国 际 电 信 联 盟

ITU-T H.235.7

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：在H.235中将MIKEY密钥管理协议用于安全实时传送协议（SRTP）

ITU-T H.235.7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.235.7建议书

H.323安全性：在H.235中将MIKEY密钥管理协议用于安全实时传送协议（SRTP）

摘　要

本建议书的目的是描述基于 H.323/H.235 系统的安全性规程，它将 MIKEY 密钥管理协议和安全实时传送协议相结合来使用。

在 H.235 子系列较早的版本中，该摘要被包含在附件 G/H.235 中。H.235.0 的附录 IV、V 和 VI 给出了 H.235 第 3 版和第 4 版之间对应的全部章节、图和表。

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.235.7 建议书。

关键词

媒体加密，MIKEY 密钥管理，多媒体安全性，安全实时传送协议，安全概要，SRTP。

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

引言

本建议书的目的是要为基于 H.323/H.235 系统的安全性规程提供建议，以使用 IETF MIKEY 密钥管理协议和安全实时传送协议。

本建议书在编写上是作为 ITU-T H.235 建议书的一个安全概要，它将作为一个选项，可以对 ITU-T H.235.6 建议书其他媒体安全性特征提供补充。

本建议书使人们可以实施 SRTP 媒体的安全，在此由 MIKEY 密钥管理在相关的端点间端到端地提供需要的密钥和安全参数。本建议书可以在 H.323 域内在有 H.235.7 能力的 H.323 系统间实施。本建议书为 H.225.0 RAS 和呼叫信令以及 H.245 并连同相应的规程定义了在安全上的协议扩展。此外，本建议书还提供能力以支持和已经实现 MIKEY 密钥管理和 SRTP 的 IETF SIP 实体进行互通。

ITU-T H.235.7建议书

H.323安全性：在H.235中将MIKEY密钥管理协议用于安全实时传送协议（SRTP）

1 范围

本建议书的目的是为基于 H.323/H.235 系统的安全性规程提供建议，以使用 MIKEY 密钥管理协议和 SRTP 安全协议。

这一安全概要是作为一个选项来提供的，它可以作为对 H.235.6 其他媒体安全性特征的补充。

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.235.1 (2005), *H.323 security: Baseline security profile.*

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

– ITU-T Recommendation H.235.4 (2005), *H.323 security: Direct and selective routed call security*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication.*

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

– ITU-T Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications.*

– ISO/IEC 10118-3:2004, *Information Technology – Security techniques – Hash functions – Part 3: Dedicated hash functions.*

– 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 3830 (2004), *MIKEY: Multimedia Internet KEYing.*

2.2 资料性参考文献和参考资料

– IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*

– IETF RFC 2327 (1999), *SDP: Session description protocol*.

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method.*

– IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

– IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP).*

– IETF RFC ssss (2005), M. Handley, Van Jacobson, C. Perkins: *SDP: Session Description Protocol,* draft-ietf-mmusic-sdp-new-24.txt.

– IETF RFC wwww (2005), J. Arkko, E. Carrara et al: *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*, Internet Draft draft-ietf-mmusic-kmgmt-ext-14.txt, Work in Progress.

– IETF RFC zzzz (2005), M. Euchner: *HMAC-authenticated Diffie-Hellman for MIKEY*, Internet Draft draft-ietf-msec-MIKEY-DHHMAC-11.txt, Work in Progress.

3 定义

无。

4 符号和缩写

本建议书使用以下缩写：

a, b, e, d	EP A、EP B、GK E 和 GK D 私用的 DH 密钥
Cert	数字证书（见 RFC 3830）
CP/C	CallProceeding-to-Connect
CSB	加密对话群（见 RFC 3830）
CT_B, CT_A	端点 B 的 ClearToken，端点 A 的 ClearToken（见 H.235.4）
DRC1	直接选路的呼叫（见 H.235.4）
$ENC_k(x)$	用密钥 *k* 对 X 加密的结果
env_key	端点 A 和端点 B 之间的封装密钥（RFC 3830）
EP	端点
ESC	H.245 EndSessionCommand
DH	Diffie-Hellman
DH_A	端点 A 的 DH 半密钥
DH_B	端点 B 的 DH 半密钥
g^a, g^b	EP A，EP B 的 Diffie-Hellman 半密钥
g^e, g^d	GK E，GK D 的 Diffie-Hellman 半密钥
GK	网守
HDR	MIKEY 包头有效载荷（见 RFC 3830）
ID_A, ID_B	端点 A 的标识符（即端点 ID），端点 B 的标识符

IETF	互联网工程任务组
Imsg	发起方的 MIKEY 消息（见 RFC 3830）
KEMAC	MIKEY KEMAC 有效载荷消息（见 RFC 3830）
MAC(*k*, *x*)	x 使用密钥 *k* 的加密钥的消息认证码
Ma	MIKEY 认证密钥（见 RFC 3830）
Me	MIKEY 加密密钥（见 RFC 3830）
MIKEY	在多媒体互联网使用密钥
NTP	网络时间协议
PKE	MIKEY PKE 有效载荷消息（见 RFC 3830）
PKI	公钥基础设施
PRF	伪随机函数（MIKEY-PRF，见 RFC 3830 第 4.1.2-4.1.4 节）
Rand	nonce 随机值（见 RFC 3830）
Rmsg	响应方的 MIKEY 消息（见 RFC 3830）
rand()	随机值
RSA	Rivest、Shamir 和 Adleman（公钥算法）
sa, *sb*	端点 A 和 GK 之间的共享秘密，端点 B 和 GK 之间的共享秘密
sl	网守之间的共享秘密
SDP	对话描述协议
SHA1	安全散列算法 1（ISO/IEC 10118-3）
SIP	对话发起协议
SP	安全政策（见 RFC 3830）
SRTCP	安全实时传输控制协议
SRTP	安全实时传输协议（见 RFC 3711）
SSRC	同步源（RTP）
T	时间标记（见 RFC 3830）
TGK	端点 A 和端点 B 之间的业务流生成密钥（见 RFC 3830）
V	核查消息字段（见 RFC 3830）
ZZ_{AB}	H.323 动态共享的秘密 ZZ_{AB}
{}	零次、一次或多次发生
[]	任选的元素

5 惯例

在文本中对象标识符是通过一个符号性的参考来引用的（例如“G1”），第 8.5 和 9.5 节已列出符号性对象标识符实际的数值，更多信息可见第 5 节/H.235.0。

表 1 定义了 MIKEY 的 5 个密钥管理协议，它们将在整个建议书中被引用：

表 1/H.235.7－MIKEY 密钥管理协议

MIKEY 协议	描　　述	OID 值	参数标识符	实 施 要 求
MIKEY	任何 MIKEY 协议	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 76}	76	强制实施
MIKEY-PS	对称的密钥分配协议，它采用预共享的对称密钥和 HMAC，（见 RFC 3830）。	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 72}	72	强制实施
MIKEY-DHHMAC	Diffie-Hellman 密钥协商协议，它采用预共享的对称密钥和 HMAC；（见 RFC zzzz）。	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 73}	73	任选的
MIKEY-PK-SIGN	（基于 RSA 的）公钥分配协议，它采用数字签字；（见 RFC 3830）。	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 74}	74	强制实施
MIKEY-DH-SIGN	Diffie-Hellman 密钥协商协议，它采用数字签字；（见 RFC 3830）。	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 75}	75	任选的

MIKEY（见表 1 中的第 1 行）是泛指整个 MIKEY 协议族，它不特定地表示以下任何具体的 MIKEY 密钥管理协议，如 MIKEY-PS、MIKEY-DHHMAC、MIKEY-PK-SIGN 或 MIKEY-DH-SIGN。与 MIKEY 相关的实现应该包括对 MIKEY 消息，例如 MIKEY 共同的包头有效载荷的处理（RFC 3830 第 6.1 节），但不需要有任何特定 MIKEY 密钥管理协议的实现或任何特定 MIKEY 信息有效负荷的实现。在 H.323 端点不知道实际使用的是何种 MIKEY 协议变种时将使用它对应的 OID 和参数标识符。但在任何其他的情况下，将建议采用实际使用的那种 MIKEY 密钥管理协议特定的 OID 和参数标识符。

6　　引言

实际上已经有兴趣使用来自 ITU-T H.235 建议书的 IETF SRTP“安全实时传送协议”的安全性特征。H.235 较早的版本中尽管已经提供了多种媒体安全性特征（如采用码块加密编码的话音加密）和一些有限的 RTP 认证（反垃圾邮件的选项），但仍然有充分的理由需要实施 SRTP：

— 使用流的加密编码来改善性能、稳健性和安全；

— 与其他 SRTP 终端进行互操作；如基于 SIP 的媒体终端。

注 — 本建议书并未规定与 SIP（RFC 3261）在安全上互通的规程；这一点还有待进一步研究；

— 改善 RTCP 保护的安全性；

— 改善整个 RTP/RTCP 数据包完整性的跨度；

— 部署最先进的 AES 加密算法；

— 在两端都使用从伪随机函数导出的对话加密/认证密钥。

此外，除了 H.235 提供的 Diffie-Hellman 密钥商议方案外，已经识别有需要提供基于 RSA 的密钥管理。类似地，在考虑不能选择公钥基础设施的场合，非基于 PKI 的密钥管理技术被认为是有用的。在密钥管理的背景下，还需要处理合法截听问题。

IETF 也已经做出努力定义了有实时能力的密钥管理方案 MIKEY（RFC 3830）。这一有普遍意义的密钥管理方案与 SRTP 接口良好，既能够提供主密钥（TGK），也能够提供对话业务流的密钥，可用于端到端，或者端到中间点，也可能是逐段转接的。MIKEY 是一个最佳化的密钥管理协议，可以在至多两个消息以内完成，这使它在 H.323 中对于快速起动的呼叫建立十分理想。

本建议书提供从 H.323/H.235 内部实施 MIKEY 密钥管理协议的安全性规程，以支持 SRTP 的媒体安全。需要说明：在 H.323/H.235 以内可能还会有其他替代的方式来支持 SRTP，但这些在本建议书中没有谈到，可保留做进一步研究。

本建议书实施 MIKEY 密钥管理协议的方式从概念上类似于 RFC wwww 描述的方法，在此 SIP（RFC 3261）在 SDP（RFC 2327，RFC ssss 和 RFC 3264）中运载 MIKEY。

本建议书提供了两种安全概要及其安全性规程，可用于两种很不相同的安全基础设施：

— 支持多网守的、对称的基于密钥的安全基础设施（见第 8 节）；和

— 支持多网守的、不对称的基于密钥的安全基础设施（PKI）（见第 9 节）。

7 概述和情形

图 1 显示了本建议书所针对的一般化情形。情形中至少将有两个不同的 H.323 端点 A 和 B。这些端点可以是 H.323 的终端或 H.323 的媒体网关，后者将可能与其他基于数据包的网络或者非基于数据包的网络接口。此外，作为其环境的一部分，将假设至少有一个网守。在只有单个网守可用的情况下，假定所有的 H.323 端点都位于这单个网守区域内。 在多网守情况下，存在相链接的网守，H.323 端点可位于不同的网守区域内。进一步假定 H.323 端点是采用 RTP 媒体协议端到端直接地通信的。

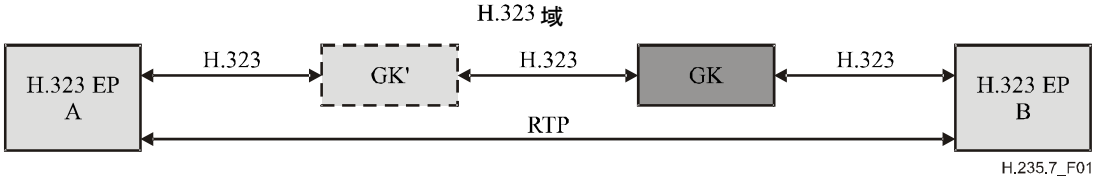

图 1/H.235.7－情形

图 2 显示了安全的一般情形，示意了 MIKEY 密钥管理协议和 STRP 媒体安全协议的使用。MIKEY 密钥管理协议在 H.323 端点 A 和 B 之间运行；MIKEY 密钥管理协议被封装在 H.245 信令握手过程的存储器之内（终端能力集、请求方式、打开逻辑信道的握手以及杂项命令），它对于任何中间的网守而言是透明的。

注意：一个 H.323 端点在实际上可以是一个网关。例如，这样的一个网关可以提供与基于 SIP 的系统接口的互通功能。在这种情况下，这网关不必要终止 MIKEY，而只是为进一步转播 MIKEY，在相关的多媒体终端之间将 MIKEY 扩展成真正端到端的密钥管理，并从而支持 SRTP 端到端的媒体安全。这种方法还将支持 H.323/H.235 和基于 SIP 的系统间在安全上的互通。有关这种网关严格的互通功能与规范不是本建议书的主题，留待进一步研究。

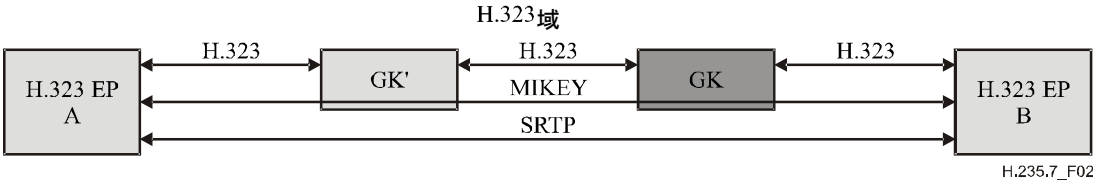

图 2/H.235.7－使用MIKEY和SRTP的安全情形

本建议书描述的所有密钥管理协议都按两个阶段进行：

— 阶段 1 发生于 H.225.0 RAS 和呼叫信令阶段。对于对称密钥的 MIKEY 协议（MIKEY-PS 或 MIKEY-DHHMAC），这一阶段在端点 A 和 B 之间建立端到端共享的 ZZ_{AB}，它被配置作为 MIKEY 预共享的秘密。对于不对称密钥的 MIKEY 协议（MIKEY-PK-SIGN 和 MIKEY-DH-SIGN），这一阶段是在端点和它的下一跳之间（典型地是为它服务的网守）建立动态共享的秘密；这动态共享的秘密与 MIKEY 并不相关，而是服务于确保端点和它下一跳之间 H.225.0 呼叫信令的安全。

— 阶段 2 发生于 H.225.0 呼叫信令/ H.245 协议阶段。这一阶段在端点 A 和 B 之间协商和运行 MIKEY（MIKEY-PS、MIKEY-DHHMAC、MIKEY-PK-SIGN 或 MIKEY-DH-SIGN），并建立 MIKEY TGK。在阶段 2 期间，MIKEY 端点还可以运行 MIKEY 的密钥重置和密钥更新协议来重施或更新 TGK。此外，一个呼叫的终了和密钥材料（TGK）的丢弃也可能在阶段 2 中发生。

7.1 在“会话层”MIKEY的操作

MIKEY 密钥管理协议可以在“会话层”操作；也即将 MIKEY TGK 施加于一个以上的媒体流。这里建议：在 **TerminalCapability** 握手期间，在“会话层”上运行 MIKEY。

TerminalCapabilitySet 必须使用 **h235SecurityCapability**，在此 **genericH235SecurityCapability** 在 **encryptionAuthenticationAndIntegrity** 内的使用应该如下：

— **capabilityIdentifier** 必须持有标准中 MIKEY OIDs 中的一个；

— **maxbitRate** 和 **collapsing** 保留不用；

— 当 MIKEY 在“会话层”执行用于所有的逻辑信道时，**nonCollapsing** 将持有如下的 **GenericParameters** 集：

- **parameterIdentifier**：在 **standard** 中采用数值 0 来指示 MIKEY 在“会话层”。
- 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**。
- **supersedes** 保留为空/不用。

— **nonCollapsingRaw** 保留不用；

— **transport**（不用或使用默认的传送参数）。

对于操作于“会话层”的 MIKEY，**OpenLogicalChannel** 和 **OpenLogicalChannelAck** 不得使用 **encryptionSync**。类似地，当 MIKEY 操作于“会话层”时，**RequestMode** 不得使用 MIKEY **ModeElement** 的 **genericModeParameters**。

MiscellaneousCommand 必须使用 **encryptionUpdate**，在此 **genericParameter** 的使用如下：

— **parameterIdentifier**：在 **standard** 中采用数值 0 来指示“会话层”MIKEY TGK 的密钥重置和 CBS 的更新。

— 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**。

— **supersedes** 保留为空/不用。

对于在“会话层”的 MIKEY，**LogicalChannelNumber** 必须被忽略，可以持任何数值。

在 **ModeElement** 的 **genericModeParameters** 内，**RequestMode** 必须如下地使用 **capabilityIdentifier**：

— **capabilityIdentifier** 应该持有标准 MIKEY OID 中的一个；

— **maxbitRate** 和 **collapsing** 保留不用；

— 当 MIKEY 在“会话层”运行用于一个特定的逻辑信道时，**nonCollapsing** 具有如下的 **GenericParameters** 集：

- **parameterIdentifier**：在 **standard** 中采用数值 0 来指示 MIKEY 在“会话层”。
- 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**。
- **supersedes** 保留为空/不用。

— **nonCollapsingRaw** 保留不用；

— **transport**（不用或使用默认的传送参数）。

7.2 在“媒体层”MIKEY的操作

类似地，作为一种选择，MIKEY 密钥管理协议可以在“媒体层”操作；也即将 MIKEY TGK 仅施加于媒体流上一个特定的逻辑信道。为协商 MIKEY 协议，应该使用 **TerminalCapability** 的握手过程，并使用 **OpenLogicalChannel/Ack** 来传送编码的 MIKEY 消息。

TerminalCapabilitySet 应该使用 **h235SecurityCapability**，在此 **genericH235SecurityCapability** 在 **encryptionAuthenticationAndIntegrity** 内的使用应该如下：

— **capabilityIdentifier** 应该持有标准 MIKEY OID 中的一个；

— **maxbitRate**、**nonCollapsing** 和 **collapsing** 保留不用；

— **nonCollapsingRaw** 保留不用；

— **transport**（不用或使用默认的传送参数）。

OpenLogicalChannel 或 **OpenLogicalChannelAck** 在 **encryptionSync** 内，必须如下地使用 **genericParameter**：

— **parameterIdentifier**：在 **standard** 中采用对应于协商的 MIKEY 协议的参数标识符数值（见表 1）；

— 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**；

— **supersedes** 保留为空/不用；

— **encryptionSync** 中的 **synchFlag** 必须被设置为动态有效载荷数。**h235key** 在本建议书中不得使用，必须是一个空八比特组串。**escrowentry** 不得使用。

MiscellaneousCommand 必须使用 **encryptionUpdate**，在此 **encryptionSync** 中的 **genericParameter** 使用如下：

— **parameterIdentifier**：在 **standard** 中采用对应于协商的 MIKEY 协议的参数标识符数值（见表 1）；

— 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**；

— **supersedes** 保留为空/不用。

在 **ModeElement** 的 **genericModeParameters** 内，**RequestMode** 必须如下地使用 **capabilityIdentifier**：

— **capabilityIdentifier** 必须持有 **standard** 内 MIKEY OID 中的一个；

— **maxbitRate** 和 **collapsing** 保留不用；

— 当 MIKEY 在“媒体层”运行用于一个特定的逻辑信道时，**nonCollapsing** 具有如下的 **GenericParameters** 集：

  • **parameterIdentifier**：在 **standard** 中采用对应于商定的 MIKEY 协议的参数标识符数值（见表 1）。

  • 在 **octetString** 内采用 MIKEY（I 或 R）二进制编码消息的 **parameterValue**。

  • **supersedes** 保留为空/不用。

— **nonCollapsingRaw** 保留不用;

— **transport**（不用或使用默认的传送参数）。

7.3 MIKEY能力的协商

如果 MIKEY 协议在终端能力组/请求模式和打开逻辑信道的握手过程中都进行传送，那么打开逻辑信道握手过程中的 MIKEY 必须优先，可以改写预先从终端能力组/请求模式期间得到的密钥管理信息。

由于端点可能不实现全套的 MIKEY 密钥管理协议，甚至不实现其中的任何协议（也即端点有可能根本不支持本建议书），主叫端点可能会不知道有关被叫端点所支持的 MIKEY 能力。为此，这里建议采用终端能力集握手过程来商议 MIKEY 的密钥管理能力。

在终端能力协商期间，主叫端点应该指示它所支持的和可接受的 MIKEY 密钥管理协议。为此，主叫端点应指示它支持 MIKEY 安全能力。在 **genericH235SecurityCapability** 中，主叫端点应按照其首选的安全概要和 MIKEY 密钥管理，将 **capabilityIdentifier** 设置成 OID 值（见表 1）。这里还鼓励主叫端点按照其安全策略和限制，按递减的优先顺序，提供所支持的其他 MIKEY 协议。

一个不支持本建议书的被叫端点必须用 **ReleaseComplete** 拒绝呼叫，并将 **ReleaseCompleteReason** 设为 **securityDenied**，如果它的安全策略规则许可，它也可以不安全地让呼叫继续。呼叫者可通过检查返回的能力中未携带 MIKEY 能力来推断被叫不支持所请求的 MIKEY 能力。

一个支持本建议书，但不支持所请求 MIKEY 协议能力的被叫端点应该在终端能力集握手协商期间指示它所支持的和可接受的 MIKEY 协议。

一个支持本建议书和所请求的 MIKEY 协议，但不支持 MIKEY/SRTP 安全算法和参数具体组合（也即 MIKEY 安全策略，SP）的被叫端点应该传送一个 MIKEY 差错消息来作为响应（见 RFC 3830，第 5.1.1、5.1.2 和 6.1.2 节）。被叫端点应该放入它所支持和可接受的、带有 MIKEY/SRTP 安全算法和参数的 MIKEY 安全策略（SP）。

本建议书必须在 H.225.0 呼叫信令中使用 H.245 消息的隧道传送，以保证 H.225.0 呼叫信令消息的安全。本建议书甚至也可以不使用 H.245 消息的隧道传送，但此时要求至少将使用有完整性保护的安全传送（TLS，IPsec）来确保 H.245 消息的安全。这一变通在本建议书中将不再进一步细述。

本建议书还更适宜于使用快速连接，在此隧道传送的 H.245 消息被包装在 H.225.0 呼叫信令的 setup 和 CallProceeding-to-Connect 中。它使 MIKEY 握手过程可以在至多两个往返中就能完成。

为了防止能力协商期间的降级攻击，一个附合本规范的端点必须遵循 RFC 3830 第 6.15 节描述的规程，在此主叫方就所提供的 MIKEY 密钥管理协议的标识符（KMID）构建一个清单；见 RFC wwww 第 8.3 节，并将这一清单放入所提供的每一个 MIKEY 协议的 MIKEY 一般性扩展有效负荷中。

对于全双工的信道，SRTP 实例将建立两次，一次一个方向；然而在 H.323 端点之间将只有一个动态的 MIKEY 主密钥（TGK）需要协商。端点将通过将不同的 MIKEY 加密对话标识符应用于 MIKEY 和 SRTP 的密钥衍生函数来建立各方向上的 SRTP 对话密钥。

8 采用对称安全技术的安全概要

本节描述本建议书的一项安全概要，所部署的仅是对称的安全技术。

在图 3 中显示了一种情形，它假设（经由管理或配置）在 H.323 域中，H.323 实体之间逐段转接地具有共享的秘密（*sa*，*sb* 和 *sl*）；因而将可以为 H.225.0 RAS 和呼叫信令协议部署 H.235.1 的基线安全性（消息的认证和/或完整性）。为了确保 EP B 和 EP A 之间所交换信令消息的真实性（也即完整性），以逐段转接的方式部署 H.235.1 的基线安全性是需要的。

这里假设：端点 B 与其他 H.323 端点是松弛地时间同步的；否则 MIKEY 将不能安全地运行。

注 — 本建议书并不描述在相关实体间（安全地）实现时钟同步的任何方法。但可以假设：这样的时间同步在企业网内一般是可以实现的。

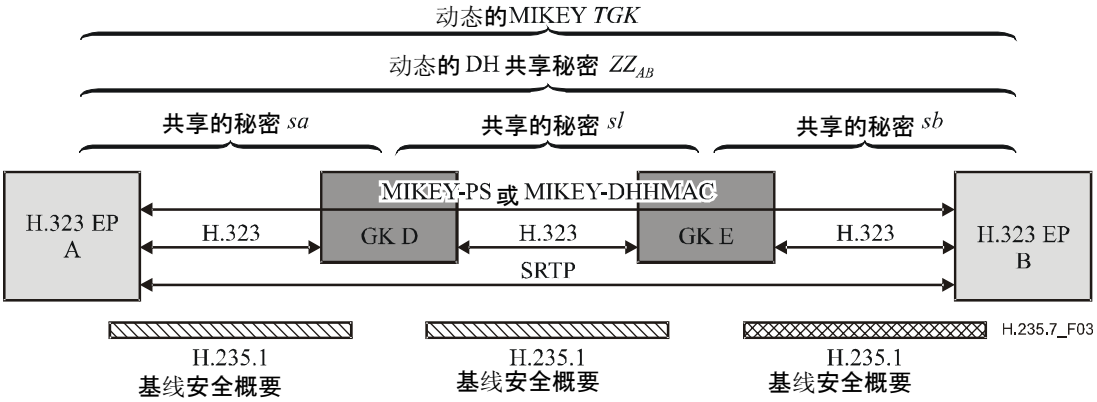

图 3/H.235.7－仅是逐段转接地具有共享秘密的情形

实现这一情形的基本方法是：在 H.323 域中部署 MIKEY-PS 的密钥分配协议（对称的、使用预共享的秘密），或者当所关注的是完善的前向保密时，部署 MIKEY-DHHMAC 密钥的一致协议（采用 HMAC 的 Diffie-Hellman）。此外 RFC zzzz 可作为一种选项来补充 MIKEY，见附录 I。

在 EP B（MIKEY 发起方）呼叫 EP A（MIKEY 响应方）时，动态共享的秘密 ZZ_{AB} 在 EP A 和 EP B 之间是作为 H.225.0 RAS 和呼叫建立的一部分建立起来的。ZZ_{AB} 动态共享的秘密用于作为 MIKEY 预共享秘密来使用，随后 EP A 和 EP B 中的 MIKEY 将从它导出对称的加密与认证密钥（图中未显示）。

主叫 EP B 为它的对等端 EP A 生成 MIKEY *TGK*（这实际上是一个主密钥）。EP B 构建 MIKEY 协议消息，并将整个 MIKEY 消息包装在隧道传送的 **TerminalCapabilitySet/ OpenLogicalChannel** 消息之中的一个存储器。在 GK 选路的环境下，GK E 将只是简单地把这 MIKEY 存储器转发给其他的端点 A，而不对 MIKEY 本身解码。EP A 在 H.323 域内终止 MIKEY 协议。

就这样 EP B 和 EP A 建立了一个 *TGK*。

MIKEY-PS 或 MIKEY-DHHMAC 协议在 EP B 和 EP A 之间运行。以这种方式，端点得到 *TGK*，并能导出 SRTP/SRTCP 的对话密钥。SRTP 和 SRTCP 协议将端到端地应用这些对话密钥。

注 1 — MIKEY，作为所传送 MIKEY 策略的一部分，将为 SRTP 提供所有必要的参数（算法、密钥长度、密钥生命等）。

网守并不活跃地参于 MIKEY 进程，它为包装的 MIKEY 消息充当存储和转发中继的角色。

当呼叫建立始发于 EP A 时，过程将以 EP A 为发起方，EP B 为接收方，在反方向类似地进行。

注 2 — 图 3 所示的情形也支持直接选路的呼叫模型，它使用非选路的网守。在这样一种直接选路的环境下，H.225.0 呼叫信令消息（Setup 等）在 H.323 域内将端到端地直接发送，不经由网守转播。见附录 II，它说明如何为此而使用 H.235.4。

注 3 — MIKEY 在安全协议中使用时间标记，作为保证密钥管理消息得到重放保护的手段。这一点要求端点的时钟能松弛地保持时间同步（在某种可接受的时钟偏差内）。可以相信，这样的时间同步可以采用人工配置的时钟，或者用某些网络时间同步协议（例如 NTP RFC 1305）来实现。由于这样 H.323 域内的时间同步至少对于企业网应该是可行的；也见 RFC 3830 的第 5.4 和 9.3 节。

注 4 — 不建议使用快速起动以及早期的媒体与 MIKEY-DHHMAC 协议相结合的组合。如果需要使用快速起动和早期的媒体，那么端点应该使用 MIKEY-PS，而不使用 MIKEY-DHHMAC。

注 5 — 只有单个网守的情形是所示多网守情形的一个特例。在这种情况下，采用 LRQ/LCF，远端网守/端点的发现是不必要的。

下面给出图 3 情形中更为详细的消息流。这一情形假设在 H.323 域内有一个或多个网守，在此 H.245 的消息将在 H.225.0 中用隧道传送，并将使用快速起动。

注 6 — 这流程图也适用于直接选路的情况（采用非选路的网守），在此 H.225.0 呼叫信令消息在端点之间直接地交换，而不是由任何网守转发，见附录 II。

本节描述的规程，在阶段 1，采用 Diffie-Hellman 密钥协定在 H.323 端点 EP A 和 EP B 之间建立端到端共享的秘密 ZZ_{AB}。这种 Diffie-Hellman 密钥协定发生在 H.225.0 RAS 注册和许可时期，多网守情况下是发生在网守间的 **LRQ/LCF** 期间。所生成的 Diffie-Hellman 共享秘密用于端到端的认证密钥，并将在呼叫期间持续使用。MIKEY-PS（或 MIKEY-DHHMAC）协议则分别地发生在阶段 2 的呼叫建立中，并将建立用于承载信道的基于呼叫的 MIKEY 秘密。

附录 II 描述一种可替代和任选的规程，它采用 H.235.4 的 DRC1 规程，让网守为 EP A 和 EP B 生成和分配共享的秘密。

图 4 中还显示了 H.235.1 基线安全概要，在此每一个消息是整体地加以安全保护的（认证和完整性）。然而，当使用仅有认证这一基线安全概要的选项（没有显示）时，得到的是类似的消息流。在这种情况下，将只对 RAS/H.225.0 消息的一个子集（**CryptoToken** 内的 **ClearToken**），而不是对整个消息计算 HMAC。

例举的消息流显示了 EP B（MIKEY 发起方）采用快速起动呼叫 EP A（MIKEY 响应方）的情况（见图 4）。H.323 端点 A 和 B 在初始时用 **RRQ** 向网守进行了注册，并递交了它们的 DH 半密钥（g^a 和 g^b）。在 **RRQ** 和 **ACF** 期间，为传递 Diffie-Hellman 半密钥，将（在 **CryptoHashedToken** 之内）使用 **ClearToken**。由于这一原因，不得使用 **challenge** 字段。

Diffie-Hellman 半密钥应该作为 **ClearToken** 的一部分在 **dhkey** 中传送。这 **ClearToken** 将使用 OID “TG”（见第 8.5 节），而不是基线的 H.235.1 **ClearToken** OID “T”，它指示：这一安全概要正与 H.235.1 相结合使用。网守应该保存每一个半密钥，只要端点已注册。端点在执行保持存活或使用简化的再注册（re-RRQ）时不得放入任何的 DH 半密钥。为指示网守支持这一安全概要，**RCF** 应该在 **ClearToken** 中使用“TG”OID。

试图呼叫 EP A 的 EP B 从网守 D 请求许可（**ARQ**）。这 **ARQ** 应该在 **ClearToken** 中使用“TG”OID。在任何其他的 RAS 消息中也必须在 **ClearToken** 中使用 OID “TG”。

这一情形适用于多个相链接的网守，但也同样支持仅有单个网守的情况。远端端点的发现应该按照第8.1.6节/H.323“任选的被叫端点信令”采用 **LRQ/LCF** 来实现。这就是发起方端点如何对远端 GK 区域进行定位，并从而得到目标被叫方端点 Diffie-Hellman 半密钥的做法。如果 GK E 需要定位远端的 GK 区域，GK E 就应该发送 **LRQ** 消息。对组播情况，**LRQ** CryptoToken 中的 **generalID** 不得使用。如果 GK D 不支持这一特性，GK D 必须回送 **LRJ**。否则 GK D 返回 **LCF**，它包含 EP A 的 Diffie-Hellman 半密钥。随后 GK E 必须用包含这 EP A Diffie-Hellman 半密钥的 **ACF** 进行应答。如果 GK E 不能够对远端端点 A 进行定位，那么 GK E 必须返回 **ARJ**。

两个网守之间的通信必须按 H.235.1 保证安全。为此这里假设已经有一个共同的共享秘密 *sl* 存在。因为网守间的 **LRQ** 通常是一个组播消息，这共享秘密 *sl* 通常不会是成对共享的秘密，实际上可以假设是一群可能的网守中一个基于组群的共享秘密。这一假设在一般情况下限制了可扩展性，且不能提供源点的认证。然而，可以相信：在具有有限的小数量已知网守的企业网中，这样的约束和安全限制仍然是可以接受的。采用数字签名来保证网守之间组播通信的安全有可能克服这些限制；然而这一点还待进一步研究。

EP B 得到 EP A 的 Diffie-Hellman 半密钥（**ACF**）。**ACF** 必须在 H.235.1 基线 **ClearToken** 内的 **dhkey** 中持有这被叫端点的 Diffie-Hellman 密钥，但它采用 OID“TG”，而不是“T”。本安全概要不得对 **ClearToken** 中任何其他的字段进行修改。

注 7 — 端点用这 DH 半密钥进行操作，它在整个注册期间，对所有呼叫是静态的。只要每个端点应用真正随机的半密钥，这一点应不会是一个安全弱点。

然而，端点应该在 **challenge** 中与 DH 半密钥一起提供 512 比特（也即 64 个字节）新鲜的随机值，（见 RFC 2631 第 2.3 节）。这些 **challenge** 值是基于呼叫的，它在 DH 密钥生成过程中引入必要的随机性和适时性。

始发的 EP B 随后可以计算 g^{ab}，并用一个随机的 **challenge** 连同 MIKEY-PRF（g^{ab}，0x12F905FE || **challenge**）的结果计算动态共享的秘密 ZZ_{AB}（见 RFC 3830 第 4.1.2-4.1.4 节）。随后 MIKEY 就能够用这 MIKEY-PRF 导出加密密钥（*Me*）和认证密钥（*Ma*）（见 RFC 3830 第 4.1.2-4.1.4 节）。

在阶段 2，始发的 EP B 必须生成一个新鲜的 MIKEY *TGK*，并随后用 *Me* 和 *Ma* 按 MIKEY-PS 协议构建 MIKEY I_ message Imsg；SRTP 的对话密钥，正如 RFC 3711 第 4.3 节所描述的，也可以从这 TGK 导出来（图中未显示）。

MIKEY I_ message 必须是二进制编码的。

始发的 EP B 应该总是将它的 DH 半密钥放入到 **ClearToken** 的 **dhkey** 中，从而也使 GK 支持的直接选路模型能够工作。**ClearToken** 必须被放入 Setup 消息中，并发送给对等的 EP A。选路的网守将把所携带的 **ClearToken**（对 MIKEY 消息不加修改地）转发到下一跳。

接收的 EP A 随后计算 g^{ab}，并从 MIKEY-PRF（g^{ab}，0x12F905FE || **challenge**）计算动态共享的秘密 ZZ_{AB}（见 RFC 3830 第 4.1.2-4.1.4 节）。然后 MIKEY 用这 MIKEY-PRF 导出加密密钥（*Me*）和认证密钥（*Ma*）（见 RFC 3830 第 4.1.2-4.1.4 节）。这样传送的 TGK 就可以得到。

此后正如 RFC 3711 第 4.3 节所描述的，接收的 EP A 可以从 *TGK* 导出 SRTP 的对话密钥（图中未显示）。

EP A 可以构建一个类似的 R_message Rmsg，但这 R_message 只有在 EP B 请求，或者有必要时（DH）才构建。这个 R_message 是在 CallProceeding-to-Connect 消息（CP/C）中传送的。

这 CallProceeding-to-Connect 消息（CP/C）被送往 EP B。

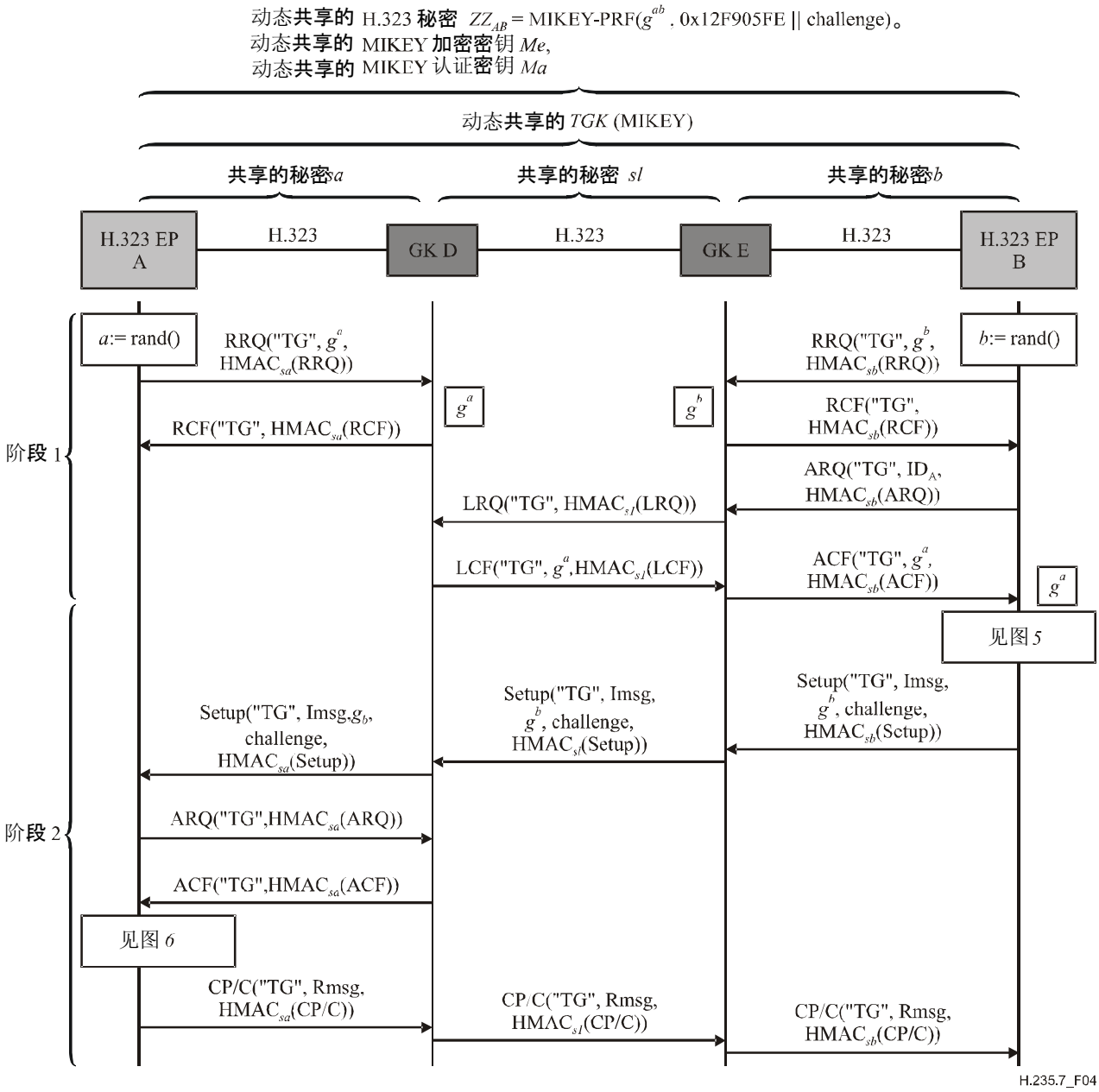

图 4/H.235.7一端点B用MIKEY预共享秘密呼叫端点A的例子（GK选路）

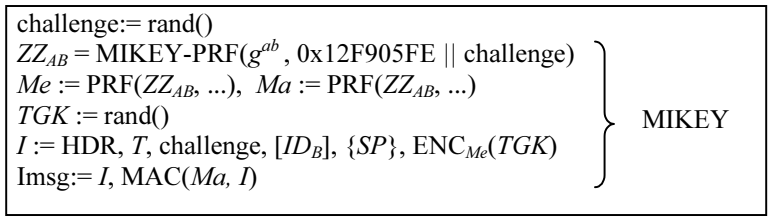

图 5/H.235.7－EP B对MIKEY预共享秘密的处理

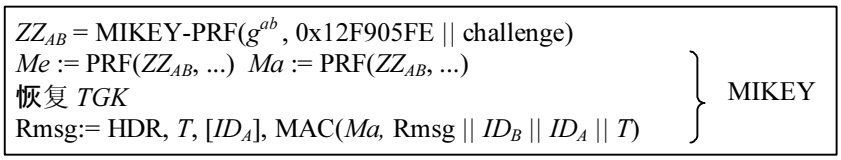

图 6/H.235.7－EP A对MIKEY预共享秘密的处理

8.1 终止一个H.323呼叫

由于相关的端点保持着 MIKEY 和 SRTP 的状态，一个适当的终止规程是重要的。图 7 显示了在 EP B（MIKEY 发起方）终止一个呼叫时消息流的例子。这消息流基本是依据 8.5/H.323“阶段 E — 呼叫终止”。

注 — 图 7 还显示了任选的脱离规程，用于端点完全解除注册时的情况。那时这端点也应该丢弃私用的 DH 密钥（*a* 或 *b*）和公用的 DH 半密钥（g^a 或 g^b）。

由于终止一个呼叫的规程是独立于本安全概要的，下层安全概要任何可应用的 OID（H.235.1，H.235.3 等）都可以使用；因此图 7 中未显示任何 OID。

如果端点再次向网守注册，那么就必须产生新的 DH 半密钥。然而，在仅仅为了终止呼叫的任何环境下，完全的解除注册是不必要的。如果端点决定保持与网守的注册关系，那么静态的 DH 半密钥可以继续使用。

在端点保持注册，不准备进行脱离的情况下，端点应该只丢弃与呼叫相关的信息，包括对等端的 DH 半密钥、**challenge**、MIKEY 密钥 *Me*、*Ma*、*TGK* 和相关的 SRTP 对话信息。

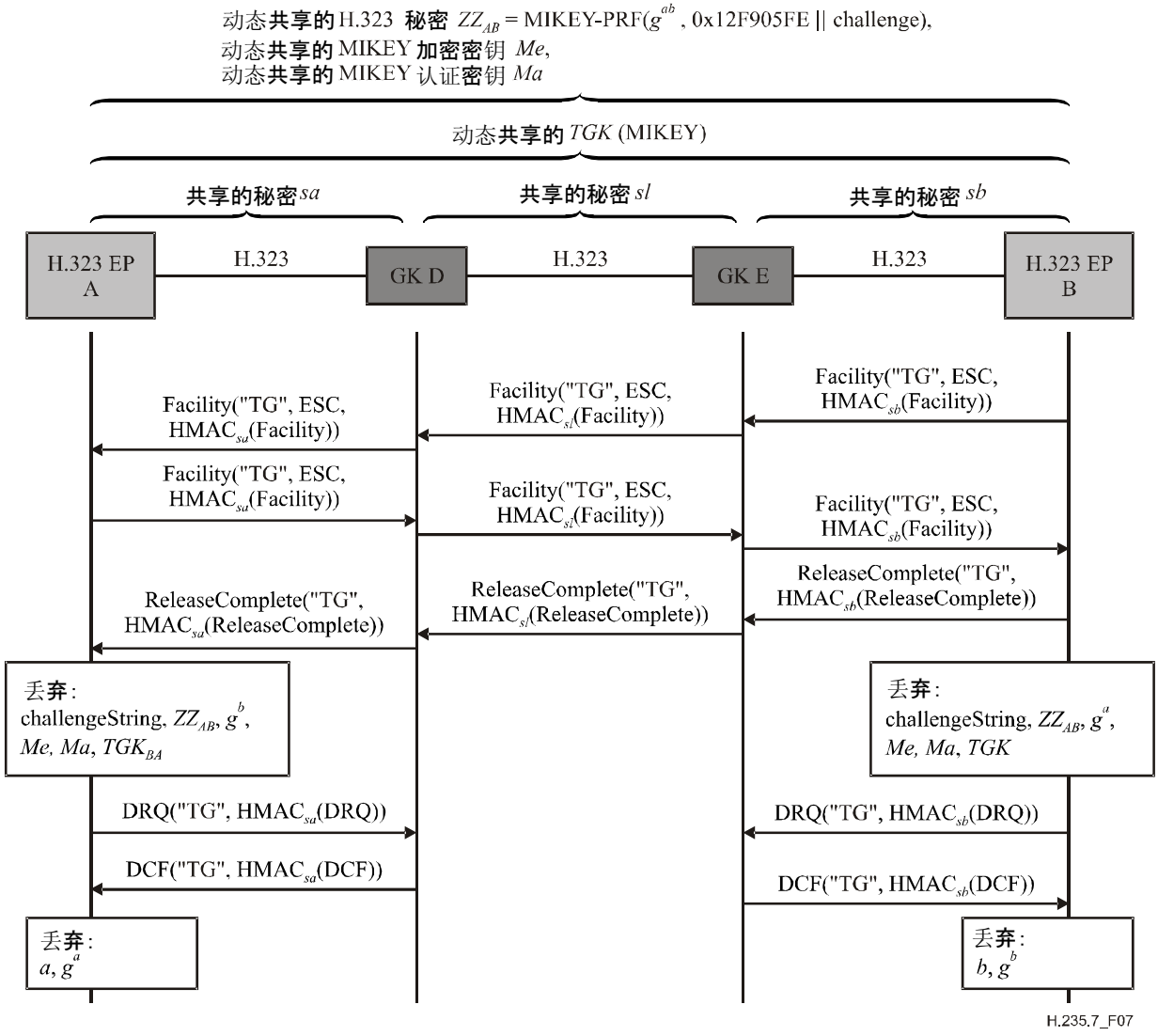

图 7/H.235.7—端点B终止一个呼叫的例子

8.2 TGK密钥重置和CSB更新

MIKEY 已经内置有对 TGK 密钥重置和/或 CSB 信息更新的支持。本建议书的安全概要必须为此而使用 RFC 3830 第 4.5 节的 MIKEY-PS 规程，或者当所关注的是完善的前向保密时使用 RFC zzzz 第 3.1 节，它们允许 TGK 在到期前更新，或不改变 TGK 而更新其他的信息。

TGK 密钥重置和 CSB 更新机制对于保护同一安全政策下的一组逻辑信道是有用的。为此，建议只对第一个逻辑信道执行第 8 节中描述的（完整的）MIKEY 预共享协议。任何随后的、应用同一 MIKEY 安全政策或同一 TGK 的逻辑信道应该使用 CBS 更新机制，而不用本节中的 TGK 密钥重置机制，这可以通过参考初始的 CSB-ID，并忽略更新的 TGK 数据来做到。这样与在每一个逻辑信道上运行完整的 MIKEY 协议相比，可以更有效地建立逻辑信道或 MIKEY 加密对话。

MIKEY TGK 密钥重置或 CSB 更新消息必须包装在 Facility 消息中的 **MiscellaneousCommand** 中进行传送。**ClearToken** 的 **tokenOID** 必须被设置为“TG”。

对于运行在“媒体层”的 MIKEY，EP B 必须确定对哪个逻辑信道进行 TGK 密钥重置和/或 CSB 更新。EP A 作为响应方，将同样地使用 Facility 消息中的 **MiscellaneousCommand** 传送 MIKEY R_message（如果有的话）。

对于 TGK 密钥重置（见图 8），EP B 作为 MIKEY 发起方，必须生成一个新的 TGK。

如果需要由 EP B 请求，作为响应方的 EP A 可以对得到的 TGK 密钥重置消息进行确认。EP A 构建类似的 R_messages。EP B 在 Facility 消息中向 EP A 发送 R_message。

对于 CSB 更新，将采用类似于上述的规程，不同的只是 MIKEY 消息中不持有任何的 TGK。

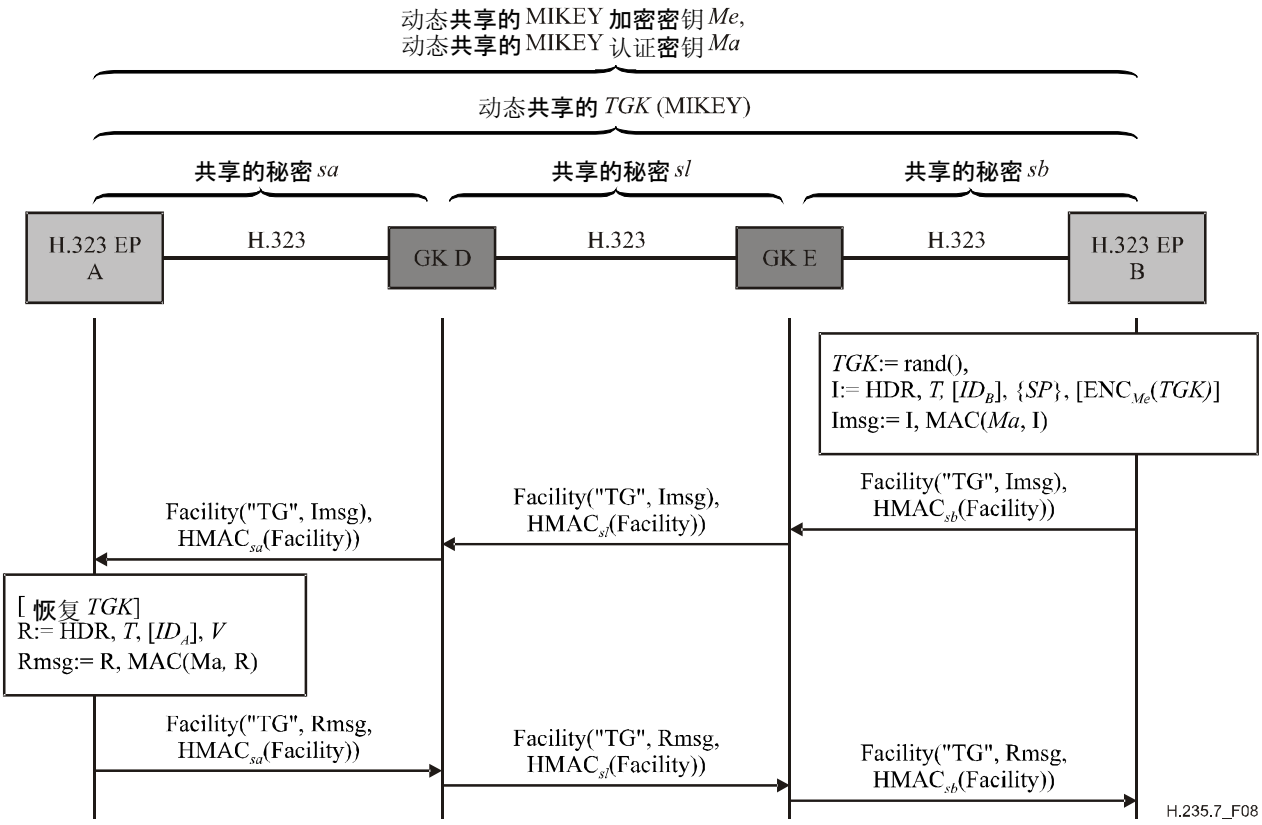

图 8/H.235.7—端点B更新一个密钥的例子

注 — 这种从 EP A 到 EP B 的确认功能是任选的，它仅当 EP B 在 MIKEY HDR 中用 V 标志请求一个检验消息（MIKEY R_message）时才是必需的。

本建议书没有定义任何由响应方请求的 TGK 密钥重置和/或 CSB 更新的规程；这一点有待进一步研究。

8.3 H.245隧道传送的支持

如果一个对话期间，有更多的逻辑信道需要加入，应该部署 H.245 隧道传送模式，在此隧道传送的 H.245 消息将承载在一个 Facility 消息中。

8.4 SRTP算法

本安全概要必须使用截取的 HMAC-SHA1-32 作为 RTP 默认的认证算法，并将认证附加码长度 *n_tag* 取为 32 比特。其他由 RFC 3711 定义的认证附加码长度也应该支持，并必须通过适当的 MIKEY 安全政策（SP）参数进行协商。

8.5 对象标识符一览

"TG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 70}	它在本建议书的背景下，指示一个 H.235.1 基线 **ClearToken**。这一 OID 还指示将使用 MIKEY-PRF 来计算共享的秘密 ZZ_{AB}。

9 采用不对称安全技术的安全概要

本节描述本建议书的一项安全概要，它部署非对称的安全技术。这种情形将提供最大的可扩展性。

能够截取 MIKEY TGK 的中间实体（即网守）的存在并不总是可以接受的。图 9 显示了一种情形，它部署了公钥基础设施（PKI）来建立 SRTP 完全端到端的媒体密钥。

假设：这里假设 EP A 和 EP B 都持有一个私钥（*SK*）以及一个有证明的公钥（*cert*）。然而 EP A 和 GK E 以及 EP B 和 GK D，在 H.225.0 RAS 的情况下，可能共享（管理的/配置的）共享秘密，且呼叫信令是用 H.235.1 来保证安全的。这里还进一步假设：EP A 和 EP B 是松弛地时间同步的，否则 MIKEY 不能安全地运行。

消息认证/完整性可以采用预先配置的共享秘密（*sa*，*sb* 和 *sl*）和 H.235.1 基线安全概要来实现，或者，在更为一般的情况下，采用 PKI 和 H.235.3 混合的安全概要来建立动态共享的秘密。

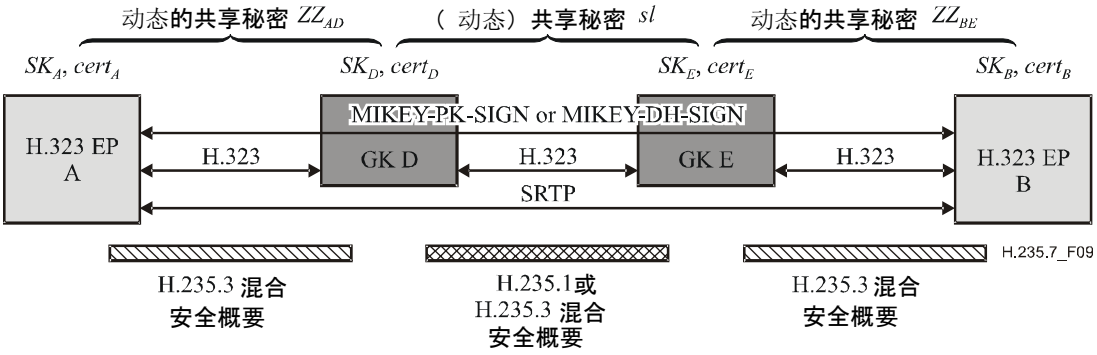

图 9/H.235.7一端到端采用PKI的情形（多GK）

EP A 和 EP B 端到端地运行 MIKEY-PK-SIGN 或 MIKEY-DH-SIGN，并从而建立 MIKET TGK，终端系统将从它导出 SRTP 的对话密钥。

注 1 — MIKEY-PK-SIGN 满足基于 RSA 的密钥管理要求。

注 2 — 与采用对称安全技术的、扩展性较差比较局限的架构相比，采用 PKI 技术，应肯定能更好地适合于更为一般的、一路上有多个相链接网守的环境。

注 3 — 不建议使用快速起动以及早期的媒体与 MIKEY-DH-SIGN 协议相结合的组合。如果需要使用快速起动和早期的媒体，那么端点应该使用 MIKEY-PK-SIGN，而不使用 MIKEY-DH-SIGN。

以下各段介绍图 9 中的情形更为详细的消息流。这一情形在 H.323 域内显示了多个网守。

随后的图中又进一步假设了一个选路的网守（GK 选路的模型），在此 H.245 消息是在 H.225.0 内由隧道传送的（快速起动）。

注 4 — 这流程图也适用于直接选路的情况（采用非选路的网守），在此 H.225.0 呼叫信令消息将在端点之间直接地交换，而不是由任何网守转发。

这流程图还显示了 H.235.3 混合安全概要，在此初始的 RAS 消息是采用数字签字和任选的证书整体地（认证和完整性）来保证安全的。它是要在端点与下一跳的网守间建立动态共享的秘密 ZZ_{BE} 和 ZZ_{AD}，从而使静态共享的秘密成为多余。此外，当使用数字签字安全概要中仅有认证这一选项时（没有显示），可得到类似的消息流。

消息流例子显示的是 EP B（MIKEY 发起方）呼叫 EP A（MIKEY 响应方）（见图 10）。

在阶段 1 期间，H.323 端点向下一跳网守进行初始的注册，并提交它们的 DH 半密钥（g^a 和 g^b）。

试图呼叫 EP A 的 EP B 向网守 E 请求许可。EP B，在证书信息对它还不具备的情况下，可以通过在 **ClearToken** 中加入一个安全概要单元来请求对端的证书 *certC*。这安全概要单元将使用如下字段：

— **elementID**，它被设置为 7，指示这是一个证书请求单元；图 10 中用 certFlag 对它进行了显示；

— **paramS** 保留不用；

— **element** 持有一个其 **flag** 被设置为 TRUE 的单元。

ARQ 和任何随后的 RAS 和 H.225.0 呼叫信令消息是采用 H.235.1 基线安全概要由动态共享的秘密 ZZ_{BE} 来保证安全的。在 EP B 请求阅读证书时，GK E 从本地或其他的证书存储点取得 certC，作为 ACF 的一部分在 **ClearToken** 的 **certificate** 中提供结果，同时加入安全概要单元。这一安全概要单元必须使用如下字段：

— **elementID**，它被设置为 8，指示这是一个证书响应单元；图 10 中用 certFlag 对它进行了显示；

— **paramS** 保留不用；

— **element** 持有一个其 **flag** 被设置为 TRUE 的元素。

在网守为一个对等端点/UA 得到多个证书时，ACF 实际上将持有多个 ClearTokens，每一个的 **certificate** 中各持有一个证书。然后端点从中选择出一个适当的。然而证书的查找有可能要花费太长的时间；例如当与外部的证书存储点相联络时。如果网守不能及时或根本不能提供证书，返回的 ACF 在其 ClearToken 中将是一个空的 **certificate**，它所持有的安全概要单元将为：

— **elementID**，它被设置为 8，指示这是一个证书响应单元；

— **paramS** 保留不用；

— **element** 持有一个其 **flag** 被设置为 FALSE 的元素。

然后是放弃还是试图对适当的证书进行定位这将是端点的任务，具体方法在本建议书中未加规定。如果网守在必要的响应时间界限以外能够得到证书时，这网守应该通过将 **certificate** 空置来指示这种情况，并在 ClearToken 中加入如下的安全概要单元：

— **elementID**，它被设置为 8，指示这是一个证书响应单元；

— **paramS** 保留不用；

— **element** 持有一个其 **flag** 被设置为 TRUE 的元素。

在这种情况下，GK 将在 ACF 中返回这一个 ClearToken。

在阶段 2 期间，始发的 EP B（MIKEY 发起方）能够随后生成一个新鲜的 MIKEY TGK，并通过应用 MIKEY-PK-SIGN 密钥管理协议计算相关的 MIKEY I_message Imsg（见图 11 和图 12）；或者当所关注的是完善的前向保密时，应用 MIKEY-DH-SIGN 密钥管理协议（采用数字签字的 Diffie-Hellman）。MIKEY-DH-SIGN 被作为一个选项来提供。

SRTP 的对话密钥可以如 RFC 3711 第 4.3 节所描述地从 TGK 导出（图中未显示）。

注 5 — 图 11 和图 12 并没有显示 MIKEY 的所有细节，有一些部分在图中未显示。

MIKEY I_message 是二进制编码的，然后被包装在 H.245 的 **OpenLogicalChannel** 中。

ClearToken 将被作为建立消息的一部分装入该消息，并送往 EP A。由选路的网守将所携带的 MIKEY I_message（对 MIKEY 消息不加修改地）转发到下一跳。

在存在有多个选路网守的情况下，网守之间的呼叫信令消息是使用管理配置的共享秘密，并采用 H.235.1 或 H.235.3 以及私钥/公钥来保证安全的。

从 *TGK*，EP A 可以随后导出 SRTP 的对话密钥，这在 RFC 3711 第 4.3 节中描述（图中未显示）。

EP A，作为 MIKEY 的响应方，能够采用 MIKEY *Ma* 密钥编辑 MIKEY R_message Rmsg，并将它放入 CallProceeding-to-Connect 消息（CP/C）中。

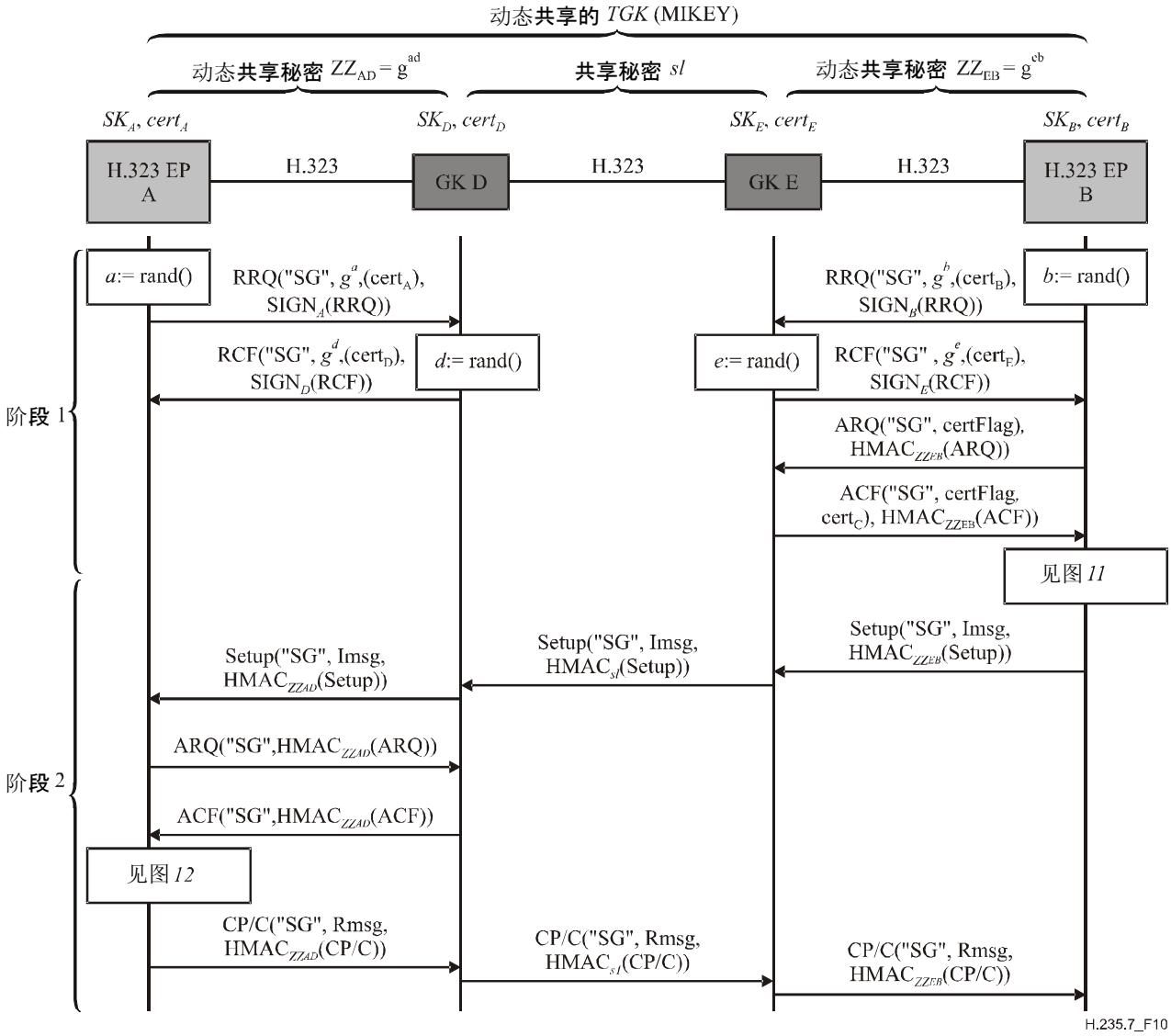

图 10/H.235.7－EP B用MIKEY-PK-SIGN 呼叫EP A的例子（多GK选路）

TGK := rand()
env-key:= rand()
Me, Ma := PRF(env-key,…|| Rand)
PKE := ENC_{PK-A}(env-key,…|| Rand)
K := ENC_{Me}(ID_B || [*TGK*])
KEMAC:= ENC_{Me}(ID_B || [*TGK*])
M := HMAC-SHA1(Ma, K)
I:= HDR, *T*, rand(), [ID_B | $Cert_B$], {*SP*}, [chash], *KEMAC*, *PKE*
Imsg:= *I*, $Sign_{SK-B}$(*I*)

图 11/H.235.7－EP B对MIKEY-PK-SIGN的处理

恢复加密密钥, TGK
Ma := PRF(env-key,…|| Rand),
Rmsg:= HDR, *T*, [ID_A], HMAC-SHA1(Ma, Rmsg || ID_A || ID_B || *T*)

图 12/H.235.7－EP A对MIKEY-PK-SIGN的处理

仅有单个网守的情形是所示多网守情形的一个特例。在这种情况下，使用 LRQ/LCF，远端网守/端点的发现已不再需要。

9.1 终止一个H.323呼叫

由于相关的端点保持着 MIKEY 和 SRTP 的状态，一个适当的终止规程是重要的。图 13 显示了在 EP B（MIKEY 发起方）终止一个呼叫时消息流的例子。这消息流基本是依据 8.5/H.323“阶段 E — 呼叫终止”。

注 — 图 13 还显示了任选的脱离规程，用于端点完全解除注册时的情况。那时这端点也应该丢弃私用的 DH 密钥（a 或 b）和公用的 DH 半密钥（g^a 或 g^b）。

由于终止一个呼叫的规程是独立于本安全概要的，下层安全概要任何可应用的 OID 都可以使用；因此图 13 中未显示任何 OID。

如果端点再次向网守注册，那么就应该产生新的 DH 半密钥。然而，在仅仅为了终止呼叫的任何环境下，完全的解除注册是不必要的。如果端点决定保持与网守的注册关系，那么静态的 DH 半密钥可以继续使用。

在端点保持注册，不准备进行脱离的情况下，端点应该只丢弃与呼叫相关的信息，包括对等端的 DH 半密钥、**challenge**、MIKEY 密钥 *Me*、*Ma*、*TGK* 和相关的 SRTP 对话信息。

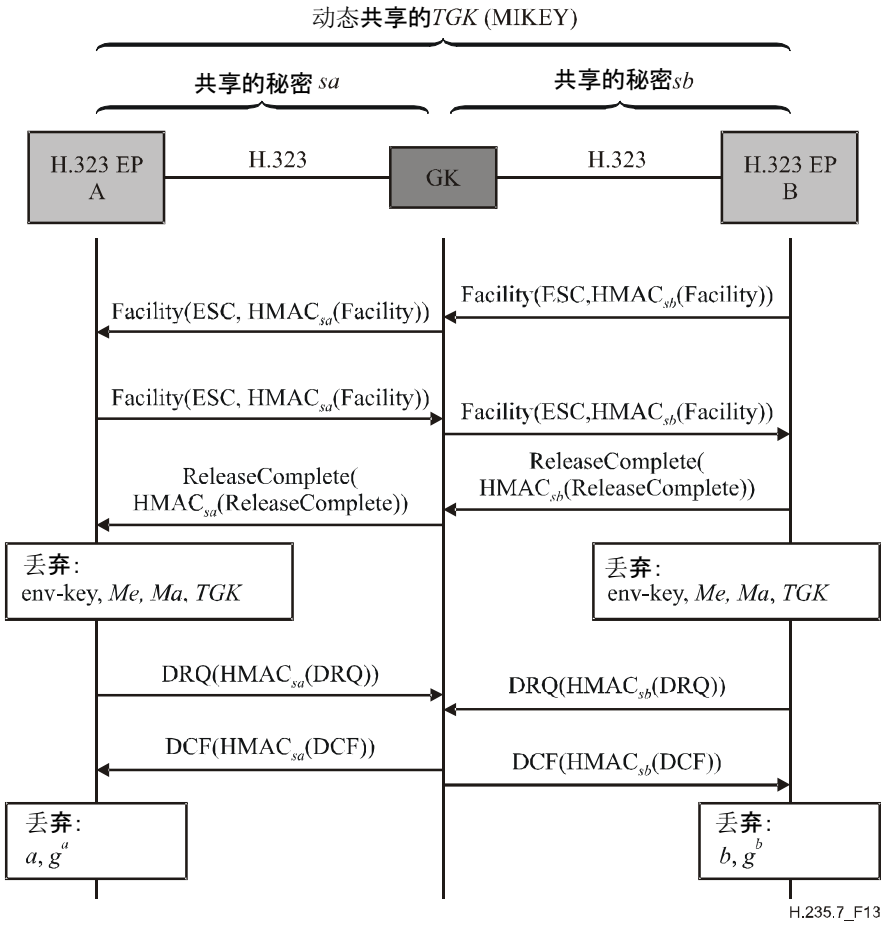

图 13/H.235.7－端点B终止一个呼叫的例子

9.2 TGK密钥重置和CSB更新

MIKEY 已经内置有对 TGK 密钥重置和/或 CSB 信息更新的支持。本建议书必须为此而使用 RFC 3830 第 4.5 节中的 MIKEY-PK-SIGN 规程，它们允许 TGK 在到期前更新，或不改变 TGK 而更新其他的信息（CSB）。

TGK 密钥重置和 CSB 更新机制对于保护同一安全政策下的一组逻辑信道是有用的。为此，建议只对第一个逻辑信道执行第 8 节中描述的（完整的）MIKEY-PK-SIGN 协议。任何随后的、应用同一 MIKEY 安全政策或同一 TGK 的逻辑信道应该使用 CBS 更新机制，而不用本节中的 TGK 密钥重置机制，这可以通过参考初始的 CSB-ID，并忽略更新的 TGK 数据来做到。这样与在每一个逻辑信道上运行完整的 MIKEY 协议相比，可以更有效地建立逻辑信道或 MIKEY 加密对话。

MIKEY TGK 密钥重置或 CSB 更新消息必须包装在 Facility 消息中的 **MiscellaneousCommand** 中进行传送。**ClearToken** 的 **tokenOID** 必须被设置为“SG”。

对于运行在“媒体层”的 MIKEY，EP B 必须确定对哪个逻辑信道进行 TGK 密钥重置和/或 CSB 更新。EP A 作为响应方，将同样地使用 Facility 消息中的 **MiscellaneousCommand** 传送 MIKEY R_message（如果有的话）。

对于 TGK 密钥重置（见图 14），EP B 作为 MIKEY 发起方，必须生成一个新的 TGK。**Mikey** 必须持有对应的 MIKEY I_message。

如果需要由 EP B 请求，作为响应方的 EP A 可以对得到的 TGK 密钥重置消息进行确认。EP A 构建类似的 R_messages。这一 R_message 将在 Facility 消息中传送。Rmsg 是对应的 MIKEY 响应消息，将承载在 **GenericParameter** 的 **octetString** 之中。EP A 将这 Facility 消息发送给 EP B。

对于发起方发起的 CSB 更新，将采用类似于上述的规程，不同的只是 MIKEY 消息中不持有任何的 TGK（见图 14）。

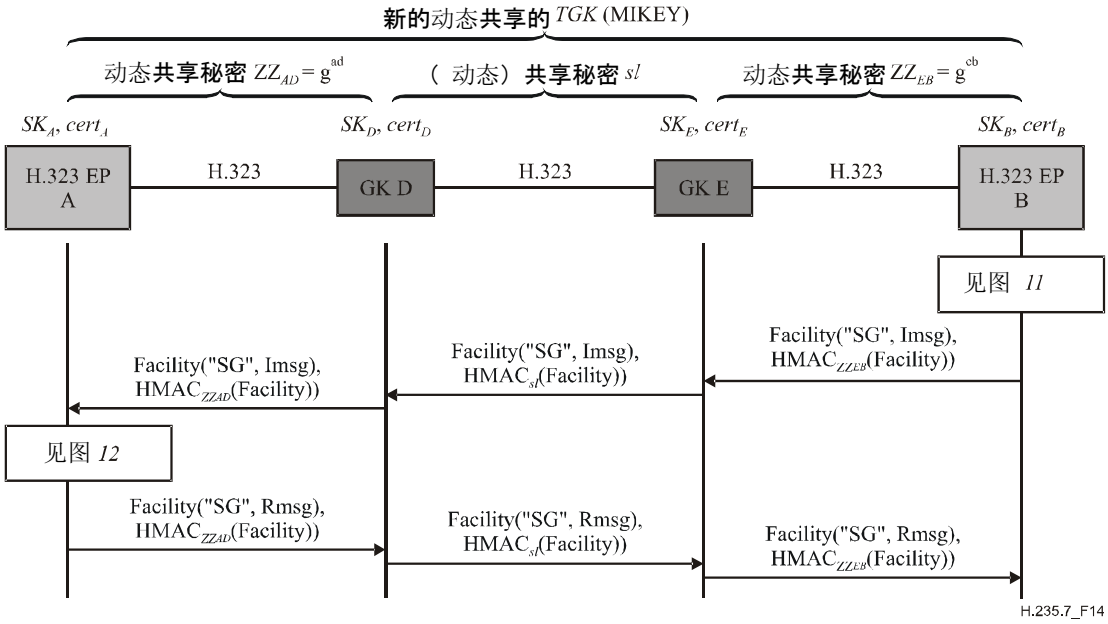

图 14/H.235.7－EP B（发起方）发起TGK密钥重置和密钥更新的例子

注 — 这种从 EP A 到 EP B 的确认功能是任选的，它仅当 EP B 在 MIKEY HDR 中用 V 标志请求一个检验消息（MIKEY R_message）时才是必需的。

本建议书没有定义任何由响应方请求的 TGK 密钥重置和/或 CSB 更新的规程；这一点有待进一步研究。

9.3 H.245隧道传送的支持

如果一个对话期间，有更多的逻辑信道需要加入，应该部署 H.245 隧道传送模式，在此隧道传送的 H.245 消息将承载在一个 Facility 消息中。

9.4 SRTP算法

本安全概要必须使用截取的 HMAC-SHA1-32 作为 RTP 默认的认证算法，并将认证附加码长度 *n_tag* 取为 32 比特。其他由 RFC 3711 定义的认证附加码长度也应该支持，并必须通过适当的 MIKEY 安全政策（SP）参数进行协商。

9.5 对象标识符一览

"SG"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 71}	它在本建议书的背景下，指示一个 H.235.3 基线 ClearToken。

附 录 I

MIKEY-DHHMAC 选项

本附录描述如何部署本安全概要中的 MIKEY-DHHMAC 的密钥管理选项。

密钥管理的这一选项仅设想了有共享密钥可用的安全基础设施。由于 Diffie-Hellman 机制的固有能力，MIKEY-DHHMAC（RFC zzzz）提供了有完善的前向保密（PFS）的安全特性。因而这一选项可使用于需要有 PFS，但同时又不具备 PKI 或数字证书的情况。

这一情形假设在 H.323 域内有若干网守。

本节描述的规程采用 Diffie-Hellman 密钥协定方案在 H.323 端点 EP A 和 EP B 间建立端到端的共享秘密。这种 Diffie-Hellman 密钥协定发生在 H.225.0 RAS 注册和许可阶段，或者，当有多个网守时发生在网守间 LRQ/LCF 期间。所生成的 Diffie-Hellman 共享秘密用于作为端到端的认证密钥，并持续整个呼叫期间。MIKEY-DHHMAC 协议则分别地发生于呼叫建立期间，它为承载信道建立基于 MIKEY 呼叫的秘密。

图 I.1 示意了端点 B 经由一个选路 GK 呼叫端 A 的例子。这一流图类似于图 4，不同的是这里部署的是 MIKEY-DHHMAC 协议。情形中假设有一或多个选路的网守（GK 选路的模型），这里 H.245 消息是放在 H.225.0 中隧道传送的（快速起动）。呼叫信令可能，也可能不通过网守；因此对于这一情形的支持，选路网守并不是必需的。

注 1 — 这流程图也适用于直接选路的情况（没有选路的网守），在此 H.225.0 呼叫信令消息是在端点间直接交换的，不经由任何网守的转发。

图 I.1 中还显示了 H.235.1 基线安全概要，在此每一个消息是整体地加以安全保护的（认证和完整性）。然而，当使用仅有认证这一基线安全概要的选项（没有显示）时，得到的是类似的消息流。在这种情况下，将只对 RAS/H.225.0 消息的一个子集（**CryptoToken** 内的 **ClearToken**），而不是对整个消息计算 HMAC。

例举的消息流显示了 EP B（MIKEY 发起方）采用快速起动呼叫 EP A（MIKEY 响应方）的情况（见图 I.1）。在阶段 1 期间，H.323 端点 A 和 B 用 **RRQ** 向网守进行初始的注册，并递交它们的 DH 半密钥（g^a 和 g^b）。在 **RRQ** 和 **ACF** 期间，为传递 Diffie-Hellman 半密钥，（在 **CryptoHashedToken** 之中）将使用 **ClearToken**。由于这一原因，不得使用 **challenge** 字段。

Diffie-Hellman 半密钥应该作为 **ClearToken** 的一部分在 **dhkey** 中传送。这 ClearToken 必须使用 OID“TG”（见第 8.5 节），而不是基线的 H.235.1 ClearToken OID“T”，它指示：这一安全概要正与 H.235.1 相结合使用。网守应该保存每一个半密钥，只要端点已注册。端点在执行保持存活或使用简化的再注册（re-RRQ）时不得放入任何 DH 半密钥。为指示网守支持这一安全概要，**RCF** 应该在 ClearToken 中使用“TG”OID。

试图呼叫 EP A 的 EP B 从网守 D 请求许可（**ARQ**）。这 **ARQ** 应该在 ClearToken 中使用“TG”OID。在任何其他的 RAS 消息中也应该在 ClearToken 中使用“TG”OID。

这一情形适用于多个相链接的网守。远端端点的发现应该按照第 8.1.6 节/H.323“任选的被叫端点信令”采用 **LRQ/LCF** 来实现。这就是发起方端点如何对远端 GK 区域进行定位，并从而得到目标被叫方端点 Diffie-Hellman 半密钥的做法。如果 GK E 需要定位远端的 GK 区域，GK E 就必须发送 **LRQ** 消息。对组播情况，**LRQ** CryptoToken 中的 **generalID** 不得使用。如果 GK D 不支持这一概要，GK D 必须回送 **LRJ**。否则 GK D 返回 **LCF**，它包含 EP A 的 Diffie-Hellman 半密钥。随后 GK E 必须用包含这 EP A Diffie-Hellman 半密钥的 **ACF** 进行应答。如果 GK E 不能够对远端端点 A 进行定位，那么 GK E 必须返回 **ARJ**。

两个网守之间的通信必须按 H.235.1 保证安全。为此这里假设已经有一个共同的共享秘密 *sl* 存在。因为网守间的 **LRQ** 通常是一个组播消息，这共享秘密 *sl* 通常不会是成对共享的秘密，实际上可以假设是可能的一群网守中一个基于组群的共享秘密。这一假设在一般情况下限制了可扩展性，且不能提供源点的认证。然而，可以相信：在具有有限的小数量已知网守的企业网中，这样的约束和安全限制仍然是可以接受的。采用数字签名来保证网守之间组播通信的安全有可能克服这些限制；然而这一点还待进一步研究。

EP B 得到 EP A 的 Diffie-Hellman 半密钥（**ACF**）。**ACF** 必须在 H.235.1 基线 **ClearToken** 内的 **dhkey** 中持有这被叫端点的 Diffie-Hellman 密钥，但它采用 OID“TG”，而不是“T”。本安全概要将不对 **ClearToken** 中任何其他的字段进行修改。

注 2 — 端点用这 DH 半密钥进行操作，它在整个注册期间，对所有的呼叫是静态的。只要每个端点应用真正是随机的半密钥，这一点应不会是一个安全弱点。

然而，端点应该在 **challenge** 中与 DH 半密钥一起提供 512 比特（也即 64 个字节）新鲜的随机值，（见 RFC 2631 第 2.3 节）。这些 **challenge** 值是基于呼叫的，它在 DH 密钥生成过程中引入必要的随机性和适时性。

始发的 EP B 随后可以计算 g^{ab}，并再用一个随机的 **challenge** 连同 MIKEY-PRF（g^{ab}，0x12F905FE || **challenge**）的结果计算动态共享的秘密 ZZ_{AB}（见 RFC 3830 第 4.1.2-4.1.4 节）。随后 MIKEY 就能够用这 MIKEY-PRF 导出加密密钥（*Me*）和认证密钥（*Ma*）（见 RFC 3830 第 4.1.2-4.1.4 节）。

在阶段 2 期间，始发的 EP B 必须生成一个新鲜的 MIKEY 随机值 *y* 连同对应的 g^y，并随后用 *Ma* 按照 MIKEY- DHHMAC 协议构建 MIKEY I_ message Imsg。

MIKEY I_ message 必须是二进制编码的。

始发的 EP B 应该总是将它的 DH 半密钥放入到 **ClearToken** 的 **dhkey** 中，从而也使 GK 支持的直接选路模型能够工作。**ClearToken** 必须被放入 Setup 消息中，发送给对等的 EP A。选路的网守将把所携带的 ClearToken（对 MIKEY 消息不加修改地）转发到下一跳。

接收的 EP A 随后计算 g^{ab}，并从 MIKEY-PRF（g^{ab}，0x12F905FE || **challenge**）计算动态共享的秘密 ZZ_{AB}（见 RFC 3830，第 4.1.2-4.1.4 节）。然后 MIKEY 用这 MIKEY-PRF 导出认证密钥（*Ma*）（见 RFC 3830 第 4.1.2-4.1.4 节）。此后 EP A 生成一个 MIKEY 随机值 *w*，并计算 g^w。利用接收到的 DH 半密钥，EP A 计算出 *TGK*。

此后正如 RFC 3711 第 4.3 节所描述的，从 *TGK* 接收的 EP A 可以导出 SRTP 的对话密钥（图中未显示）。

EP A 可以构建一个类似的 R_message Rmsg，这个 R_message 是在 CallProceeding-to-Connect 消息（CP/C）中传送的。Rmsg 是对应的 MIKEY 响应消息，它在 CallProceeding-to-Connect 消息（CP/C）中送往 EP B。

CallProceeding-to-Connect 消息（CP/C）被送往 EP B。

EP B 取出 DH 半密钥并计算 *TGK*。然后 EP B 如 RFC 3711 第 4.3 节所描述的，从 TGK 导出 SRTP 对话密钥（图中未显示）。

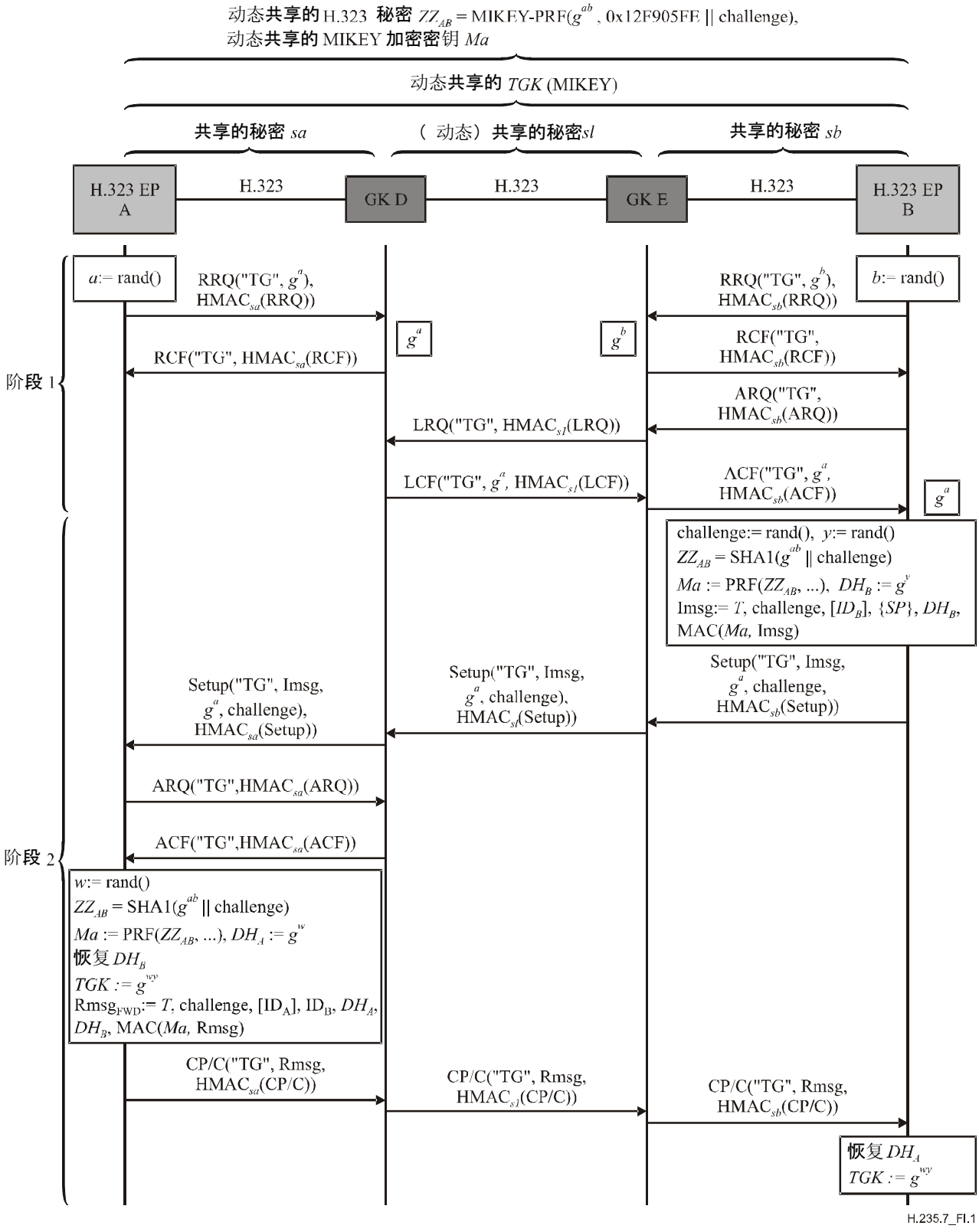

图 I.1/H.235.7－端点B用MIKEY-DHHMAC呼叫端点A的例子（GK选路）

I.1 终止一个H.323呼叫

由于相关的端点保持着 MIKEY 和 SRTP 的状态，一个适当的终止规程是重要的。图 I.2 显示了在 EP B（MIKEY 发起方）终止一个呼叫时消息流的例子。这消息流基本是依据 8.5/H.323“阶段 E — 呼叫终止”。

注 — 图 I.2 还显示了任选的脱离规程，用于端点完全解除注册时的情况。那时这端点也应该丢弃私用的 DH 密钥（a 或 b）和公用的 DH 半密钥（g^a 或 g^b）。

由于终止一个呼叫的规程是独立于本安全概要的，下层安全概要任何可应用的 OID（H.235.1，H.235.3 等）都可以使用；因此图 I.2 中未显示任何 OID。

如果端点再次向网守注册，那么就必须产生新的 DH 半密钥。然而，在仅仅为了终止呼叫的任何环境下，完全的解除注册是不必要的。如果端点决定保持与网守的注册关系，那么静态的 DH 半密钥可以继续使用。

在端点保持注册，不准备进行脱离的情况下，端点应该只丢弃与呼叫相关的信息，包括对等端的 DH 半密钥、**challenge**、MIKEY 密钥 *Me*、*Ma*、*TGK* 和相关的 SRTP 对话信息。

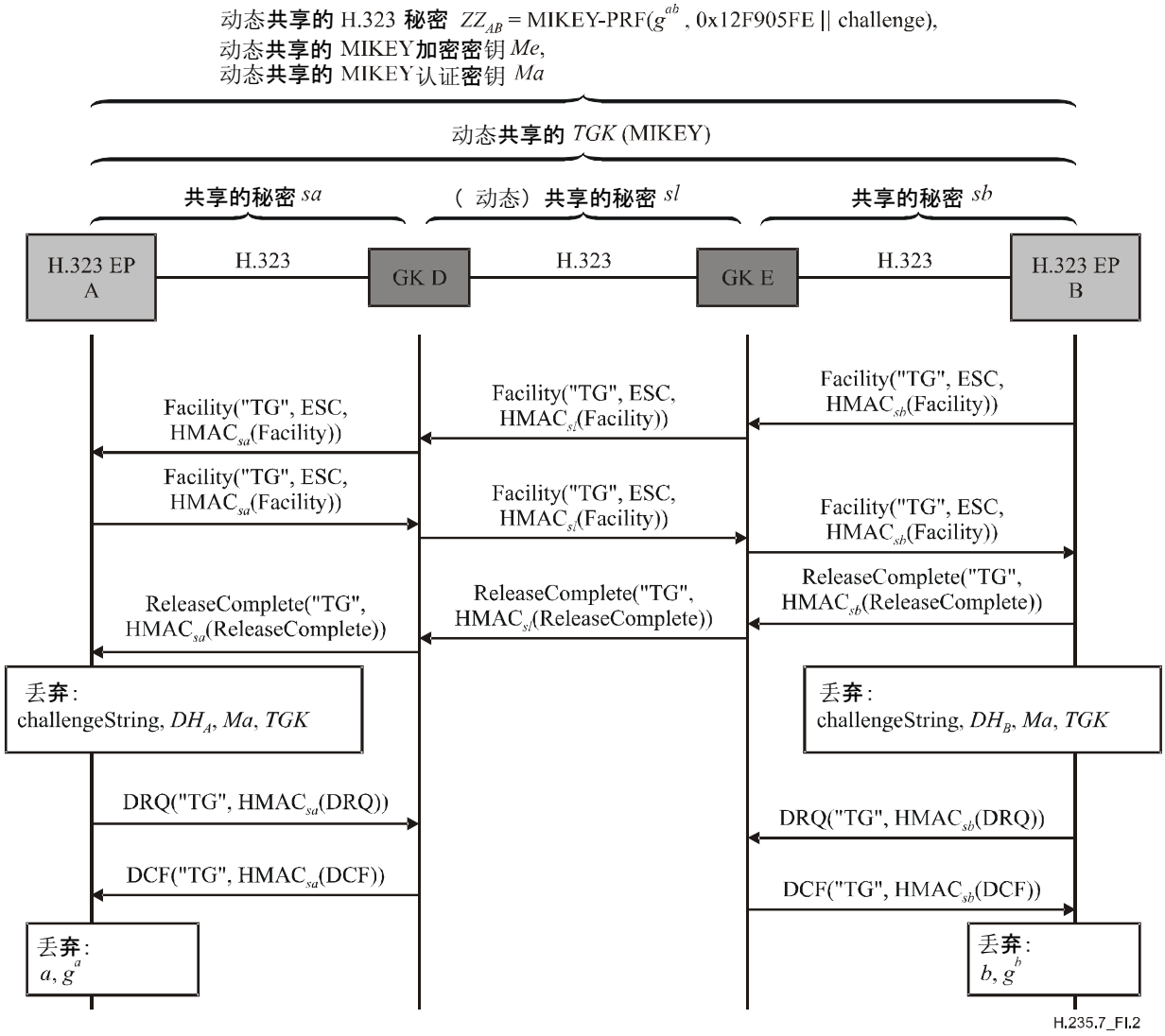

图 I.2/H.235.7－端点B终止一个呼叫的例子

I.2 TGK密钥重置和CSB更新

MIKEY 已经内置有对 TGK 密钥重置和/或 CSB 信息更新的支持。本建议书的安全概要必须为此而使用 RFC zzzz 第 3.1 节的 MIKEY-DHHMAC 规程，它们允许 TGK 在到期前更新，或不改变 TGK 而更新其他的信息。

TGK 密钥重置和 CSB 更新机制对于保护同一安全政策下的一组逻辑信道是有用的。为此，建议只对第一个逻辑信道执行上面描述的（完整的）MIKEY-DHHMAC 协议。任何随后的、应用同一 MIKEY 安全政策或同一 TGK 的逻辑信道应该使用 CBS 更新机制，而不用本节中的 TGK 密钥重置机制，这可以通过参考初始的 CSB-ID，并忽略更新的 Diffie-Hellman 密钥来做到。这样与在每一个逻辑信道上运行完整的 MIKEY 协议相比，可以更有效地建立逻辑信道或 MIKEY 加密对话。

MIKEY TGK 密钥重置或 CSB 更新消息必须包装在 Facility 消息中的 **MiscellaneousCommand** 中进行传送。**ClearToken** 的 **tokenOID** 必须被设置为“TG”。

对于运行在“媒体层”的 MIKEY，EP B 必须确定对那个逻辑信道进行 TGK 密钥重置和/或 CSB 更新。EP A 作为响应方，应该同样地使用 Facility 消息中的 **MiscellaneousCommand** 传送 MIKEY R_message（如果有的话）。

对于 TGK 密钥重置（见图 I.3），EP B 作为 MIKEY 发起方，必须生成一个新的 TGK。**parameterValue** 应持有对应的二进制编码的 MIKEY I_message。

如果需要由 EP B 请求，作为响应方的 EP A 可以对得到的 TGK 密钥重置消息进行确认。EP A 构建类似的 R_messages。这 R_message 将放在 Facility 消息中传送。EP B 发送这 Facility 消息给 EP A。

对于 CSB 更新，将采用类似于上述的规程，不同的只是 MIKEY 消息中不持有任何的 TGK。

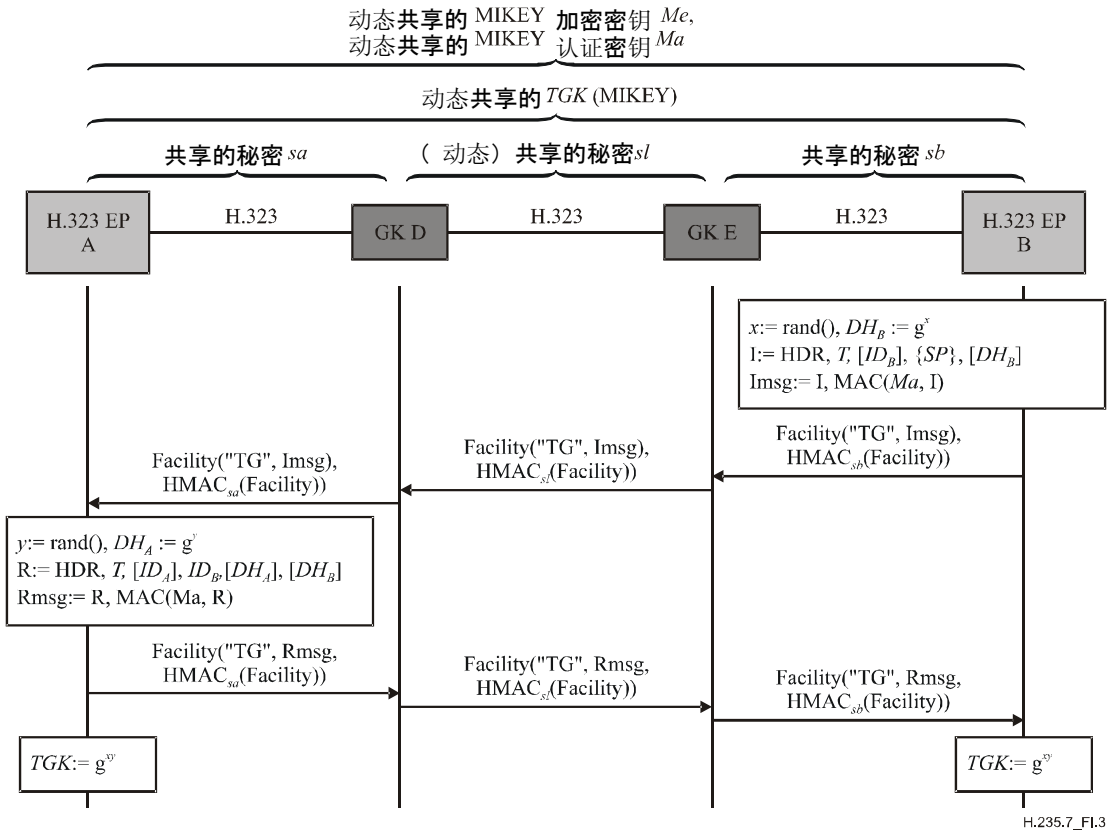

图 I.3/H.235.7－端点B更新一个密钥的例子

本建议书没有定义任何由响应方请求的 TGK 密钥重置和/或 CSB 更新的规程；这一点有待进一步研究。

附 录 II

使用H.235.4来建立预共享的秘密

这一附录定义如何部署 ITU-T H.235.4 建议书的 DRC1 规程，这一规程用于在端点 B 和端点 A 之间建立预共享的秘密 ZZ_{AB}，它假设端到端在事前不存在秘密。本附录描述的方法可应用于有单个网守的情形或有多个网守的情形。本附录中的规程并不涉及 RAS 注册或许可期间的 DH 计算，而是部署对称的加密方法。

图 II.1 显示了端点 B 呼叫端点 A 时流程图的一个例子。

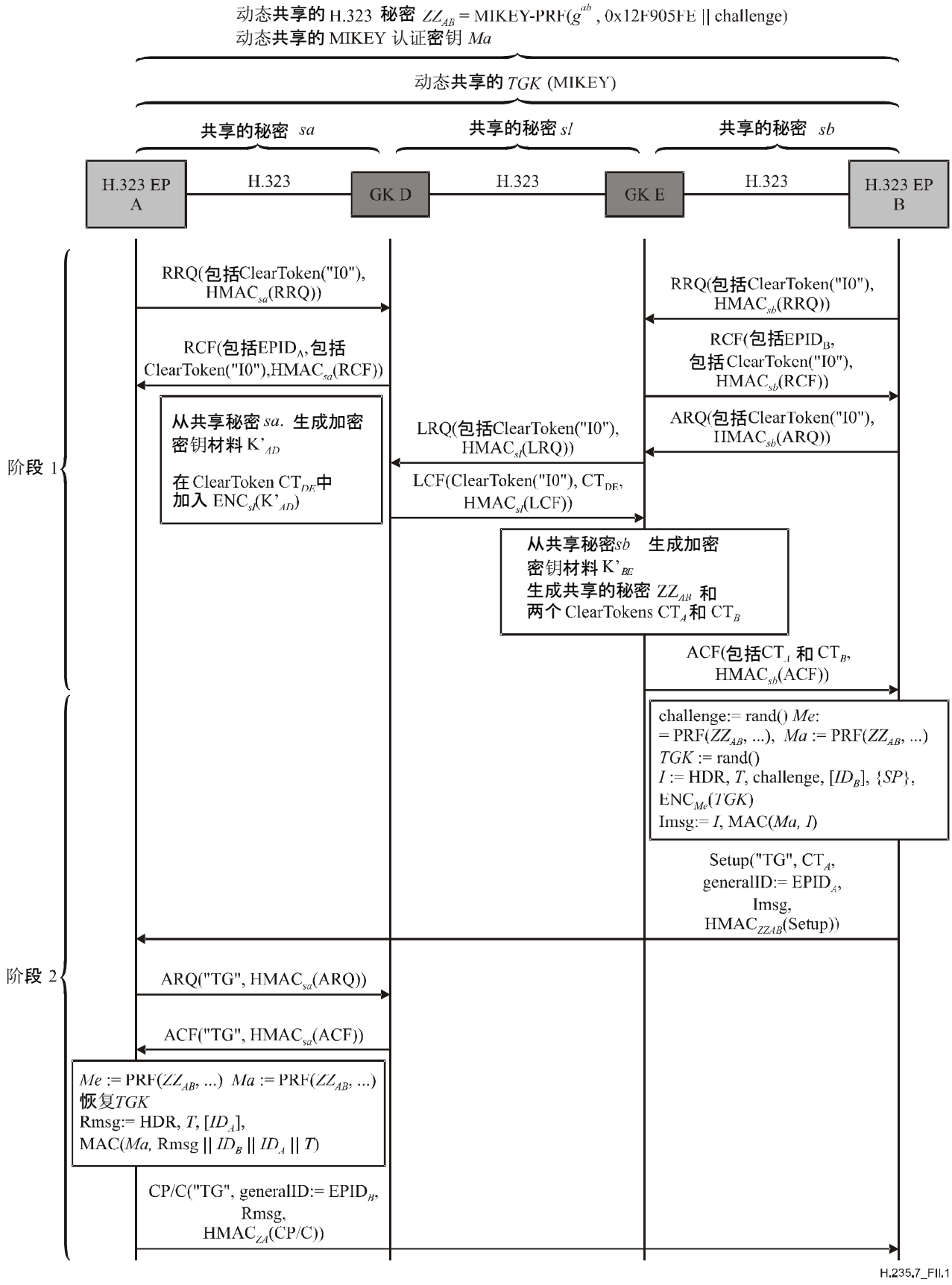

图 II.1/H.235.7一端点B采用MIKEY预共享秘密和H.235.4 DRC1
呼叫端点A的例子（非GK选路）

II.1 终止一个H.323呼叫

终止一个 H.323 呼叫的过程必须按第 8.1 节所描述的进行处理。

II.2 TGK密钥重置和CSB更新

TGK 密钥重置和/或 CSB 更新的规程必须按第 8.2 节所描述的进行处理。

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