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 1769—2021

移动警务　PKI 系统总体技术要求

Mobile police—General technical requirements for PKI system

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　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密码算法的证书认证系统密码及其相关安全技术规范

RFC 5280　互联网X.509公钥基础设施证书和证书吊销列表（CRL）配置文件[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）