



中华人民共和国公共安全行业标准

GA/T 1059—2013

警用数字集群(PDT)通信系统 安全技术规范

Police digital trunking communication system—
Security technical specifications

2013-03-20 发布

2013-03-20 实施

中华人民共和国公安部 发布

目 次

| | |
|------------------------------|-----|
| 前言 | III |
| 引言 | IV |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语、定义和缩略语 | 1 |
| 4 基本要求 | 4 |
| 5 鉴权要求 | 5 |
| 6 空口安全 | 16 |
| 7 端到端语音加密 | 27 |
| 8 端到端数据安全 | 33 |
| 附录 A (资料性附录) MSC 图 | 36 |
| 图 1 PDT 协议分层架构图 | 4 |
| 图 2 安全机制示意图 | 5 |
| 图 3 双向鉴权及遥晕/遥毙/复活流程 | 8 |
| 图 4 序列号同步流程 | 9 |
| 图 5 登记过程中的双向鉴权信令流程 | 10 |
| 图 6 TS 主动发起的双向鉴权信令流程 | 11 |
| 图 7 遥晕/遥毙/复活信令流程 | 12 |
| 图 8 序列号同步信令流程 | 12 |
| 图 9 空口密钥关系示意图 | 18 |
| 图 10 SYNC 信息单元示意图 | 18 |
| 图 11 EMB 信息单元示意图 | 18 |
| 图 12 SLOT TYPE 信息单元示意图 | 19 |
| 图 13 CACH 信息单元示意图 | 19 |
| 图 14 嵌入式信令帧信息单元示意图 | 19 |
| 图 15 数据控制帧信息单元示意图 | 19 |
| 图 16 语音帧信息单元示意图 | 20 |
| 图 17 密钥流产生示意图 | 22 |
| 图 18 复帧结构示意图 | 23 |
| 图 19 完整性校验码生成示意图 | 26 |
| 图 20 BCK 密钥更新示意图 | 27 |
| 图 21 语音时隙图 | 28 |

| | | |
|-------|--|----|
| 图 22 | 承载在 PI 头中的端到端加密控制帧格式 | 29 |
| 图 23 | 承载在嵌入式信令中的端到端加密控制帧格式 | 30 |
| 图 24 | 移动台与安全芯片的交互示意图 | 30 |
| 图 25 | 同步机制示意图 | 31 |
| 图 26 | 端到端加密呼叫流程示意图 | 32 |
| 图 27 | 数据时隙图 | 33 |
| 图 28 | 数据加密流程 | 34 |
| 图 A.1 | MSC 图 | 36 |
| | | |
| 表 1 | 业务流程的鉴权要求 | 5 |
| 表 2 | 鉴权参数 | 6 |
| 表 3 | 鉴权密码算法 | 7 |
| 表 4 | C_ALOHA 信令中的 AIETYPE 信息单元 | 13 |
| 表 5 | C_RAND 信令(请求登记/鉴权)中的 SO, SECDEV 信息单元 | 13 |
| 表 6 | C_AUTH 信令 | 13 |
| 表 7 | AUTH_AP 信令 | 13 |
| 表 8 | C_RES/C_NRES 信令 | 14 |
| 表 9 | C_ACKD/C_NACKD 信令中的 ARC 信息单元 | 14 |
| 表 10 | C_STUNKILL 信令 | 15 |
| 表 11 | C_AUTHSYNCD 信令 | 15 |
| 表 12 | AUTHSYNCD_AP 信令 | 15 |
| 表 13 | C_AUTHSYNCU 信令 | 16 |
| 表 14 | AUTHSYNCU_AP 信令 | 16 |
| 表 15 | 空口密码算法 | 17 |
| 表 16 | 嵌入式信令帧的空口加密指示 | 20 |
| 表 17 | 数据控制帧的空口加密指示 | 20 |
| 表 18 | 语音业务 GRANT 信令 | 21 |
| 表 19 | 密钥的选择 | 22 |
| 表 20 | SLC 形式的复帧帧号高位广播消息结构 | 24 |
| 表 21 | C_BCAST/P_BCAST 形式的复帧帧号广播消息结构 | 24 |
| 表 22 | 空口初始向量的构造 | 24 |
| 表 23 | 密钥流长度 | 25 |
| 表 24 | 完整性校验码的长度 | 26 |
| 表 25 | 端到端加密控制帧结构 | 28 |
| 表 26 | PI 标识 | 29 |
| 表 27 | 嵌入式信令中的端到端加密控制帧信息单元定义 | 29 |
| 表 28 | 端到端加密数据头 | 33 |
| 表 29 | DPF 和 SAP 信息单元 | 34 |

前 言

本标准是警用数字集群(PDT)通信系统技术规范系列标准之一。该系列标准文件的结构及名称预计如下:

- 警用数字集群(PDT)通信系统 总体技术规范;
- 警用数字集群(PDT)通信系统 空中接口物理层及数据链路层技术规范;
- 警用数字集群(PDT)通信系统 空中接口呼叫控制层技术规范;
- 警用数字集群(PDT)通信系统 移动终端技术规范;
- 警用数字集群(PDT)通信系统 安全技术规范;
- 警用数字集群(PDT)通信系统 互联技术规范;
- 警用数字集群(PDT)通信系统 测试技术规范。

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

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、公安部第一研究所。

本标准主要起草人:马晓东、朱振荣、周昕、李江、宋振苏、蒋庆生、陈妍、刘衍斐、王为民、钱志红。

引 言

为了规范警用数字集群(PDT)通信系统的安全技术体制,使不同供应商提供的安全设备具有互操作性,特制定本标准。

本标准不提供系统实施的规格或操作详情,仅规定与安全相关的适当要求。

警用数字集群(PDT)通信系统 安全技术规范

1 范围

本标准规定了应用于警用数字集群(PDT)通信系统中鉴权、空中接口安全和端到端安全等方面的技术规范和要求。

本标准适用于警用数字集群(PDT)通信系统安全加密子系统的建设和应用。

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。

GA/T 1056—2013 警用数字集群(PDT)通信系统 总体技术规范

GA/T 1057—2013 警用数字集群(PDT)通信系统 空中接口物理层及数据链路层技术规范

GA/T 1058—2013 警用数字集群(PDT)通信系统 空中接口呼叫控制层技术规范

3 术语、定义和缩略语

3.1 术语和定义

GA/T 1056—2013、GA/T 1057—2013 和 GA/T 1058—2013 界定的以及下列术语和定义适用于本文件。

3.1.1

鉴权 authentication

验证通信参与方身份合法性的过程。

3.1.2

遥晕 stun

利用空口信令临时禁用移动台的过程。

3.1.3

复活 revive

利用空口信令解禁被遥晕移动台的过程。

3.1.4

遥毙 kill

利用空口信令永久禁用移动台的过程,被遥毙的移动台无法通过空口信令解禁。

3.1.5

鉴权中心 authentication centre

负责与移动台进行鉴权的安全实体。

3.1.6

鉴权密钥 authentication key

鉴权过程中使用的密钥。