



中华人民共和国密码行业标准

GM/T 0098—2020

基于 IP 网络的加密语音通信 密码技术规范

**Cryptographic technical specifications for encrypted voice
communication based on IP network**

2020-12-28 发布

2021-07-01 实施

国家密码管理局 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 基于 IP 网络的加密语音通信系统	3
5.1 概述	3
5.2 系统框架	4
5.3 业务过程	4
6 密钥管理	5
6.1 概述	5
6.2 终端证书及密钥对	5
6.3 服务器证书及密钥对	6
6.4 会话密钥	7
7 安全协议	7
7.1 会话建立	7
7.2 开户绑定	8
7.3 密钥分发	11
7.4 密钥协商	15
7.5 通信数据	18
7.6 Sip 流程	19
8 密码模块	20
8.1 功能	20
8.2 接口	20
8.3 安全性	20
9 其他安全要求	21
9.1 敏感数据保护	21
9.2 管理安全	21
9.3 角色设定	21
9.4 身份鉴别	21
9.5 日志管理	21
9.6 密钥备份	21
10 产品检测基本要求	21
10.1 产品功能检测基本要求	21
10.2 产品性能检测基本指标	22

10.3	密钥管理检测要求	22
10.4	密码模块检测要求	23
10.5	其他安全检测基本要求	23
附录 A (规范性)	基于 SM9 密码算法的加密语音通信系统	24
附录 B (资料性)	基于 SM9 密码算法的安全协议 SIP 报文	35
附录 C (资料性)	会话过程示例	37
附录 D (资料性)	安全协议 SIP 报文	39

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。

本文件按照 GB/T 1.1—2009 给出的规则起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京三未信安科技发展有限公司、山东大学软件学院、北京数字认证股份有限公司、公安部第一研究所、数安时代科技股份有限公司、北京创原天地科技有限公司、大唐高鸿数据网络技术股份有限公司、国家信息中心、北京数盾信息科技有限公司、成都二零瑞通移动通信有限公司、青岛海信通信有限公司、深圳奥联信息安全技术有限公司。

本文件主要起草人：高志权、刘晓东、张玉涛、张永强、亢洋、赵振涛、张磊、王胜男、方恒禄、王允升、许涛、李耀龙、吕国栋、吕士鹏、白顺东。

基于 IP 网络的加密语音通信 密码技术规范

1 范围

本文件定义了基于 IP 网络的加密语音通信系统、密钥管理、安全协议、密码模块、安全要求和产品检测基本要求。

本文件适用于指导基于 IP 网络的加密语音通信系统应用中密码安全方案设计、产品研制,也可用于指导基于 IP 网络的加密语音通信系统产品的检测。

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 32905 信息安全技术 SM3 密码杂凑算法
- GB/T 32907 信息安全技术 SM4 分组密码算法
- GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法
- GB/T 33133.1 信息安全技术 祖冲之序列密码算法 第 1 部分:算法描述
- GB/T 35291 信息安全技术 智能密码钥匙应用接口规范
- GB/T 36322 信息安全技术 密码设备应用接口规范
- GB/T 37092 信息安全技术 密码模块安全要求
- GM/T 0027 智能密码钥匙技术规范
- GM/T 0028 密码模块安全要求
- GM/T 0030 服务器密码机技术规范
- GM/T 0044 SM9 标识密码算法
- GM/T 0044.1 SM9 标识密码算法 第 1 部分:总则
- GM/T 0044.2 SM9 标识密码算法 第 2 部分:数字签名算法
- GM/T 0044.3 SM9 标识密码算法 第 3 部分:密钥交换协议
- GM/T 0044.4 SM9 标识密码算法 第 4 部分:密钥封装机制和公钥加密算法
- GM/T 0062 密码产品随机数检测要求
- GM/Z 4001—2013 密码术语
- RFC3261 SIP:Session Initiation Protocol

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用于本文件。

3.1

鉴别 authentication

为一个实体声称的特征是正确的而提供的保障措施。