ICS 35.040
CCS L 80

GM

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

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、成都三零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。

3.2

被叫　callee

通话过程中，接受呼叫的一方。

3.3

主叫　caller

通话过程中，主动发起呼叫的一方。

3.4

机密性　confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.5

密码模块　cryptographic module

具有安全边界的用于进行密码相关的存储和计算操作的软件、固件或硬件组合。

3.6

密码协议　cryptographic protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到某种特定目的而采用的一系列步骤。

3.7

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.8

实体　entity

人、组、设备或进程。

3.9

原发抗抵赖　non-repudiation of origin

旨在防止原发者否认其已创建了消息内容和已发送了消息的服务。

3.10

公钥密码算法/非对称密码算法　public-key cryptographic algorithm /asymmetric cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥（公钥）可公开，另一个密钥（私钥）必须保密，且由公钥求解私钥的计算是不可行的。

3.11

敏感数据　sensitive data

从用户的角度看，需要被保护的数据。

3.12

服务器证书　server certificate

由证书认证机构（CA）签发的用于标识服务器身份的数字证书。

3.13

会话　session

一次通信过程中所有参与者之间的关联关系以及他们之间的媒体流的集合。

3.14

会话密钥　session key

处于层次化密钥结构中的最低层，仅在一次会话中使用的密钥，依据用途可分为会话加密密钥和会话鉴别密钥。

3.15

SM2 算法　SM2 alogrithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.16

SM3 算法　SM3 algorithm

一种密码杂凑算法，杂凑值长度为 256 比特。

3.17

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.18

SM9 密码算法　SM9 algorithm

一种基于标识的非对称密码算法。

3.19

对称密码算法　symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。

3.20

通讯加密密钥　traffic encryption key

多媒体互联网密钥管理约定的用于保密会话的加密密钥。

3.21

通讯加密密钥生成密钥　TEK generation key

多媒体互联网密钥管理约定的流量加密密钥的生成密钥。

3.22

终端　terminal

具有通信能力的智能设备，包括手机、平板电脑等。

3.23

用户密钥　user key

存储在用户密码模块的用于密码运算的非对称密钥，包含签名密钥对和加密密钥对。

3.24

ZUC 算法　ZUC algorithm

一种分组密码算法。

4　缩略语

下列缩略语适用于本文件。

CA：数字证书认证中心(Certificate Authority)

PKI：公钥基础设施(Public Key Infrastructure)

SDP：会话描述协议(Session Description Protocol)

SIP：会话发起协议(Session Initiation Protocol)

VoIP：网际协议通话技术(Voice over Internet Protocol)

5　基于 IP 网络的加密语音通信系统

5.1　概述

基于 IP 网络的加密语音通信系统是指完全以 IP 网络为传输通道的实时语音传输通信系统，不包

含电信运营商的IP电话业务。

基于IP网络的加密语音通信系统将密码技术与VoIP通信技术有机结合，既能够提供语音业务的互联网传输，又在数据传输过程中有效保障数据的有效性、机密性和完整性。

本标准支持基于SM2密码算法的PKI密码体系。如采用基于SM9密码算法的标识密码体系，技术要求应符合附录A，安全协议报文见附录B。

5.2 系统框架

基于IP网络的加密语音通信系统组成见图1，由通信平台和通信终端两大部分组成，其中通信平台由通信系统和密钥管理模块组成。

通信终端作为系统内的主叫方或被叫方，拥有系统内唯一的VoIP账号，完成语音数据的采集和发送、语音数据加解密等功能。

通信平台负责完成用户终端VoIP账号的注册申请、语音数据传递、通信终端接入认证和会话密钥分发。

证书认证系统为通信终端和通信平台签发数字证书。

通信终端在通信平台完成VoIP账号的申请后，向通信平台提交VoIP账号和数字证书等信息完成终端开户。

主叫方发起会话，经由通信平台与被叫方建立语音通话，通信平台为通信双方分发会话密钥（或双方协商会话密钥），主被叫通话数据由会话密钥保护。

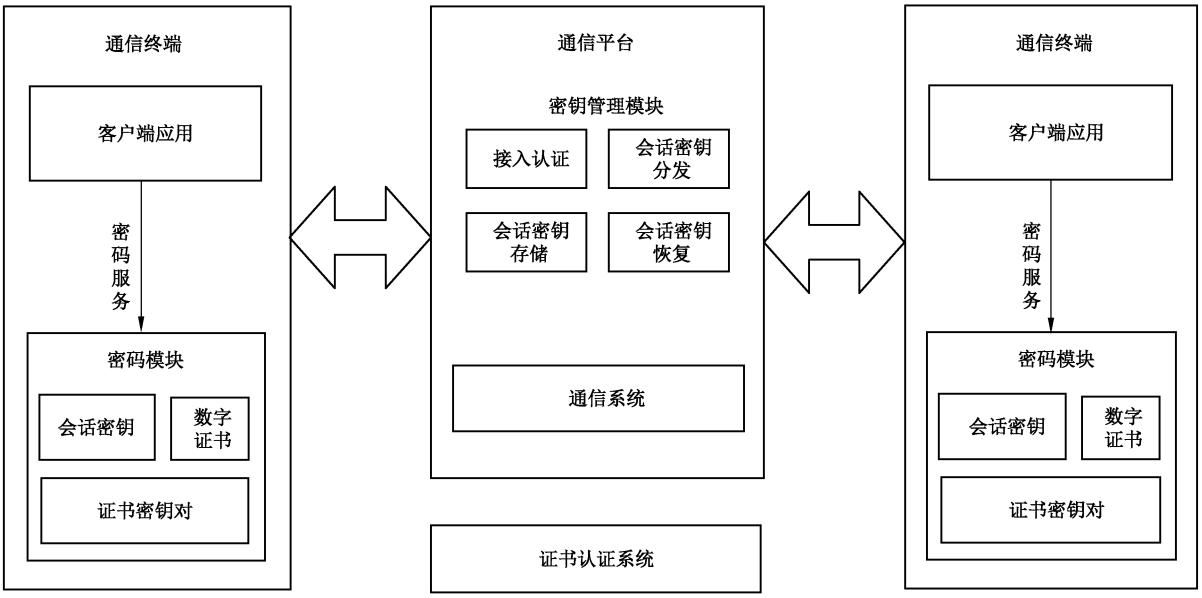

图1 基于IP网络的加密语音通信系统组成

5.3 业务过程

5.3.1 终端开户

5.3.1.1 VoIP账号申请

通信终端的VoIP账号应向通信平台的通信系统申请。

5.3.1.2 证书申请

系统内数字证书采用SM2密码算法，通信终端用户证书和通信平台服务器证书应向证书认证系统申请。

5.3.1.3 账号与证书关联

用户完成VoIP账号和用户证书申请后，应将用户VoIP账号及用户证书信息提交通信平台，通信平台在系统中实现两者之间的关联，完成终端开户。

5.3.2 会话建立及解除

5.3.2.1 会话发起

在语音通话之前，主叫可通过通信系统向被叫发起会话。

5.3.2.2 密钥分发/协商

在语音通话之前，系统应完成会话密钥的分发或协商。密钥分发/协商过程中，通信双方要进行基于数字签名的实体身份认证。

本标准仅定义基于非对称密码算法认证和保护的密钥分发或协商。

5.3.2.3 密钥存储

通信平台如需要存储会话密钥，应加密后存储。

5.3.2.4 语音通话

通话双方应使用会话密钥对语音数据进行加解密，完成密文语音的交互。

5.3.2.5 会话解除

当通话结束时，主叫与被叫通过通信系统解除会话，双方应删除会话密钥。

6 密钥管理

6.1 概述

基于IP网络的加密语音通信系统采用基于SM2密码算法PKI密码体系的密钥管理。

6.2 终端证书及密钥对

6.2.1 密钥用途

终端证书及密钥对包括用户签名证书及签名密钥对、用户加密证书及加密密钥对。用户签名密钥对用于对基于IP网络的加密语音通信系统中等关键业务数据（如登录请求数据）进行签名，提供终端侧用户身份鉴别和抗抵赖服务；用户加密密钥对用于对系统中的会话密钥进行加解密，以保障会话密钥的分发安全。

6.2.2 密钥生成

终端产生用户签名密钥对，向证书认证系统提交签名公钥申请用户签名证书，并将证书安装在终端；证书认证系统生成用户加密密钥对并签发用户加密证书，再通过数字信封方式下发到用户终端，用户终端保存加密密钥对并安装加密证书。

6.2.3 密钥存储

用户签名密钥对在终端生成并存储，用户签名证书在证书认证系统签发并保存到平台数据库中，同时用户签名证书需导入并存储在终端中。用户加密证书和加密密钥对保存在平台数据库中，同时两者均需导入并存储在终端中。

签名私钥和加密私钥必须安全存储到终端密码模块中，确保私钥存储的安全，防止私钥的泄露和非法替换。签名公钥及证书、加密公钥及证书没有机密性的要求，但是应确保公钥的真实性与完整性。

6.2.4 密钥使用

用户签名密钥对用于签名和签名验证，用户加密密钥对用于加密和解密。

用户签名私钥用于对基于 IP 网络的加密语音通信系统中等关键业务数据（如登录请求数据）进行签名，用户签名公钥用于对数字签名进行验证；用户加密公钥用于对系统中的会话密钥进行加密，用户加密私钥用于对会话密钥密文进行解密。

6.2.5 密钥更新

用户签名密钥对和用户加密密钥对应根据系统定义的密钥更新策略，达到密钥更新条件时（包括密钥到期、密钥泄露、怀疑密钥不安全等）进行密钥更新。

新的签名密钥对和加密密钥对生成见 6.2.2 密钥生成的要求。

6.2.6 密钥销毁

根据密钥管理策略，可对签名密钥对和加密密钥对进行销毁。销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

6.3 服务器证书及密钥对

6.3.1 密钥用途

服务器证书私钥用于对基于 IP 网络的加密语音通信系统中平台侧向终端侧发送的业务数据进行签名，提供平台身份鉴别服务。终端使用服务器证书验证平台身份合法性。

6.3.2 密钥生成

平台通过服务器密码机生成服务器证书密钥对，向证书认证系统提交服务器证书公钥申请服务器证书。

生成服务器密钥对的服务器密码机应符合 GM/T 0030。

服务器证书私钥需使用物理噪声源产生。随机性检测应符合 GM/T 0062。

6.3.3 密钥存储

服务器证书密钥对保存在服务器密码机内部。

服务器证书保存在平台数据库中。

6.3.4 密钥使用

服务器证书私钥用于对基于 IP 网络的加密语音通信系统中平台侧向终端侧发送的业务数据进行签名，签名运算在服务器密码机内部完成。

6.3.5 密钥更新

服务器证书密钥对应根据定义的密钥更新策略，达到密钥更新条件时（包括密钥到期、密钥泄露、怀疑密钥不安全等）进行密钥更新。

新的服务器证书密钥对生成见 6.3.2 密钥生成的要求。

6.3.6 密钥销毁

根据密钥管理策略，可对服务器证书密钥对进行销毁。

服务器证书密钥对销毁应在授权状态下执行。

销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

6.4 会话密钥

6.4.1 密钥用途

会话密钥分为会话加密密钥和会话鉴别密钥。

会话加密密钥用于加密双方语音通话数据，保障语音通话数据的机密性。

会话鉴别密钥用户保证双方语音通话数据的完整性。

6.4.2 密钥生成

会话密钥为 SM4 密码算法或 ZUC 密码算法对称密钥。会话密钥由平台服务器密码机生成，采用数字信封方式传递给终端，终端使用私钥解密得到会话密钥；会话密钥也可在语音通话前由通话双方安全协商生成。

6.4.3 密钥存储

会话密钥采用“一话一密”机制，每次通话的对称密钥都重新产生，可不进行长期存储。

6.4.4 密钥使用

终端一方使用会话加密密钥加密通话数据，另一方使用会话加密密钥解密通话数据。

终端一方使用会话鉴别密钥对通话数据进行完整性保护，另一方使用会话鉴别密钥进行通话数据完整性判定。

如采用 SM4 密码算法应遵循 GB/T 32907，如采用 ZUC 密码算法应遵循 GB/T 33133.1。

6.4.5 密钥更新

会话密钥采用“一话一密”机制，每次通信交互的对称密钥都重新产生。

6.4.6 密钥销毁

会话密钥采用“一话一密”机制，通信终端用完即刻销毁，不再复用，如会话密钥采用密钥分发的模式，则会话密钥密文在密钥管理模块继续保存。

7 安全协议

7.1 会话建立

整个会话过程中会话密钥生成模式分为密钥分发和密钥协商两种，示例见附录 C。

终端应在会话建立时(SIP invite 阶段),对 RFC3261 中的 INVITE 方法扩展 Authorization 头域,上报支持的密码算法及运算模式,会话建立流程见图 2。

Authorization:Capability algorithm="Algo1/Mode1:Algo2/Mode2" version="1"

Capability 代表算法能力,具有 algorithm 和 version 两个参数。

Algorithm 参数描述终端支持的对称算法和非对称算法,格式为"对称算法/模式;非对称算法",多种算法之间用冒号分隔,例如"SM4/ECB:SM4/CBC:SM2"。对称算法对数据填充采用 PKCS7Padding 方式,如需初始化向量 IV,则 IV 值为全 0。

Version 参数为算法能力协议版本,当前为 1。

协议 SIP 报文示例如下:

INVITE sip:dingyi@biloxi.com SIP/2.0

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds

Max-Forwards: 70

To: Dingyi 〈sip:dingyi@biloxi.com〉

From: Wangxiao 〈sip:wangxiao@atlanta.com〉;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Contact: sip:wangxiao@pc33.atlanta.com

Authorization:Capability algorithm="SM4/ECB:SM4/CBC:SM2" version="1"

Content-Type: application/sdp

Content-Length: 142

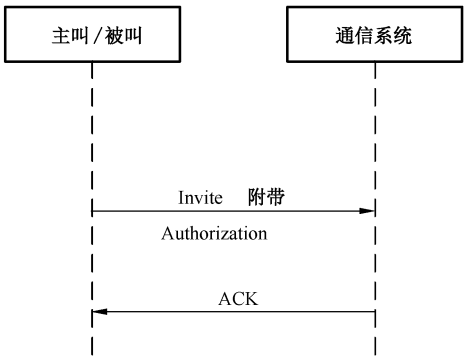

图 2 会话建立

7.2 开户绑定

7.2.1 开户绑定流程

开户绑定过程包括用户、通信系统和密钥管理模块三个参与方,用户发送请求到通信系统,通信系统转发至密钥管理模块,密钥管理模块处理完成后响应数据传递到通信系统,后者再将响应信息反馈到用户。开户绑定流程中 SM3 摘要运算应遵循 GB/T 32905,SM2 签名运算应遵循 GB/T 32918.2。

开户绑定流程见图 3。

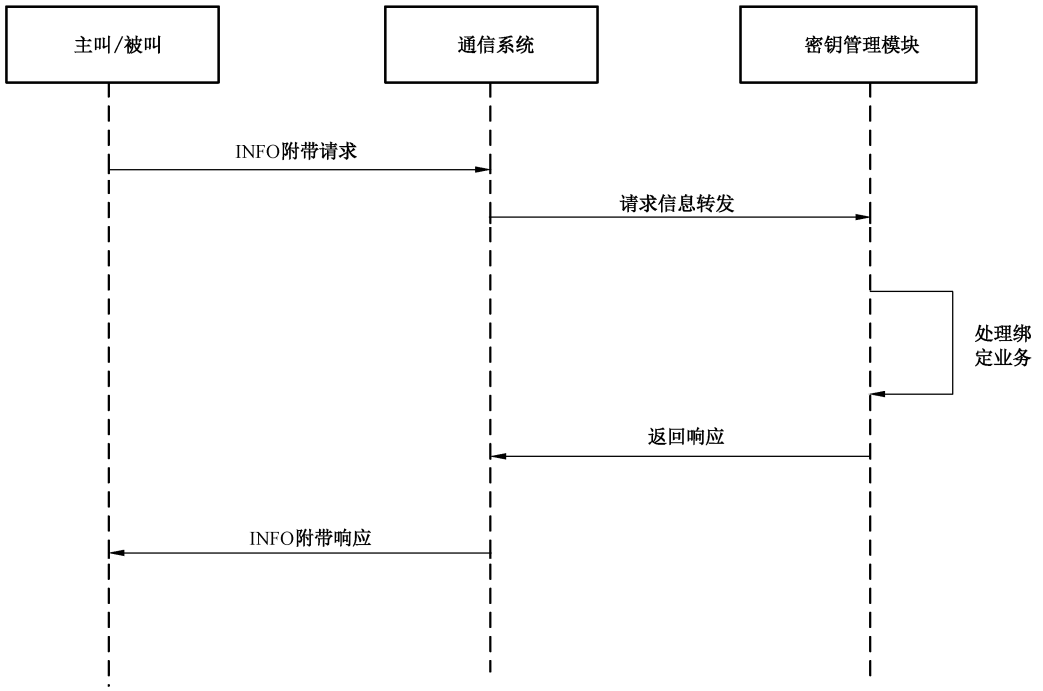

图 3　开户绑定

7.2.2　开户绑定请求

开户绑定请求数据见表 1，包含用户数字证书（可选）、用户特性数据等，该请求将被发送到密钥管理模块并得到服务。

密钥服务请求报文在向通信系统传递过程中采用基于 SIP 协议 INFO 方法进行传输，报文数据为 Base64 编码。增加 Content-Type 类型：message/userbin，来标识该 SIP INFO 请求为开户绑定请求。

开户绑定请求包含以下数据：

- 版本（当前为 1）；
- 用户 ID；
- 私钥算法；
- 请求时间；
- 随机信息；
- 请求信息的签名；
- 用户数字证书。

表 1　开户请求数据表

名称	简写表示	长度（字节）	描述	备注
版本	Ver	1	当前为 1	
用户 ID	N1	16	请求方 ID	一般应为 VoIP 帐号
私钥算法	Algo	1	非对称算法类型	SM2 算法
请求时间	ReqTime	20	请求时间	格式为 yyyy.MM.dd HH:mm:ss

表 1（续）

名称	简写表示	长度(字节)	描述	备注
随机信息	Nonce	8	随机信息	
签名值	SignVal	64	请求者对以上信息的SM2 签名	Priv_key:请求者私钥 Plain_msg=Ver|N1|Algo|ReqTime|Nonce Hash_I=SM3_Hash(Plain_msg) SignVal=SM2_Sign(Hash_I, Priv_key)
证书长度	Cert1Len	2	数字证书 1 字节长度	
证书信息	Cert1	Cert1Len	数字证书 1	SM2 签名数字证书
证书长度	Cert2Len	2	数字证书 2 字节长度	
证书信息	Cert2	Cert2Len	数字证书 2	SM2 加密数字证书

开户绑定请求 SIP 报文示例如下：

INFO sip:wangxiao@pc33.example.com SIP/2.0

Via: SIP/2.0/UDP 192.0.2.2:5060;branch=z9hG4bKnabcdef

To: Dingyi <sip:dingyi@example.com>;tag=a6c85cf

From: Wangxiao <sip:wangxiao@example.com>;tag=1928301774

Call-Id: a84b4c76e66710@pc33.example.com

CSeq: 314333 INFO

Info-Package: foo

Content-type: message/userbind

Content-length: 142

（开户绑定请求报文 base64 编码后数据）

7.2.3 开户绑定响应

密钥管理模块对开户请求的处理响应。

开户绑定响应在向用户间传递时采用基于 SIP 协议 INFO 方法进行传输，内容数据为 Base64 编码格式。

开户绑定响应数据见表 2，包含以下数据：

- 版本（当前为 1）；
- 用户 ID；
- 响应结果；
- 响应时间；
- 随机信息；
- 响应信息的签名。

表 2　开户响应数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
用户 ID	N1	16	请求方 ID	一般应为 VoIP 帐号
响应结果	Res	4	注册处理结果	0 为成功,其他为错误码
响应时间	ResTime	20	响应时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	数据和请求中相同
签名值	SignVal	64	密钥管理模块对以上信息的 SM2 签名	Server_priv_key:密管私钥 Plain_msg=Ver|N1|Res|ResTime|Nonce Hash_I=SM3_Hash(Plain_msg) SignVal=SM2_Sign(Hash_I, Server_priv_key)

开户绑定响应 SIP 报文示例如下:

SIP/2.0 200 OK

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877;received=192.0.2.4

To:〈sip:carol@chicago.com〉;tag=93810874

From: Wangxiao〈sip:wangxiao@atlanta.com〉;tag=1928301774

Call-ID: a84b4c76e66710

CSeq: 314333 INFO

Contact:〈sip:carol@chicago.com〉

Contact:〈mailto:carol@chicago.com〉

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE

Content-Length: 365

(开户绑定响应报文 base64 编码后数据)

7.3　密钥分发

7.3.1　密钥分发流程

密钥分发过程由用户发起,包括用户、通信系统和密钥管理模块三个参与方,用户发送密钥分发请求到通信系统,通信系统将请求信息转发至密钥管理模块,密钥管理模块处理完成后响应数据传递到通信系统,后者再将响应信息反馈到用户。密钥分发的数据报文在密钥管理模块后台存储,用于会话密钥的恢复取证。密钥分发流程中 SM3 摘要运算应遵循 GB/T 32905,SM2 签名运算应遵循 GB/T 32918.2,SM2 公钥加密运算应遵循 GB/T 32918.4。

密钥分发流程见图 4。

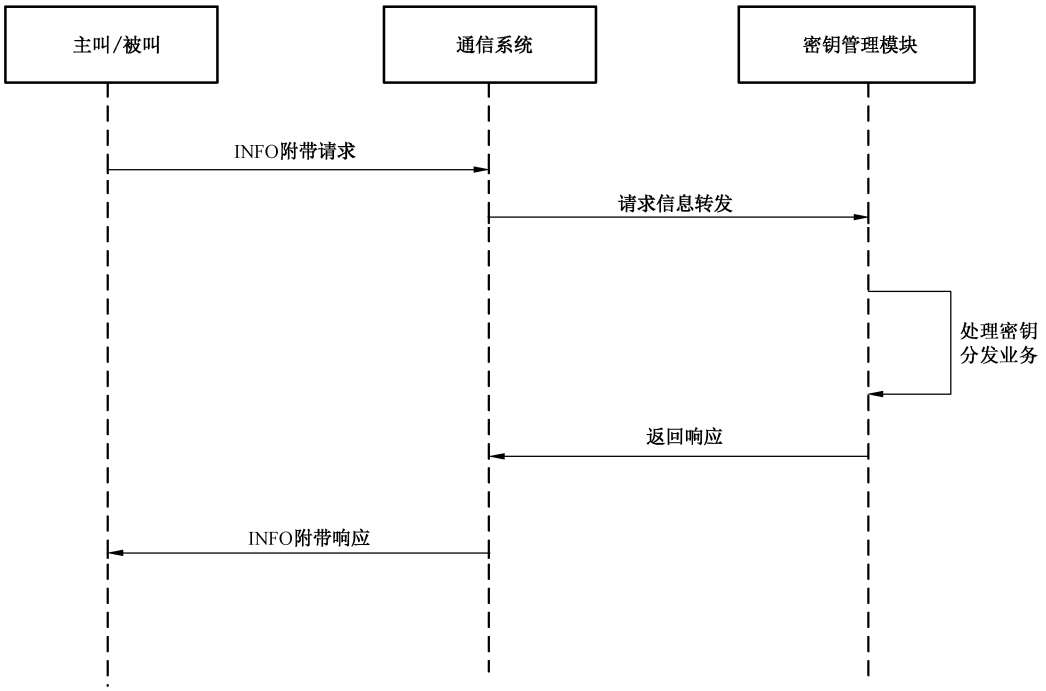

图 4　密钥分发

7.3.2　密钥分发请求

密钥分发请求数据见表 3，包含请求类型、特性数据等，该请求将被发送到密钥管理模块并得到服务。

密钥分发请求报文在向通信系统传递过程中采用基于 SIP 协议 INFO 方法进行传输，报文数据为 Base64 编码。增加 Content-Type 类型：message/keyrequest，来标识该 SIP INFO 请求为密钥服务请求。

服务请求包含以下数据：

- 版本（当前为 1）；
- 标识符；
- 会话 ID；
- 主叫 ID；
- 被叫 ID；
- 请求时间；
- 随机信息；
- 请求信息的签名。

表 3　密钥分发请求数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
标识符	RoleType	1	标识请求者是主叫方 还是被叫方	
会话 ID	SessionID	16	会话 ID,会话的唯一标识	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
请求时间	ReqTime	20	请求时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	
签名算法	SignAlgo	1	签名算法类型	SM2 算法
签名值	SignVal	64	主叫或被叫对以上信息的 SM2 签名	Priv_key:请求者私钥 Plain_msg=Ver|RoleType|SessionID|N1|N2| ReqTime|Nonce Hash_I=SM3_Hash(Plain_msg) SignVal=SM2_Sign(Hash_I, Priv_key)

密钥分发请求 SIP 报文示例如下：

INFO sip:wangxiao@pc33.example.com SIP/2.0

Via: SIP/2.0/UDP 192.0.2.2:5060;branch=z9hG4bKnabcdef

To: Dingyi <sip:dingyi@example.com>;tag=a6c85cf

From: Wangxiao <sip:wangxiao@example.com>;tag=1928301774

Call-Id: a84b4c76e66710@pc33.example.com

CSeq: 314333 INFO

Info-Package: foo

Content-type: message/keyrequest

Content-length: 142

(密钥服务请求报文 base64 编码后数据)

7.3.3　密钥分发响应

密钥管理模块对密钥分发请求的处理响应。

密钥分发响应报文基于 SIP 协议 INFO 方法进行传输,内容数据为 Base64 编码格式。

密钥分发响应数据见表 4,包含以下数据：

- 版本(当前为 1)；
- 会话 ID；
- 主叫 ID；
- 被叫 ID；
- 响应时间；
- 随机信息；

- 会话加密密钥；
- 会话鉴别密钥；
- 响应信息的签名。

表 4　密钥分发响应数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
会话 ID	SessionID	16	会话 ID,会话的唯一标识	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
响应时间	ResTime	20	响应时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	数据和请求中相同
加密算法类型	EncAlgo	1	加密密文采用的非对称密码算法	SM2 算法
会话加密密钥密文	EncKey	112	会话加密密钥密文,使用主叫方或被叫方的 SM2 公钥加密	SessionEncKey:密管生成的会话加密密钥 Client_pub_key:请求者的加密公钥 EncKey=SM2_Encrypt(SessionEncKey,Client_pub_key)
会话鉴别密钥密文	MacKey	112	会话鉴别密钥密文,使用主叫方或被叫方的公钥加密	SeesionMacKey:密管生成的会话鉴别密钥 Client_pub_key:请求者的加密公钥 MacKey=SM2_Encrypt(SessionMacKey,Client_pub_key)
签名算法类型	SignAlgo	1	签名数据采用的签名算法	SM2 算法
签名值	SignVal	64	密钥管理模块对以上信息的 SM2 签名	Server_priv_key:密管私钥 Plain_msg=Ver|SessionID|N1|N2|ResTime|Nonce|EncKey|MacKey Hash_I=SM3_Hash(Plain_msg) SignVal=SM2_Sign(Hash_I,Server_priv_key)

密钥分发响应 SIP 报文示例如下：

SIP/2.0 200 OK

Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877;received=192.0.2.4

To:〈sip:carol@chicago.com〉;tag=93810874

From: Wangxiao〈sip:wangxiao@atlanta.com〉;tag=1928301774

Call-ID: a84b4c76e66710

CSeq: 314333 INFO

Contact:〈sip:carol@chicago.com〉

Contact:〈mailto:carol@chicago.com〉

Allow：INVITE，ACK，CANCEL，OPTIONS，BYE

Content-Length：365

（密钥服务响应报文 base64 编码后数据）

7.4 密钥协商

7.4.1 密钥协商流程

密钥协商根据终端支持的密码算法，协商产生会话加密密钥和会话鉴别密钥，密钥协商的计算过程支持 SM2 密钥交换协议和数字信封保护两种方式。主叫通过 INVITE 指令将密钥协商的请求数据发送到被叫，被叫通过 183 Session Progress 或 200 OK 指令将密钥协商的响应数据返回给主叫。密钥协商的数据报文在通信系统后台存储，用于会话密钥的恢复取证。密钥协商流程中 SM3 摘要运算应遵循 GB/T 32905，SM2 签名运算应遵循 GB/T 32918.2，SM2 密钥交换协议应遵循 GB/T 32918.3，SM2 公钥加密运算应遵循 GB/T 32918.4。

密钥协商流程见图 5，协议 SIP 报文示例见附录 D。

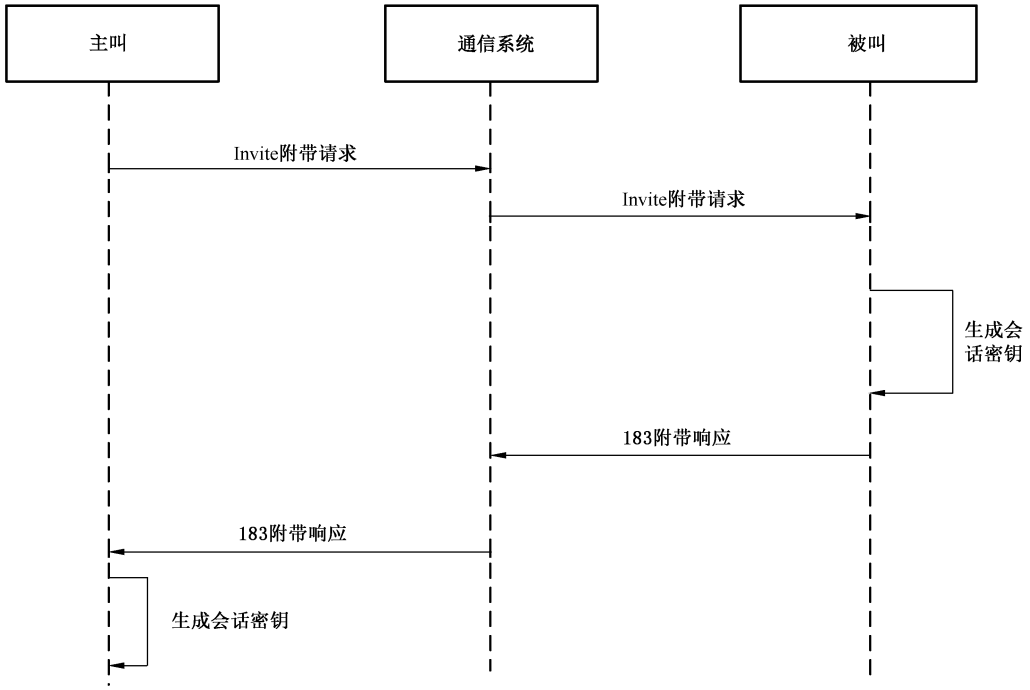

图 5 密钥协商

7.4.2 密钥协商请求

密钥协商请求报文基于 SIP 协议 INVITE 指令进行传输，使用 SDP 会话描述协议承载会话的信息，密钥协商数据整合到 SDP 协议中，报文数据为 Base64 编码。SDP 协议的密钥管理属性 key-mgnt 带有两个参数：使用的密钥方案（密钥交换协议：keyexchange，数字信封保护：envlope）和这个方案的属性（一个 base64 编码的数据包），其表达式如下：

a＝key-mgmt：keyexchange〈base64 编码值〉

其中，a 是 SDP 协议中用来描述媒体特征的一个可扩展参数，keyexchange 或 envlope 为协商方案名称，〈base64 编码值〉为协商消息内容的 base64 编码值。

密钥协商请求数据表见表5。

表5　基于SM2密码算法的密钥协商请求数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为1	
类型	Type	1	密钥协商	值为1:表示提供主叫方的加密证书，请被叫方产生密钥
时间	Time	20	密钥协商时间	格式为yyyy.MM.dd HH:mm:ss
证书数目	CertQty	1	证书数量	默认双证书:2
证书长度	Cert1Len	2	数字证书1字节长度	
证书信息	Cert1	Cert1Len	数字证书1	主叫SM2签名数字证书
证书长度	Cert2Len	2	数字证书2字节长度	
证书信息	Cert2	Cert2Len	数字证书2	主叫SM2加密数字证书
签名值	SignVal	64	主叫对以上信息的SM2签名	Priv_key:请求者私钥 Plain_msg=Ver|Type|Time|CertQty|Cert1Len|Cert1|Cert2Len|Cert2|TmpPub Hash_I=SM3_Hash(Plain_msg) SignVal=SM2_Sign(Hash_I, Priv_key)

密钥协商发起SIP报文示例如下：

INVITE sip:wangxiao@192.168.4.4　SIP/2.0

Via: SIP/2.0/UDP 192.168.4.4:26000;rport

Max-Forwards: 70

Contact: 〈sip:dingyi@192.168.4.4:26000〉

To: "wangxiao"〈sip:wangxiao@192.168.4.4〉

From: "Dingyi"〈sip:dingyi@192.168.4.4〉;tag=15c8325a

Call-ID: YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.

CSeq: 1 INVITE

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO

Content-Type: application/sdp

Content-Length: ***

//以下为SDP消息体信息

v=0

o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com

s=test

t=2873397496 2873404696

a=key-mgmt:envelope AQAFgM0XflABAAAAAAAAAAAAAAsAyONQ6gAAAAAGEEoo2pee4hp2

UaDX8ZE22YwKAAAPZG9uYWxkQGR1Y2suY29tAQAAAAAAAQAk0JKpgaVkDaawi9whVBtBt

0KZ14ymNuu62＋Nv3ozPLygwK/GbAV9iemnGUIZ19fWQUOSrzKTAv9zV

m＝audio 49000 RTP/SAVP 98

a＝rtpmap:98 AMR/8000

m＝video 52230 RTP/SAVP 31

a＝rtpmap:31 H261/90000

7.4.3 密钥协商响应

被叫方对密钥协商请求的处理响应。

被叫方首先验证密钥协商请求数据，通过后产生会话密钥，并生成密钥协商响应报文。

密钥协商响应报文基于 SIP 协议 183 Session Progress 或 200 OK 指令进行传输，密钥协商数据仍承载于 SDP 协议的密钥管理属性扩展中。

密钥协商响应数据表见表 6。

表 6 基于 SM2 密码算法的密钥协商响应数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
参数	Type	1	密钥协商参数	值为 2:表示本方产生密钥，并用对方的加密公钥加密
时间	Time	20	协商时间	格式为 yyyy.MM.dd HH:mm:ss
证书长度	Cert1Len	2	数字证书 1 字节长度	
证书信息	Cert1	Cert1Len	数字证书 1	被叫 SM2 签名数字证书
证书长度	Cert2Len	2	数字证书 2 字节长度	
证书信息	Cert2	Cert2Len	数字证书 2	被叫 SM2 加密数字证书
临时公钥	TmpPub	64	临时公钥	密钥方案采用 SM2 密钥交换协议(keyexchange)时有效，否则为空
会话密钥	SeesionKey	224	会话加密密钥和会话鉴别密钥的密文，使用主叫方或被叫方的公钥加密	SeesionEncKey:被叫方生成的会话加密密钥 SeesionMacKey:被叫方生成的会话鉴别密钥 SeesionKey＝SeesionEncKey|SessionMacKey Client_pub_key:请求者的公钥 SeesionKey＝SM2_Encrypt(SessionKey，Client_pub_key) 密钥方案采用数字信封保护(envlope)时有效，否则为空
签名值	SignVal	64	被叫对以上信息的 SM2 签名	priv_key:应答者私钥 Plain_msg＝ver|Type|Time|Cert1Len|Cert1|Cert2Len|Cert2| TmpPub|SeesionKey Hash_I＝SM3_Hash(Plain_msg) SignVal＝SM2_Sign(Hash_I，priv_key)

密钥协商响应 SIP 报文示例如下：

SIP/2.0 183 Session Progress
Via：SIP/2.0/UDP 192.168.4.4:26000;brport=26000
From："Dingyi"<sip:dingyi@192.168.4.4>;tag=15c8325a
To："wangxiao"<sip:wangxiao@192.168.4.4>;tag=cDg7NyjpeSg4m
Call-ID：YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.
CSeq：2 INVITE
Contact：<sip:wangxiao@192.168.4.4:5060;transport=udp>
User-Agent：FreeSWITCH-mod_sofia/1.0.trunk-16981M
Accept：application/sdp
Allow：INVITE，ACK，BYE，CANCEL，OPTIONS，MESSAGE，UPDATE，INFO，REGISTER，
REFER，NOTIFY，PUBLISH，SUBSCRIBE
Supported：timer，precondition，path，replaces
Allow-Events：talk，presence，dialog，line-seize，call-info，sla，
include-session-description，presence.winfo，message-summary，refer
Content-Type：application/sdp
Content-Disposition：session
Content-Length：**
//以下为 SDP 消息体信息
v=0
o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com
s=test
a=key-mgmt：envelope AQAFgM0XflABAAAAAAAAAAAAAAsAyONQ6gAAAAAGEEoo2pee4hp2UaDX8ZE22YwKAAAPZG9uYWxkQGR1Y2suY29tAQAAAAAAAQAk0JKpgaVkDaawi9whVBtBt0KZ14ymNuu62+Nv3ozPLygwK/GbAV9iemnGUIZ19fWQUOSrzKTAv9zV
m=audio 49000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 52230 RTP/SAVP 31
a=rtpmap:31 H261/90000

7.5 通信数据

通信数据的保护包括加密和 MAC 值计算两个过程。

加密是对已被编码过的整个语音包进行对称算法加密运算的过程。

MAC 值计算是对已被编码过的整个语音包进行校验计算的过程。

通信数据的接收方，在收到数据后，要做解密运算，并对解密后的数据进行 MAC 值校验。

通信数据的加密流程（语音包加密）见图 6。

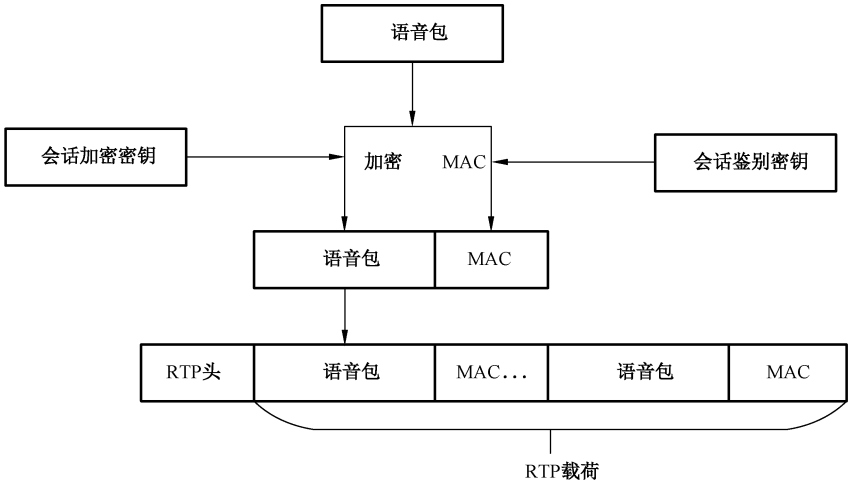

图 6　通信数据包

7.6　Sip 流程

安全协议数据以 Sip 协议作为载体，嵌入会话建立、会话密钥获取、加密语音通信等各环节协议数据的 Sip 流程示例如图 7 和图 8 所示。

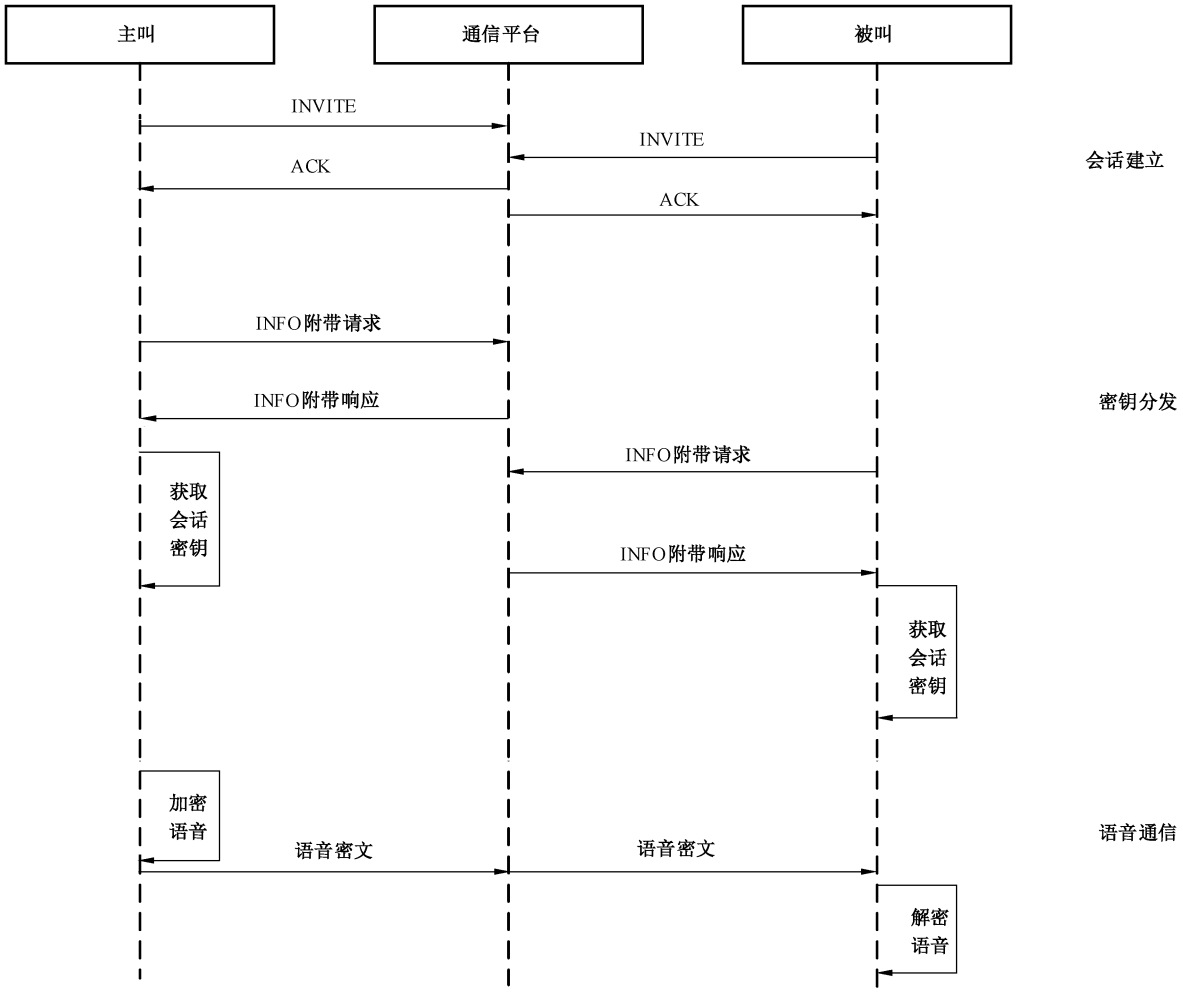

图 7　含密钥分发的 Sip 流程

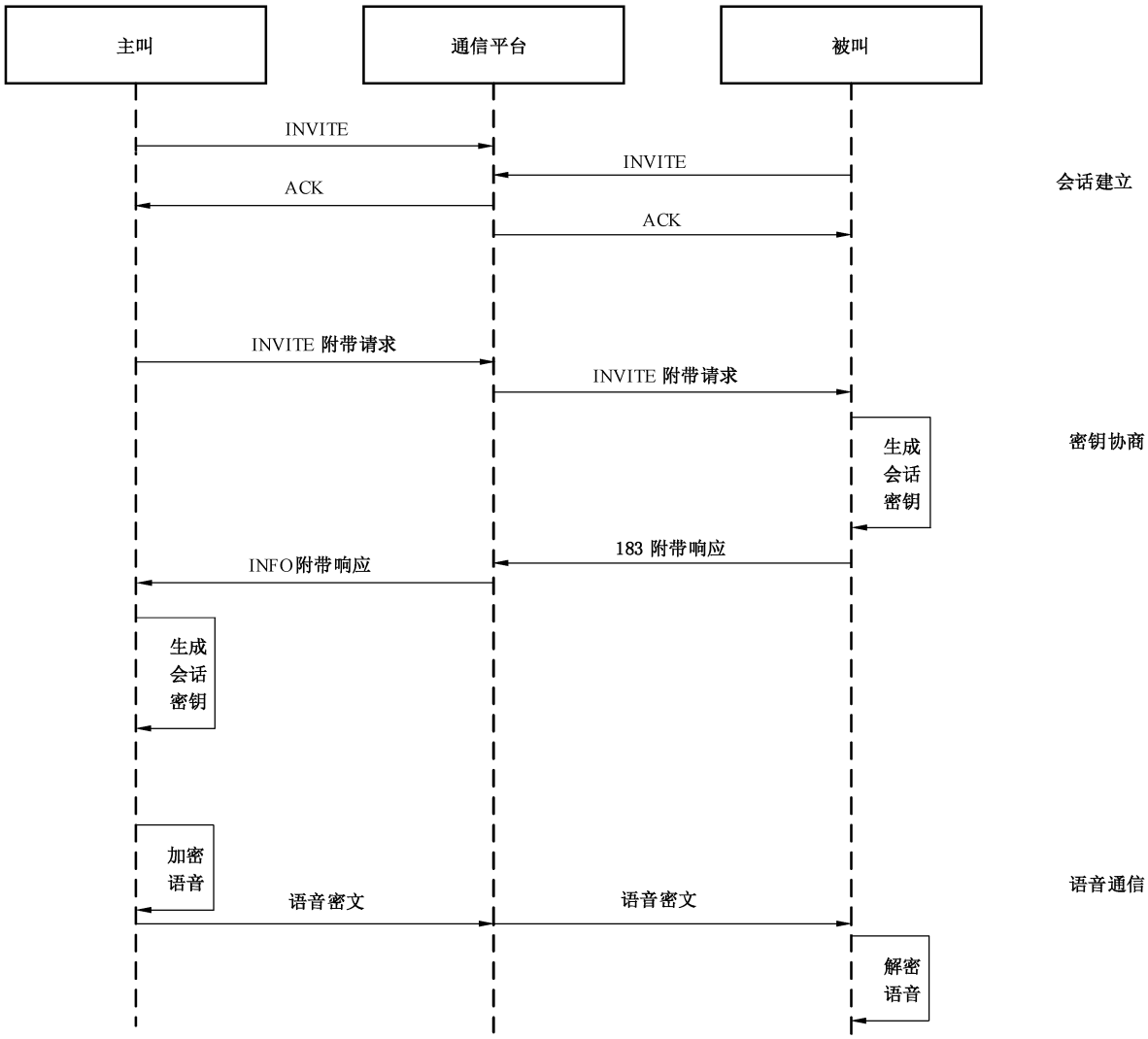

图 8　含密钥协商的 Sip 流程

8　密码模块

8.1　功能

密码模块向客户端或服务端应用提供产生随机数、生成非对称密钥对、导入非对称密钥对、导入数字证书、导出公钥、导入加密的会话密钥、数字签名、验证签名、对称加密、对称解密等密码服务。

8.2　接口

客户端密码模块的接口应符合 GB/T 35291。

服务端密码模块接口应符合 GB/T 36322。

8.3　安全性

通信终端使用的密码模块应满足 GB/T 37092 中规定的安全一级及以上要求。

若通信终端使用智能密码钥匙作为其密码模块，智能密码钥匙应遵循GM/T 0027。服务器密码机应符合GM/T 0030。

9 其他安全要求

9.1 敏感数据保护

个人身份信息、通话清单等敏感数据应加密存储。

个人身份信息的查询、导出等功能应设定相关权限，该项功能只能由安全管理员使用。

9.2 管理安全

服务运营机构应将系统的业务办理与密钥管理划属不同的管理单元。

9.3 角色设定

系统应设置系统管理员、安全管理员、密钥管理员、审计管理员以及业务操作员等操作角色。其中：

a) 系统管理员进行系统参数配置、导入/导出配置文件、系统状态监控等相关操作；

b) 安全管理员负责个人身份信息的查询、修改、导出、统计等相关操作；

c) 密钥管理员进行系统根密钥、用户密钥以及会话密钥等生成、备份、恢复、归档等相关操作；

d) 审计管理员进行日志审计、查询、导出、备份等相关操作；

e) 业务操作员进行号码开通、号码注销、号码停机等日常业务办理相关操作。

9.4 身份鉴别

系统的各类操作人员应通过身份鉴别才能进行相应的授权操作。

身份鉴别应采用两种或两种以上组合的鉴别技术。

9.5 日志管理

系统应提供日志记录功能，用于日志审计。日志内容包括：

a) 操作行为，包括登录认证、参数配置、策略配置、密钥管理、业务管理等操作，记录内容包括操作主体、操作时间、操作对象、操作结果等；

b) 用户访问行为，包括用户注册、申请证书、申请会话密钥等，记录内容包括用户主体、时间、操作内容、操作结果等，不应存储密钥信息；

c) 安全事件，密钥申请成功及失败、终端认证成功及失败等，日志记录事件发生主体、时间内容和事件结果，但是不应存储密钥信息；

d) 异常事件，解密失败、完整性校验失败、认证失败、非法访问等异常事件统计。

9.6 密钥备份

为增强容灾性，管理系统应对各种形态的密钥数据进行备份，可采用异地备份、异机备份等。

10 产品检测基本要求

10.1 产品功能检测基本要求

10.1.1 会话发起

检测产品为通信类产品，通信的发起方应能够发起语音会话。

10.1.2 会话建立

检测产品为通信类产品，在通信应答方确认建立通信时应能够建立会话。

10.1.3 会话解除

检测产品为通信类产品，通信双方任意一方选择结束会话时会话可正常解除。

10.1.4 密钥分发/协商

会话过程中能够通过密钥分发或者密钥协商的方式获取到会话加密密钥和会话鉴别密钥。

10.1.5 语音加解密

会话过程中能够使用会话加密密钥和会话鉴别密钥对语音数据进行有效加解密和完整性校验。

10.2 产品性能检测基本指标

10.2.1 密钥分发/协商

密钥分发过程在 WiFi、4G 环境中不超过 1 s。

密钥协商过程在 WiFi、4G 环境中不超过 1 s。

10.2.2 并发会话

并发会话数在 10 Mbps 带宽下不低于 500。

10.2.3 语音延时

会话过程中语音延时＜500 ms。

10.3 密钥管理检测要求

10.3.1 密钥生成

依据密钥类型的不同，检测结果应符合 6.2.2、6.3.2、6.4.2 的要求。

10.3.2 密钥存储

依据密钥类型的不同，检测结果应符合 6.2.3、6.3.3、6.4.3 的要求。

10.3.3 密钥使用

依据密钥类型的不同，检测结果应符合 6.2.4、6.3.4、6.4.4 的要求。

10.3.4 密钥更新

依据密钥类型的不同，检测结果应符合 6.2.5、6.3.5、6.4.5 的要求。

10.3.5 密钥销毁

依据密钥类型的不同，检测结果应符合 6.2.6、6.3.6、6.4.6 的要求。

10.4 密码模块检测要求

10.4.1 功能

检测结果应符合 8.1 的要求。

10.4.2 接口

检测结果应符合 8.2 的要求。

10.4.3 安全性

检测结果应符合 8.3 的要求。

10.5 其他安全检测基本要求

10.5.1 敏感数据保护

检测结果应符合 9.1 的要求。

10.5.2 管理安全

检测结果应符合 9.2 的要求。

10.5.3 角色设定

检测结果应符合 9.3 的要求。

10.5.4 身份鉴别

检测结果应符合 9.4 的要求。

10.5.5 日志管理

检测结果应符合 9.5 的要求。

10.5.6 密钥备份

检测结果应符合 9.6 的要求。

附 录 A
（规范性）
基于 SM9 密码算法的加密语音通信系统

A.1 基于 SM9 密码算法的加密语音通信系统概述

基于 SM9 密码算法的加密语音通信系统，以 VoIP 账号为公钥，不依托数字证书认证系统，可应用于非跨信域系统，在支持系统参数可靠交换的环境中，可应用于跨信任域系统。

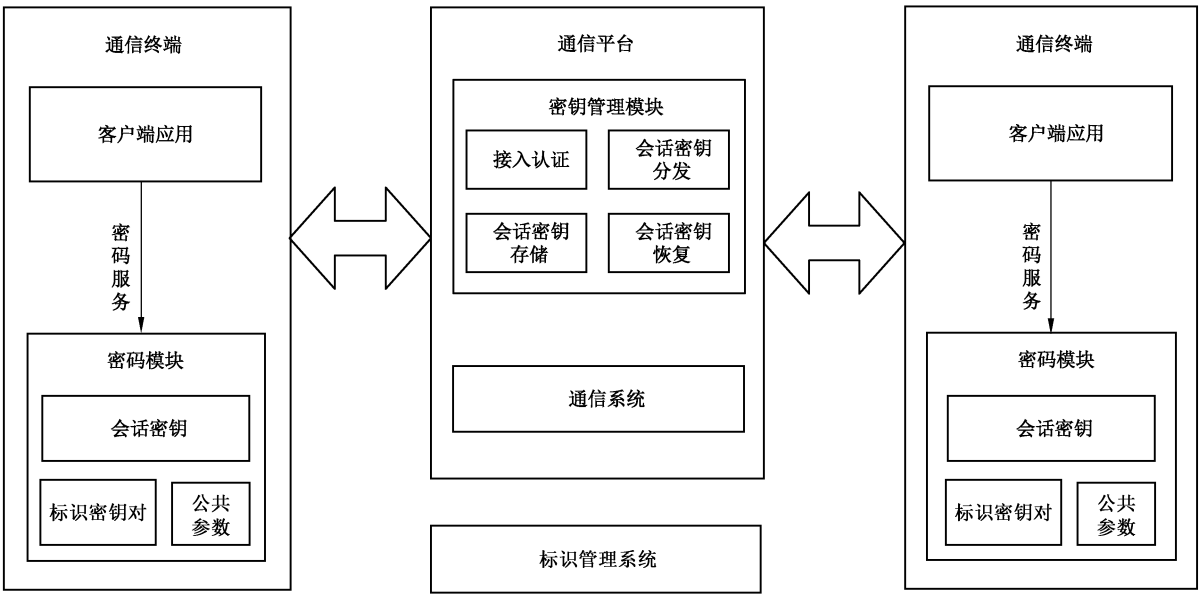

图 A.1 基于 IP 网络的加密语音通信系统组成（标识密码）

基于 IP 网络的加密语音通信系统组成见图 A.1，由通信平台和通信终端两大部分组成，其中通信平台由通信系统和密钥管理模块组成。

标识管理系统为终端和密钥管理模块提供标识私钥的生成、分发、撤销、更新等服务。

通信终端作为系统内的主叫方或被叫方，拥有系统内唯一的 VoIP 账号，完成语音数据的采集和发送、语音数据加解密等功能。

通信平台负责完成用户终端 Voip 账号的注册申请、语音数据传递、通信终端接入认证和会话密钥分发。

主叫方发起会话，经由通信平台与被叫方建立通话，通信平台为通信双方分发会话密钥（或双方协商会话密钥），主被叫通话数据由会话密钥保护。

A.2 业务过程

A.2.1 终端开户

通信终端的 VoIP 账号应向通信系统申请，同时基于 VoIP 账号向标识管理系统申请对应标识的私钥。在 SM9 标识密码体系中，VoIP 账号即公钥，因此不需要账号与公钥进行关联。

A.2.2 会话建立及解除

通信终端在会话建立前首先向通信平台进行注册，告知服务器该终端用户可被访问到的地址，注册成功则会收到服务器返回的注册成功信息。

会话建立时，呼叫方向服务器发起对被叫方的呼叫信息，服务器在单次或多次转发后将呼叫信息发送至被叫方。同时，服务器将基于密钥分发/协商的流程进行呼叫双方的会话密钥处理，待被叫接听时双方已经具有本次通话的会话密钥。

解除会话时，由会话的任一方向另一方发起终止会话请求，响应方返回确认信息后双方解除会话进入待机状态。

A.3 密钥管理

A.3.1 概述

本节描述了基于 IP 网络的加密语音通信系统采用基于 SM9 标识密码算法的非对称密钥管理。

A.3.2 终端 SM9 标识私钥

A.3.2.1 标识私钥用途

终端 SM9 标识为用户 VoIP 账号，SM9 私钥由标识密码系统生成并安全分发到终端。SM9 标识密钥可用于对系统中的会话密钥进行加解密，以保障会话密钥的分发安全；也可用于对系统中如登录请求数据等关键业务数据进行签名，提供终端侧用户身份鉴别。

A.3.2.2 标识私钥生成

SM9 标识私钥由标识密码系统生成。

A.3.2.3 标识私钥存储

SM9 标识私钥安全分发到终端后，应安全存储到终端密码模块中，确保私钥存储的安全，防止私钥的泄露和非法替换。

A.3.2.4 标识私钥使用

用户标识私钥既可用于签名和签名验证，也可用于加密和解密。

SM9 标识私钥用于对系统中如登录请求数据等关键业务数据进行签名，SM9 标识用于对数字签名进行验证；SM9 标识用于对系统中的会话密钥进行加密，使用 SM9 私钥对会话密钥密文进行解密。

A.3.2.5 标识密钥更新

SM9 标识私钥应根据系统定义的密钥更新策略，达到密钥更新条件时（包括密钥到期、密钥泄露、怀疑密钥不安全等）进行密钥更新。

A.3.2.6 标识密钥销毁

根据密钥管理策略，可对 SM9 标识私钥进行销毁。销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

A.3.3 服务器标识私钥

A.3.3.1 标识私钥用途

以服务器 ID 为服务器 SM9 标识，对应的服务器 SM9 标识私钥可用于对基于 IP 网络的加密语音通信系统中平台侧向终端侧发送的业务数据进行签名，提供平台身份鉴别服务。终端使用服务器 SM9 标识验证平台身份合法性。

服务器 SM9 标识私钥也可用于对终端上传的以服务器 SM9 标识加密的消息进行解密。

A.3.3.2 标识私钥生成

服务器 ID 即为服务器 SM9 标识；对应的服务器 SM9 私钥由标识密码系统生成，标识密码系统中的服务器密码机应符合 GM/T 0030。

A.3.3.3 标识私钥存储

服务器 SM9 标识私钥存储在服务器密码机内部，服务器密码机应符合 GM/T 0030。

A.3.3.4 标识密钥使用

服务器 SM9 标识私钥可用于对系统中平台侧向终端侧发送的业务数据进行签名，签名运算应在服务器密码机内部完成。服务器 SM9 私钥可用于对系统中终端侧向平台侧发送的加密业务数据进行解密，解密运算应在服务器密码机内部完成，服务器密码机应符合 GM/T 0030。

A.3.3.5 标识密钥更新

服务器 SM9 标识私钥应根据定义的密钥更新策略，达到密钥更新条件时（包括密钥到期、密钥泄露、怀疑密钥不安全等）进行密钥更新。

A.3.3.6 标识密钥销毁

根据密钥管理策略，可对服务器标识私钥进行销毁。

服务器标识私钥销毁应在授权状态下执行。

销毁结果要求不可逆，不可从销毁结果中恢复原密钥。

A.3.4 会话密钥

本节要求同 6.4。

A.4 安全协议

A.4.1 会话建立

整个会话过程分为密钥分发模式和密钥协商模式两种，示例见附录 C。

终端应在会话建立时（SIP invite 阶段），对 RFC3261 中的 INVITE 方法扩展 Authorization 头域，上报支持的密码算法和运算模式，会话建立流程见图 A.2，协议 SIP 报文示例参见附录 D。对称算法对数据填充采用 PKCS7Padding 方式，如需初始化向量 IV，则 IV 值为全 0。

Authorization：Capability algorithm＝"Algo1/Mode1；Algo2/Mode2" version＝"1"

Capability 代表算法能力。具有 algorithm 和 version 两个参数。

Algorithm 参数描述终端支持的对称算法和非对称算法，格式为“对称算法/模式；非对称算法”，多

种算法之间用冒号分隔。例如"SM4/ECB:SM4/CBC;SM2:SM9"。

Version 参数为算法能力协议版本,当前为 1。

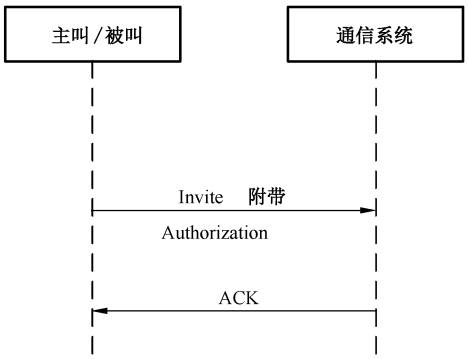

图 A.2 会话建立

A.4.2 开户绑定

A.4.2.1 开户绑定流程

开户绑定过程包括用户、通信系统和密钥管理模块三个参与方,用户发送请求到通信系统,通信系统转发至密钥管理模块,密钥管理模块处理完成后响应数据传递到通信系统,后者再将响应信息反馈到用户。开户绑定流程中 SM3 摘要运算应遵循 GB/T 32905,SM9 签名运算应遵循 GM/T 0044.2。

开户绑定流程见图 A.3,协议 SIP 报文示例见附录 D。

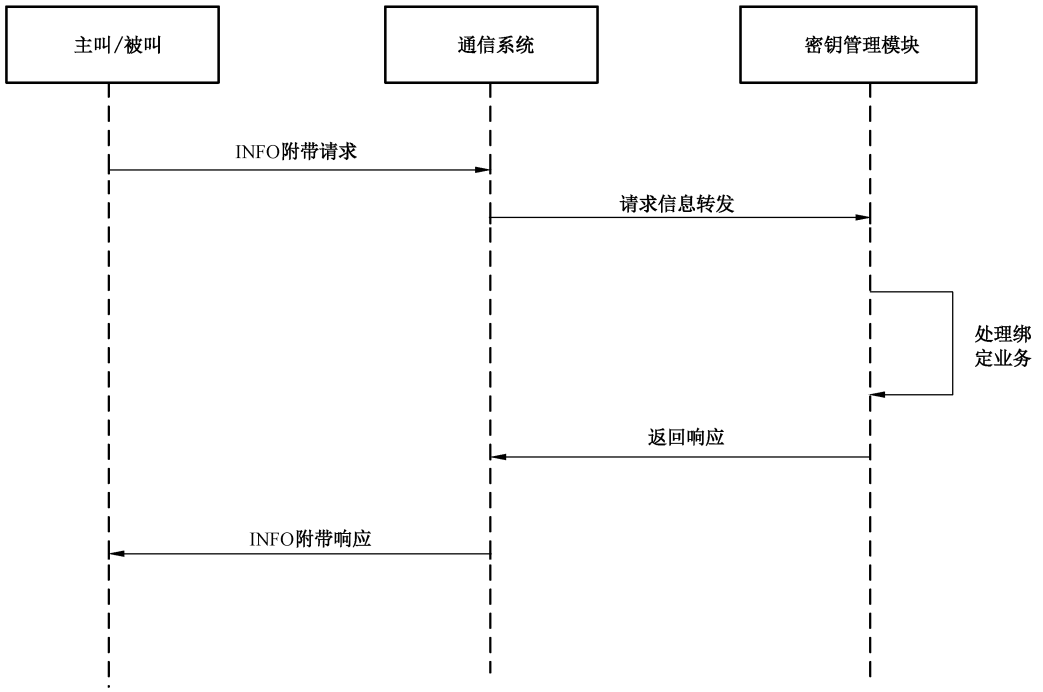

图 A.3 开户绑定

A.4.2.2 开户绑定请求

开户绑定请求数据见表 A.1,包含用户特性数据等,该请求将被发送到密钥管理模块并得到服务。

密钥服务请求报文在向通信系统传递过程中采用基于 SIP 协议 INFO 方法进行传输，报文数据为 Base64 编码。增加 Content-Type 类型：message/userbin，来标识该 SIP INFO 请求为开户绑定请求。

开户绑定请求包含以下数据：

- 版本（当前为 1）；
- 用户 ID；
- 私钥算法；
- 请求时间；
- 随机信息；
- 请求信息的签名。

表 A.1　开户请求数据表

名称	简写表示	长度（字节）	描述	备注
版本	Ver	1	当前为 1	
用户 ID	N1	16	请求方 ID	一般应为 VoIP 帐号
私钥算法	Algo	1	非对称算法类型	SM9 算法
请求时间	ReqTime	20	请求时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	
签名值	SignVal	64	请求者对以上信息的 SM2/SM9 签名	Priv_key：请求者私钥 Plain_msg＝Ver|N1|Algo|ReqTime|Nonce Hash_I＝SM3_Hash(Plain_msg) SignVal＝Asym_Sign(Hash_I, Priv_key)， Asym 为 SM9 算法
证书长度	Cert1Len	2	数字证书 1 字节长度	SM9 算法此值为 0
证书信息	Cert1	Cert1Len	数字证书 1	SM9 算法此值为 NULL
证书长度	Cert2Len	2	数字证书 2 字节长度	SM9 算法此值为 0
证书信息	Cert2	Cert2Len	数字证书 2	SM9 算法此值为 NULL

A.4.2.3　开户绑定响应

密钥管理模块对开户请求的处理响应。

开户绑定响应在向用户间传递时采用基于 SIP 协议 INFO 方法进行传输，内容数据为 Base64 编码格式。

开户绑定响应数据见表 A.2，包含以下数据：

- 版本（当前为 1）；
- 用户 ID；
- 响应结果；
- 响应时间；
- 随机信息；
- 响应信息的签名。

表 A.2　开户响应数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
用户 ID	N1	16	请求方 ID	一般应为 VoIP 帐号
响应结果	Res	4	注册处理结果	0 为成功,其他为错误码
响应时间	ResTime	20	响应时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	数据和请求中相同
签名值	SignVal	97	密钥管理模块对以上信息的 SM9 签名	Server_priv_key:密管私钥 Plain_msg=Ver|N1|Res|ResTime|Nonce Hash_I=SM3_Hash(Plain_msg) SignVal=Asym_Sign(Hash_I, Server_priv_key),Asym 支持 SM9 算法

A.4.3　密钥分发

A.4.3.1　密钥分发流程

密钥分发过程由用户发起,包括用户、通信系统和密钥管理模块三个参与方,用户发送密钥分发请求到通信系统,通信系统将请求信息转发至密钥管理模块,密钥管理模块处理完成后响应数据传递到通信系统,后者再将响应信息反馈到用户。密钥分发的数据报文在密钥管理模块后台存储,用于会话密钥的恢复取证。密钥分发流程中 SM3 摘要运算应遵循 GB/T 32905,SM9 算法签名应遵循 GM/T 0044.2。

密钥分发流程见图 A.4,协议 SIP 报文示例见附录 D。

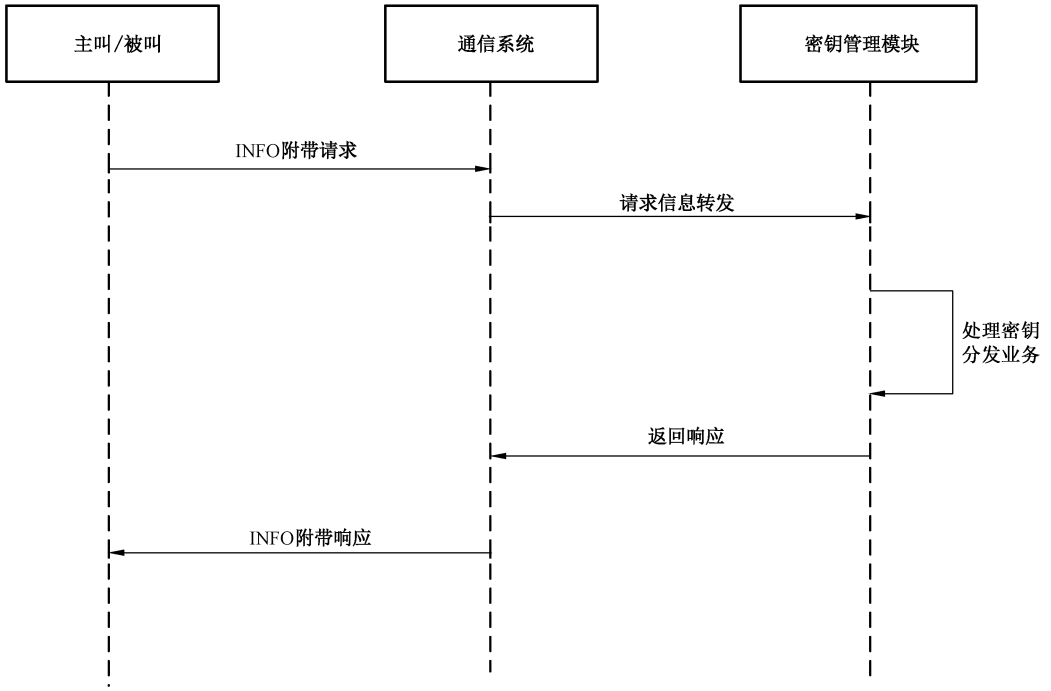

图 A.4　密钥分发

A.4.3.2 密钥分发请求

密钥分发请求数据见表 A.3，包含请求类型、特性数据等，该请求将被发送到密钥管理模块并得到服务。

密钥分发请求报文在向通信系统传递过程中采用基于 SIP 协议 INFO 方法进行传输，报文数据为 Base64 编码。增加 Content-Type 类型：message/keyrequest，来标识该 SIP INFO 请求为密钥服务请求。

服务请求包含以下数据：

- 版本（当前为 1）；
- 标识符；
- 会话 ID；
- 主叫 ID；
- 被叫 ID；
- 请求时间；
- 随机信息；
- 请求信息的签名。

表 A.3 密钥分发请求数据表

名称	简写表示	长度（字节）	描述	备注
版本	Ver	1	当前为 1	
标识符	RoleType	1	标识请求者是主叫方还是被叫方	
会话 ID	SessionID	16	会话 ID，会话的唯一标识	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
请求时间	ReqTime	20	请求时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	
签名算法	SignAlgo	1	签名算法类型	SM9 算法
签名值	SignVal	97	主叫或被叫对以上信息的 SM9 签名	Priv_key：请求者私钥 Plain_msg＝Ver|RoleType|SessionID|N1|N2|ReqTime|Nonce Hash_I＝SM3_Hash(Plain_msg) SignVal＝Asym_Sign(Hash_I，Priv_key)，Asym 支持 SM9 算法

A.4.3.3 密钥分发响应

密钥管理模块对密钥分发请求的处理响应。

密钥分发响应报文基于 SIP 协议 INFO 方法进行传输，内容数据为 Base64 编码格式。

密钥分发响应数据见表 A.4，包含以下数据：

- 版本（当前为 1）；

- 会话 ID；
- 主叫 ID；
- 被叫 ID；
- 响应时间；
- 随机信息；
- 会话加密密钥；
- 会话鉴别密钥；
- 响应信息的签名。

表 A.4　密钥分发响应数据表

名称	简写表示	长度(字节)	描述	备注
版本	Ver	1	当前为 1	
会话 ID	SessionID	16	会话 ID,会话的唯一标识	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
响应时间	ResTime	20	响应时间	格式为 yyyy.MM.dd HH:mm:ss
随机信息	Nonce	8	随机信息	数据和请求中相同
加密算法类型	EncAlgo	1	加密密文采用的非对称密码算法	SM9 算法
会话加密密钥密文	EncKey	112	会话加密密钥密文,使用主叫方或被叫方的SM9 标识加密	SessionEncKey:密管生成的会话加密密钥 Client_pub_key:采用 SM9 算法时为请求者的加密标识。 EncKey=Asym_Encrypt(SessionEncKey,Client_pub_key),Asym 支持 SM9 算法
会话鉴别密钥密文	MacKey	112	会话鉴别密钥密文,使用主叫方或被叫方的公钥加密	SeesionMacKey:密管生成的会话鉴别密钥 Client_pub_key:采用 SM9 算法时为请求者的加密标识。 MacKey=Asym_Encrypt(SessionMacKey,Client_pub_key) ,Asym 支持 SM9 算法
签名算法类型	SignAlgo	1	签名数据采用的签名算法	SM9 算法
签名值	SignVal	97	密钥管理模块对以上信息的SM9 签名	Server_priv_key:密管私钥 Plain_msg=Ver|SessionID|N1|N2|ResTime|Nonce|EncKey|MacKey Hash_I=SM3_Hash(Plain_msg) SignVal=Asym_Sign(Hash_I,Server_priv_key),Asym 支持 SM9 算法

A.4.4 密钥协商

A.4.4.1 密钥协商流程

密钥协商根据终端支持的密码算法，协商产生会话加密密钥和会话鉴别密钥，密钥协商的计算过程支持 SM2 密钥交换协议和数字信封保护两种方式。主叫通过 INVITE 指令将密钥协商的请求数据发送到被叫，被叫通过 183 Session Progress 或 200 OK 指令将密钥协商的响应数据返回给主叫。密钥协商的数据报文在通信系统后台存储，用于会话密钥的恢复取证。密钥协商流程中 SM3 摘要运算应遵循 GB/T 32905，SM9 签名运算应遵循 GM/T 0044.2，SM9 密钥交换协议应遵循 GM/T 0044.3，SM9 公钥加密运算应遵循 GM/T 0044.4。

密钥协商流程见图 A.5，协议 SIP 报文示例参见附录 B。其中 SM9 密钥协商支持单报文和两报文协议。单报文协议中被叫以 200 OK 响应主叫发起的合法请求。

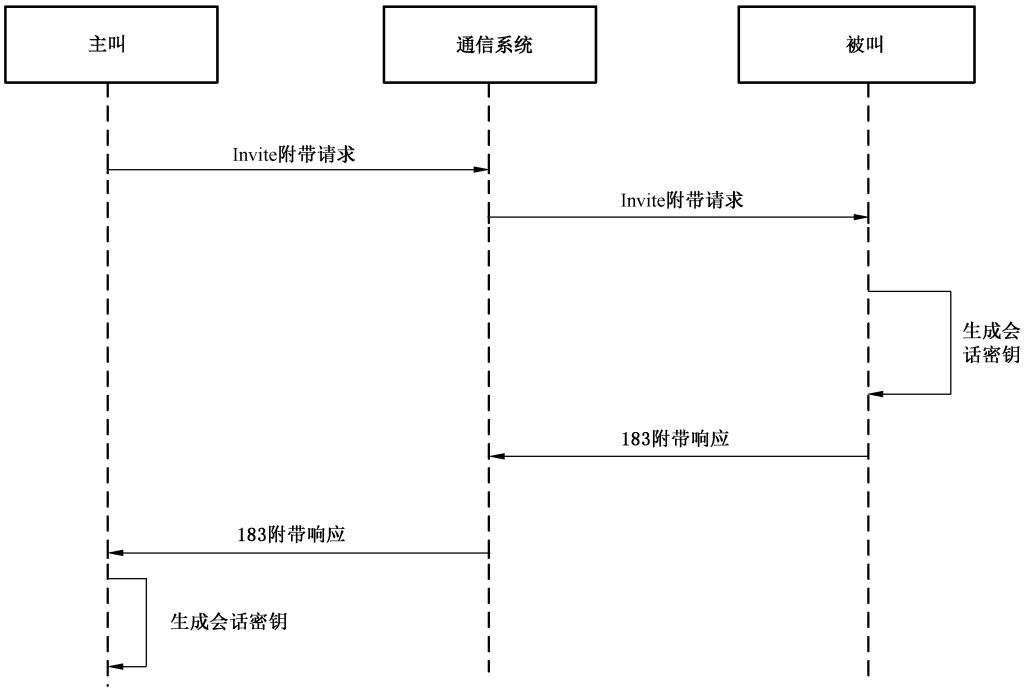

图 A.5 密钥协商

A.4.4.2 密钥协商请求

采用 SM9 密钥协商请求数据见表 A.5，包含请求类型、特性数据等，该请求将被发送到被叫方并得到响应服务。

密钥协商请求报文基于 SIP 协议 INVITE 指令进行传输，使用 SDP 会话描述协议承载会话的信息，密钥协商数据整合到 SDP 协议中，报文数据为 Base64 编码。SDP 协议的密钥管理属性 key-mgmt 带有两个参数：使用的密钥方案（keyexchange 或 mikey）和这个方案的属性（一个 base64 编码的数据包），其表达式如下：

SM9 算法使用 a=key-mgmt：mikey〈base64 编码值〉

其中，a 是 SDP 协议中用来描述媒体特征的一个可扩展参数，keyexchange 或 mikey 为协商方案名称，〈base64 编码值〉为协商消息内容的 base64 编码值。如采用 keyexchange 密钥方案则遵循

GM/T 0044.3，如采用 mikey 密钥方案则遵循 RFC3830。

表 A.5　基于 SM9 密码算法的密钥协商请求数据表

名称	简写表示	长度(字节)	描述	备注
时间	Time	8	标准时间	
随机信息	Nonce	32	随机信息	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
被叫 SM9 系统参数标识	KMS_R	32	被叫方所在标识密码系统参数的标识	可选，会话两方在同一个 SM9 系统中则无需传递该域
主叫密钥协商参数	KR_I	32	SM9 密钥交换协议中发起方产生的随机密钥协商参数	如果密钥协商方案为 keyexchange，此值即为 SM9 密钥交换协议中的 R_A 值，否则为空
标识密文	ENC_I	162	标识密文，使用被叫方终端标识公钥进行加密	如果密钥协商方案为 mikey，此值的计算过程如下：R_I=[r_i]G，其中 G 为 SM2 椭圆曲线公钥密码算法推荐曲线参数约定的 G，r_i 为随机数，[r_i]G 为 r_i 个 G 之和，ENC_I=SM9_Enc(R_I,N1)。 如果密钥协商方案为 keyexchange，此值为空
签名值	SignVa1	97	主叫对以上信息的 SM9 签名	Hash_I=SM3_Hash(Time || Nonce ||N1|| N2||KMS_I||KMS_R||ENC_I|KAT_I)，如密钥协商方案为 keyexchange，则 KAT_I=KR_I； 如密钥协商方案为 mikey，则 KAT_I=ENC_I。 SignVal=SM9_Sign(Hash_I,Priv_key)

A.4.4.3　密钥协商响应

被叫方对密钥协商请求的处理响应。

被叫方首先验证密钥协商请求数据，通过后产生会话密钥，并生成密钥协商响应报文。

密钥协商响应报文基于 SIP 协议 183 Session Progress 或 200 OK 指令进行传输，密钥协商数据仍承载于 SDP 协议的密钥管理属性扩展中。SM9 单报文协议协商的流量加密密钥生成密钥为 R_I，SM9 双报文协议协商的流量加密密钥生成密钥为 DH，具体的由流量加密密钥生成密钥派生会话密钥的过程见 RFC3830。

采用 SM9 密码算法的密钥协商响应数据见表 A.6。

表 A.6　基于 SM9 密码算法的密钥协商响应数据表

名称	简写表示	长度(字节)	描述	备注
时间	Time	8	标准时间	
主叫 ID	N1	16	主叫方 ID	一般应为 VoIP 帐号
被叫 ID	N2	16	被叫方 ID	一般应为 VoIP 帐号
随机信息	Nonce	32	随机信息	
被叫密钥协商参数	KR_R	32	SM9 密钥交换协议中响应方产生的随机密钥协商参数	如果密钥协商方案为 keyexchange,此值即为 SM9 密钥交换协议中的 R_B 值,否则为空
标识密文	ENC_R	194	标识密文,使用主叫方终端标识公钥进行加密	如果密钥协商方案为 mikey,此值的计算过程如下: R_R=[r_r]G,r_r 为随机数 DH=[r_2]R_I Hash_R=SM3_Hash(Time|| Nonce ||N1||N2 R_I||R_R||DH) ENC_R=SM9_Enc(R_R||Hash_R,N1)。 如果密钥协商方案为 keyexchange,此值为空

A.4.5　通信数据

通信数据的保护见 7.5。

A.5　密码模块

A.5.1　功能

密码模块向客户端或服务端应用提供产生随机数、生成非对称密钥对、导入非对称密钥对、导入数字证书、SM9 标识私钥管理、导出公钥、导入加密的会话密钥、数字签名、验证签名、对称加密、对称解密等密码服务。

A.5.2　接口

客户端密码模块的接口应符合 GB/T 35291。

服务端密码模块接口应符合 GB/T 36322。

A.5.3　安全性

通信终端使用的密码模块应满足 GM/T 0028 中规定的安全一级及以上要求。

若通信终端使用智能密码钥匙作为其密码模块,所使用的智能密码钥匙应符合 GM/T 0027。服务器密码机应符合 GM/T 0030。

附 录 B
（资料性）
基于 SM9 密码算法的安全协议 SIP 报文

基于 SM9 密码算法的密钥协商，密钥协商发起 SIP 报文：

INVITE sip:wangxiao@192.168.4.4 SIP/2.0

Via: SIP/2.0/UDP 192.168.4.4:26000;branch=z9hG4bK-d8754z-56adad736231f024-1---d8754z-;rport

Max-Forwards: 70

Contact:<sip:dingyi@192.168.4.4:26000>

To: "wangxiao"<sip:wangxiao@192.168.4.4>

From: "Dingyi"<sip:dingyi@192.168.4.4>;tag=15c8325a

Call-ID: YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.

CSeq: 1 INVITE

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO

Content-Type: application/sdp

Content-Length: ***

//以下为 SDP 消息体信息

v=0

o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com

s=test

t=2873397496 2873404696

a=key-mgmt:mikey

ARYFALUwkagBAAB75qwuAAAAAAAAAAAAAAAAAAoAAAAAAFufBpMLAAAADwABAQIBAQUBAAcBAQgBARYgcVxIHcgKevUQPPF6Qn8plMf082iqZw3BiVAk0epolFEGAMIDf205v4/KHAKVjYjJ+u01XrBvUHphiZUH+0Iw1xpzalxdXCMRD3kYId8ZXKLEvXAVQBfvPirF4cvgXDcY8IzbaUz5ZU9wJ

m=audio 49000 RTP/SAVP 98

a=rtpmap:98 AMR/8000

m=video 52230 RTP/SAVP 31

a=rtpmap:31 H261/90000

密钥协商响应 SIP 报文：

SIP/2.0 200OK

Via: SIP/2.0/UDP 192.168.4.4:26000;branch=z9hG4bK-d8754z-87d60b47b6627c3a-1---d8754z-;rport=26000

From: "Dingyi"<sip:dingyi@192.168.4.4>;tag=15c8325a

To: "wangxiao"<sip:wangxiao@192.168.4.4>;tag=cDg7NyjpeSg4m

Call-ID: YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.

CSeq: 2 INVITE

Contact:<sip:wangxiao@192.168.4.4:5060;transport=udp>

User-Agent: FreeSWITCH-mod_sofia/1.0.trunk-16981M

Accept：application/sdp

Allow：INVITE，ACK，BYE，CANCEL，OPTIONS，MESSAGE，UPDATE，INFO，REGISTER，REFER，NOTIFY，PUBLISH，SUBSCRIBE

Supported：timer，precondition，path，replaces

Allow-Events：talk，presence，dialog，line-seize，call-info，sla，include-session-description，presence.winfo，message-summary，refer

Content-Type：application/sdp

Content-Disposition：session

Content-Length：**

//以下为 SDP 消息体信息

v=0

o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com

s=test

a=key-mgmt：mikey

ARcFALUwkagBAAB75qwuAAAAAAAAAAAAAAAAAAoAAAAAAFufBpMLAAAADwABAQIBAQUBA

AcBAQgBARYgcVxIHcgKevUQPPF6Qn8plMf082iqZw3BiVAk0epolFEGAMIDbmTnOxFi4h1j0SA1sciecy

AUyCTbBbpmH0062Em/LgDMHfJwZigOkjkXTZJAWhDIZ1M8YaBTZnDuDv1lhzoik4pmppDGx

m=audio 49000 RTP/SAVP 98

a=rtpmap：98 AMR/8000

m=video 52230 RTP/SAVP 31

a=rtpmap：31 H261/90000

附 录 C
（资料性）
会话过程示例

C.1 密钥分发模式

密钥分发模式会话流程见图 C.1。

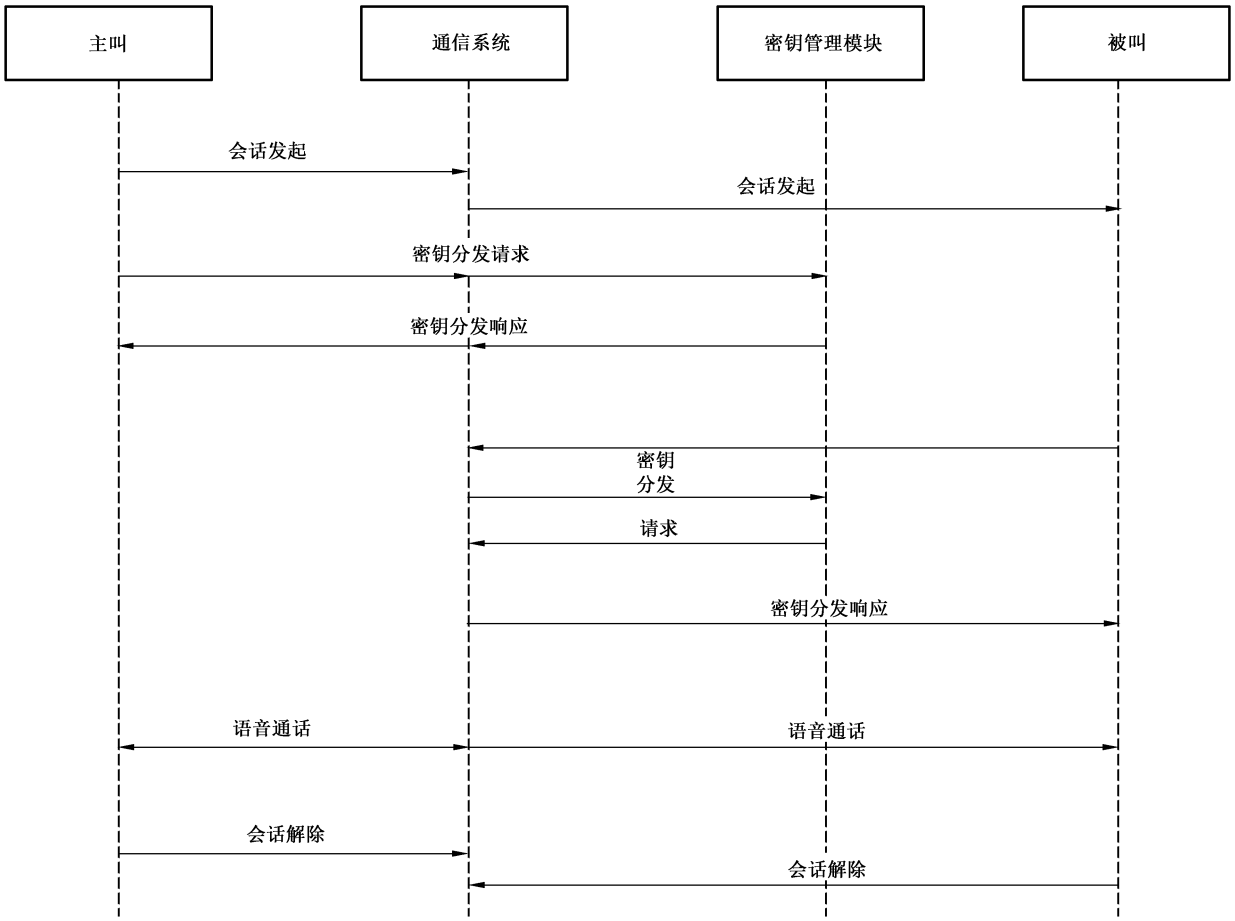

图 C.1 密钥分发模式会话流程

C.2 密钥协商模式

密钥协商模式会话流程见图 C.2。

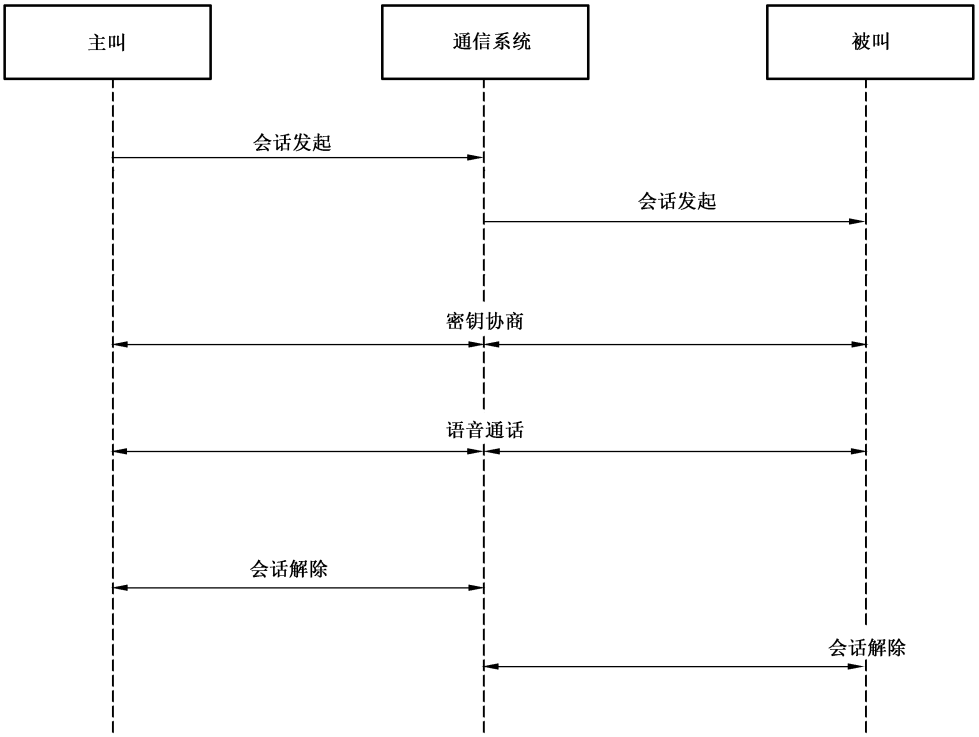

图 C.2 密钥协商模式会话流程

附 录 D
（资料性）
安全协议 SIP 报文

D.1 会话建立

INVITE sip:dingyi@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Dingyi <sip:dingyi@biloxi.com>
From: Wangxiao <sip:wangxiao@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: sip:wangxiao@pc33.atlanta.com
Authorization:Capability algorithm="SM4/ECB:SM4/CBC;SM2" version="1"
Content-Type: application/sdp
Content-Length: 142

D.2 开户绑定

开户绑定请求 SIP 报文：
INFO sip:wangxiao@pc33.example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.2:5060;branch=z9hG4bKnabcdef
To: Dingyi <sip:dingyi@example.com>;tag=a6c85cf
From: Wangxiao <sip:wangxiao@example.com>;tag=1928301774
Call-Id: a84b4c76e66710@pc33.example.com
CSeq: 314333 INFO
Info-Package: foo
Content-type: message/userbind
Content-length: 142
（开户绑定请求报文 base64 编码后数据）

开户绑定响应 SIP 报文：
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877;received=192.0.2.4
To: <sip:carol@chicago.com>;tag=93810874
From: Wangxiao <sip:wangxiao@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314333 INFO
Contact: <sip:carol@chicago.com>
Contact: <mailto:carol@chicago.com>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE

Content-Length：365

（开户绑定响应报文 base64 编码后数据）

D.3 密钥分发

密钥分发请求 SIP 报文：

INFO sip:wangxiao@pc33.example.com SIP/2.0

Via：SIP/2.0/UDP 192.0.2.2:5060;branch=z9hG4bKnabcdef

To：Dingyi〈sip:dingyi@example.com〉;tag=a6c85cf

From：Wangxiao〈sip:wangxiao@example.com〉;tag=1928301774

Call-Id：a84b4c76e66710@pc33.example.com

CSeq：314333 INFO

Info-Package：foo

Content-type：message/keyrequest

Content-length：142

（密钥服务请求报文 base64 编码后数据）

密钥分发响应 SIP 报文：

SIP/2.0 200 OK

Via：SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKhjhs8ass877;received=192.0.2.4

To：〈sip:carol@chicago.com〉;tag=93810874

From：Wangxiao〈sip:wangxiao@atlanta.com〉;tag=1928301774

Call-ID：a84b4c76e66710

CSeq：314333 INFO

Contact：〈sip:carol@chicago.com〉

Contact：〈mailto:carol@chicago.com〉

Allow：INVITE，ACK，CANCEL，OPTIONS，BYE

Content-Length：365

（密钥服务响应报文 base64 编码后数据）

D.4 基于 SM2 密码算法的密钥协商

密钥协商发起 SIP 报文：

INVITE sip:wangxiao@192.168.4.4 SIP/2.0

Via：SIP/2.0/UDP 192.168.4.4:26000;rport

Max-Forwards：70

Contact：〈sip:dingyi@192.168.4.4:26000〉

To："wangxiao"〈sip:wangxiao@192.168.4.4〉

From："Dingyi"〈sip:dingyi@192.168.4.4〉;tag=15c8325a

Call-ID：YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.

CSeq：1 INVITE

Allow：INVITE，ACK，CANCEL，OPTIONS，BYE，REFER，NOTIFY，MESSAGE，SUBSCRIBE，INFO

Content-Type：application/sdp

Content-Length：***
//以下为 SDP 消息体信息
v=0
o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com
s=test
t=2873397496 2873404696
a=key-mgmt:envelope AQAFgM0XflABAAAAAAAAAAAAAAsAyONQ6gAAAAAGEEoo2pee4hp2UaDX8ZE22YwKAAAPZG9uYWxkQGR1Y2suY29tAQAAAAAAAQAk0JKpgaVkDaawi9whVBtBt0KZ14ymNuu62+Nv3ozPLygwK/GbAV9iemnGUIZ19fWQUOSrzKTAv9zV
m=audio 49000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 52230 RTP/SAVP 31
a=rtpmap:31 H261/90000

密钥协商响应 SIP 报文：
SIP/2.0 183 Session Progress
Via：SIP/2.0/UDP 192.168.4.4:26000;brport=26000
From："Dingyi"<sip:dingyi@192.168.4.4>;tag=15c8325a
To："wangxiao"<sip:wangxiao@192.168.4.4>;tag=cDg7NyjpeSg4m
Call-ID：YWEwYjNlZTZjOWZjNDg3ZjU3MjQ3MTA1ZmQ1MDM5YmQ.
CSeq：2 INVITE
Contact：<sip:wangxiao@192.168.4.4:5060;transport=udp>
User-Agent：FreeSWITCH-mod_sofia/1.0.trunk-16981M
Accept：application/sdp
Allow：INVITE，ACK，BYE，CANCEL，OPTIONS，MESSAGE，UPDATE，INFO，REGISTER，REFER，NOTIFY，PUBLISH，SUBSCRIBE
Supported：timer，precondition，path，replaces
Allow-Events：talk，presence，dialog，line-seize，call-info，sla，include-session-description，presence.winfo，message-summary，refer
Content-Type：application/sdp
Content-Disposition：session
Content-Length：**
//以下为 SDP 消息体信息
v=0
o=wangxiao 2891092738 2891092738 IN IP4 w-land.example.com
s=test
a=key-mgmt：envelope AQAFgM0XflABAAAAAAAAAAAAAAsAyONQ6gAAAAAGEEoo2pee4hp2UaDX8ZE22YwKAAAPZG9uYWxkQGR1Y2suY29tAQAAAAAAAQAk0JKpgaVkDaawi9whVBtBt0KZ14ymNuu62+Nv3ozPLygwK/GbAV9iemnGUIZ19fWQUOSrzKTAv9zV
m=audio 49000 RTP/SAVP 98
a=rtpmap:98 AMR/8000
m=video 52230 RTP/SAVP 31
a=rtpmap:31 H261/90000

中华人民共和国密码
行业标准
**基于IP网络的加密语音通信
密码技术规范**
GM/T 0098—2020

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 3　字数 90 千字
2021年5月第一版　2021年5月第一次印刷

*

书号:155066·2-35844　定价 50.00 元

GM/T 0098-2020

码上扫一扫　正版服务到