国 际 电 信 联 盟

ITU-T H.235.8

国际电信联盟
电信标准化部门

(09/2005)

H系列：视听和多媒体系统

视听业务的基础设施 — 系统概况

H.323安全性：使用安全信令信道的SRTP的密钥交换

ITU-T H.235.8建议书

国际电信联盟

ITU-T H系列建议书

视听和多媒体系统

可视电话系统的特性	H.100-H.199
视听业务的基础设施	
概述	H.200-H.219
传输多路复用和同步	H.220-H.229
系统概况	**H.230-H.239**
通信规程	H.240-H.259
活动图像编码	H.260-H.279
相关系统概况	H.280-H.299
视听业务的系统和终端设备	H.300-H.349
视听和多媒体业务的号码簿业务体系结构	H.350-H.359
视听和多媒体业务的服务质量体系结构	H.360-H.369
多媒体的补充业务	H.450-H.499
移动性和协作程序	
移动性和协作、定义、协议和程序概述	H.500-H.509
H系列多媒体系统和业务的移动性	H.510-H.519
移动多媒体协作应用和业务	H.520-H.529
移动多媒体应用和业务的安全性	H.530-H.539
移动多媒体协作应用和业务的安全性	H.540-H.549
移动性互通程序	H.550-H.559
移动多媒体协作互通程序	H.560-H.569
宽带和三网合一多媒体业务	
在VDSL上传送宽带多媒体业务	H.610-H.619

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T H.235.8建议书

H.323安全性: 使用安全信令信道的SRTP的密钥交换

摘　要

本建议书的目的是描述用于在 H.323/H.235 网络上使用安全信令信道的 SRTP 的密钥交换的安全规程。

本建议书应与 ITU-T H.323 建议书和 ITU-T H.225.0 建议书第 4 版或更新版本一起使用。

来　源

ITU-T 第 16 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 9 月 13 日批准了 ITU-T H.235.8 建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

		页
1	范围	1
2	参考文献	2
	2.1 规范性参考文献	2
	2.2 资料性参考文献	2
3	符号和缩写	2
4	参数描述	3
	4.1 SRTP 参数传输	3
	4.2 SrtpCryptoCapability 参数描述	4
	4.3 SrtpKey 参数描述	6
	4.4 SRTP 密码报文初始化	7
5	规程	9
	5.1 安全能力交换	9
	5.2 最初的协商	10
	5.3 对话修改	13
	5.4 无协商	14
	5.5 前向纠错	14
6	用于保护 SRTP 的密钥交换的公钥密码术	14
	6.1 端点标识符	15
	6.2 SRTP 密钥交换规程	15
	6.3 CMS 主体的使用	16
7	H.235 SRTP 安全描述句法	19

ITU-T H.235.8建议书

H.323安全性: 使用安全信令信道的SRTP的密钥交换

1 范围

本建议书的目的是在用于媒体信道的密码材料在安全的信令信道上传输的情况下，为支持 H.323 端点之间的 IETF 安全实时协议（SRTP）提供安全规程的建议，例如 Ipsec（RFC 2401）、TLS（RFC 2246）或其他 H.235 机制。这些安全规程提供作为支持 SRTP 的其他 H.235 安全规程的替代。

本建议书描述了用于支持 ITU-T H.323 中的 IETF 安全实时协议（SRTP）的规程。SRTP 提供用于 RTP 媒体的安全性业务，并依据不同的协议分别提供密钥管理业务和密码参数的协商。当安全信令规程在中介系统终止时，这些规程应不使用，在这样的情况下，SRTP 密码材料应由安全的端到端机制传输。

这些规程支持 H.323 端点之间的 SRTP 密钥、认证和加密算法标识符以及其他对话参数的信令、协商和传输。

这些规程的关键问题是，H.245 的从属方与 H.245 的主控方一样，必须能够生成和分发密钥。

SRTP 安全能力和使用现有的终端能力交换进行交换，现有的终端能力交换使用 H.245 TerminalCapabilitySet 消息的 capabilityTable 中的 h235SecurityCapability 条目。在 h235SecurityCapability 条目的 encryptionAuthenticationAndIntegrity 字段中的 genericH235SecurityCapability 字段包含将规定 SRTP 密码组的 SrtpCryptoCapability 字段。

SRTP 密码参数被规定用来发送和协商 SRTP 密码参数。本建议书中密码参数的定义限制于双方单播媒体流，其中每个源具有一个惟一的密钥；对组播媒体流或多点单播媒体流的支持有待进一步研究。

SRTP 密码参数旨在能够在单个消息或单个往返消息交换中确定 SRTP 密码参数。在往返消息交换的情况下，可以协商密码参数。例如，在快速连接中，提议的 H.323 端点发送一套提议的 SRTP 密码参数给应答的 H.323 端点，每个都在 H.245 OpenLogicalChannel 消息中提供封装。然后应答的 H.323 端点可接收提议参数中的一个，用包括在 H.245 OpenLogicalChannel 消息中封装的选择的参数子集的回答来响应。

在单个消息交换的情况下，无协商。提议的 H.323 端点发送 SRTP 密码参数给应答的 H.323 端点，应答的端点接受提供的参数或拒绝呼叫。

在封装安全性协议，例如 IPsec 和 TLS，在中介设备上终止并因此不提供端到端安全性的情况下，通过加密然后标记 SRTP 密钥材料，可增加公钥密码术规程，以提供在 H.323 端点之间 SRTP 对话密钥材料的端到端机密性和认证。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems.*

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

– ITU-T Recommendation H.460.11 (2004), *Delayed call establishment within H.323 Systems*.

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

– IETF RFC 2733 (1999), *An RTP Payload Format for Generic Forward Error Correction.*

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

– IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP).*

– IETF RFC 3852 (2004), *Cryptographic Message Syntax (CMS)*.

2.2 资料性参考文献

– IETF Draft, F. Andreasen, M. Baugher, D. Wing: *Session Description Protocol Security Descriptions for Media Streams,* <draft-ietf-mmusic-sdescriptions-11.txt>.

3 符号和缩写

本建议书采用下列缩写：

AES	高级加密算法
ASN.1	抽象句法符号 1
CA	认证机构
CEK	内容加密密钥
CMS	密码消息句法
EP	端点
FEC	前向纠错
FFS	有待进一步研究
F8	UMTS 加密算法
GK	网守

GW	网关
HMAC	散列消息认证码
IETF	互联网工程任务组
KDR	密钥衍生率
MAC	消息认证码
MKI	主密钥标识符
OID	对象标识符
OLC	开放逻辑信道
PKI	公钥基础设施
RAS	注册、认可和状态
ROC	轮滚计数器
RTCP	实时传输控制协议
RTP	实时传输协议
SHA1	安全散列算法 1
SRTCP	安全实时传输控制协议
SRTP	安全实时传输协议
SSRC	同步源
TLS	传输层安全性
WSH	窗口大小示意

4 参数描述

SRTP 密码能力和密钥材料使用两个参数交换：

— **StrpCryptoCapability** 内的 **SrtpCryptoInfo** 必须包含密码组和对话参数。**SrtpCryptoInfo** 参数必须在 H.245 **genericH235SecurityCapability** 参数中传输以标志和协商 SRTP 密码参数。

— **SrtpKeys** 内的 **SrtpKeyParameters** 必须包含 SRTP 密钥材料。H.245 **h235Key** 参数中的 **SrtpKeys** 存储器必须传输一个或多个具有 SRTP 密钥的 **SrtpKeyParameters**。

本建议书中 SRTP 密码参数的使用限制于双方单播媒体流，其中每个源具有一个惟一的密钥；对组播媒体流或多点单播媒体流的支持有待进一步研究。

4.1 SRTP参数传输

全双工 SRTP 媒体连接包含两条单向信道，每个方向上一条。每个提议的密码在单个 H.245 **OpenLogicalChanne** 消息中传输。

4.1.1 SrtpKeys参数

SRTP 密钥材料 **SrtpKeys** 必须在 **secureSharedSecret**（**V3KeySyncMaterial**）参数的 **genericKeyMaterial** 字段中传输，该参数被包含在 H.245 **OpenLogicalChannel** 消息的 **encryptionSync** 参数中的 **h235Key** 存储器内。

genericKeyMaterial 存储器内的 SRTP 密钥内容必须使用 OLC **dataType** 的 **h235Media** 内的 **encryptionAuthenticationAndIntegrity** 的 **genericH235SecurityCapability** 字段内的 **capabilityIdentifier** 的 **standard** 字段中的 H.235.8 对象标识符值（见表 1）标识。

在 **H2250LogicalChannelParameters** 内包含相同 **sessionID** 值的同一信道的替代 **OpenLogicalChannel** 提议可使用相同的提议的密码。因为这些替代对话中只有一个将被接受，所以将确保密钥惟一性。

4.1.2 SrtpCryptoCapability传输

SrtpCryptoCapability 参数必须在 **OpenLogicalChannel** 消息的 **dataType** 参数的 **h235Media** 中的 **encryptionAuthenticationAndIntegrity** 的 **genericH235SecurityCapability** 字段中传输。

H.245 **TerminalCapabilitySet** 消息可以在 **capabilityTable** 中包括一个或多个 **h235SecurityCapability** 条目。为了指示支持这些规程，H.323 端点必须如下地在 **h235SecurityCapability** 条目的 **encryptionAuthenticationAndIntegrity** 内设置 **genericH235SecurityCapability**:

- **capabilityIdentifier** 必须在 **standard** 字段内包含 H.235.8 OID（见表 1）；
- **maxbitRate**、**collapsing**、**nonCollapsing** 和 **transport** 不得使用；
- **nonCollapsingRaw** 必须包含 **SrtpCryptoCapability** 参数。

表 1/H.235.8－H.235.8 对象标识符

OID值
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 90 }

4.2 SrtpCryptoCapability参数描述

SrtpCryptoCapability 可包含一个或多个可用于规定 SRTP 对话的能力的 **SrtpCryptoInfo** 参数。**BOOLEAN OPTIONAL** 单元必须如下解释:

1） 若为 FALSE，则不支持该能力；

2） 若为 TRUE，则支持且需要该能力；

3） 若缺省，则支持但不需要该能力。

当在能力交换中使用 **SrtpCryptoCapability** 时，在一个通用能力内指示所有可接受的选项是可能的。在该使用中，**BOOLEAN OPTIONAL** 单元的省略将被解释为意味着支持但不需要能力。

当在 OLC **dataType** 表达式中使用时，可仅使用一个选项。出于此目的，必须遵守下列规则：

- **FecOrder** 可仅包含这些任选值中的一个。
- 在 **SrtpSessionParameters** 中，**BOOLEAN OPTIONAL** 值务必是 TRUE 或 FALSE。
- **SrtpCryptoCapability** 必须仅包含一个 **SrtpCryptoInfo** 单元。

SrtpCryptoInfo 参数由一个强制的 **cryptoSuite** 字段和多个任选的 **sessionParams** 合 **allowMKI** 字段组成，如下所描述的。

表 2/H.235.8－H.235.8密码组对象标识符

密　码　组	OID值
AES_CM_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 91 }
AES_CM_128_HMAC_SHA1_32	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 92 }
F8_128_HMAC_SHA1_80	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 93 }

4.2.1　cryptoSuite

字段 **cryptoSuite** 中的对象标识符（见表 2）标识将在 SRTP 对话中使用的期望的加密和认证算法。SRTP 规范有很多参数，它们被捆绑成 3 个被称为“密码组”的选项。由于可以加入新的密码组，这些选项是可扩展的。这 3 个被定义的密码组是 AES_CM_128_HMAC_SHA1_80 、AES_CM_128_HMAC_SHA1_32 和 F8_128_HMAC_SHA1_80。这些被绑定的 SRTP 参数在表 3 中分别按列示出。

表 3/H.235.8－密码组默认值

SRTP参数	AES_CM_128_ HMAC_SHA1_80	AES_CM_128_ HMAC_SHA1_32	F8_128_ HMAC_SHA1_80
主密钥长度	128 比特	128 比特	128 比特
补白值	112 比特	112 比特	112 比特
生命周期	2^31 个包	2^31 个包	2^31 个包
密码	AES 计数器	AES 计数器	F8
加密密钥	128 比特	128 比特	128 比特
MAC	HMAC-SHA1	HMAC-SHA1	HMAC-SHA1
认证标记长度	80 比特	32 比特	80 比特
SRTP 认证密钥长度	160 比特	160 比特	160 比特
SRTCP 认证密钥长度	160 比特	160 比特	160 比特

字段 **cryptoSuite** 是一个协商的参数。

4.2.2　sessionParams

对话参数可以是协商的或声明的；特定对话参数的定义必须指示其是协商的还是声明的。协商的参数适用于在两个方向上发送的数据，而声明的参数仅适用于由生成对话的实体发送的媒体。这样，在提议中声明的参数适用于由提议方发送的媒体，而在回复中的声明的参数适用于由回答方发送的媒体。

任选字段 **sessionParams** 包含 SRTP 对话参数。

4.2.2.1　kdr

KDR 规定了密钥衍生率，如 RFC 3711 的第 4.3.1 节中描述的。值必须是一个在子集{1, 2, ..., 24}中的整数，指示 2 的幂，从 2^1 到 2^24（包括在内）。SRTP 密钥衍生率控制从一个 SRTP 主密钥（RFC 3711）衍生一个新的对话密钥的频次。当密钥衍生率未规定（即 KDR 参数被省略），执行一个单个的初始密钥衍生（RFC 3711）。KDR 是一个声明的参数。

4.2.2.2 unencryptedSrtp

这是一个任选的布尔字段：如果显示，它标志 SRTP 有效载荷未加密。这是一个协商的参数。

4.2.2.3 unencryptedSrtcp

这是一个任选的布尔字段：如果显示，它标志 SRTP 有效载荷未加密。这是一个协商的参数。

4.2.2.4 unauthenticatedSrtp

SRTP 和 SRTCP 包有效载荷默认地是已认证的。这是一个任选的布尔字段：如果显示，它表明 SRTP 有效载荷未认证。SRTP 规范要求使用 SRTCP 的消息认证，但是不要求使用 SRTP 的消息认证（RFC 3711）。这是一个协商的参数。

4.2.2.5 fecOrder

fecOrder 表明相对于在发送方的 SRTP 加密，RTP 包的前向纠错处理次序（RFC 3550，RFC 2733）。**FecBeforeSrtp** 的 **fecOrder** 值表明在 SRTP 媒体的发送方进行 SRTP 处理之前和在 SRTP 媒体的接收方进行 SRTP 处理之后，FEC 适用；**fecBeforeSrtp** 是默认的。**fecAfterSrtp** 是处理的相反次序。**FecOrder** 是一个声明的参数。

4.2.2.6 windowSizeHint

SRTP 定义 SRTP-WINDOW-SIZE（RFC 3711，第 3.3.2 节）参数来保护以放置回放的攻击。最小值是 64（RFC 3711），但这一值可能被认为对于某些应用（如视频）太低。

窗口大小示意（WSH）对话参数提供该窗口应为多大才能令人满意地工作（例如，基于发送方知道每秒有多少个包）示意。然而，可能在媒体分组描述符中给出了足够的信息，允许接收方令人满意地衍生出参数。因此，该值仅被看做是对可选择忽略提供的值的接收方的示意。

WindowSizeHint 是一个声明的参数。

4.2.2.7 定义新的SRTP对话参数

新的 SRTP 对话参数是强制的默认值。**NewParameter** 字段被用做新的对话参数的扩展机制。如果一个较旧的 H.323 端点接收在 **newParameter** 字段中具有未知的对话参数的 **SrtpCryptoInfo** 参数，则必须认为新的 **SrtpCryptoInfo** 参数是无效的。

4.3 SrtpKey参数描述

字段 **SrtpKey** 包含一个或多个将用于 SRTP 对话的密钥参数 **SrtpKeyParameter**。每个 **SrtpKeyParameter** 包含密钥材料（主密钥和补白）和与那一主密钥相关的所有政策，包括它可被使用多久（生命周期）和它是否使用主密钥标识符（MKI）将入网 SRTP 包与一个特定的主密钥联系起来，且不得接受违反政策（例如在主密钥生命周期已经过期后）的入网分组。

4.3.1 masterKey

这是一个将用于 SRTP 对话的密码主密钥。密钥的长度由密钥采用的密码组确定。如果长度与对密码组的规定不匹配，则讨论中的密码参数必须被认为是无效的。每个主密钥必须是随机的密码数，必须对于提议的媒体流是惟一的。

4.3.2 masterSalt

这是一个将用于 SRTP 对话的密码主控补白。补白的长度由密钥采用的密码组确定。如果长度与对密码组的规定不匹配，则讨论中的密码参数必须被认为是无效的。每个主控补白必须是随机的密码数，必须对于提议的媒体流是惟一的。

4.3.3 lifetime

该字段是主密钥的任选生命周期，它使用那一主密钥在最多的 SRTP 或 SRTCP 包中测量（即 SRTP 包的数量和 SRTCP 包的数量都必须比生命周期短）。生命周期值可写为非 0、负整数或 2 的幂。“生命周期”值不得超过密码组的最大包生命周期。如果生命周期字段不显示，则将使用默认的生命周期。当 SRTP 密钥生命周期是默认值时，这是方便的。

4.3.4 masterKeyId

这一任选字段规定对于 SRTP 对话密钥将如何被标识的政策。MKI 是与 SRTP 主密钥相关的主密钥标识符。如果 MKI 已给出，则 MKI 的长度也必须提供。MKI 长度是在 SRTP 包中的 MKI 字段的大小，按字节规定。如果 MKI 未给出或其值超过 128（字节），则整个密码参数必须被认为是无效的。

如上提到的，密钥参数可包含一个或多个主密钥。当密钥参数包含一个或多个主密钥时，在那一密钥参数中的所有主密钥必须包括一个 MKI 值。当使用 MKI 时，MKI 长度必须与给定的密码参数中的所有密钥一样。

4.4 SRTP 密码报文初始化

除了以上定义的各种 SRTP 参数外，还有 3 类信息对缺省的 SRTP 密码的运算很关键：

- SSRC：同步源
- ROC：给定 SSRC 的轮滚计数器
- SEQ：给定 SSRC 的序列号

在单播的对话中，如此处定义的，有关于这些值的 3 种限制。第一类限制是关于 SSRC，它使得来自其他参与方的 SRTP 密钥流是惟一的。如在 SRTP 中描述的，密钥流不得在两个或多个不同的未加密报文中再用。

密钥流再用使得密码报文易受密码分析学的攻击。易受攻击性表现为在一个媒体流中的已知未加密报文会暴露再用密钥流中的一部分，这会进一步暴露其他流中的更多未加密报文。由于所有当前的 SRTP 加密传送使用密钥流，密码共享是一个普遍问题（RFC 3711）。 SRTP 通过在加密流中包括发送者的 SSRC 减轻这一问题。但是 SRTP 不能在其整个媒体流中解决这一问题，因为实时传输流协议有 SSRC 冲突，这非常少见（RFC 3550）但确实可能存在。在冲突中，共享一个主密钥的两个或多个 SSRC 将具有同样的 RTP 序列号空间的重叠部分的密钥流。SRTP 安全性描述通过制作安全性描述的发送方和接收方必需的惟一的主密钥来避免密钥流再用。

也应注意到 SSRC 冲突有一个次要问题。SSRC 被用于标识密码报文从而标识密码、密钥、ROC 等，来处理入网分组。在 SSRC 冲突的情况下，密码报文标识变得模棱两可，可能不能进行正确的分组处理。而且，如果为了一个冲突的 SSRC 发送一个 RTCP BYE 分组，则分组也可能必须是安全的。

第二类限制是在每个 SSRC 开始发送分组的时候，ROC 必须为 0。这样，在 SRTP 安全性描述中就没有“新加入者”的概念了，它被限制为单播和成对传播。按照本建议书，ROC 和 SEQ 在默认的 SRTP 传输中构成“分组索引”，ROC 在对话开始时始终被设置为 0。

第三个限制是 SEQ 的初始值应在 0..2^15 – 1 的范围内选择；这避免了当分组在对话开始时丢失时的模糊性。如果在对话开始时，SSRC 源可随机地选择一个高序列号值，将接收方放置在一个模糊的情况下：如果初始分组在传输中直到序列号限制（即超过 2^16 – 1）的点丢失，则接收方可能未认识到其 ROC 需要增加。通过限制初始的 SEQ 到 0..2^15 – 1 的范围内，SRTP 分组索引限定将找到正确的 ROC 值，除非所有的第一个 2^15 分组丢失（这看起来即使不是决不可能的，也是相当不可能的）。关于分组索引限定（RFC 3771）的 SRTP 规范见第 3.3.1 节。

4.4.1 SSRC到密码报文的最新绑定

因此，分组索引取决于 SSRC、入网分组的 SEQ 和 ROC，其中 ROC 是可变的 SRTP 密码报文。因此，SRTP 具有取决于 SSRC 惟一性的极大的安全性。考虑到以上限制，单播 SRTP 密码报文可以建立，无需在 SRTP 安全性描述中协商 SSRC 值。本建议书建议了另一个被称为“最新捆绑”的方法。当一个包到达时，被包含在其中的 SSRC 可在对话开始时（即 SRTP 包到达时）而不是在对话发送信令时（即接收 H.245 消息时）与密码报文捆绑在一起。随着包含 SSRC 的包的到来，SRTP 密码报文所需的所有数据项由接收方持有（注意，定义的 ROC 值是 0；如果支持非 0 值，则需要另外的信令）。换句话说，使用最新捆绑的安全 RTP 对话的密码报文最初由 H.245 消息标识如下：

<*, address, port>

其中‘*’是通配符 SSRC，“address”是来自 **mediaChannel** 的本地接收地址，且“port”是来自 **portNumber** 的本地接收端口。当第一个在其 SSRC 字段中具有 ssrcX 的包到达时，密码报文

<ssrcX, address, port>

以下列限制为条件示例：

- 媒体包被认证：认证务必成功；否则，密码报文不示例。
- 媒体包未认证：密码报文自动示例。

应注意，当无 SRTP 媒体包的认证时，最新捆绑的使用遭受大量安全性攻击，所以不建议采用它（当然，通常可以说 SRTP 未认证）。

注意，无认证最近捆绑的使用将导致从任何未知的 SSRC 接收包的后果是创建本地状态。因此，不建议使用未认证 SRTP，因为它易受业务拒绝的攻击。与此相比，认证的最新捆绑没有此缺点。

4.4.2 在对话或SSRC中共享密码报文

根据以上描述的限制和规程，对于一个单播 RTP 对话，不必明确示意 SSRC、ROC 和 SEQ。因此不存在示意 SSRC、ROC 和 SEQ 的 SRTP 密码参数。这样，来自同一实体的多个 SSRC 当使用最新捆绑时，将共享 SRTP 密码参数。出现来自同一实体的多个 SSRC 是因为在那同一个对话中有多个源（麦克风、照相机，等等），或 RTP 有效载荷要求 SSRC 复用。

H.245 允许在同一个媒体描述中定义多个 RTP 对话，这些 RTP 对话也将共享 SRTP 密码参数。以此方法使用 SRTP 密码参数的一项应用在 RTP 对话或 SSRC 中共享一个主钥，当在所有 SSRC 中的包总数接近 2^31 个包时，必须替换主钥。共享一个主要的 SSRC 必须彼此间是惟一的。

从一个主钥中衍生出来的所有密钥的生命周期由主钥的生命周期确定。所以，如果主钥的生命周期是 2^31 个包且一个衍生密钥已经发送 2^31 – y 个包，则仅有 y 个包可由来自那一主钥的任何密钥发送。这是因为生命周期取决于密钥中熵或随机数（密钥具有的所有随机数或熵）的数量，从主钥衍生密钥不会引入随机数。

4.4.3 密码报文的移除

以上定义的机制进行创建密码报文的发布工作。但是，在实践中，对话的参与方可能想要在对话终止之前移除密码报文。由于密码报文包括不能自动被移除的信息（例如 ROC），重要的是当密码报文可被移除时，发送方和接收方要达成一致，当密码报文不能被移除时，这一点可能更为重要。

即使当最新捆绑被用于单播流时，一旦密码报文被移除，ROC 丢失，且不能自动回复（除非它是 0）。

收到 **CloseLogicalChanne** 时必须移除密码报文。另外，密码报文的移除必须遵循与从子句表（RFC 3711）中移除 SSRC 相同的规则；注意，作为由于失效造成的 SRTCP BYE 包或简单的超时带来的后果，这可能发生。希望确保其密码报文未超时的失效的对话参与方因此务必以规则的间隔发送 SRTCP。

5 规程

在 H.245 信令信道受封装的数据安全性协议（例如 IPsec（RFC 2401）、TLS（RFC 2246））的保护的情况下，以下描述的 SRTP 规程必须仅被用于协商双方单播媒体流的安全性。SRTP 使用 H.245 消息的密码参数的交换必须提供下列功能：

1） SRTP 加密和完整性能力的交换和协商。

2） 在每个方向上用于 SRTP 的初始加密和算法、密钥和对话参数的协商和确定。

3） 在 SRTP 对话期间的任何时间进行的加密和算法、密钥和对话参数的修改。

5.1 安全能力交换

H.323 端点能够支持的 SRTP 密码组、加密和完整性算法必须由 **SrtpCryptoCapability** 标识。

将使用 H.245 **TerminalCapabilitySet** 消息中的 **capabilityTable** 中的一个或多个 **h235SecurityCapability** 条目来提供安全能力交换。**capabilityTable** 中的 **h235SecurityCapability** 条目的 **mediaCapability** 字段被用于将安全能力与 **capabilityTable** 中的特定媒体能力条目联合。

h235SecurityCapability 条目中的 **encryptionAuthenticationAndIntegrity** 字段包含 **genericH235SecurityCapability** 字段，它将规定由 H.235.8 OID 标识的 SRTP 密码组。如果 **genericH235SecurityCapability** 字段的 **capabilityIdentifier** 的 **standard** 字段包含 H.235.8 OID（见表 1），则 **SrtpCryptoCapability** 将包含一个或多个 **SrtpCryptoInfo** 参数，这些参数表示 H.323 端点支持的密码组。**SrtpCryptoInfo** 字段中的 **cryptoSuite** 字段包含一个 OID，如表 2 中所定义的，该 OID 标识一个特定的密码组。在 **SrtpCryptoInfo** 字段内，**sessionParams** 字段标识对话参数，**allowMKI** 字段指示 H.323 端点是否支持 MKI。

5.2 最初的协商

5.2.1 最初的密码提议

每个密码提议在一个单独的 **OpenLogicalChannel** 消息中传输。每个密钥提议必须在 **SrtpCryptoCapability** 内包含一个 **SrtpCryptoInfo** 结构和在 **SrtpKey** 中包含一个或多个 **SrtpKeyParameters**。

对于标准的 H.245（非快速连接）规程，H.323 端点必须包含密码提议，如对于发送方向（从提议的 H.323 端点到答复的 H.323 端点）在 H.245 **OpenLogicalChannel** 消息的 **SrtpCryptoInfo** 和 **SrtpKeyParameters** 结构中描述的。H.323 端点应提供主控方最优选的安全能力，如在终端能力交换过程中指示的、其本身具有的能力中的能力。

对于快速连接规程，提议的 H.323 端点必须发送每个提议的密码，如对于发送方向（从提议的 H.323 端点到答复的 H.323 端点）在 H.245 **OpenLogicalChannel** 消息的 **SrtpCryptoInfo** 和 **SrtpKeyParameters** 结构中描述的。

提议的 **OpenLogicalChannel** 消息必须按优先级排序，最优先的密码组最先列出，次优先的密码组应比优先级略低的密码组在密码上更强。一般地，次优先的密码组应比优先级略低的密码组在密码上更强。

当发布一个提议的密码时，提议方必须按照任何提议的密码参数准备好支持媒体安全性。与此相关的有两个问题。第一，提议方不知道回答方将使用哪种密钥将媒体发送给提议方。由于媒体可能在密码回复之前到达，所以可能发生延误或截短。如果对于提议方这是不可接受的，则提议方应使用机制（如 H.460.11 延迟呼叫建立规程）来防止上述问题的出现。

当有多个提议时可能发生另一个问题：提议方不能推论出哪一个提议被回答方接受，直到接收到密码回答，而媒体可能在密码回答之前到达。如果这对于提议方是不可接受的，则提议方应不发送多于一个提议，或如 H.460.11 延迟呼叫建立规程之类的规程应被用于防止上述问题的出现。

SrtpCryptoInfo 可能包括对话参数。

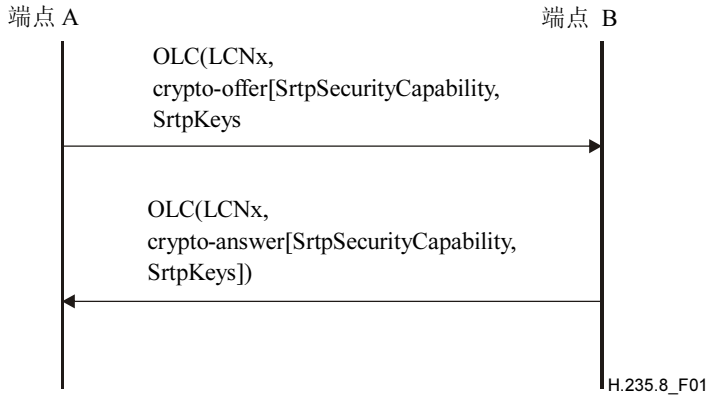

图 1/H.235.8－快速连接提议—回答交换

5.2.1.1 最初的密码回答

5.2.1.1.1 概述

这些规程适用于快速连接和标准 H.245 规程。密码回答必须在 **SrtpCryptoCapability** 内包含一个 **SrtpCryptoInfo** 结构和在 **SrtpKeys** 中包含一个或多个 **SrtpKeyParameters**。

回答方 H.323 端点必须采用从密码提供方选择的密码组到相反方向上的对应的单向 SRTP 信道，必须生成在相反方向上的 SRTP 信道使用的密钥。

另外，回答方 H.323 端点必须包括 **SrtpKeys** 中的一个或多个密钥，它们将被用于从回答方 H.323 端点到提议方 H.323 端点的 SRTP 流。回答方 H.323 端点也可能包括来自其希望协商的密码提供方的任何对话参数。

仅有效的参数可被接受；有效参数不违反任何为安全性描述定义的任何一般性原则，同样也不违反为讨论中的传输和密钥方法定义的任何规定的原则。

对于快速连接，考虑到回答方的能力和安全政策，当选择有效密码提议其一时，回答方将选择其能支持的最优先的密码提议，即列表中的第一个有效参数。如果提议都无效，或不支持任何一个有效提议，则提议的媒体流必须被拒绝。

当一个密码提议被接受时，密码回答必须包含回答方将用于发送媒体给提议方的密钥。注意，不考虑在提议方或回答方的任何方向的参数，必须提供密钥。

而且，协商的任何对话参数必须被包括在密码回答中。由提议方提供的声明的对话参数不包括在密码回答中，然而回答方可提供其自己的声明的对话参数集。

一旦回答方已经接受一个提议的密码参数，回答方可能按照选择的密码提议开始发送媒体给提议方。但是注意，提议方可能直到已经收到密码回答才能正确处理这样的媒体包。

5.2.1.1.2 快速连接规程

对于快速连接规程，在一个或多个 H.245 **OpenLogicalChannel** 消息中接收密码提议的回答方 H.323 端点必须通过发送一个包含密码回答的 H.245 **OpenLogicalChannel** 接受其中一个密码提议来响应，如图 1 所示，或通过发送具有被设置为 **securityDenied** 的 **ReleaseCompleteReason** 的 **ReleaseComplete** 拒绝所有密码提议来响应，或通过在 H.225.0 消息中发送 **FastConnectRefused** 单元来响应。如果回答方 H.323 端点不支持此建议书或密码提议中的任何建议，则它必须通过发送具有被设置为 **securityDenied** 的 **ReleaseCompleteReason** 的 **ReleaseComplete**，或通过在 H.225.0 消息中发送 **FastConnectRefused** 单元来拒绝密码提议。

5.2.1.1.3 标准的H.245规程

对于标准的 H.245（非快速连接）规程，适用下列规程。如果 H.323 端点在接收到包含密码提议的 **OpenLogicalChannel** 之前还没有发送包含密码提议的 **OpenLogicalChannel**，则它必须发送 **OpenLogicalChannelAck**，后随包含密码回答的 **OpenLogicalChannel**，如图 2 所示。

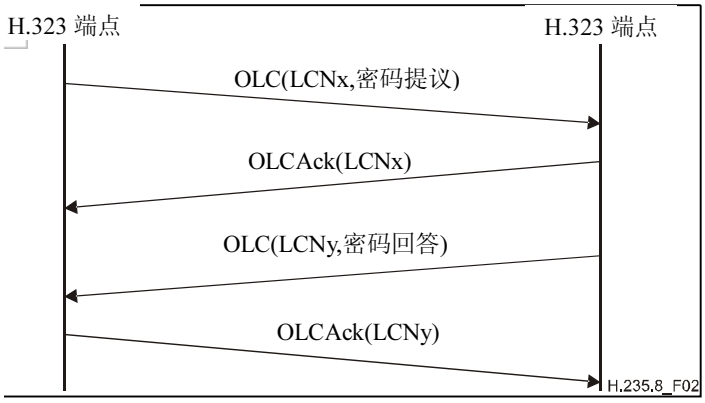

图 2/H.235.8－提议—回答交换

如果 H.323 端点在接收到包含密码提议的 **OpenLogicalChannel** 之前已经发送包含密码提议的 **OpenLogicalChannel**，则主控方和从属方端点采取的行动如下：

1） 主控 H.323 端点必须处理接收到的密码提议，如果该提议与其已经发送的密码提议兼容，则端点必须发送 **OpenLogicalChannelAck** 作为密码回答来接受接收到的密码提议，如图 3 所示。如果该提议与其已经发送的密码提议不兼容，则端点必须发送具有 **securityDenied** 的 **cause** 值的 **OpenLogicalChannelReject** 来拒绝接收到的密码提议，如图 4 所示。术语兼容意指在密码回答中与对应的参数（**cryptoSuite** 和协商的对话参数）匹配。

2） 从属 H.323 端点必须处理接收到的密码提议，如果该提议与其已经发送的密码提议兼容，则端点必须发送 **OpenLogicalChannelAck** 作为密码回答来接受接收到的密码提议，如图 3 所示。如果该提议与其已经发送的密码提议不兼容，且如果其希望接受密码提议，则它必须发送如图 4 所示的下列消息：

a）**OpenLogicalChannelAck**，接受来自主控方的最初的密码提议；

b）**CloseLogicalChannel**，如果还没有从主控方接收到 **OpenLogicalChannelReject**，终止其自己的最初的密码提议；

c）具有匹配来自主控方的密码提议的密码回答的 **OpenLogicalChannel**。

如果从属 H.323 端点不支持在提议中的建议，或不希望接受密码提议，它必须发送具有被设置为 **securityDenied** 的 **cause** 值的 **OpenLogicalChannelReject** 来拒绝密码等提议。

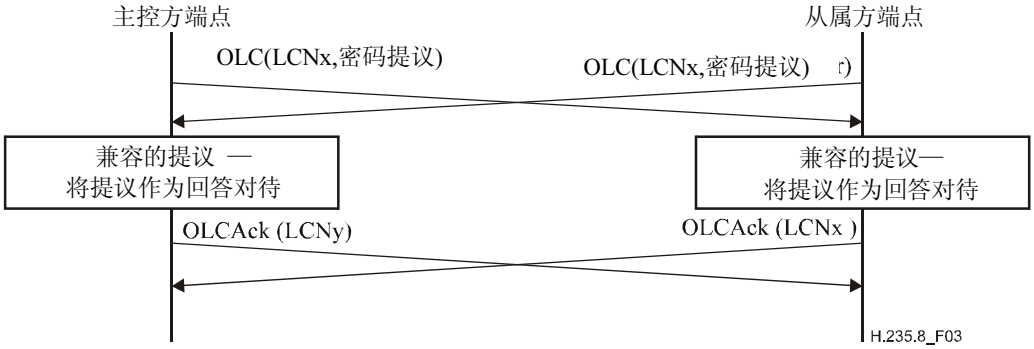

图 3/H.235.8－同时兼容的提议—回答交换

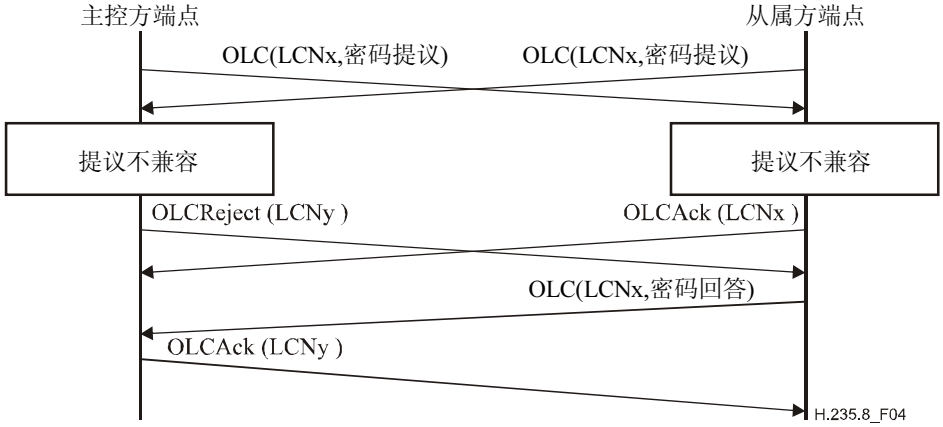

图 4/H.235.8－同时不兼容的提议—回答交换

5.2.1.2 提议方对最初回答的处理

当提议方接收到密码回答，提议方必须核实最初的密码提议之一在密码回答中被接受和回应。而且，密码回答必须包括一个或多个密钥，它们将被用于从回答方发送媒体到提议方。

提议方必须核实密码回答中的密钥与密码提议中的任何密钥都不匹配。如果密码提议包含任何强制协商的对话参数，则提议方必须核实所说的参数被包括在密码回答中且匹配在密码提议中的对应参数。如果密码回答包含任何强制声明的对话参数，则提议方必须能够支持那些参数。

如果上述任何处理失败，协商必须被认为是已经失败。

5.3 对话修改

一旦已经建立 SRTP 媒体流，它可在任何时间使用新的提议—回答交换修改，以执行密码组的重新加密或交换。新的密码提议和密码回答必须在 H.245 **OpenLogicalChannel** 的 **SrtpCryptoCapability** 和 **SrtpKeys** 参数中传输，以开放新的逻辑信道，新的信道将使用 **replacementFor** 规程取代现有的逻辑信道。提议方 H.323 端点必须在 H.225.0 消息内的一个或多个 **OpenLogicalChannel** 消息中包括密码提议。

收到密码提议的回答方 H.323 端点必须通过发送 H.225.0 消息内的 H.245 **OpenLogicalChannel** 来接受提议之一，或用具有被设置为 **securityDenied** 的 **cause** 的 **OpenLogicalChannelReject** 消息拒绝提议来响应。如果密码提议被拒绝，则旧的密码参数适当保留。

当建立一个新的主控方密钥时，在 H.323 端点务必按照新旧提议—回答交换接收加密的媒体期间将有一个时窗。来自入网 SRTP 包的 MKI 必须被用于将包与旧的主控方密钥或新的主控方密钥关联起来。出于这个理由，如果预计密钥在不改变源/目的地地址和端口的对话期间将被改变，则 MKI 强制使用，以允许接收方在密钥交换期间标识关联的密钥材料。

5.4 无协商

在密码组、密钥或对话参数无协商的情况下，发送方确定媒体的安全性参数。由于存在无协商机制，所以发送方必须确切地包括一个密码提议，接收方必须接受它，或者通过发送具有被设置为 **securityDenied** 的 **ReleaseCompleteReason** 的 **ReleaseComplete** 或者是具有被设置为 **securityDenied** 的 **cause** 的 **OpenLogicalChannelReject** 来拒绝提议。发送方应选择出于其目的它认为最安全的安全性描述。

5.5 前向纠错

必须规定一个不同的主控方密钥来保护发送到不同 IP 地址和/或端口对的 FEC 流，而不是其适用的 SRTP 媒体流，如 RFC 2733 第 11.1 节所描述的。这一 FEC 流必须使用具有 **fec** 的 **dataType** 的单独的 H.245 **OpenLogicalChannel** 建立。FEC 流的主控方密钥必须在 **secureSharedSecret**（**V3KeySyncMaterial**）参数的 **genericKeyMaterial** 字段中传输，该参数包含在 H.245 **OpenLogicalChannel** 消息的 **encryptionSync** 参数的 **h235Key** 存储器中。主控方密钥必须与为关联的媒体流提议的所有其他主控方密钥不同。

6 用于保护SRTP的密钥交换的公钥密码术

通过加密然后标记 SRTP 密钥材料，可增加公钥密码术规程，以提供在 H.323 端点之间 SRTP 对话密钥材料的端到端机密性和认证。公钥密码术可用在封装安全性协议，例如 IPsec 和 TLS，在中介设备上终止并因此不提供端到端安全性的情况下。

加密从主叫方端点到被叫方端点的 SRTP 媒体的 SRTP 对话密钥必须使用被叫方端点的公钥加密，并用主叫方端点的私钥标记。同样，另一个加密从被叫方端点到主叫方端点的 SRTP 媒体的 SRTP 对话密钥必须使用主叫方端点的公钥加密，并用被叫方端点的私钥标记。在本节中描述的规程可在网关或网守以及端点上终止。

SRTP 对话密钥必须使用 H.245 消息内的密码消息句法（CMS）正文传输。密码消息句法（RFC 3852）被用于用数字标记和加密任意的消息内容。CMS 句法允许多个封装，这使得一个封装的包封可嵌套在另一个包封内。特别地，SRTP 对话密钥材料必须在一个使用 CMS **SignedData** 主体标记的 CMS **EnvelopedData** 主体内传输。

6.1 端点标识符

以下必须被用于在公钥证书中标识端点、网关或网守：

- H.323 URL；
- 非 H.323 标准 URL，例如 *tel*；
- 设备标识/证书（FFS）。

公钥证书必须被用于声明端点的标识符与其公钥的关联。H.323 URL 或非 H.323 标准 URL 必须被存储在证书的 **subjectAltName** 字段中。

端点可能保持本地密钥存储，这包含其他端点的公钥证书，它希望建立安全的端到端通信。发送标记的内容以提供端到端认证的端点必须包括承载验证签名所必需的公钥证书。接收方端点必须：

a） 核实发送方的证书由经过验证的认证机构（CA）签署；或

b） 信任由第三方给出的关于证书的声明。声明务必由全球可证实的密钥材料签署。

注 — 在不能获得全球用户 PKI 且正使用自签署证书或设备的情形中，这可能是有利的。

6.2 SRTP密钥交换规程

如果在呼叫建立穿越一个或多个中介信令设备的情况下，主叫方和被叫方的端点希望确保其 SRTP 对话密钥材料的端到端机密性和认证，则它们应使用公钥密码术和 X.509（RFC 3280）公钥证书交换。

在上一节中描述的提议—回答规程不交换，以下所规定的除外。

6.2.1 能力交换

为了协商将公钥证书用于 SRTP 密钥交换，H.323 端点必须在 H.245 **TerminalCapabilitySet** 消息的 **capabilityTable** 中的 **h235SecurityCapability** 条目的 **encryptionAuthenticationAndIntegrity** 内设置 **genericH235SecurityCapability** 如下：

- **capabilityIdentifier** 必须在 **standard** 字段内包含 H.235.8 CMS 对象标识符（见表 4）；
- **maxbitRate**、**collapsing**、**nonCollapsing** 和 **transport** 必须不使用；
- **nonCollapsingRaw** 必须包含 **SrtpCryptoCapability** 参数。

6.2.2 密钥交换

如果 SRTP 对话密钥将使用公钥加密，则加密的 SRTP 对话密钥 H.245 消息内的密码消息句法（CMS）正文中传输。CMS **EnvelopedData** 主体和 CMS **SignedData** 主体必须取代 **SrtpKey** 在 **secureSharedSecret**（**V3KeySyncMaterial**）参数的 **genericKeyMaterial** 字段中传输，该参数包含在 H.245 **OpenLogicalChannel** 消息的 **encryptionSync** 参数中的 **h235Key** 存储器内。CMS **EnvelopedData** 主体必须被放置在 **genericKeyMaterial** 字段中，后紧随的是 CMS **SignedData** 主体。

结构 **SrtpKey** 必须使用 CMS 内容加密密钥（CEK）加密，并在 CMS **EnvelopedData** 主体的 **EncryptedContentInfo** 结构中传输。

在 **genericKeyMaterial** 存储器中包含 SRTP 对话密钥材料的 CMS 主体的存在必须使用 H.235.8 CMS 对象标识符值（见表 4）标识，该值在 OLC **dataType** 的 **h235Media** 中的 **encryptionAuthenticationAndIntegrity** 的 **genericH235SecurityCapability** 字段内的 **capabilityIdentifier** 的 **standard** 字段中。

表 4/H.235.8－H.235.8 CMS对象标识符

OID值
{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 94 }

6.3 CMS主体的使用

生成 SRTP 对话密钥材料 **SrtpKeys** 的端点，即发送方端点必须使用 CMS 内容加密密钥（CEK）加密（该密钥自身由另一个端点即接收方端点的公钥加密），必须将加密的 SRTP 对话密钥材料放置在 CMS **EnvelopedData** 主体中。然后，发送方端点必须用数字标记 **EnvelopedData** 主体及其私钥，并创建“独立签名”CMS **SignedData** 主体。发送方端点必须在其 CMS **SignedData** 主体中包括具有其公钥的证书。发送方端点必须向接收方端点发送 **EnvelopedData** 主体和“独立签名”**SignedData** 主体。由发送方端点创建 **EnvelopedData** 和 **SignedData** 主体在以下章节中详细描述。

EnvelopedData 主体和“独立签名”**SignedData** 主体在图 5 中示出。

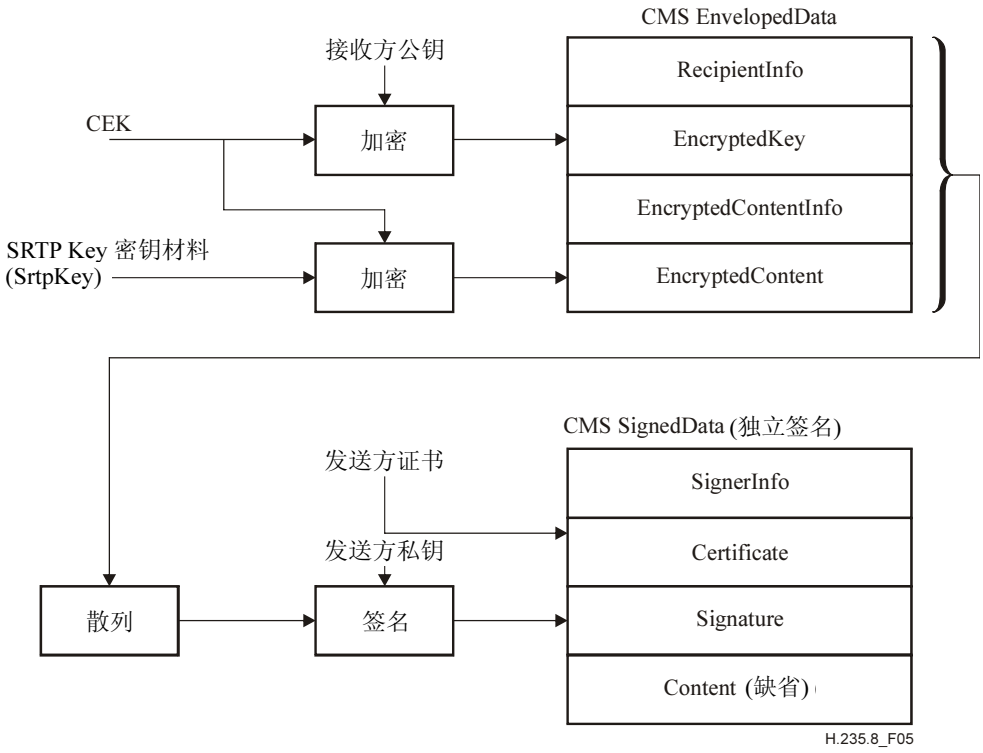

图 5/H.235.8－CMS EnvelopedData和SignedData主体

6.3.1 发送方端点规程

发送方端点必须执行下列规程来生成、加密和签署 SRTP 对话密钥材料。

6.3.1.1 EnvelopedData主体

发送方端点必须如下构建 **EnvelopedData** 主体：

1） 生成用于密码组的 SRTP 对话密钥材料 **SrtpKeys**。

2） 生成随机内容加密密钥（CEK）。

3） 使用接收方端点的公钥加密 CEK。假定发送方端点已经具有接收方端点的公钥和证书。将 CEK 的加密中使用的算法的标识符放置在 **RecipientInfo.ktri** 结构的 **keyEncryptionAlgorithm** 字段中。

4） 将加密的 CEK 放置在 **EnvelopedData** 主体的 **RecipientInfo** 结构的 **encryptedKey** 字段中。**RecipientInfo.ktri** 结构的 **rid** 字段被用于标识用于加密 CEK 的接收方端点的证书和公钥。

5） 使用 CEK 加密 SRTP 密钥材料 **SrtpKeys**，将在加密中使用的算法放置在 **EncryptedContentInfo** 结构的 **contentEncryptionAlgorithm** 字段中。

6） 将加密的 SRTP 密钥材料放置在 **EncryptedContentInfo** 结构的 **encryptedContent** 字段中。

6.3.1.2 SignedData主体

发送方端点必须如下构建“独立签名”**SignedData** 主体：

1） 在 **EnvelopedData** 主体上计算消息类别或散列值。消息类别算法标识符被放在 **SignerInfo** 结构的 **digestAlgorithm** 字段中。

2） 使用发送方端点的私钥标记消息类别，并将签名放置在 **SignerInfo** 结构的 **signature** 字段中。签名算法标识符被放置在 **SignerInfo** 结构的 **signatureAlgorithm** 字段中。

3） 将包含发送方端点的公钥的证书放置在 **SignerData** 结构的 **certificates** 结构中。必须设置 **SignerInfo** 结构的 **sid** 字段以使用发布者可识别名和证书序列号或 X.509 subjectKeyIdentifier 扩展值标识证书。

4） 在 **SignedData** 主体中 **encapContentInfo** 结构的 **eContentType** 字段必须包含对象标识符 id-envelopedData。在 **SignedData** 主体中 **encapContentInfo** 结构的 **eContentType** 字段必须缺省，因为这是一个独立签名，且实际的标记内容是 **EnvelopedData** 主体。

6.3.2 接收方端点规程

接收方端点必须执行下列规程以核实并解密 SRTP 对话密钥材料。

如果接收方端点在以下描述的规程中遇到任何确认失效，则通过发送具有被设置为 **securityDenied** 的 **ReleaseCompleteReason** 的 **ReleaseComplete**，或在 H.225.0 消息中发送 **FastConnectRefused** 单元，来拒绝呼叫。

6.3.2.1 SignedData主体

接收方端点必须如下合适接收到的“独立签名”**SignedData** 主体：

1） 从 **SignerData** 结构的 **certificates** 结构中获得发送方端点的证书。

2） 验证发送方端点的证书。证书路径生效的详情超出了本建议书的范围。如果接收方不能够认证发送的端点，则它可能拒绝呼叫。

3） 然后接收方端点可能将生效的证书加入到其密钥存储中。

4） 使用来自生效的证书的发送方端点公钥验证 **SignerInfo** 结构中的 **signature** 字段中的签名值。使用在 **SignerInfo** 结构的 **signatureAlgorithm** 字段中规定的签名算法。解密的结果是由发送方端点计算的在 **EnvelopedData** 主体上的消息类别。

5） 使用在 **SignerInfo** 结构的 **digestAlgorithm** 字段中规定的消息类别算法标识符，计算在 **EnvelopedData** 主体上的消息类别。

6） 比较解密消息类别值和计算得到的消息类别值。如果消息类别匹配，则随后将处理 **EnvelopedData** 主体。如果消息类别不匹配，则接收方端点必须拒绝呼叫。

6.3.2.2 EnvelopedData主体

接收方端点必须如下地从 **EnvelopedData** 主体抽取 SRTP 对话密钥材料：

1） 使用 **RecipientInfo** 结构的 **rid** 字段标识在接收方端点的密钥存储中的证书和对应的私钥。如果接收方端点收到用接收方未知的公钥加密的 **EnvelopedData** 主体，则它必须拒绝呼叫。

2） 从 **EnvelopedData** 主体的 **RecipientInfo.ktri** 结构的 **encryptedKey** 字段中抽取加密的 CEK。

3） 使用接收方端点的私钥和在 **RecipientInfo.ktri** 结构的 **keyEncryptionAlgorithm** 字段中规定的算法，解密被加密的 CEK。

4） 从 **EncryptedContentInfo** 结构的 **encryptedContent** 字段中的加密 SRTP 对话密钥材料中抽取加密的 SRTP 对话密钥材料。

5） 使用 CEK 和 **EncryptedContentInfo** 结构的 **contentEncryptionAlgorithm** 字段中规定的算法解密被加密的 SRTP 对话密钥材料。

7 H.235 SRTP安全性描述句法

ASN.1 句法定义如下。

```
H235-SRTP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
     GenericData
FROM H323-MESSAGES;


 SrtpCryptoCapability ::= SEQUENCE OF SrtpCryptoInfo -- 在 H.245 中使用
 genericH235SecurityCapability


 SrtpCryptoInfo ::= SEQUENCE
 {
    cryptoSuite                                 OBJECT IDENTIFIER OPTIONAL ,
    sessionParams                               SrtpSessionParameters OPTIONAL,
    allowMKI                                    BOOLEAN OPTIONAL,
    ...
 }

 SrtpKeys ::= SEQUENCE OF SrtpKeyParameters  -- 在 H.235 V3KeySyncMaterial 中使用

 SrtpKeyParameters ::= SEQUENCE
 {
    masterKey                                   OCTET STRING,
    masterSalt                                  OCTET STRING,
    lifetime                                    CHOICE
    {
       powerOfTwo                               INTEGER,
       specific                                 INTEGER,
       …
    } OPTIONAL,
    mki                                         SEQUENCE
    {
       length                                   INTEGER(1..128),
       value                                    OCTET STRING,
     ...
    } OPTIONAL,
    ...
 }


 SrtpSessionParameters ::= SEQUENCE
 {
    kdr                                        INTEGER(0..24) OPTIONAL, -- 2 的幂
    unencryptedSrtp                            BOOLEAN OPTIONAL,
    unencryptedSrtcp                           BOOLEAN OPTIONAL,
    unauthenticatedSrtp                        BOOLEAN OPTIONAL,
    fecOrder                                   FecOrder OPTIONAL,
    windowSizeHint                             INTEGER(64..65535) OPTIONAL,
    newParameter                               SEQUENCE OF GenericData  OPTIONAL,
    ...
 }

 FecOrder ::= SEQUENCE
 {
    fecBeforeSrtp                              NULL OPTIONAL,
    fecAfterSrtp                               NULL OPTIONAL,
    ...
 }

END
```

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	**视听和多媒体系统**
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置和本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦