国 际 电 信 联 盟

ITU-T H.235.4

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：直接和选择性选路呼叫安全性

ITU-T H.235.4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.235.4建议书

H.323安全性：直接和选择性选路呼叫安全性

摘　要

本建议书的目的是提供使用直接选路呼叫信令的安全性规程和 H.235.1 及 H.235.3 安全概要的建议。该安全概要被提供作为一个选择，可补充 ITU-T H.235.1 和 H.235.3 建议书中的安全概要。它也提供了使用对称加密管理技术的第 8.4 节/H.235.0 的实施详情。

在 H.235 子系列的较早版本中，该概要被包含在附件 I/H.235 中。H.235.0 的附录 IV、V 和 VI 示出 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.235.4 建议书。

关键词

认证，直接选路呼叫安全性，加密，完整性，密钥管理，多媒体安全性，安全概要，选择性选路呼叫安全性。

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

ITU-T H.235.4建议书

H.323安全性：直接和选择性选路呼叫安全性

1 范围

本建议书的目的是提供使用直接选路呼叫信令的安全性规程和 H.235.1 及 H.235.3 安全概要的建议。

该安全概要被提供作为一个选择，可补充 ITU-T H.235.1 和 H.235.3 建议书中的安全概要。它也提供了使用对称加密管理技术的第 8.4 节/H.235.0 的实施详情。

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 (2003), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals,* Corrigendum 1 (2005), plus Erratum 1 (2005).

– 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.235.6 (2005), *H.323 security: Voice encryption profile with native H.235/H.245 key management*.

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

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

ISO/IEC 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference model – Part 2: Security Architecture.*

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

2.2 资料性参考文献

— ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile.*

— IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5).*

3 术语和定义

出于本建议书的目的，ITU-T H.323 建议书的第 3 节、H.225.0、H.235.0 和 X.800 建议书|ISO 7498-2 中给出的定义适用。

4 符号和缩写

本建议书使用下列缩写：

CT	ClearToken
DH	Diffie-Hellman
DRC	直接选路呼叫
EK_{AG}	EP A 和 GK G 之间共享的加密密钥
EK_{BH}	EP B 和 GK H 之间共享的加密密钥
EK_{GH}	GK G 和 GK H 之间共享的加密密钥
$ENC_{K;\,S,\,IV}(M)$	使用秘密密钥 *K*、秘密补白密钥 *S* 和初始化矢量 *IV* 的 *M* 的 EOFB 加密
EPID	端点标识符
GK	网守
GKID	网守标识符
g^x，g^y	GK G，GK H 的 Diffie-Hellman 半密钥
K_{AB}	EP A 和 EP B 之间共享的加密密钥
K_{AG}	EP A 和 GK G 之间共享的秘密（H.235.1，H.235.3）
K_{BH}	EP B 和 GK H 之间共享的秘密（H.235.1，H.235.3）
K_{GH}	GK G 和 GK H 之间共享的秘密（H.235.1，H.235.3）
KS_{AG}	秘密，EP A 和 GK G 之间共享的补白密钥
KS_{BH}	秘密，EP B 和 GK H 之间共享的补白密钥
KS_{GH}	秘密，GK G 和 GK H 之间共享的补白密钥
PRF	伪随机函数

5 惯例

本建议书中使用下列惯例：

— “须（Shall）”表明是强制性要求。

— “应（Should）”表明是推荐采取的非强制性措施。

— “可（May）”表明是非强制性措施，但并未建议采取这种措施。

对象标识符通过在报文中的符号参考符（例如，“I11”）引用，第 14 节列出了符号的对象标识符的实际数值，也见第 5 节/H.235.0。

6 引言

通常在使用网守选路模型时采用 H.323。例如使用这一模型支持最佳的计费和其他功能性。网守选路呼叫模型的广泛使用也是正是集中于这种呼叫模型的不同安全概要在 ITU-T H.235.0 建议书（如 H.235.1、H.235.2、H.235.3）内定义的原因。

然而，随着需要支持数目正在增加的并行信道，具有一个网守的直接选路呼叫模型可有较好的性能和可扩展的特性。这一模型的优点是利用网守来注册、允许、地址解析和带宽控制，而直接以端到端方式在端点之间直接进行呼叫确定。

本建议书描述了对用网守支持直接选路呼叫的 H.235.1 基线概要和 H.235.3 混合安全概要的增强。

7 概述

H.235.1 基线与 H.235.3 混合安全概要（见 H.235.3）一样（在第一次握手之后）采用一个共享的秘密，将网守作为可信的中介主机使用，以逐段转接的方式来确保消息认证和/或完整性。使用直接选路呼叫模型，不能假定在两个端点之间共享一个秘密。使用预设定的共享秘密来保证通信的安全也是不可行的，因为在这一情况下，所有的端点都必须预先知道将呼叫其他的哪些端点。

ITU-T H.235.4 显示了如图 1 所示的情形，其中端点与单独的网守相连，采用直接选路呼叫信令。这情形假定在网守区内一个非安全的 IP 网络。

假定每个端点有一个通信联络和与网守关联的安全性，每个端点和网守使用基线或混合安全概要安全地注册了。

因此，初始化端点（DRC1）的网守或终接端点（DRC2）的网守能够使用类 Kerberos 方法（见 RFC 4120）为直接通信的端点提供一个共享的秘密。

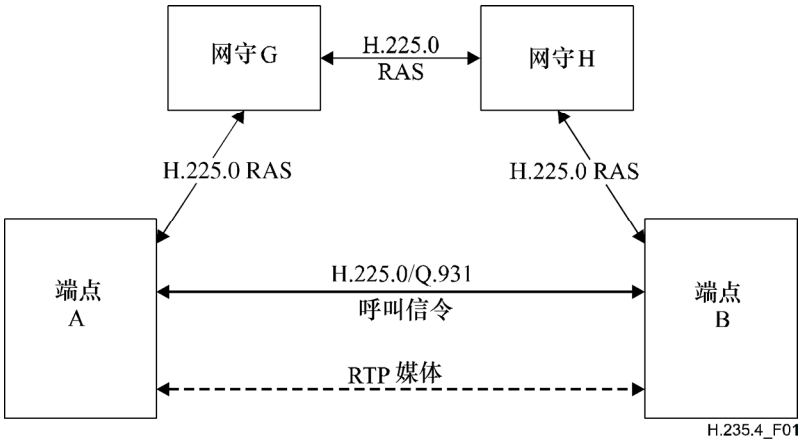

图 1/H.235.4－直接选路呼叫情形

本建议书为不同的环境描绘了两种规程：DRC1 和 DRC2。

规程 DRC1（见第 9 节）适用于共同环境，即网守位于不用（本地）站点，但站点采用共用的共同的安全性政策。在这样的环境下，假定始发网守 G 为将要建立的呼叫确定有效的安全性政策是可接受的；这样始发网守 G 挑选和选定适用的安全性参数。终接网守 H 将接收选定的安全性参数。

规程 DRC2（见第 10 节）和 DRC3（第 11 节）适用于域内环境，即网守位于不用的管理域，每个管理域采用不同的安全性政策。

规程 DRC2 适用于这样的环境，即呼叫端点或网守不支持 Diffie-Hellman 算法。在这样的环境下，假定终接网守 H 为将要建立的呼叫确定有效的安全性政策是可接受的；这样终接网守 H 挑选和选定适用的安全性参数。始发网守 G 将接受选定的安全性参数。

规程 DRC3 适用于这样的环境，即呼叫端点或网守不支持 Diffie-Hellman 算法，而在呼叫域和被呼叫域中的网守都支持 Diffie-Hellman 算法。

在呼叫注册开始时，规程提供信令含义以协商采用 DRC1、DRC2 或 DRC3 中的哪一个。

8 限制

本建议书目前不涉及直接选路情形。这有待进一步研究。

9 规程DRC 1（共同环境）

本节中描述的规程适用于共同环境，即网守位于不用（本地）站点，但站点采用共用的共同的安全性政策。在这样的环境下，假定始发网守 G 为将要建立的呼叫确定有效的安全性政策是可接受的；这样始发网守 G 挑选和选定适用的安全性参数。终接网守 H 将接收选定的安全性参数。

9.1 GRQ/RRQ阶段

能够支持这一安全概要的端点必须通过包括一个单独的 ClearToken（其 **tokenOID** 设置为“I10”）指示在 **GRQ** 和/或 **RRQ** 期间的事实；任何在那个 ClearToken 的其他字段不应使用。能迅速提供这一功能性的 H.235.4 可能的网守必须用 **GCF** 代替 **RCF** 回答，包括单独的 ClearToken，其 **tokenOID** 设置为“I10”，ClearToken 中的所有字段不使用。

9.2 ARQ阶段

在端点 A 开始直接向端点 B 发送呼叫信令消息之前，端点 A 或 B 必须在网守 G 或 H 处使用 ARQ 请求认可。端点 A 必须在 **ARQ** 内包括一个单独的 ClearToken，其 **tokenOID** 设置为“I10”，在 ClearToken 内的所有其他字段不使用。

9.3 LRQ阶段

该规程涉及一个单独的共用网守到端点的情况和多个链接的网守的情况。在多个有关的网守的情况下，在呼叫始发的那个区内的网守 G，应使用（多个）**LRQ** 机制定位网守，如 ITU-T H.323 建议书第 8.1.6 节“任选的被叫端点信令”所描述的。两个网守之间的通信必须按照 H.235.1 来保护安全。为此，假定可获得一个共用的共享秘密 K_{GH}。因为典型地网守之间的 **LRQ** 是一个组播的消息，典型地共享秘密 K_{GH} 不能是一对共享秘密，但假定是在潜在的网守群内的基于组的共享秘密。

注 — 这假定在一般情况下限制具有可伸缩性，不允许远认证。但是，相信具有有限的、少量的已知网守的企业网的情况下，这样的约束和安全性限制还是可接受的。使用数字签名保护网守内的组播通信可克服这些限制：但是，这有待进一步研究。

如果 **LRQ** 机制被用于定位远端网守，则 **LRQ** 必须传送一个单独的（其 **tokenOID** 被设置为“I10”）；在那一 ClearToken 内的其他字段都应不使用。对于组播的情况，**LRQ** 的 ClearToken 内的 **generalID** 不得使用。使用 H.501 和/或 H.510 的网守间通信有待进一步研究。

9.4 LCF阶段

EK_{BH} 表示在端点 B 和网守 H 之间共享的加密密钥，KS_{BH} 表示表示在端点 B 和网守 H 之间共享的加密补白密钥。如下所述，网守 H 和端点 B 使用 PRF 分别从共享秘密 K_{BH} 中计算出这一加密材料。

网守 H 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-B 替代 **challenge**，CT_{HG}**→h235Key→secureSharedSecret→keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，见第 14 节），从共享秘密 K_{BH} 中得出生成一个随机的 Challenge-B、加密密钥材料 EK_{BH} 和补白密钥材料 KS_{BH}。

EK_{GH} 表示在端点 G 和网守 H 之间共享的加密密钥，KS_{GH} 表示表示在端点 G 和网守 H 之间共享的加密补白密钥。网守 H 必须生成一个随机的 Challenge-G。网守 H 必须使用如第 14 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-G 替代 **challenge**），从共享秘密 K_{GH} 中得出生成一个随机的 Challenge-G、加密密钥材料 EK_{GH} 和补白密钥材料 KS_{GH}。CT_{HG}**→challenge** 必须掌握 Challenge-G，端点 B 的端点 ID 必须在 CT_{HG}**→h235Key→secureSharedSecret→generalID** 中设置。

网守 H 必须传送加密的 EK_{BH} 和加密的 KS_{BH} 到网守 G。增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{BH} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）：任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 H 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_{HG}**→h235Key→secureSharedSecret→params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_{HG}**→h235Key→secureSharedSecret→params→iv16** 内传送。

网守 H 必须在 ClearToken CT_{HG}（其 **tokenOID** 被设置为“I13”）中包括 $ENC_{EK_{GH},KS_{GH},IV}$ (EK_{BH})和 $ENC_{EK_{GH},KS_{GH},IV}$ (KS_{BH})。然后，获得的密文 $ENC_{EK_{GH},KS_{GH},IV}$ (EK_{BH}) 必须在 CT_{HG}**→h235Key→secureSharedSecret→encryptedSessionKey** 传送；获得的密文 $ENC_{EK_{GH},KS_{GH},IV}$ (KS_{BH}) 必须在 CT_{HG}**→h235Key→secureSharedSecret→encryptedSaltingKey** 中传送。加密算法必须在 CT_{HG}**→h235Key→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。Challenge-B 必须被放置在 CT_{HG}**→h235Key→secureSharedSecret→clearSaltingKey** 内。CT_{HG}**→generalID** 必须被设置为网守标识符 G，而 CT_{HG}**→sendersID** 必须被设置为网守标识符 H。

Challenge-B 必须通过将 **profileInfo** 包含在 **ClearToken** CT_{HG}→**profileInfo**→**elementID**= 0 内标识这一特定的概要元素被传送给端点 B；

CT_{HG}→**profileInfo**→**paramS** 保留不使用，CT_{HG}→**profileInfo**→**element**→**octets** 必须掌握 Challenge-B。

LCF 响应必须掌握 ClearToken CT_{HG}。

9.5 ACF阶段

认识到端点 A 和 B 都支持本建议书，网守 G 必须如下所规定的，生成密钥资料和 ClearToken。

除了常规的 **ARQ** 运算以外，网守能够计算出基于呼叫的共享秘密 K_{AB}。然后这一基于呼叫的共享秘密用 ClearToken 传播给两个端点。这些 ClearToken 在 **ACF** 消息内传送并被回送给主叫方。

必须包括两个 ClearToken，其中一个是 CT_A，用于主叫方 A，另一个是 CT_B，用于被叫方 B。每个 **ClearToken** 必须在 **tokenOID** 内包含一个 OID（“I11”或“I12”），指示令牌是去往主叫方（OID “I11”或 CT_A）还是被叫方（OID“I12”，对于 CT_B）的。

GK G 必须解密 CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** 来获得 EK_{BH}，必须解密 CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSaltingKey** 来获得 KS_{BH}。

如本建议书定义的，**ClearToken** 可与其他同样采用了 **ClearToken** 的安全概要（如 H.235.1 或 H.235.2）一起使用。在这样的情况下，本建议书的 ClearToken 必须也使用那些其他的 **ClearToken** 字段。例如，为了与 ITU-T H.235.1 建议书一起使用本建议书，字段 **timestamp**、**random**、**generalID**、**sendersID** 和 **dhkey** 必须存在和使用，如由 H.235.1 安全概要所规定的。

网守 G 的网守 ID（GKID）必须被放在 CT_A→**sendersID** 和 CT_B→**sendersID** 内，但是 CT_A→**generalID** 必须掌握端点 A（CT_A）的端点标识符，CT_B→**generalID** 必须掌握端点 B（CT_B）的端点标识符。

网守 G 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，**challenge** 被替代为 CT_{HG}→**challenge**），从 K_{GH} 中生成补白密钥材料 KS_{GH} 和加密密钥材料 EK_{GH}

加密端到端密钥 K_{AB} 的加密密钥 EK_{AG} 和 EK_{BH} 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，CT_A→**h235Key**→**secureSharedSecret**→**keyDerivationOID** 和 CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** 都必须掌握“AnnexI-HMAC-SHA1-PRF”，见第 14 节，且 CT_A→**challenge** 必须掌握 Challenge-A）从网守和端点之间的共享秘密（EK_{AG} 或 EK_{BH}）中生成。

网守 G 必须从 CT_{HG}→**h235Key**→**secureSharedSecret**→**clearSaltingKey** 复制 Challenge-B 到 CT_B→**challenge**。

CT_B→**profileInfo** 必须掌握在 CT_{HG} **profileInfo** 中传送的概要元素，以便于在末端端点 B 获得 Challenge-B。

这一对话秘密 K_{AB} 必须使用一个加密算法，由 EK_{AG}（对于去往端点 A 的 CT）或 EK_{BH}（对于去往端点 B 的 CT）算出。

增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{AG} 或 KS_{BH} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）：任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 G 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_A→**h235Key→secureSharedSecret→params→iv8** 和 CT_B→**h235Key→secureSharedSecret→params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_A→**h235Key→secureSharedSecret→params→iv16** 和 CT_B→**h235Key→secureSharedSecret→params→iv16** 内传送。

获得的密文 $ENC_{EK_{AG,}KS_{AG,}IV}$ (K_{AB})必须在 CT_A→**h235Key→secureSharedSecret→encryptedSessionKey** 中传送；获得的密文 $ENC_{EK_{BH,}KS_{BH,}IV}$ (K_{AB}) 必须在 CT_B→**h235Key→secureSharedSecret→encryptedSessionKey** 中传送。加密算法必须在 CT_A→**h235Key→secureSharedSecret→algorithmOID** 和 CT_B→**h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。

对于去往端点 A 的 ClearToken，端点 B 的端点标识符（$EPID_B$）必须被放置在 CT_A→**h235Key→secureSharedSecret→generalID** 内。同样地，对于去往端点 B 的 ClearToken，端点 A 的端点标识符（$EPID_A$）必须被放置在 CT_B→**h235Key→secureSharedSecret→generalID** 内。

对于 EOFB 加密算法，**encryptedSaltingKey** 不得使用。

网守 G 必须在去向端点 A 的 **ACF** 中包括 ClearTokens CT_A 和 CT_B。

9.6 SETUP阶段

端点 A 必须检查 ClearToken 内的 **tokenOID**“I11”来识别 CT_A。

端点 A 必须检查 **timestamp** 来检验已获得的 CT_A 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **V3KeySyncMaterial** 内的 **generalID**。如果接收到的 CT_A 被验证为是最新的，对于网守，端点 A 必须恢复 IV 并计算 EK_{AG} 和 KS_{AG}，如以上对网守 G 所描述的。端点 A 必须解密 **encryptedSessionKey** 信息来获得 K_{AB}，该信息在 CT_A 的 **SecureSharedSecret** 内找到。

如果接收到的 CT_A 被验证为是最新的，端点 A 能够发送一个 SETUP 消息给端点 B。这一 SETUP 消息包括 CT_B。依照 ITU-T H.235.1 建议书或 ITU-T H.235.3 建议书使用 K_{AB} 作为适用的共享秘密，SETUP 消息必须是安全的（认证和/或完整性保护）。为此 H.235.1 散列 ClearToken（不是 CT_B!）中的 **generalID** 中的 **generalID** 不得使用，除非端点 A 已有一个可获得的 $EPID_B$（例如通过配置或从原来的通信中记忆）。如果端点 A 在 SETUP 中使用 generalID 的 $EPID_B$，则端点 A 必须接收在返回的呼叫信令消息中的 sendersID 的值作为真实的 $EPID_B$。

端点 B 必须检查 ClearToken 内的 **tokenOID**“I12”来识别 CT_B。

端点 B 必须检查 **timestamp** 来检验已获得的 CT_B 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_B 被验证为是最新的，对于网守，端点 B 必须从 CT_{HG}→**profileInfo→element→octets** 中检索 Challenge-B，恢复 IV 并计算 EK_{BH} 和 KS_{BH}，Challenge-B 在第 12 节中替代 **challenge**，如以上对网守所描述的。端点 B 必须解密 **encryptedSessionKey** 信息来获得 K_{AB}，该信息在 CT_B 的 **SecureSharedSecret** 内找到。

在 CT_B 被验证为是最新的情况下，端点 B 能够通过用 CALL-PROCEEDING、ALERTING 或 CONNECT 等适当地回复来进行呼叫的信号发送。在 CT_B 被发现不是最新或 SETUP 消息的安全性验证失败的情况下，端点 B 必须用 RELEASE-COMPLETE 和设置为安全性错误的 **ReleaseCompleteReason** 来回复，如 11.1/H.235.0 所定义的。

当将采用媒体安全性（见 6.1/H.235.6）时，端点 A 和端点 B 必须依照 8.5/H.235.6 交换 Diffie-Hellman 半密钥，并确定一个动态的基于对话的主密钥，然后从该密钥中可得出特定媒体的对话密钥。

端点 B 必须包括设置为 $EPID_A$ 的 **generalID** 和设置为 $EPID_B$ 的 **sendersID** 来保护去往 EP A 的任何 H.225.0 呼叫信令消息（例如呼叫进行、告警或连接）。

图 2 示出基本的通信流：

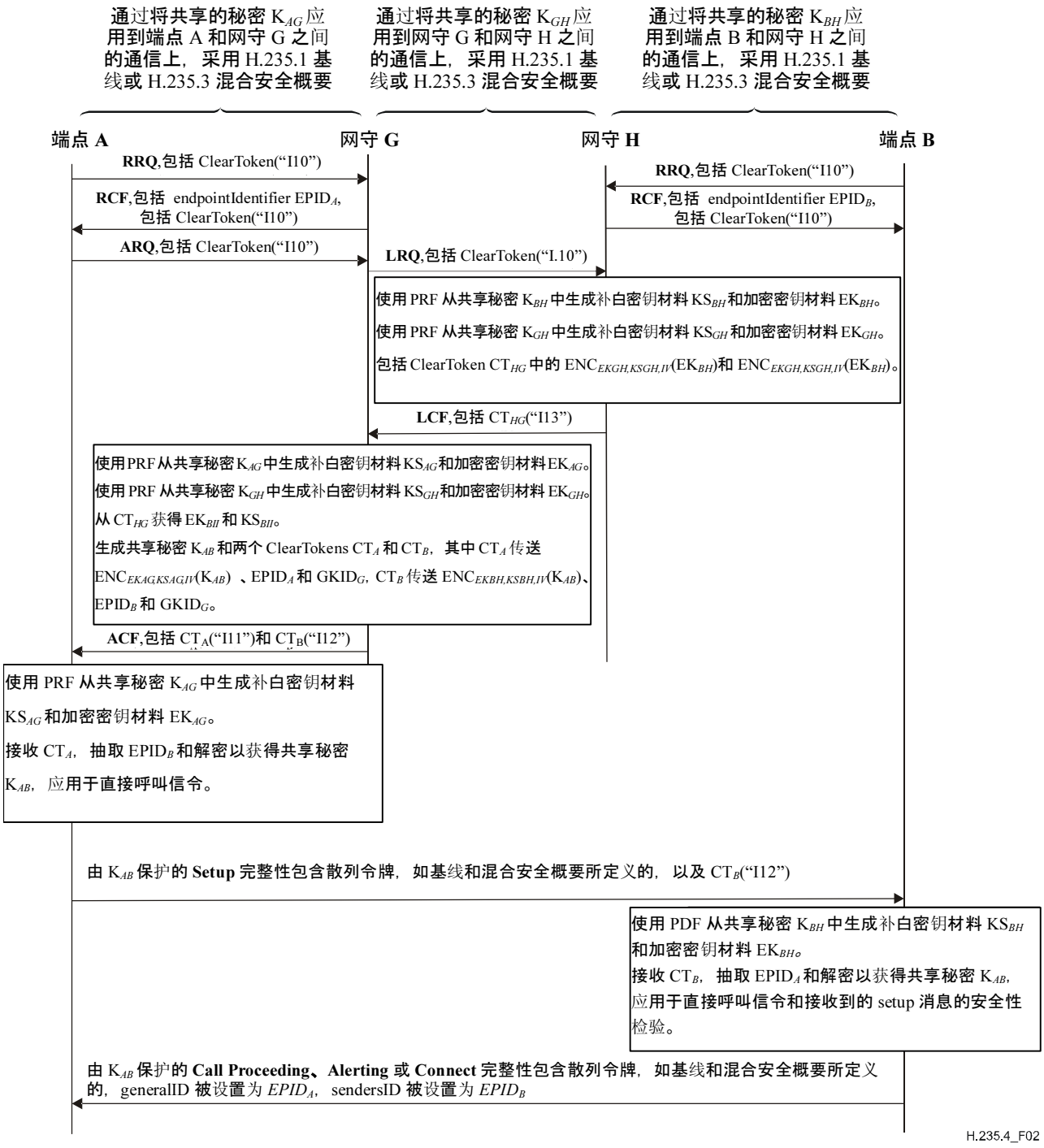

图 2/H.235.4－基本通信流（DRC1）

10 规程DRC2（域内环境）

本节中描述的规程在域内环境中适用，在这类环境中，网守位于不同的管理域，每个域可采用不同的安全性政策。规程 DRC2 适用于呼叫端点或网守不支持 Diffie-Hellman 算法的情况。

在这样的环境下，假定终接网守 H 为将要建立的呼叫确定有效的安全性政策是可接受的；这样终接网守 H 挑选和选定适用的安全性参数。始发网守 G 将接受选定的安全性参数。

10.1 GRQ/RRQ阶段

能够支持这一安全概要的端点必须通过包括一个单独的 ClearToken（其 **tokenOID** 设置为“I20”）指示在 **GRQ** 和/或 **RRQ** 期间的事实；任何在那个 ClearToken 的其他字段不应使用。愿意提供这一功能性的 H.235.4 可能的网守必须用 **GCF** 代替 **RCF** 回答，包括单独的 ClearToken，其 **tokenOID** 设置为“I20”，ClearToken 中的所有字段不使用。

10.2 ARQ阶段

在端点 A 开始直接向端点 B 发送呼叫信令消息之前，端点 A 或 B 必须在网守 G 或 H 处使用 ARQ 请求认可。端点 A 必须在 **ARQ** 内包括一个单独的 ClearToken，其 **tokenOID** 设置为“I20”，在 ClearToken 内的所有其他字段不使用。

10.3 LRQ阶段

该规程涉及一个单独的共用网守到端点的情况和多个链接的网守的情况。在多个有关的网守的情况下，在呼叫始发的那个区内的网守 G，应使用（多个）**LRQ** 机制定位网守，如 ITU-T H.323 建议书第 8.1.6 节“任选的被叫端点信令”所描述的。两个网守之间的通信必须按照 ITU-T H.235.1 建议书来保护安全。为此，假定可获得一个共用的共享秘密 K_{GH}。因为典型地网守之间的 **LRQ** 是一个组播的消息，典型地共享秘密 K_{GH} 不能是一对共享秘密，但假定是在潜在网守群内的基于组的共享秘密。

注 — 这假定在一般情况下限制具有可伸缩性，不允许远认证。但是，相信在具有有限的、少量的已知网守的企业网的情况下，这样的约束和安全性限制还是可接受的。使用数字签名保护网守内的组播通信可克服这些限制：但是，这有待进一步研究。

如果 **LRQ** 机制被用于定位远端网守，则 **LRQ** 必须传送一个单独的（其 **tokenOID** 被设置为“I10”）；在那一 ClearToken 内的其他字段都应不使用。对于组播的情况，**LRQ** 的 ClearToken 内的 **generalID** 不得使用。使用 H.501 和/或 H.510 的网守间通信有待进一步研究。

10.4 LCF阶段

认识到端点 A 和 B 都支持本建议书，网守 H 必须如下所规定的，在 **LCF** 中生成密钥资料和 ClearToken。

K_{BH} 表示在端点 B 和网守 H 之间共享的共享密钥。EK_{BH} 表示在端点 G 和网守 H 之间共享的加密密钥，KS_{BH} 表示表示在端点 G 和网守 H 之间共享的加密补白密钥。网守 H 生成一个随机的 Challenge-B。网守 H 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-B 替代 **challenge**，CT_B**→h235Key→secureSharedSecret→keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，见第 14 节），从共享秘密 K_{BH} 中生成一个加密密钥材料 EK_{BH}。

网守 H 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-B 替代 **challenge**）从 K_{BH} 中生成一个补白密钥 KS_{BH}。

EK_{GH} 表示在端点 G 和网守 H 之间共享的加密密钥，KS_{GH} 表示表示在端点 G 和网守 H 之间共享的加密补白密钥。网守 H 生成一个随机的 Challenge-G。网守 H 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-B 替代 **challenge**，CT_{HG}→**h235Key→secureSharedSecret→ keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，见第 14 节），从共享秘密 K_{GH} 中生成一个加密密钥材料 EK_{GH}。

网守 H 必须使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-G 替代 **challenge**）从 K_{GH} 中生成 KS_{GH}。

网守 H 在 **LCF** 消息中创建两个 ClearTokens。一个是 CT_{HG}，用于网守 G，另一个是 CT_B，用于被叫方 B。CT_{HG}→**tokenOID** 必须包含一个 OID “I23”，而 CT_B→**tokenOID** 必须包含一个 OID“I12”。

Challenge-G 必须在 CT_{HG}→**challenge** 中设置，网守 H 的网守 ID 必须在 CT_{HG}→**sendersID** 中设置，网守 G 的网守 ID（从 **LRQ** 中复制）必须在 CT_{HG}→**generalID** 中设置。

Challenge-B 必须在 CT_B→**challenge** 中设置，网守 H 的网守 ID 必须在 CT_B→**sendersID** 中设置，端点 G 的端点 ID 必须在 CT_B→**generalID** 中设置。如果 **LRQ** 在其端点标识符字段中具有端点 A 的端点 ID，则网守 H 必须将其复制到 CT_B→**h235Key→secureSharedSecret→generalID** 中，也必须将其复制到 CT_{HG}→**h235Key→secureSharedSecret→generalID** 中。

如果网守 H 和端点 B 也支持本建议书的 DRC2，则 **LCF** 响应必须掌握 ClearToken CT_{HG} 和 CT_B。

已经从网守 H 接收到 **LCF** 消息的网守 G，检查 ClearToken CT_B 和 $CT_{HG.}$。网守 G 使用 Challenge-G 作为 **challenge**，使用第 12 节中规定的 PRF，来从 K_{GH} 中计算出 KS_{GH} 和 EK_{GH}，然后解密 CT_{HG}→**h235Key→secureSharedSecret→encryptedSessionKey**，得到端点 A 和端点 B 共享的 K_{AB}。

10.5 ACF阶段

网守计算出端点 A 和 B 共享的基于呼叫的共享秘密 K_{AB}。然后这一基于呼叫的共享秘密用 ClearToken 传播给两个端点。ClearToken 首先被发送回始发端网守 G，然后网守 G 在 **ACF** 消息内传送信息回送给主叫方。

网守 H 必须将 EK_{GH} 作为 $ENC_{EK_{HG,}KS_{HG,}IV}(K_{AB})$来加密 K_{AB}，将被加密的 K_{AB} 放置到 CT_{HG}→**h235Key→secureSharedSecret→encryptedSessionKey** 中。

增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{GH} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）： 任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 H 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_{HG}→**h235Key→secureSharedSecret→ params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_{HG}→**h235Key→secureSharedSecret→params→iv16** 内传送。

加密算法必须在 CT_{HG}→**h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。对于 EOFB 加密算法，不得使用 **encryptedSaltingKey**。

否则，网守 H 必须将 EK_{BH} 作为 $ENC_{EK_{BH},KS_{BH},IV}(K_{AB})$来加密 K_{AB}，将被加密的 K_{AB} 放置到 CT_B→**h235Key→secureSharedSecret→encryptedSessionKey** 中。

对于端点 B（CT_B），增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{BH} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）： 任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 H 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_B→**h235Key→secureSharedSecret→ params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_B→**h235Key→secureSharedSecret→params→iv16** 内传送。

加密算法必须在 CT_B→**h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。对于 EOFB 加密算法，不得使用 **encryptedSaltingKey**。

对于对端点 A 的 **ACF** 响应，必须包括两个 ClearToken，一个是 CT_A，用于主叫方 A，另一个是 CT_B，用于被叫方 B。**ClearToken** CT_A→**tokenOID** 必须包含一个 OID “I11”。

网守 G 生成一个 Challenge-A，使用如第 12 节所规定的基于 PRF 的密钥衍生规程（其中，Challenge-A 替代 **challenge**，CT_A→**h235Key→secureSharedSecret→keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，见第 14 节，且设置 CT_A→**challenge** 为 Challenge-A），从共享秘密 K_{AG} 中生成一个加密密钥材料 EK_{AG}。

网守 G 必须使用加密算法将 EK_{AG} 作为 $ENC_{EK_{AG},KS_{AG},IV}(K_{AB})$来加密 K_{AB}，将被加密的 K_{AB} 放置到 CT_A→**h235Key→secureSharedSecret→encryptedSessionKey** 中。

增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{AG} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）： 任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 G 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_A→**h235Key→secureSharedSecret→params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_A→**h235Key→secureSharedSecret→params→iv16** 内传送。加密算法必须在 CT_A→**h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。

网守 G 的网守 ID 必须在 CT_A→**sendersID** 中设置，端点 A 的端点 ID 必须在 CT_A→**generalID** 中设置。端点 B 的端点 ID 必须从 CT_B→**generalID** 复制到 CT_A→**h235Key**→**secureSharedSecret**→**generalID**。

如果网守 G 之前还未在 **LRQ** 的端点标识符字段中填充端点 A 的端点 ID，则网守 G 必须将端点 A 的端点 ID 填充到 CT_B→**h235Key**→**secureSharedSecret**→**generalID** 中。

对于 EOFB 加密算法，不得使用 **encryptedSaltingKey**。

如本建议书定义的，**ClearToken** 可与其他同样采用了 **ClearToken** 的安全概要（如 H.235.1 或 H.235.2）一起使用。在这样的情况下，本建议书的 ClearToken 必须也使用那些其他的 **ClearToken** 字段。例如，为了与 ITU-T H.235.1 建议书一起使用本建议书，字段 **timestamp**、**random**、**generalID**、**sendersID** 和 **dhkey** 必须存在和使用，如由 H.235.1 安全概要所规定的。

网守 G 的网守 ID（GKID）必须被放在 CT_A→**sendersID** 内，但是 CT_A→**generalID** 必须掌握端点 A（CT_A）的端点标识符。

端点 A 必须检查 CT_A→**tokenOID** “I21”来识别 CT_A。端点 A 必须检查 **timestamp** 来检验已获得的 CT_A 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_A 被验证为是最新的，对于网守，端点 A 必须恢复 IV 并计算 EK_{AG} 和 KS_{AG}，如以上对网守 G 所描述的，在第 12 节中以 **challenge** 替代 Challenge-A 使用 CT_A→**challenge**。端点 A 必须解密 CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** 来获得 K_{AB}。

10.6 SETUP阶段

端点 A 必须检查 CT_A→**tokenOID** “I11”来识别 CT_A。端点 A 必须检查 timestamp 来检验已获得的 CT_A 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_A 被验证为是最新的，对于网守，端点 A 必须恢复 IV 并计算 EK_{AG} 和 KS_{AG}，如以上对网守 G 所描述的，使用 CT_A→**challenge** 作为 Challenge-A。端点 A 必须解密 CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** 来获得 K_{AG}。

如果接收到的 CT_A 被验证为是最新的，端点 A 能够发送一个 SETUP 消息给端点 B。这一 SETUP 消息包括 CT_B。依照 ITU-T H.235.1 建议书或 ITU-T H.235.3 建议书使用 K_{AB} 作为适用的共享秘密，SETUP 消息必须是安全的（认证和/或完整性保护）。为此 H.235.1 散列 ClearToken（不是 CT_B!）中的 **generalID** 不得使用，除非端点 A 已有一个可获得的 $EPID_B$（例如通过配置或从原来的通信中记忆）。如果端点 A 在 SETUP 中使用 generalID 的 $EPID_B$，则端点 A 必须接收在返回的呼叫信令消息中的 sendersID 的值作为真实的 $EPID_B$。

端点 B 必须检查 ClearToken 内的 **tokenOID**“I12”来识别 CT_B。

端点 B 必须检查 **timestamp** 来检验已获得的 CT_B 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_B 被验证为是最新的，对于网守，端点 B 必须恢复 IV 并计算 EK_{BH} 和 KSB_H，如第 12 节中所描述的，以 **challenge** 替代 Challenge-B 使用 CT_B→**challenge**。端点 B 必须解密 CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** 来获得 K_{AB}。

在 CT_B 被验证为是最新的情况下，端点 B 能够通过用 CALL-PROCEEDING、ALERTING 或 CONNECT 等适当地回复来进行呼叫的信号发送。在 CT_B 被发现不是最新或 SETUP 消息的安全性验证失败的情况下，端点 B 必须用 RELEASE-COMPLETE 和设置为安全性错误的 **ReleaseCompleteReason** 来回复，如 11.1/H.235.0 所定义的。

当将采用媒体安全性（见 6.1/H.235.6）时，端点 A 和端点 B 必须依照 8.5/H.235.6 交换 Diffie-Hellman 半密钥，并确定一个动态的基于对话的主密钥，然后从该密钥中可得出特定媒体的对话密钥。

端点 B 必须包括设置为 $EPID_A$ 的 **generalID** 和设置为 $EPID_B$ 的 **sendersID** 来保护去往 EP A 的任何 H.225.0 呼叫信令消息（例如呼叫进行、告警或连接）。

图 3 示出基本的通信流：

图 3/H.235.4－基本通信流（DRC2）

11 规程DRC3（域内环境）

本节中描述的规程在域内环境中适用，在这类环境中，主叫端点不支持 Diffie-Hellman 算法，而主叫域和被叫域中的网守都能够计算 DH 交换。在这样的环境下，会话密钥通过在始发网守和终接网守之间交换 DH 参数来计算。

11.1 GRQ/RRQ阶段

这一情形涵盖多个链接的网守。能够支持这一安全概要的端点必须通过包括一个单独的 ClearToken（其 **tokenOID** 设置为“I30”）指示在 **GRQ** 和/或 **RRQ** 期间的事实；任何在那个 ClearToken 的其他字段不应使用。愿意提供这一功能性的 H.235.4 可能的网守必须用 **GCF** 代替 **RCF** 回答，包括单独的 ClearToken，其 **tokenOID** 设置为“I30”，ClearToken 中的所有字段不使用。

11.2 ARQ阶段

在 EP A 使用 DRC3 呼叫 EP 端点 B 之前，端点 A 发送一个 **ARQ** 消息给 GK G，**ARQ** 消息包括一个单独的 ClearToken，其 **tokenOID** 设置为“I30”，在 ClearToken 内的所有其他字段不使用。

11.3 LRQ阶段

接收到由 EP A 发送的 **ARQ** 消息，因为 EP B 不属于 GK G 的域，所以 GK G 发送 **LRQ** 到 GK H 询问 EP B 的地址。GK G 检查 **ARQ** 消息携载的 ClearToken，发现 **tokenOID** 被设置为“I30”，如果 GK G 支持 DH 算法，则它采用确定 DRC3 将被选择的某些预先配置的原则。

然后 GK G 生成一个 **LRQ** 消息，该消息包含一个 ClearToken（在 CryptoHashedToken 内），其 **tokenOID** 被设置为“I30”，向 GK H 指示需要 DH 密钥算法协商。ClearToken 的 **dhkey** 字段用由 GK G 生成的主叫方的 DH 参数（g，p，g^x）填充，其他字段不使用。

然后 GK G 发送这一 **LRQ** 消息到 GK H。在 GK 群的情况下，GK G 发送 **LRQ** 消息到其紧邻的 GK，该 GK 依次发送 **LRQ** 消息到其紧邻的 GK。发送过程持续直到 **LCF** 消息最终到达 GK H。

对于组播的情况，**LRQ** 的 CryptoToken 内的 **generalID** 不得使用，如果 GK G 不能够位于远端端点 B，则 GK G 必须返回 **ARJ** 给端点 A。两个网守之间的通信必须按照 ITU-T H.235.1 建议书来保护安全。

如果 GK G 不支持概要，则 GK G 可自由选择是退回 DRC2 还是返回 ARJ 给端点 A。如果选择 DRC2，则包括 **LRQ** 阶段的所有后续阶段与 DRC2 中的那些阶段是相同的。

11.4 LCF阶段

在接收到来自 GK G 的 **LRQ** 消息后，认识到端点 A 和 B 都支持本建议书，GK H 必须如下所规定的，生成会话密钥 K_{AB}。

首先，GK H 生成一个随机的 Challenge-B，它将被设置成 CT_B→**challenge**，CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，然后使用基于 PRF 的密钥生成规程从加密密钥 K_{GH} 和 Challenge-B 中得到密钥材料 EK_{GH} 和补白密钥 KS_{GH}。

Challenge-B 必须在 CT_B→**challenge** 中设置，GK H 的网守 ID 必须在 CT_B→**sendersID** 中设置，EP B 的端点 ID 必须在 CT_B→**generalID** 中设置。如果 **LRQ** 在其端点标识符字段中具有端点 A 的端点 ID，则网守 H 必须将其复制到 CT_B→**h235Key**→**secureSharedSecret**→**generalID** 中，也必须将其复制到 CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID** 中。

然后 GK H 在 **LCF** 消息中创建两个 ClearTokens。其一是 CT_{HG}，用于 GK G，其 **tokenOID** 被设置为“I33”，另一个是 CT_B，用于 EP B，其 **tokenOID** 被设置为“I12”。GK H 生成被叫方的 DH 参数（g，p，g^y）。利用从 **LRQ** 消息中获得的主叫方的 DH 参数，GK H 必须计算会话密钥 $K_{AB} = g^{xy} \bmod p$。

最后，GK H 必须使用 EK_{BH} 和 KS_{BH} 作为 $ENC_{EK_{BH},KS_{BH},IV}$（K_{AB}）来加密 K_{AB}，将被加密的 K_{AB} 放置到 CT_B**→h235Key→secureSharedSecret→encryptedSessionKey** 中，将被叫方的 DH 参数放置到 CT_{HG} 的 **dhkey** 中。

增强型的 OFB（EOFB）加密模式（见 8.4/H.235.6）必须和秘密、特定端点的补白密钥 KS_{GH} 一起使用。可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）： 任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，网守 H 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_B**→h235Key→secureSharedSecret→ params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_B**→h235Key→secureSharedSecret→params→iv16** 内传送。

加密算法必须在 CT_B**→h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。对于 EOFB 加密算法，不得使用 **encryptedSaltingKey**。

GK H 发送 **LCF** 消息给 GK G。如果 GK 群存在，则 **LCF** 消息以中继的方式传送。沿着这一路径，每个 GK 从其上行紧邻的 GK 接收 **LCF** 消息，检查包含 CT_{HG} 的 **LCF** 消息，发送 **LCF** 消息给其下行紧邻的 GK。

如果 GK H 不支持 DH 算法，或 DRC3 不允许安全性政策，将发生返回 DRC2。因此，**LCF** 阶段和所有后续阶段与 DRC2 中的那些阶段是相同的。

11.5 ACF阶段

在接收到 **LCF** 消息后，认识到在单个 ClearToken 中的 **tokenOID** 被设置为“I33”，GK G 获得被叫方的 DH，按以下描述的方法创建一个 ClearToken 表示的 CT_A，其 **tokenOID** 被设置为“I11”。

首先，GK G 生成一个随机的 Challenge-A，它将被设置成 CT_A**→challenge**，CT_A**→h235Key→secureSharedSecret→keyDerivationOID** 必须掌握“AnnexI-HMAC-SHA1-PRF”，然后使用基于 PRF 的密钥衍生规程从加密密钥 K_{AG} 和 Challenge-A 中得到密钥材料 EK_{AG} 和补白密钥 KS_{AG}。

然后，GK G 使用在 **LRQ** 阶段保留的主叫方的 DH 参数，和被叫方的 DH 参数一起，计算会话密钥 $K_{AG} = g^{xy} \bmod p$。

而后 GK G 从 **LCF** 消息复制 ClearToken CT_B 到 **ACF** 消息中，其 **tokenOID** 被设置为“I12”。

最后，GK G 必须使用 EK_{AG} 和 KS_{AG} 作为 $ENC_{EK_{AG},KS_{AG},IV}$（K_{AB}）来加密 K_{AB}，将被加密的 K_{AB} 放置到 CT_A**→h235Key→secureSharedSecret→encryptedSessionKey** 中，从 **LCF** 消息复制 ClearToken CT_B 到 **ACF** 消息中。

可适用的加密算法有（见表 6/H.235.6）：

— 在 EOFB 模式中使用 OID“Y1”的 DES（56 比特）：任选；

— 在外部 EOFB 模式中使用 OID“Z1”的 3DES（168 比特）： 任选；

— 在 EOFB 模式中使用 OID“Z2”的 AES（128 比特）：缺省或建议的；

— 在 EOFB 模式中使用 OID“X1”的 RC2 兼容的（56 比特）：任选。

对于 EOFB 加密模式，GK G 必须生成一个随机初始值 IV。对于 OID“X1”、OID“Y1”和 OID“Z1”，IV 有 64 比特，必须在 CT_A→**h235Key→secureSharedSecret→ params→iv8** 内传送；但是对于 OID“Z2”，IV 有 128 比特，必须在 CT_A→**h235Key→secureSharedSecret→params→iv16** 内传送。加密算法必须在 CT_A→**h235Key→secureSharedSecret→algorithmOID**（“X1”、“Y1”、“Z1”或“Z2”）中指示。

如果发现 ClearToken（在 **LCF** 内）**tokenOID** 是“I23”，可以判断为返回 DRC2 已经发生，GK G 可自由选择是否接受 GK H 的安全性政策。如果它接受，则 **ACF** 阶段和所有后续阶段将与 DRC2 中的那些阶段是相同的。否则，用一个对应的拒绝消息响应，通过设置拒绝理由为 securityDenial 来指示安全性失效。

GK G 发送 **ACF** 消息给 EP A。

11.6 SETUP阶段

端点 A 必须检查 CT_A→**tokenOID** “I11”来识别 CT_A。端点 A 必须检查 timestamp 来检验已获得的 CT_A 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_A 被验证为是最新的，对于网守，端点 A 必须恢复 IV 并计算 EK_{AG} 和 KS_{AG}，如以上对网守 G 所描述的，使用 CT_A→**challenge** 作为 Challenge-A。端点 A 必须解密 CT_A→**h235Key→secureSharedSecret→encryptedSessionKey** 来获得 K_{AG}。

如果接收到的 CT_A 被验证为是最新的，端点 A 能够发送一个 SETUP 消息给端点 B。这一 SETUP 消息包括 CT_B。依照 ITU-T H.235.1 建议书或 ITU-T H.235.3 建议书使用 K_{AB} 作为适用的共享秘密，SETUP 消息必须是安全的（认证和/或完整性保护）。为此 H.235.1 散列 ClearToken（不是 CT_B!）中的 **generalID** 中的 **generalID** 不得使用，除非端点 A 已有一个可获得的 $EPID_B$（例如通过配置或从原来的通信中记忆）。如果端点 A 在 SETUP 中使用 generalID 的 $EPID_B$，则端点 A 必须接收在返回的呼叫信令消息中的 **sendersID** 的值作为真实的 $EPID_B$。

端点 B 必须检查 ClearToken 内的 **tokenOID**“I12”来识别 CT_B。

端点 B 必须检查 timestamp 来检验已获得的 CT_B 是否是最新的。更进一步的安全性检查必须检验 ClearToken 的 **generalID** 和 **sendersID** 以及 **SecureSharedSecret** 内的 **generalID**。如果接收到的 CT_B 被验证为是最新的，对于网守，端点 B 必须恢复 IV 并计算 EK_{BH} 和 KSB_H，使用 CT_B→**challenge** 作为 Challenge-B。端点 B 必须解密 CT_B→**h235Key→secureSharedSecret→encryptedSessionKey** 来获得 K_{AB}。

在 CT_B 被验证为是最新的情况下，端点 B 能够通过用 CALL-PROCEEDING、ALERTING 或 CONNECT 等适当地回复来进行呼叫的信号发送。在 CT_B 被发现不是最新或 SETUP 消息的安全性验证失败的情况下，端点 B 必须用 RELEASE-COMPLETE 和设置为安全性错误的 **ReleaseCompleteReason** 来回复，如 11.1/H.235.0 所定义的。

当将采用媒体安全性（见 6.1/H.235.6）时，端点 A 和端点 B 必须依照 8.5/H.235.6 交换 Diffie-Hellman 半密钥，并确定一个动态的基于对话的主密钥，然后从该密钥中可得出特定媒体的对话密钥。

端点 B 必须包括设置为 $EPID_A$ 的 **generalID** 和设置为 $EPID_B$ 的 **sendersID** 来保护去往 EP A 的任何 H.225.0 呼叫信令消息（例如呼叫进行、告警或连接）。

图 4 示出基本的通信流：

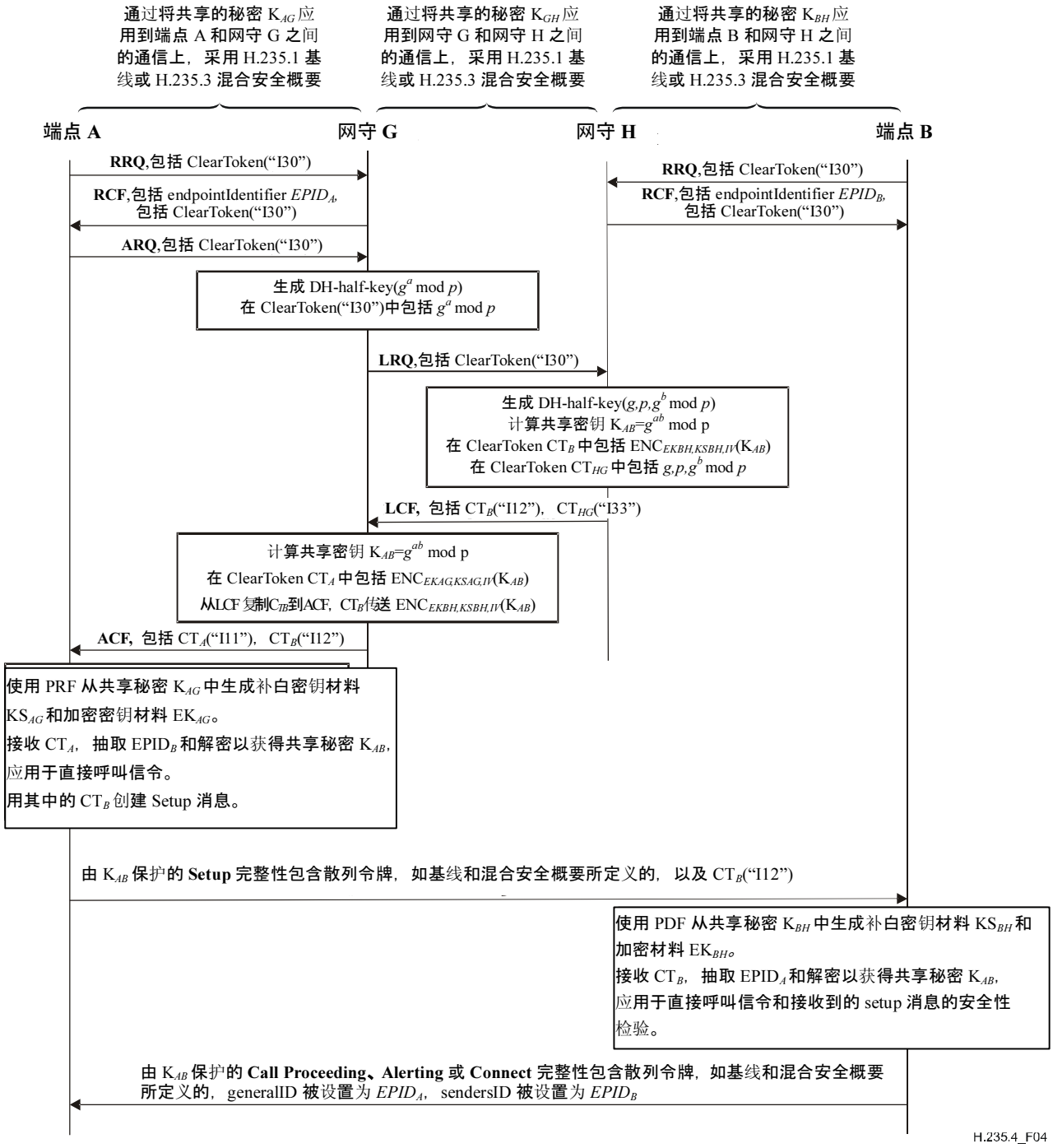

图 4/H.235.4－DRC3中的通信流

12 基于PRF的密钥衍生规程

本节描述定义如何从共享的秘密和其他参数中得出密钥资料的规程。

本节中的规程允许从一个共享密钥计算除加密密钥和补白密钥。规程是统一的，与哪一个共享秘密（K_{AG}、K_{BH}或K_{GH}）无关。

为了获得目标密钥材料（e.g.，EK_{AG}），PRF（见第 10 节/H.235.0）必须与从表 1 中得到的参数一起使用，其中 *inkey* 参数被设置为对应的共享密钥（e.g.，K_{AG}），*label* 必须被设置为对应的常数（例如 0x2AD01C64 || **challenge-A**），其中||表示串联。*outkey_len* 必须被设置为目标密钥材料所需长度，这取决于选择的加密算法。

注 — 对于 EK_{AG}、KS_{AG}、EK_{BH}和 KS_{BH}，32 比特常量整数（即 0x2AD01C64 等）从 *e*（即 2.7182...）的十进制数中得出，对于 EK_{GH}和 KS_{GH}，32 比特常量整数从 π（即 3.14159...）的十进制数中得出。对于 EK_{AG}、EK_{BH}、KS_{AG}和 KS_{BH}，32 比特整数从 9 个十进制数块（分别是第 1、2、4、7 个数块）中得出。EK_{GH}从 π 的第一个 10 位十进制数中得出，而 KS_{GH}从 π 的后续 8 位十进制数中得出。

表 1/H.235.4－从共享秘密中计算加密和补白密钥

目标密钥	PRF inkey	常量|| challenge
EK_{AG}	K_{AG}	0x2AD01C64 || **Challenge-A**
KS_{AG}	K_{AG}	0x150533E1 || **Challenge-A**
EK_{BH}	K_{BH}	0x1B5C7973 || **Challenge-B**
KS_{BH}	K_{BH}	0x39A2C14B || **Challenge-B**
EK_{GH}	K_{GH}	0x54655307 || **Challenge-G**
KS_{GH}	K_{GH}	0x35855C60 || **Challenge-G**

13 基于FIPS-140的密钥衍生规程

本节可描述定义如何从一个共享秘密和其他参数中使用 FIPS-140 适应性的密码模型得出密钥资料的规程。这有待进一步研究。

14 对象标识符一览

表 2/H.235.4－H.235.4所使用的对象标识符

对象标识符参考符	对象标识符值	描 述
“I10”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 48}	在规程 DRC1 中 GRQ/RRQ、GCF/RCF 和 ARQ 期间使用，让 EP/GK 指示支持 DRC1。
“I11”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 49}	对于 ClearToken tokenOID，在规程 DRC1、DRC2 和 DRC3 中使用，指示 ClearToken CT_A 掌握一个主叫方的端到端密钥。
“I12”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 50}	对于 ClearToken tokenOID，在规程 DRC1、DRC2 和 DRC3 中使用，指示 ClearToken CT_B 掌握一个被叫方的端到端密钥。
“I13”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 52}	对于网守间 ClearToken tokenOID，在规程 DRC1 中使用，指示 ClearToken CT_{HG} 掌握始发网守的加密密钥。
“I20”	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 53}	在规程 DRC2 中 GRQ/RRQ、GCF/RCF 和 ARQ 期间使用，让 EP/GK 指示支持 DRC2。
“I23”	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 56}	对于网守间 ClearToken CT_{HG} tokenOID，在规程 DRC2 中使用，指示 ClearToken 掌握始发网守的加密密钥。
“I30”	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 34}	对于在 GRQ/RRQ、GCF/RCF 和 ARQ 期间的单独的 ClearToken 中使用，指示支持 DRC3。 对于在 LRQ 期间的单独的 ClearToken 中使用，指示携载主叫方的 DH 参数。
“I33”	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 37}	对于在 LCF 期间的单独的 ClearToken 中使用，指示携载被叫方的 DH 参数。
“Annex I -HMAC-SHA1-PRF”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 51}	对于 V3KeySyncMaterial 内的 keyDerivationOID，在规程 DRC1、DRC2 和 DRC3 中使用以指示在第 12 节中使用 HMAC-SHA1 伪随机函数应用的衍生方法。

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