识等；

e) 系统软硬件环境、配置参数或安全策略等的改变，应经主管部门批准后再实施。

9.2 审计管理

审计管理应满足下列要求：

a) 对移动警务数字证书的申请、审批、签发、更新、撤销、备份和恢复等行为进行审计；

b) 审计记录包括时间、对象、操作类型、操作是否成功等信息；

c) 对审计记录进行保护、备份；

d) 对审计过程进行保护。

附录 A
（规范性附录）
发证流程

A.1 概述

证书发放方式流程包括出空中发证、有线发证和离线发证三种。

A.2 空中发证流程

空中发证基于移动警务 PKI 系统，通过空中发证客户端、密码模块、空中发证服务端、身份认证服务实现。空中发证流程示意图见图 A.1。

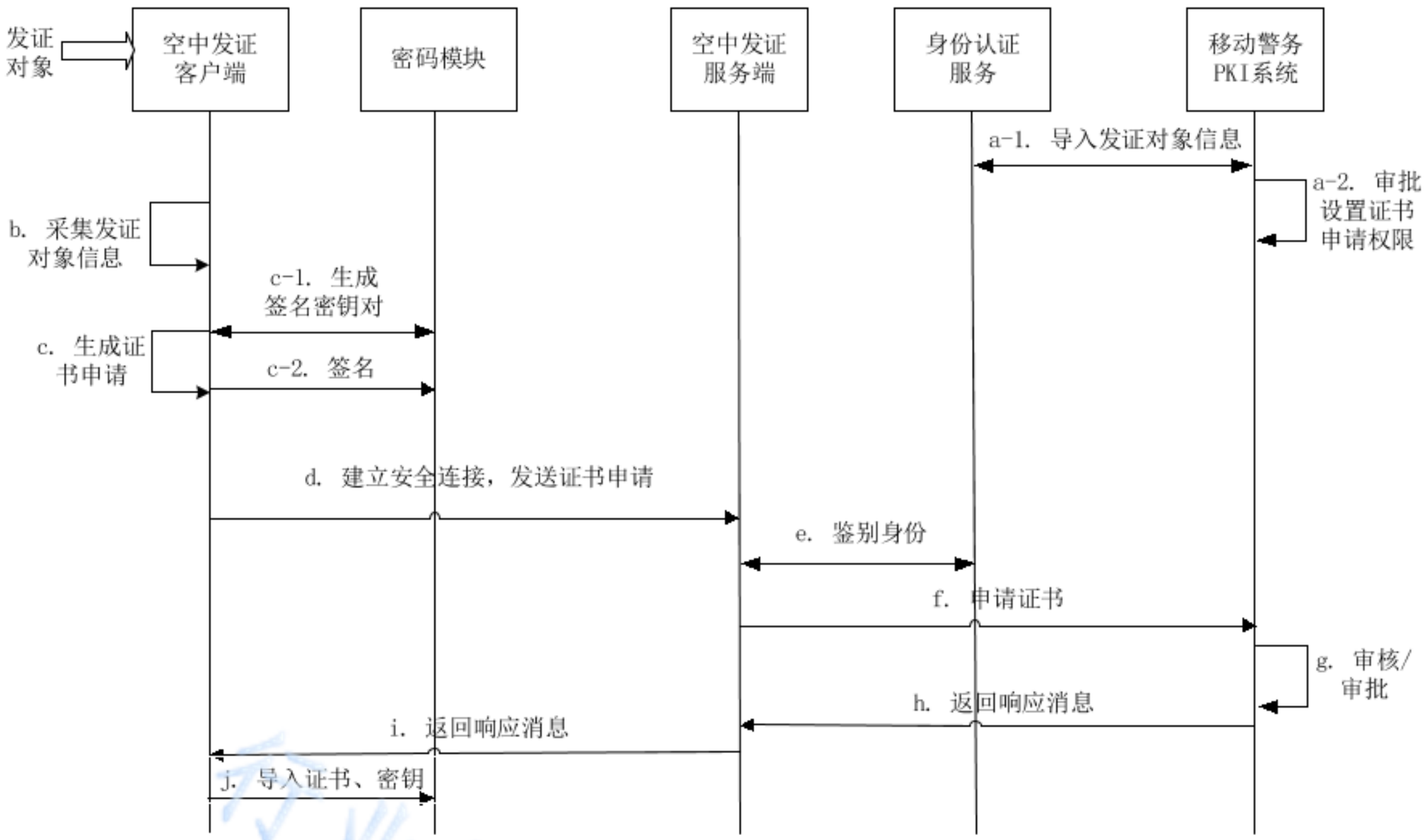

图 A.1 空中发证流程示意图

具体步骤为：

a) 预先录入发证对象信息，并导入身份认证服务和移动警务 PKI 系统，审批设置证书申请权限；
b) 空中发证客户端采集发证对象信息；
c) 空中发证客户端调用密码模块生成密钥对，私钥不可导出，空中发证客户端生成证书申请，调用密码模块对申请进行签名；
d) 空中发证客户端与空中发证服务端建立安全连接，发送证书申请消息；
e) 空中发证服务端调用身份认证服务，对收到的对象特征信息进行鉴别；
f) 空中发证服务端提交证书申请至移动警务 PKI 系统；
g) 移动警务 PKI 系统对证书申请操作进行审核、审批；
h) 移动警务 PKI 系统生成加密密钥对、加密证书、签名证书，返回响应消息至空中发证服务端；
i) 空中发证服务端将响应消息发送至空中发证客户端；
j) 空中发证客户端解析、验证响应消息，取出加密私钥、加密证书和签名证书，导入密码模块。

A.3 有线发证流程

有线发证基于移动警务 PKI 系统，通过密码模块和发证系统管理端实现。有线发证流程示意图见图 A.2。

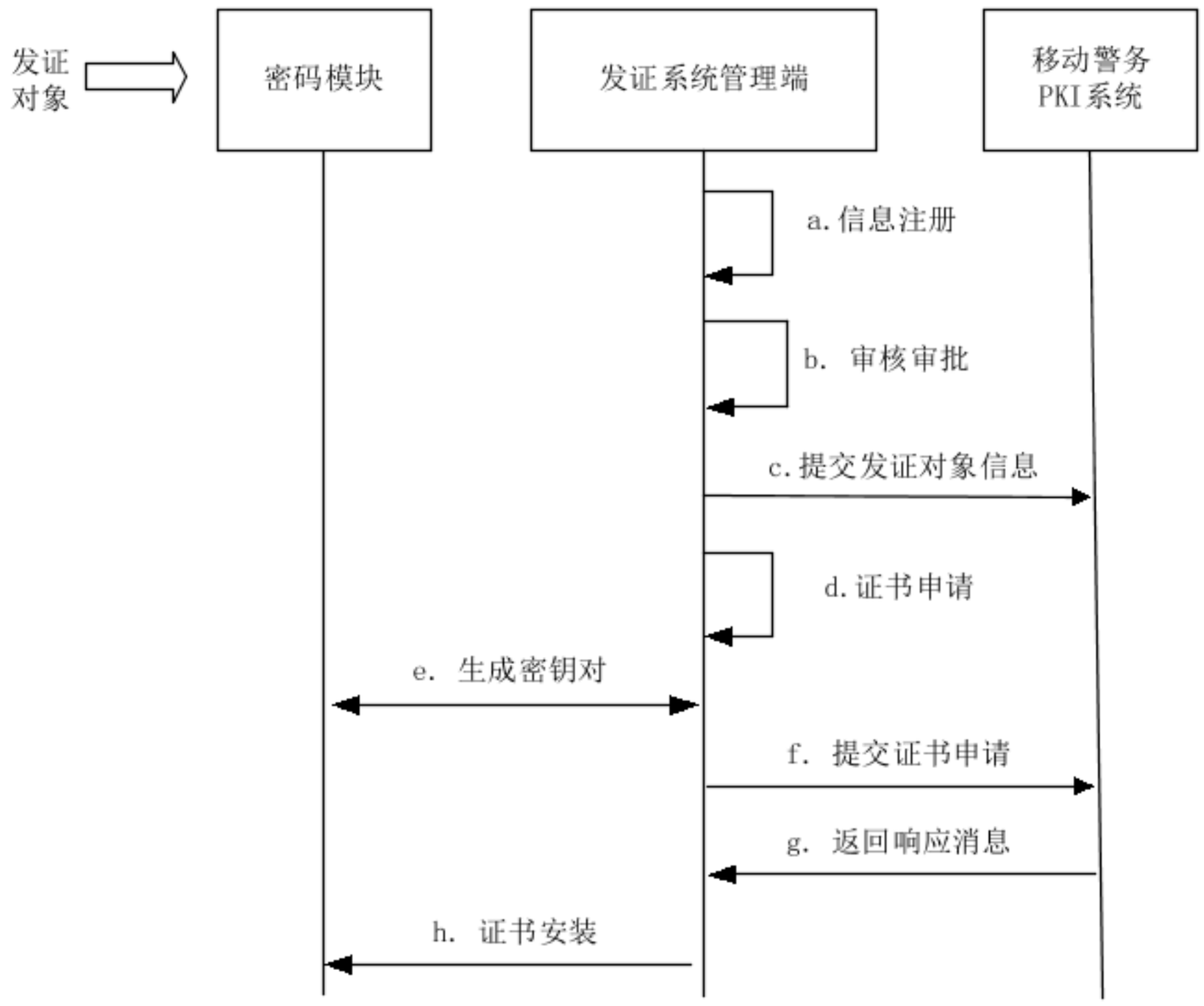

图 A.2 有线发证流程示意图

具体步骤为：

a) 在发证系统管理端注册发证对象信息；
b) 在发证系统管理端进行审核、审批；
c) 发证系统管理端向移动警务 PKI 系统提交发证对象信息；
d) 在发证系统管理端为发证对象申请证书；
e) 发证系统管理端调用密码模块，生成密钥对；
f) 发证系统管理端向移动警务 PKI 系统提交证书申请；
g) 移动警务 PKI 系统向发证系统管理端返回响应消息；
h) 发证系统管理端解析、验证响应消息，取出加密私钥、加密证书和签名证书，导入密码模块。

A.4 离线发证流程

离线发证基于移动警务 PKI 系统，通过密码模块和发证系统管理端实现，离线发证流程示意图见图 A.3。

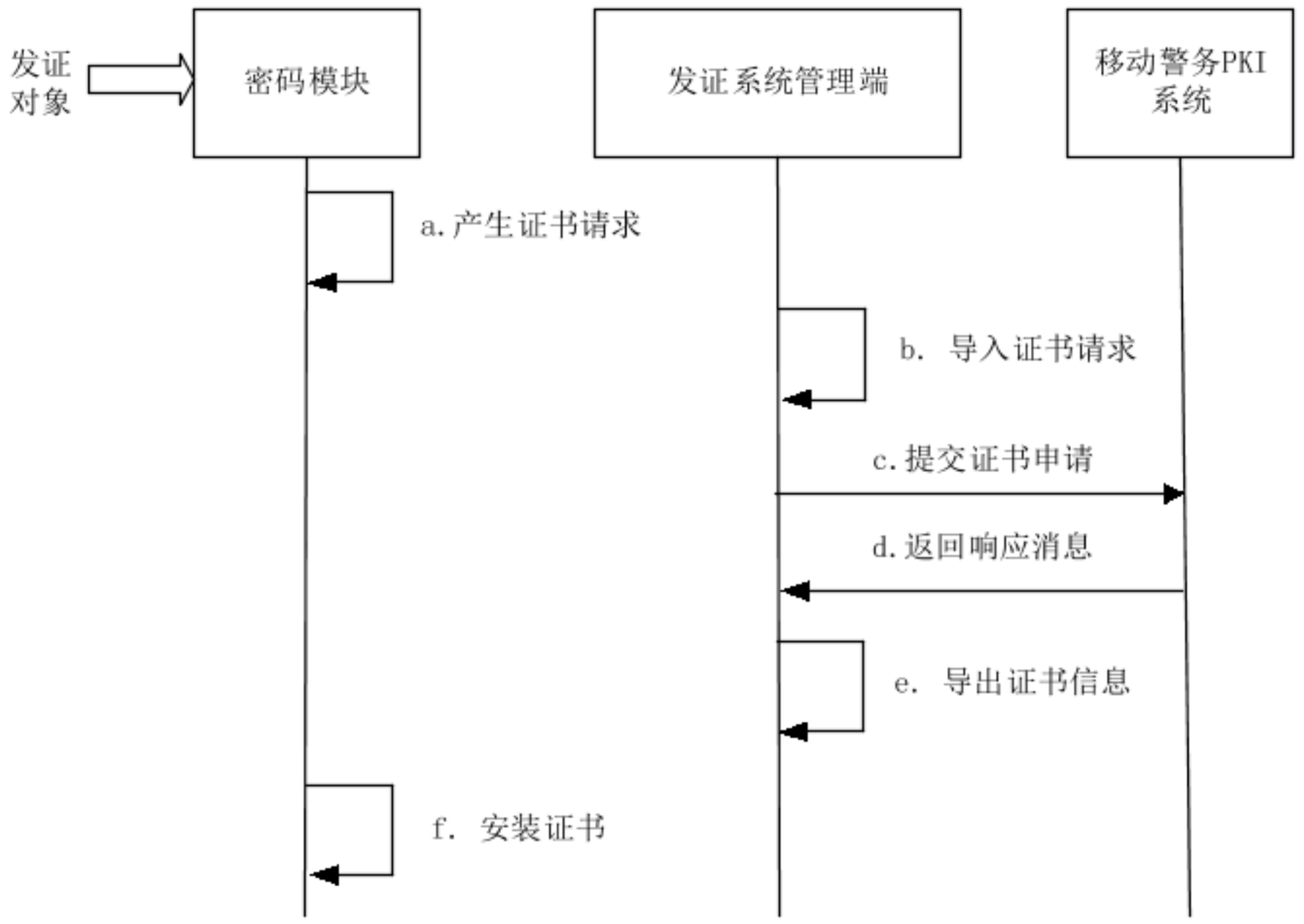

图 A.3 离线发证流程示意图

具体步骤为：

a) 调用密码模块产生证书请求；
b) 证书请求导入发证系统管理端；
c) 发证系统管理端向移动警务 PKI 系统提交证书申请；
d) 移动警务 PKI 系统向发证系统管理端返回响应消息；
e) 发证系统管理端解析、验证响应消息，取出加密私钥、加密证书和签名证书，并导出证书信息；
f) 导出的证书信息安装至密码模块。