国 际 电 信 联 盟

ITU-T H.235.3

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：混合安全概要

ITU-T H.235.3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.235.3建议书

H.323安全性：混合安全概要

摘　要

本建议书的目的是描述用于 ITU-T H.235.0 建议书的第 2 版或更高版本的一个有效的、可升级的基于 PKI 的混合安全概要。在此包含的混合安全概要通过采用来自 ITU-T H.235.2 建议书的数字签名和采用来自 ITU-T H.235.1 建议书的基线安全概要，利用 ITU-T H.235.1 和 H.235.2 建议书中的安全概要。

在 H.235 子系列的较早版本中，该概要被包含在附件 F/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.235.3 建议书。

关键词

认证，证书，数字签名，加密，完整性，密钥管理，多媒体安全性，安全概要。

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，国际电联已经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.235.3建议书

H.323安全性：混合安全概要

1 范围

本建议书的目的是描述用于 ITU-T H.235.0 建议书的第 2 版或更高版本的一个有效的、可升级的基于 PKI 的混合安全概要。在此包含的混合安全概要通过采用来自 ITU-T H.235.2 建议书的数字签名和采用来自 ITU-T H.235.1 建议书的基线安全概要，利用 ITU-T H.235.1 和 H.235.2 建议书中的安全概要。

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, version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals*.

– ITU-T Recommendation H.235, version 2 (2000), *Security and encryption for H-series (H.323 and other H.245-Based) multimedia terminals.*

– 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.235.2 (2005), *H.323 security: Signature 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.245 (2005), *Control protocol for multimedia communication.*

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

– ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control.*

– ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

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

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

– ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

– ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

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

2.2 资料性参考文献

[ISO|IEC 14888-3] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix; Part 3: Certificate-based mechanisms*.

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm*.

3 术语和定义

出于本建议书的目的，第 3 节/H.323、第 3 节/H.225.0 和第 3 节/H.245 中给出的定义适用。本建议书中使用的一些术语也在 ITU-T X.800 建议书| ISO 7498-2、X.803 建议书| ISO/IEC 10745、X.810 建议书| ISO/IEC 10181-1 和 X.811 建议书| ISO/IEC 10181-2 和 H.235.0 中定义。

4 符号和缩写

本建议书采用下列缩写：

ALG	应用层网关
ASN.1	抽象句法记法 1
BRJ	带宽拒绝
BRQ	带宽请求
CA	认证机构
CRL	证书撤销一览表
DB	数据库
DH	Diffie-Hellman
DN	可识别名
EP	端点
GCF	网守确认
GK	网守
GKID	网守标识符
GKSP	网守安全性处理器

GRJ	网守拒绝
GRQ	网守请求
HMAC	散列消息认证码
ICV	综合检验值
ID	标识符
IP	网际协议
LDAP	轻便式号码簿接入协议
LRQ	定位请求
MCU	多点控制单元
MD5	消息类别 5
NAT	网络地址解析
OID	对象标识符
PDU	协议数据单位
PKI	公钥基础设施
RAS	注册、认可和状态
RCF	注册确认
RRJ	注册拒绝
RRQ	注册请求
RSA	Rivest、Shamir 和 Adleman 加密算法
RTP	实时传输协议
SHA	安全散列算法
UDP	用户数据报协议
URQ	未注册请求
VoIP	在网际协议上的话音

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。

混合安全概要使用来自 ITU-T H.235.1 和 H.235.2 建议书的术语和定义。

虽然消息完整性业务始终也提供消息认证，但反过来却不一定始终正确。对于仅认证方式，确保的完整性仅跨越消息字段的某些子集。这适用于通过非对称手段（例如数字签名）所实现的完整性业务。因此，实际上，组合的认证和完整性业务采用相同的密钥资料而未引进安全性弱点。

该安全概要潜在地具有很多终端的环境中适用，其中静态密码/对称密钥分配不灵活，例如在大规模或全球规模的情况下。该安全概要假定可以获得具有指定的证书和私钥/公钥、号码簿等的公钥基础设施。另外，该安全概要在适用时采用了对称加密技术。

该安全概要引入了术语发送的“第一个”消息和“最后一个”消息。第一个消息（可能也是最后一个消息）的保护与剩下的其他消息的安全保护不同。

发送的“第一个”消息理解为在两个 H.323 实体之间流动的消息，确定一个安全的语境。它使得对称密钥资料对于两个实体都是可获得的，例如，标记呼叫的开始。对于 H.225.0 RAS，第一个消息是 RRQ 及相关的响应消息。对于使用快速起动的 H.225.0 呼叫信令，第一个消息是 SETUP 和 CONNECT。

“最后一个”消息终止确定的安全的语境。确定的密钥资料必须被破坏。对于 H.225.0 RAS，最后一个消息是 URQ 及相关的响应消息，而对于使用快速起动的 H.225.0 呼叫信令，最后一个消息是 RELEASE-COMPLETE。

6 概述

本建议书描述有效的、可升级的基于 PKI 的混合安全概要，它采用来自 ITU-T H.235.2 建议书的数字签名和来自 ITU-T H.235.1 建议书的基线安全概要。建议本建议书作为一个选项。为改进安全性或每当需求时，H.323 安全性实体（终端、网守、网关、MCU 等）可以实施该混合安全概要。

在此节中“混合”的概念必须意味着来自 ITU-T H.235.2 建议书中的签名概要的安全性规程实际上应用在无足轻重的意义上，数字签名仍遵循 RSA 规程。但是，仅在绝对必需的时候才采用数字签名，否则使用来自 ITU-T H.235.1 建议书中的基线安全概要的高度有效的对称安全技术。

混合安全概要适用于“全球”IP 电话。该安全概要在严格应用时克服了 ITU-T H.235.1 建议书的简单的基线安全概要的局限。此外，这一安全概要克服了 ITU-T H.235.2 建议书的某些缺陷，如需要较高的带宽和对于处理增加了性能需要。例如，混合安全概要不取决于不同域的逐段转接的互相共享秘密的（静态）管理。因而，用户可更容易地选择其 VoIP 提供商。因此这一安全概要同样支持某一类型的用户移动性。它仅当必需时将不对称密码数应用到签名和证书中，否则使用更简单和更有效的对称技术。对于 H.245 消息的完整性，它提供 H.245 消息的隧道传送，也实施某些不可否认消息的提供。

混合安全概要要求 GK 选路模型并基于 H.245 隧道传送技术。对非 GK 选路模型的支持有待进一步研究。

本概述提供的特征如下：

对于 RAS，H.225.0 和 H.245 消息：

— 所需实体的用户认证不考虑该消息所历经的应用等级分段转接个数。

注 1 — 在此，分段转接在涵义上理解为可信的 H.235 网络单元（例如 GK、GW、MCU、代理服务器、防火墙）。这样，伴随对称技术所使用的应用级逐段转接安全性不提供终端之间真正的端到端安全性。

— 到达实体的消息的全部分段或核心分段（字段）的完整性不考虑该消息所历经的应用等级分段转接个数。消息自身的完整性使用严格生成的随机数是任选的。

— 应用等级逐段转接消息认证、完整性和不可否认对整个消息提供这些安全性业务。

— 使用可获得的公钥基础设施，用户可选择其服务提供商。对话密钥分配的密钥管理在混合安全概要中很好地整合了。

通过提供以上适当方式的安全性业务可以抵御若干攻击，它们包括：

— 中间人攻击：当中间人处于应用等级分段转接之间，即强占路由器时，应用等级逐段转接消息认证和完整性可以防止此类攻击。

— 重放攻击：使用时间标记和序列号可以防止此类攻击。

— 电子欺骗：用户认证可以防止此类攻击。

— 连接劫持：对每个信令消息使用认证/完整性可以防止此类攻击。

该安全概要假定是采用快速连接呼叫信令方法的 GK 选路呼叫模型。H.245 呼叫控制消息安全地在 H.225.0 呼叫信令消息中隧道传送，从而继承 H.225.0 安全保护机制。

签名安全概要允许在 H.225.0 设备小心中安全地隧道传送 H.245 呼叫控制 PDU。H.245 密钥更新和同步机制要求将被发送的密钥更新 FACILITY 消息的隧道传送，而且很有用，例如对于持续时间很长的呼叫。

表 1 中的斜阴影部分表示由混合安全概要使用的安全机制。

注 2 — RSA 认证和 MD5 散列不是该安全概要的一部分。

ITU-T H.235.6 建议书的话音加密安全概要（见 6.1/H.235.6）可任选地与混合安全概要一起使用。它的使用作为呼叫建立信令的一部分协商。

表 1/H.235－混合安全概要概述

安全性业务	呼叫功能			
	RAS	**H.225.0**	**H.245（注 3）**	**RTP**
认证	RSA 数字签名（SHA1） HMAC-SHA1-96	RSA 数字签名（SHA1） HMAC-SHA1-96	RSA 数字签名（SHA1） HMAC-SHA1-96	
不可否认	（仅在第一个消息上可能）	（仅在第一个消息上可能）		
完整性	RSA 数字签名（SHA1） HMAC-SHA1-96	RSA 数字签名（SHA1） HMAC-SHA1-96	RSA 数字签名（SHA1） HMAC-SHA1-96	
机密性				
接入控制				
密钥管理	证书分配 认证的 Diffie-Hellman 密钥交换	证书分配 认证的 Diffie-Hellman 密钥交换		

注 1 — 混合安全概要必须也被其他 H.235 实体（例如网守、网关和 H.235 代理服务器）所支持。

注 2 — 证书中有效的密钥使用比特也能确定由终端所提供的安全性业务（例如所断言的不可否认）。

注 3 — 在 H.225.0 快速连接内部隧道传送的 H.245 或嵌入的 H.245。

本建议书可应用消息完整性保护跨越整个消息。对于 H.225.0 RAS，完整性保护覆盖整个 RAS 消息；对于呼叫信令，完整性保护则覆盖包括在 Q.931 头中的整个 H.225.0 呼叫信令消息。

对于认证，用户应使用公钥/私钥签名方法。该方法一般提供较好的呼叫完整性和不可否认。

本建议书不描述以下规程：来自委托中心的注册、证书和证书分配及私钥/公钥指派、目录查询业务、特定的 CA 参数、证书撤销、密钥对更新/恢复以及其他证书操作或管理规程诸如证书或公钥/私钥与证书在终端中的交付及安装。这些规程可以利用不在本建议书范围内的手段进行。

通过估计该消息中签署的安全性对象标识符赋值（**tokenOID 及 algorithmOID**；也见第 10 节/H.235.2）所涉及的通信实体能够隐含地确定 ITU-T H.235.1 建议书基线安全概要、ITU-T H.235.2 建议书签名概要或者该混合安全概要的用法。

6.1 H.323需求

假定实施该签名概要的 H.323 实体支持以下 H.323 特征：

— 快速连接；

— H.245 隧道传送；和

— GK 选路模型。

6.2 认证和完整性

本建议书使用以下术语以提供安全性业务：

Authentication and integrity 认证和完整性：此为组合的安全性业务，在支持用户认证的同时支持消息完整性。当用户通过私钥准确地数字化签署某些数据块时，用户就进行了认证。除此之外，可以保护消息抵御窜改。这两类安全性业务由同一种安全性机制提供。组合的认证和完整性仅在逐段转接基础上是可行的。

注 — 当采用数字签名时，不可否认安全性业务也可以支持；这也取决于证书中签署密钥的密钥使用比特的设置（也见 RFC 3280）。

用该概要描述下列规程。

为了提供 RAS、Q.931 和 H.245 消息的认证、完整性和不可否认，规程 IV 基于使用私钥/公钥对的数字签名。只要请求不可否认和更为高级的完整性，终端就需要使用该方法。

依据安全性政策，认证可以是单向的或相互的（即在相反方向上使用认证/完整性，并由此提供更高的安全性）。首选的安全模式将具有互认证。

网守从终端/对等网守接收的 RAS/呼叫信令消息中检测到无效的认证和无效的完整性确认可以采用相应的拒绝消息响应。通过设置拒绝理由为 **securityDenial** 或根据 11.1/H.235.0 来采用其他适当的安全误差编码指示安全性失效。根据识别攻击的能力和重新激活它的最适当的方法，接收到具有未定义的对象标识符（**tokenOID、algorithmOID**）的安全 **xRQ** 的网守应用一个非安全的 xRJ 响应，用设置为 securityDenial 的理由拒绝，或可丢弃那个消息。端点必须丢弃接收到的非安全的消息、暂停时间，可再次尝试考虑选择不同的 OID。否则，接收具有未定义的对象标识符（**tokenOID、algorithmOID**）的安全的 H.225.0 SETUP 消息的网守可用非安全的 RELEASE COMPLETE 响应，用设置为 **securityDenied** 的理由拒绝，或可丢弃那个消息；而接收到具有未定义的对象标识符（**tokenOID、algorithmOID**）的安全的 H.225.0 FACILITY 的网守应用一个非安全的 xRJ 响应，用设置为 **undefinedReason** 的理由拒绝，或可丢弃那个消息。类似地，遭遇的安全性事件应记入日志。作为返回的响应，发送者可提供单个令牌中的可接受的证书的清单，以便于接收者选择适当的一个。

存在隐含的 H.235 信令，表明使用了规程 IV，并根据对象标识符的值表明采用的安全性机制（也见第 13 节）和插入的消息字段。本文中对象标识符是通过符号化的字母（例如“A”）引用的。

本概要不使用 H.235 ICV 字段，而是当提到 H.235.2 时在 **cryptoSignedToken** 中 **token** 的 **signature** 字段中放置密码完整性检测值，或当提到 H.235.1 时在 **CryptoToken** 的散列字段中放置完整性检验值。

7 规程IV

只要规程 IV 从事于逐段转接的安全性，就必须依从以下规程。本规程结合了第 7 节/H.235.1 的规程 I 和第 7 节/H.235.2 的规程 II。

对于第一个消息，包括在每个方向上发送的相应的响应，ITU-T H.235.2 建议书的规程 II（逐段转接认证和完整性，见第 7 节/H.235.2）必须伴随着下列设置一起使用：

— OID“A1”取代 OID“A”，OID“S1”取代 OID“S”。这些 OID 的使用允许识别混合安全概要。

— **tokenOID** 中的 **algorithmOID** 必须设置为“W”，指示使用 RSA-SHA1 签名。

— **signature** 必须包含 ASN.1 编码的 RSA 签名（见第 12 节/H.235.2）。

— **certificate** 应包含发送者的用户证书，否则接收者不能获得；**type** 必须掌握 OID “W”，指示包括的 RSA-SHA1 证书或 OID“P”（见第 20 节/H.235.2），指示 **certificate** 掌握一个 URL。

在单一的管理域的情况下，“第一个消息/响应”定义为等于初始的 H.225.0 RAS 消息/响应；这通常是 GRQ/GCF 或 RRQ/RCF。在多个管理域的情况下，在每个域内的“第一个消息/响应”定义如上；域之间的第一个消息定义被为 SETUP。

每当在一个消息中传送一个数字证书，为了阻止中间人攻击，依据第 14 节/H.235.2 中的规程，接收消息的实体都必须对着证书的标识符检验发送者的标识符。

发送者和接收者交换和计算经认证的 Diffie-Hellman 秘密比特串。表 4/H.235.6 提供 Diffie-Hellman 组参数的实例，出于安全理由，建议每当可能时采用 1024 比特素数。不管话音加密概要采用与否，对于每条分段路径，都必须计算 Diffie-Hellman 秘密。

通过取出最不重要的 160 比特，两方都可从两方都计算的通用比特串中抽取一个 160 比特的秘密。结果的 160 比特秘密作为 ITU-T H.235.1 建议书中使用的口令/共享秘密作用。

在网守在不同的管理域中的情况下，对于 H.225.0 呼叫信令，发送者和接收者必须在每个方向上使用两个令牌：

— **CryptoToken** 中的 **ClearToken**，它用于极端在终端中共享的媒体密钥（见 8.5/H.235.6）。这仅当要采用话音加密时才必需。

— 对于信令链路的保护，一个单独的 **ClearToken** 用于计算链路密钥，该密钥在发送者和接收者之间共享。该链路密钥取代 ITU-T H.235.1 建议书中的在网守中共享的口令。那个 **ClearToken** 的 **tokenOID** 必须设置为“Q”，指示使用 Diffie-Hellman 和混合安全概要。链路密钥的计算以与媒体密钥的计算一样的方式进行（见 8.5/H.235.6）。

注 1 — 对于直接选路环境，发送者/接收者实体与终端对应。对于 GK 选路环境，当媒体密钥在端到端的基础上共享时，链路密钥在每对对等网守之间逐段转接共享。

在 GK 选路的环境下，GK 必须从端点向下一个段前送接收到的 Diffie-Hellman 令牌。

对于在每个方向上的除了第一个消息/响应之外的所有消息，必须使用 H.235.1 规程 I（见第 7 节/H.235.1）。这在多个网守位于一个管理域内的情况下也适用。在这一情况下，不需要对称密钥管理，H.235.1 就已经足够。

当照顾到 **sendersID** 和一般 ID 的受限制的使用时，本建议书可与 H.235 第 1 版系统一起使用，如第 19 节/H.235.2 中所描述的。

预期网守应从特定的固定端点仅接收一个单一的 **RRQ**，它包括具有数字签名的 DH-token。然而，**RCF/RRJ** 消息的丢失或延迟可导致使用另一个标记的 **RRQ** 重放。

在对应的注册消息没有及时到达端点的情况下，端点可进行另一个尝试。为此，端点必须使用最近的 DH 令牌，但使用一个新的号码和新的时间标记。

对于特殊的固定端点，不管 GK 是否已经有一个可获得的共享秘密，网守必须使用最近接收到的签字的 **RRQ** 消息和从那个 DH 令牌得到共享的秘密。因此，GK 必须用最近得到的秘密重写任何已经存在的共享秘密。GK 必须用一个签字的 **RCF** 响应，该 **RCF** 掌握响应 DH 令牌。更适宜地，响应 DH 令牌应重新再生成。

注 2 — 密钥更新的建议的和首选的方法是使用 FACILITY 消息，如第 9 节所描述的。然而，认识到，密钥更新可使用另一个附加的具有新 DH 令牌的签字的 **RRQ** 完成。

注 3 — 拥有共享秘密的网守必须用 HMAC 保护响应消息响应 HMAC 保护 **RRQ**（依照 ITU-T H.235.1 建议书）。

8 并发呼叫的安全性关联

对于固定的实体对使用单个呼叫信令信道并行处理几个独立的呼叫的情况，提供了最优化的方法。定义跨越多个并发呼叫的安全性关联，而不是每个呼叫确定几个链路密钥。

更好的是，只要呼叫信令信道存在，安全性关联在固定的实体对之间跨越所有呼叫。实体在 SETUP 内使用 **multipleCalls** 标记来指示在单个呼叫信令连接上发送多个呼叫信令的性能（见 7.3/H.323）。

如果使用单个呼叫信令连接，那么只有一个通用链路密钥需要确定，见图 1。

另一方面，如果在 SETUP 内没有设置 **multipleCalls** 标记，那么对于每个呼叫，必须单独计算链路密钥。

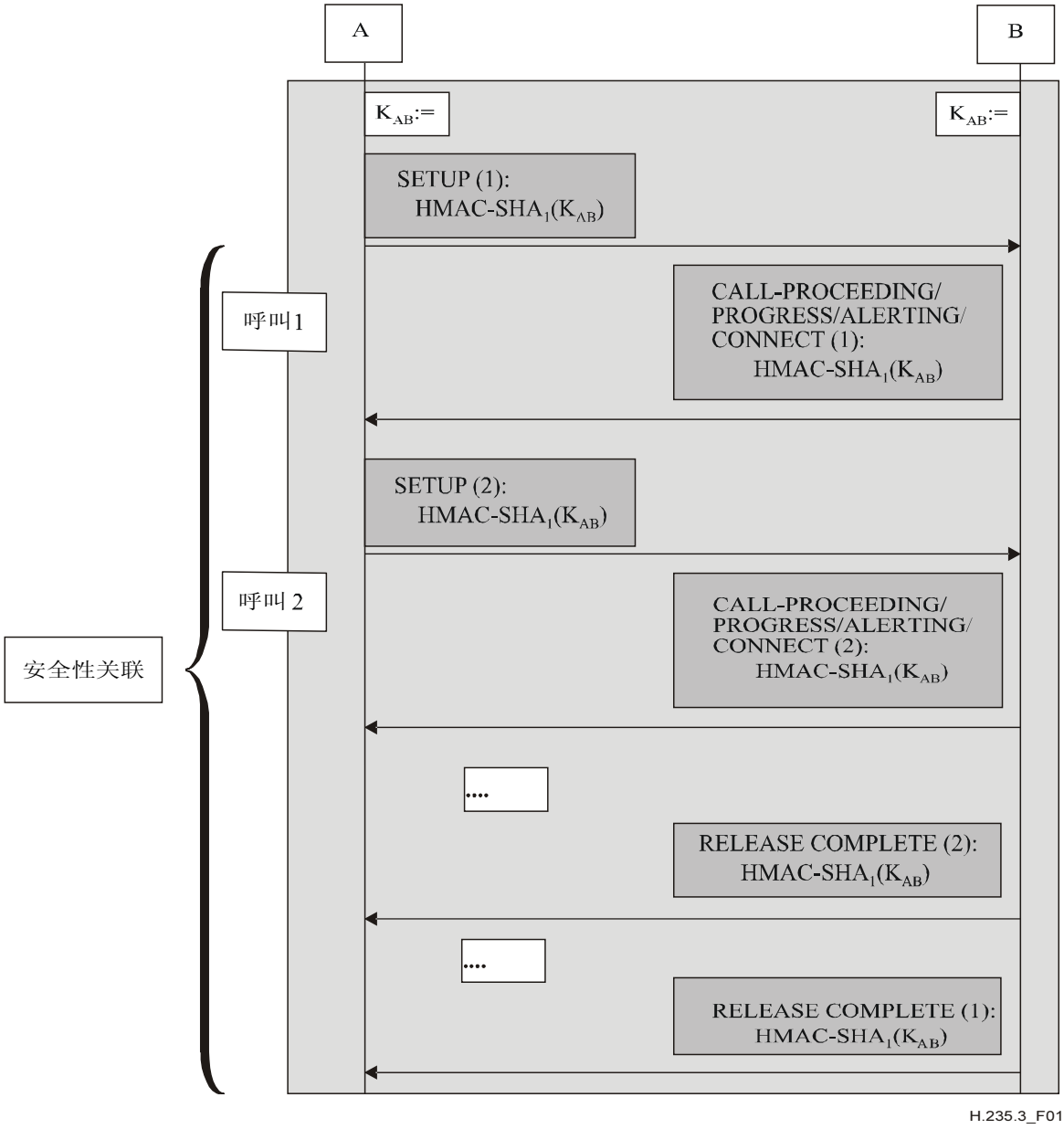


图 1/H.235.3－并发呼叫的安全性关联

9 密钥更新

任选的密钥更新程序允许通信实体用新密钥（GK 或终端）更新当前使用的对话密钥。这样的密钥更新应由任何一个感觉需要它的实体初始化。密钥更新可由折中的对话密钥（察觉对话密钥有或将要不安全）或其他安全政策准则激活。这些方面都超出了本建议书的范围。

发起人用 FACILITY 消息调用密钥更新。密钥更新的 FACILITY 消息发送一个新的 Diffie-Hellman 令牌、一个任选的数字证书和发起人的数字签名。基于 FACILITY 消息的接收，接收者用一个类似的 FACILITY 消息传送其 Diffie-Hellman 令牌、一个任选的数字证书和接收者的数字签名来回复。基于密钥更新程序的完成，发起人和应答者必须使用计算出来的新的链路密钥。

— FACILITY 内 **ClearToken** 的 **tokenOID** 必须设置为“Q”，指示使用 Diffie-Hellman 和混合安全概要。链路密钥的计算以与媒体对话密钥的计算同样的方式进行（见 8.5/H.235.6）。

依照 H.235.2 规程 II，必须保护出于密钥目的更新的 FACILITY 消息。出于密钥更新的目的，不得采用没有传送的 Diffie-Hellman 令牌的任何其他 FACILITY 消息，依照第 7 节/H.235.1 规程 I，必须保护这些消息。

10 椭圆曲线技术的使用

有待进一步研究。

11 图解实例

图 2 和 F.3 中的下列图表图解说明本建议书在基本消息流中的使用。注意图表并没有显示完整的消息流，为简便起见，省略了几个消息。涉及签名概要 H.235.2 的消息用浅灰色突出，而深灰色表示涉及基线概要 H.235.1 的消息。图强调了每个消息（H.235 CryptoToken、Token）中（最重要的）安全性部分，而省略了细节。

图 2 中的流程图图解说明在一个管理域内只有一个网守的情况下的基本消息流。假定所有涉及的终端都知道网守证书，而且终端同样知道网守证书，则不需要在注册规程期间在频带内发送证书。

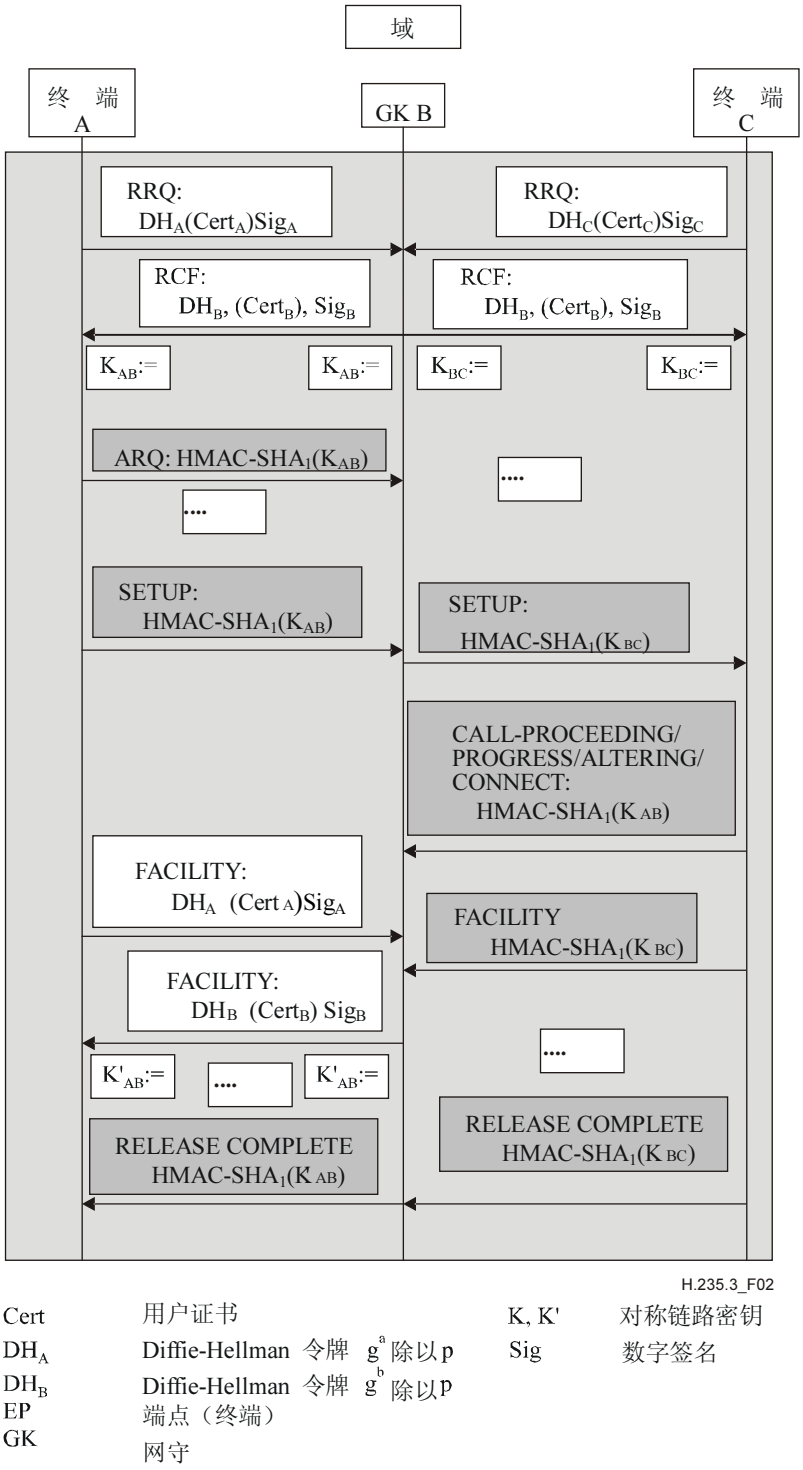


图 2/H.235.3－单一管理域中的流程图

注 1 — 当呼叫信令消息 SETUP 和 CALL PROCEEDING/PROGRESS/ALERTING/CONNECT 包括 faststart 令牌（见 8.1.7/H.323）时，图 2 和图 3 也包含了快速起动规程。否则，依照 7.3.1/H.323，假定为非快速起动模式。图 2 也使用 FACILITY 示出终端 A 和网守 B 之间的密钥更新规程。

图 3 示出在不同管理域的情况下的消息流的例子。如图 2 图解说明的，当混合安全概要在终端与网守之间的每个域内适用时，混合安全概要在呼叫确定阶段在两个域之间也可适用。

注 2 — 图 3 省略了在边界单元（BE）之间的通信和 GK 到 BE 之间的任何通信。图 3 也用 FACILITY 示出了两个域之间的密钥更新规程。

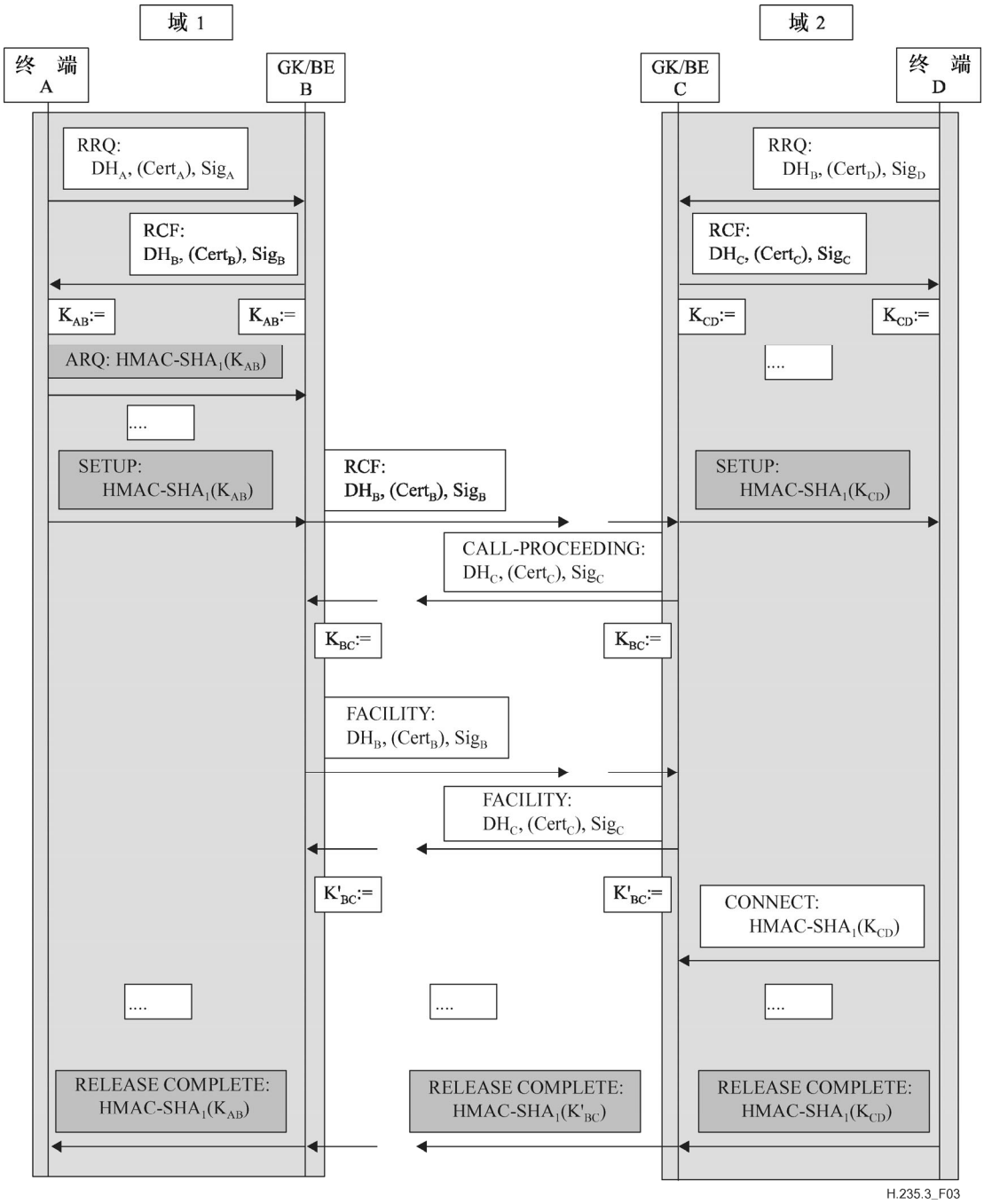


图 3/H.235.3－多个管理域中的流程图

12 组播特性

H.225.0 组播消息，诸如 **GRQ** 或 **LRQ**，依据 **generalID** 未予设置场合下的规程 II 必须包括 **CryptoToken**。当此类消息单播发送时，那么该消息也必须包括具有 **generalID** 设置的 **CryptoToken**。

13 安全信令消息一览

根据情况和实际的消息，如以下所指示的，规程 IV 采用了 H.235.1 的规程 I 或 H.235.2 的规程 II。

13.1 H.225.0 RAS

H.225.0 RAS 消息	H.235 信令字段	认证和完整性	不可拒绝
GatekeeperRequest、GatekeeperConfirm、GatekeeperReject，如果采用 GK 发现的话；RegistrationRequest，RegistrationConfirm，RegistrationReject，如果不采用 GK 发现的话	CryptoToken，ClearToken	过程 II	规程 II
任何其他的 RAS 消息（注 2）	CryptoToken	规程 I	
注 1 — 对于单播的消息，必须在使用的 **CryptoToken** 中用安全字段适用规程 II。 注 2 — GK 发现和组播消息不发送。			

13.2 H.225.0呼叫信令（单个管理域）

H.225.0 呼叫信令消息	H.235 信令字段	认证和完整性	不可拒绝
Setup-UUIE, Connect-UUIE (注 1), Facility-UUIE (注 2), Alerting-UUIE, CallProceeding-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken，ClearToken	规程 I	
Facility-UUIE (注 3)	CryptoToken	规程 II	规程 II
注 1 — 假定任一消息在每个方向上都是第一个。 注 2 — 不用于密钥更新。 注 3 — 用于密钥更新。			

13.3 H.225.0呼叫信令（多个管理域）

H.225.0 呼叫信令消息	H.235 信令字段	认证和完整性	不可拒绝
Setup-UUIE, Connect-UUIE (注 1), Alerting-UUIE (注 2), CallProceeding-UUIE, Facility-UUIE (注 3), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE	CryptoToken， ClearToken	规程 II	规程 II
Alerting-UUIE (注 4), CallProceeding-UUIE, Facility-UUIE (注 5), Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken， ClearToken	规程 I	规程 I
注 1 — 假定任一消息在每个方向上都是第一个。 注 2 — 这些消息中的任何一个在任一方向上作为第一个消息出现。 注 3 — 用于密钥更新。 注 4 — 这些消息中的任何一个在任一方向上作为第一个消息出现。 注 5 — 不用于密钥更新。			

14 对象标识符一览

表 2 列出所有引用的 OID。

表 2/H.235－对象标识符

对象标识符参考符	对象标识符值	描　　述
“A1”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 20}	在 CryptoToken-tokenOID 的 ITU-T H.235.2 建议书的规程 II 中代替 OID“A”使用，指示 RSA 签名/散列包括在 H.225.0 RAS 或呼叫信令消息（认证和完整性）中的所有字段。
“S1”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 21}	在 ClearToken-tokenOID 的 ITU-T H.235.2 建议书的规程 II 中代替 OID“S”使用，指示 ClearToken 用于消息认证和完整性。在端到端 CryptoToken 中的这一 OID 暗含指示在快速起动过程中也使用 DH。
“Q”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 22}	在规程 IV 中使用，指示在逐段转接链路上的 ClearToken 携载 Diffie-Hellman 令牌。
“W”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 23}	在规程 IV 中作为 algorithmOID 使用，指示使用基于 RSA-SHA1 的数字签名。

附 录 I

H.235.3允许的网守安全性处理器

这一资料性附录描述了一个 H.235.3 允许的网守安全性处理器（GKSP）与一个网守结合的实施例子。GKSP 的目的是将某些 H.235.3 特定安全性任务，例如性能高超的 DH 操作、数字签名计算和验证以及 X.509 证书处理的执行，从单块集成电路 GK 中脱载到一个新的单独的网守安全性处理器（GKSP）功能性实体。每个 GK 至少有一个 GKSP 实体，然而一个 GK 可为多个 GKSP 服务以在服务的端点数量和整个系统的稳健性提高方面增强可升级性。

图 I.1 示出 GKSP 具有 H.235.3 安全性功能情况下的这样一个已分解的 GK。

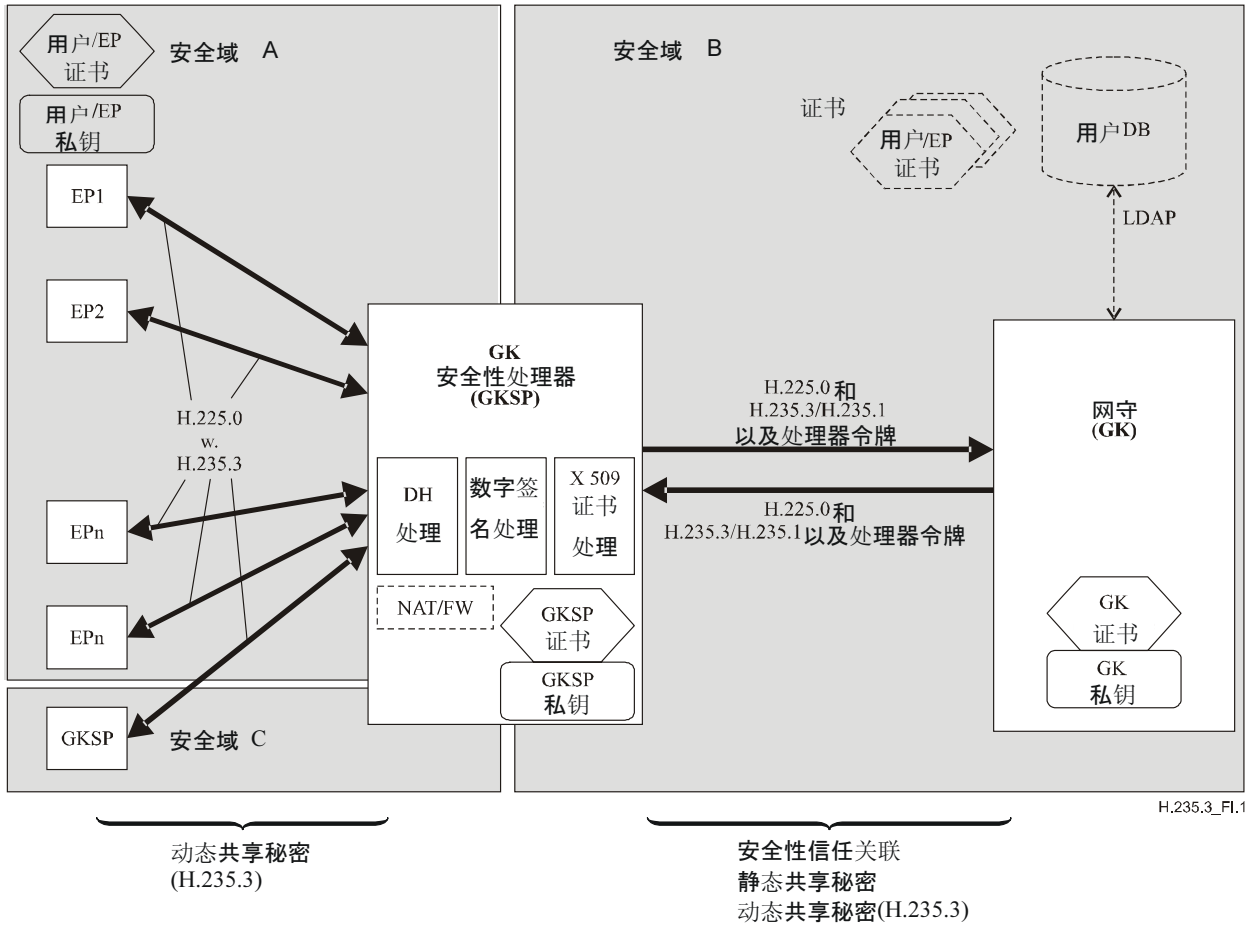


图 I.1/H.235.3－网守安全性处理器结构

注 1 — GKSP 可拥有更有用的功能，例如 NAT（网络地址解析功能）、防火墙、应用级网关（ALG）等等；这样的功能可能是安全性处理的一部分或可能保持为一个单独的内部功能，然而这样的功能未在本节中描述，留待进一步研究。

GKSP 在管理安全域 A 中为特定数量的端点服务。GKSP 也可在某些其他的管理安全域 C（未示出）中与另一个 GKSP 通信。

注 2 — 3 个管理安全域在实际中不必要是明显区别的。GKSP 可以被整个放置在 GK 所属的管理安全域 B 中，或替代地，GKSP 可以被放置在安全域 A 中或一个单独地、自身安全的域（未示出）中。

使用 GKSP，网守将不需要涉及到耗费计算的安全性操作。GK 仍通过匹配适当的证书（例如化名/DN 名/证书序列号、X.509 证书）确定认证和授权，以防止（内部/外部）数据库以预定用户的许可和证书持有这些用户。第 I.3 节定义由 H.235.3 允许的 GKSP 所使用的适当的证书。

注 3 — GK 和客户/用户数据库之间的可能的 LDAP 接口不属于本建议书。也留待网守的政策来实现介入控制决策，在该网守上保存判据和证书（例如化名/DN 名/证书序列号）。留待这样的用户数据库判断哪些证书（例如化名/DN 名/证书序列号）存储在那里。

注 4 — GKSP 不需要涉及任何与用户的配置或管理相关的事务，客户和 GKSP 不需要接入用户数据库。

注 5 — 那些采用 H.235.3 和 GKSPD 的端点典型地也持有根证书（未在图 I.1 中示出）。根证书允许实体验证实体的证书（EP,GKSP）。

GKSP 及其 GK 之间或两个 GKSP 之间的通信是安全的。例如,当假定了一个统计地配置的共享秘密时 H.235.1 适用。H.235.3 适用允许确定一个动态的共享秘密。在任一情况下，GK 和 GKSP 被假定已经确定了相互信任关系，具有静态或动态关系。当涉及多个 GKSP 时，信任的关系可联结。

这样，对于执行远端认证规程和正确地认识安全性规程，GK 信任 GKSP。GKSP 使用代表 GK 的处理器令牌在一个简单的安全声明中报告其安全处理的结果。

假定每个 H.235.3 允许的 EP 和 GKSP 持有 X.509 证书，该证书深信不疑地约束公钥和用于签名的对应私钥的合法持有者的标识符。

注 6 — 对应于私钥的公钥未在图 I.1 中明确示出；典型地，被确定的公钥在 X.509 用户/EP 证书中传送。

注 7 — 没有示出用于多有端点/GKSP 的所有的证书/私钥。

注 8 — 典型地，GKSP 证书是一个服务器证书。

如果 GK 采用 H.235.3 与 GKSP 通信，则要求 GK 仅持有一个明确的、惟一的 GK 证书和一个私钥。

GKSP 是一个正式的代理服务器，它在端点和 GK 之间或两个网守之间操作。每个 GK 至少有 1 个 GKSP，然而一个 GK 也可以为多个 GKSP 服务以增强服务端点数量的可升级性，提高整个系统的稳健性。如图 I.2 所示，线性地安排链接的 H.235.3 特定的 GKSP 单元是可能的。以体系结构安排 H.235.3 特定的 GKSP 单元，如图 I.3 所示。

每个 GK 至少有一个一般的 GKSP 实体，然而一个 GK 也可以为多个 GKSP 服务以增强服务端点数量的可升级性，提高整个系统的稳健性。端点和 GK 之间可以有 1 或多个一般的 GKSP 实体：因此，几个 GKSP 的线性或体系的层叠的配置在原则上应是可能的。一个端点总是通过一个或多个 GKSP 确定与其相关的 GK 的信任关系。单个的 GK 可具有与多个 EP 的多种信任关系。

图 I.2 示出线性链接 GKSP 单元的结构。

图 I.2/H.235.3－链接的GKSP结构

在图 I.2 中，GKSP1 认证从 EP1 接收的 RRQ 消息，而 GK1 或 GK2 对 EP1 的认证做出判决。GKSP1、GKSP2（顾及 GKSP3 和 GKSP4）依赖于 EP1 和 GK1（顾及 GK1 和 GK2）之间的 H.323 信令消息。

图 I.3 示出分级的、级联的 GKSP 单元结构。

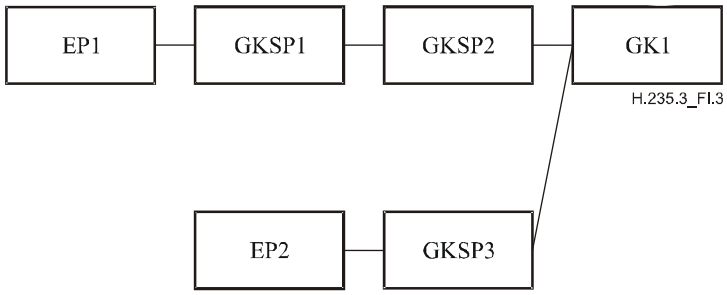


图 I.3/H.235.3－GKSP分级结构

GKSP 至少有一个 IP 地址；典型地，一个 GKSP 是位于两个不同的管理安全域的边界的边缘安全设备。因此，GKSP 可以拥有两个 IP 地址，一个 IP 地址面向 H.323 端点/对等 GKSP（管理安全域 A 和 C），另一个是内部地面向 GK（管理安全域 B）。

I.1 网守安全性处理器的发现

假定 H.323 端点不要求知道 GKSP 的存在。端点可能已经配置 GKSP 的 IP 地址作为 GK 的接触点。在存在 GKSP 的情况下，EP 的行为正与不存在 GKSP 的情况一样。EP 可能使用采用 **GRQ** 来定位其服务的 GKSP 的 GK 发现阶段。

在存在为请求 EP 服务的 GKSP 的情况下，GKSP 需要证实其 GK 是否支持安全性处理器。

在 GKSP 旨在使用对于 GK 的 H.235.1，但是共享秘密尚未在 GKSP 和 GK 之间配置的情况下，GKSP 返回一个 **GRJ** 给端点，**reason** 被设置为 **securityDenial/securityDenied**。否则，GKSP 发送 **GRQ** 并包括一个处理器 ClearToken，且设置具有 elementID 0 的概要单元，如表 I.1 所定义的。因为在这一情况下，GK 支持 GKSP，所以 GK 返回一个 **GCF/GRJ**，并包括一个处理器令牌。

在 GKSP 旨在使用对于 GK 的 H.235.3 的情况下，GKSP 发送 **GRQ** 到具有处理器令牌的内含物的 GK，并设置具有 elementID 0 的概要单元，如表 I.1 所定义的。支持该附录的 GKSP 允许的 GK 响应 **GCF** 和处理器 ClearToken 内含物。

不支持安全性处理区的 GK 和不实施该附录的 GK 将忽略被传送的令牌环，将响应 **GCF/GRJ**。GKSP 能够认识到这一状况，而接收到的 **GRQ/GRJ** 不传送处理器令牌。然后 GKSP 发送一个 **GRJ** 给具有被设置为 **securityDenial/securityDenied** 的 **reason** 的端点。

已经通过一个 GKSP 直接无延误地从端点接收到 **GRQ** 的 GK，当 GK 知道 GKSP 时，用具有被设置为 **securityDenial/securityDenied** 的 **reason** 的 **GRJ**（未包括处理器令牌）响应。

I.2 网守安全性处理器的操作

GK 安全性处理器至少执行下列功能：

— 终止 H.235.3 协议到 H.323 端点，或到对等 GKSP，如规程 IV 所定义的。

— 向 H.323 端点/对等 GKSP 运行 Diffie-Hellman H.235.3 协议；即执行 Diffie-Hellman 模数指数操作。

— 对在 H.235.3 安全消息中，接收来自 H.323 端点或对等 GKSP 的数字签名执行验证。

— 对接收的 X.509 数字证书的安全校验：路径验证、有效性校验、CRL 校验，等等。

— 对于从 GKSP 发送到 GK 或另一个 GKSP 的消息，GKS 生成新的 H.235 令牌（H.235.1 或 H.235.3）。GKSP 使用其 GKSP 标识符作为 **sendersID**，并在基线 H.235 ClearToken 中使用网守标识符（GKID）作为 **generalID**。

— 对于从 H.323 端点接收的消息，GKSP 包括一个处理器令牌。对于初始 **RRQ/GRQ** 消息，处理器令牌持有具有 ElementID 0 的安全概要单元，它指示遇到的认证方法。GKSP 在任何其他的 H.225.0 RAS 和/或呼叫信令消息中也可能包括具有 ElementID 0 的安全概要单元。

此外，处理器令牌持有一个或多个发送证书的安全概要单元。

在本建议书上下文中的合适的证书有：

— ElementID 1，用于提供在 X.509 证书中发现的主体；

— ElementID 2，用于提供在 X.509 证书中发现的 subjectAltName；

— ElementID 3，用于提供在 X.509 证书中发现的序列号；

— ElementID 4，用于提供在 X.509 证书中发现的发布者名称；

— ElementID 5，用于提供 H.323 终端的端点标识符。

注 — 另外，GK 可能将 H.225.0 消息中的 H.323 化名单元解释为证书。因为无论如何化名单元在消息中存在，所以不需要在安全概要单元内定义单独的化名单元。

GKSP 也包括具有 ElementID 6 的安全概要单元来指示遇到的错误。如果 H.323 端点和 GKSP 之间的认证已经成功，则 GKSP 可包括具有 ElementID 0 的安全概要单元来指示没有遇到安全性错误。

— 在 GKSP 在从 H.323 端点或对等 GKSP 中接收的消息中遇到安全性错误的情况下（数字签名错误，证书验证失败，等等），GKSP 记录错误并将消息发送给 GK，通过指示错误类型包括一个具有 ElementID 6 的安全概要单元的处理器令牌，让 GK 决定和相应地反应。

— 在 GKSP 在从 GK 或另一个 GKSP 中接收的消息中遇到安全性错误的情况下，GKSP 记录错误并丢弃消息。

— 计算到 H.323 端点或对等 GKSP 的出网 H.235.3 消息的数字签名。

— 重放在 H.323 端点和网守之间或 GKSP 前后的任何 H.225.0 消息，执行下列有关令牌的操作：

- 使用标记 H.235.3 的 H.225.0 协议与其网守的通信被剥夺，该协议在第一次握手时接收自 H.323 端点或对等的 GKSP。
- 验证从 H.323 端点或对等的 GKSP 接收的嵌入的 H.235.1 令牌，并为了进一步转送消息到网守将其剥去。
- 终止到其网守的 H.235.1/H.235.3 协议。
- 对于出网消息，包含去往 H.323 端点或对等 GKSP 的 H.235.1/H.235.3 令牌。
- 让从 H.323 EP 或 GK 接收的 H.225.0 消息基本完整；仅如上定义地重写令牌。
- GKSP 及其 GK 之间的 H.225.0 协议用 H.235.1 基线安全概要或 H.235.3 混合安全概要保护。

— 在 GKSP 和 GK 或 GKSP 与另一个 GKSP 采用 H.235.3 混合安全概要的情况下，GKSP 如下其一：

a） 为了确定一个新的动态密钥以从第一端点或对等 GKSP 接收第一个消息，向 GK 或 GKSP 运行 H.235.3 协议；或

b） 为了在任何其他的 H.323 端点或对等 GKSP 开始通信之前确定一个新的动态密钥，向 GK 或 GKSP 初始化 H.235.3 协议。这将允许一个动态的共享秘密在适当的地方，以备应用来保护从 H.323 终端或对等 GKSP 接收的第一次握手消息；这将进一步缩短整个与安全性关联的建立时间。

— 为了密钥更新，GKSP 不发送任何 H.235.3 特定的 FACILITY 消息。

— 在 GKSP 和 GK 或 GKSP 与另一个 GKSP 采用 H.235.1 基线安全概要的情况下，GKSP 采用静态共享密钥来保护 H.225.0 RAS 和/或呼叫信令消息。

— 继续跟踪安全性关联，即确定 DH 共享秘密；保留动态共享秘密。依据其安全性政策，GKSP 可使用 FACILITY 消息调用保持的动态共享秘密的重置密钥。一旦 H.323 终端或对等 GKSP 已经注销，则 GKSP 应丢弃动态共享密钥并认为无适当的安全性关联。

— 一对一映射 H.225.0 RAS 和/或呼叫信令消息协议的传输端口（EP-GKSP 和 GKSP-GK）。

I.3 处理器令牌

接收到具有传送的 X.509 证书和数字签名的一个 H.235.3 安全的 H.225.0 RAS 和/或呼叫信令消息，GKSP 移除 H.235.3 令牌，并包括一个单独的处理器令牌以发送消息到其 GK 或下一个 GKSP（如果有的话）。

和处理器令牌一起，GKSP 报告遇到的认证方法、遇到的端点标识符、在证书中遇到的名称（名称或 subjectAltName、在 X.509 证书中遇到的序列号以及在 X.509 证书中遇到的发布者名称或一个错误指示。处理器令牌的作用是简单的安全证明声明，用以声明 GKSP 与 H.323 端点之间对 GK 的安全性关系（成功或失败）。

GK 能够通过检查接收的消息和认识被包括的处理器令牌察觉 GKSP 的存在。GK 解释任何处理器的存在来指示任何 GKSP 的不存在。

处理器令牌是具有下列字段的 ClearToken：

— **tokenOID** 持有“PT”的 OID，见表 I.2。

— **generalID** 持有下列之一：

- 在从 H.323 端点接收或持有 H.235 安全消息的情况下，H.323 端点的端点标识符；
- 在从 GK 接收 H.235 安全消息的情况下，GK 标识符。

— **certificate** 可以任选地持有从 H.323 端点或对等 GKSP 接收的 H.235.2/H.235.3 证书。如果该特征实施，GKSP 发送证书给 GK。

subject/subjectAltName 的使用，或端点 ID 或证书序列号或其他轻加权证书，应在 **certificate** 字段内的包括整个证书上是首选的。这是因为 X.509 证书趋向于成为一个较大的数据片，也因为认证时消息片段的潜在问题包括在 UDP 传输的 H.225.0 消息中。

— **profileInfo** 具有至少一个概要单元。

处理器令牌可具有几个概要单元，列于表 I.1 中：

GK 安全性处理器 ClearToken 内的其他字段保留不使用。

表 I.1/H.235.3－概要单元规范

ElementID 值	描　　述	规　　范
0	指示传送认证方法的概要单元。 该概要单元的使用对于初始握手（GRQ 或 RRQ）是强制的，对于其他是任选的。	• **ParamS** 保留不使用。 • **Element** 具有一个 **integer** 被设置为下列之一的单元以指示在 H.323 端点或对等 GKSP 遇到的认证方法： 1）其他，未规定和非标准认证方法； 2）无（即无认证）； 3）H.235.1 共享秘密（本附录未定义）； 4）H.235.2； 5）H.235.3； 6）H.235.5，（本附录未定义）； 7）H.235.4，（本附录未定义）； 8）H.530，（本附录未定义）。

表 I.1/H.235.3－概要单元规范

ElementID 值	描　　述	规　　范
1	指示具有接收的证书的 **subject** 的概要单元。 该概要的使用是任选的。	• **ParamS** 保留不使用。 • **Element** 具有 **name** 或 **octets** 具有接收的证书的 **subject** 的一个单元。 注 — GKSP 可能需要重新编码来自 X.509 名称表示的 **subject** 为 **octets** 串或 BMP **name** 表示。
2	指示具有接收的证书的 **subjectAltName** 的概要单元。 该概要的使用是任选的。	• **ParamS** 保留不使用。 • **Element** 具有 **name** 或 **octets** 具有接收的 X.509 证书的 **subjectAltName** 的一个单元。 注 — GKSP 可能需要重新编码来自 X.509 名称表示的 **subjectAltName** 为 **octets** 串或 BMP **name** 表示。
3	指示具有证书序列号的概要单元。 该概要的使用是强制的。	• **paramS** 保留不使用。 • **element** 具有 **integer** 具有接收到的 X.509 证书的 **CertificateSerialNumber** 的一个单元。
4	指示具有证书发布者的概要单元。 该概要的使用是强制的。	• **paramS** 保留不使用。 • **element** 具有 **name** 或 **octets** 具有接收的 X.509 证书的 **issuer** 名称的一个单元。 注 — GKSP 可能需要重新编码来自 X.509 名称表示的 **issuer** 名称为 **octets** 串或 BMP **name** 表示。
5	指示具有始发端点/终端的端点 ID 的概要单元。 该概要的使用是任选的。	• **paramS** 保留不使用。 • **element** 具有 **name** 具有始发端点/终端的端点标识符的一个单元。
6	指示具有一个错误指示的概要单元。 该概要单元的使用在任何错误情况（> 0）中是强制的，但任选地以指示无错误（0）。	• **paramS** 保留不使用。 • **element** 具有 **integer** 具有下列编码错误值中之一的一个单元： 0：无错误 1：securityDenied 2：securityWrongSyncTime 3：securityReplay 4：securityWrongGeneralID 5：securityWrongSendersID 6：securityMessageIntegrityFailed 7：securityWrongOID 8：securityDHmismatch 9：securityCertificateExpired 10：securityCertificateDateInvalid

表 I.1/H.235.3－概要单元规范

ElementID 值	描　　述	规　　范
		11：securityCertificateRevoked 12：securityCertificateNotReadable 13：securityCertificateSignatureInvalid 14：securityCertificateMissing 15：securityCertificateIncomplete 16：securityUnsupportedCertificateAlgOID 17：securityUnknownCA 18：未规定的安全错误 19：不支持 GKSP。

I.4　GKSP图解实例

本节示出在管理安全域中操作的 GK 安全性处理器的实例消息流程图（见图 I.4 和图 I.5）。注意图 I.4 和 I.5 仅示出那些对于 H.235.3 来说很关键的消息，在实际中可能由很多个 H.225.0 RAS 和/或呼叫信令消息。

在两个图中，允许 H.235.3 的 H.323 终端 A 和 GKSP 采用 H.235.3 混合安全概要；因此终端 A 和 GKSP B 不共享任何静态秘密。在图 I.4 中，GKSP 和 GK 采用 H.235.1 基线安全概要来保护 H.225.0 RAS 和/或呼叫信令消息。K_{BC} 表示 GKSP B 和 GK C 共享的静态共享秘密。

图 I.4 示出从终端 A 通过 GKSP B 和 GK C 的整个呼叫。该呼叫是 GK 选路的。开始时，终端 A 和 GKSP B 按照 H.235.3，在 RAS 注册期间协商一个动态的链接密钥 K_{AB}。为此，终端 A 生成传送 A 的 DH 半密钥 DH_A 的 **RRQ** 消息，具有 A 的证书（任选）以及所有或部分 **RRQ** 消息上 A 的数据签名。

GKSP B 收到 **RRQ** 并检验数字签名。这包括确定和验证传送的数字 X.509 证书（如果包括的话）反对 A 的根证书、路径验证、CRL 校验，等等。

GKSP 发送 **RRQ** 到 GK C，增加包括安全概要的处理器令牌（PT）：

— 0 指示 H.235.3（5）；

— 2 具有 A 的证书的 subjectAltName；

— 3 具有 A 的证书的序列号；

— 5 指示 A 的端点 ID，

并采用具有共享密钥 K_{BC} 的 H.235.1 基线安全性；HMAC-SHA1 完整性校验在整个 **RRQ** 消息或仅在 **RRQ** 消息的某些部分计算。

在证书验证或数字签名验证失败的情况下，GKSP B 不能认证和授权给终端 A；然后 GKSP 记录错误，发送不正确的 RRQ 给 GK C。

网守 C 收到 **RRQ** 消息，通过 K_{BC} 采用检验完整性校验，处理具有包含的概要单元的处理器令牌 PT。如果 GK 能够成功地验证 **RRQ**，GK C 授权给终端 A。然后 GK C 用被发送给 GKSP B 的 **RCF** 响应。

GKSP B 收到 **RCF**,认识到 GK C 已经成功地授权给终端 A，并通过计算和包含其 DH 半密钥 DH_B、其证书（任选）发送 **RCF** 给终端 A，用其私钥签署 **RRQ**（完整地或部分地）。终端 A 验证接收的 **RCF** 消息的认证。

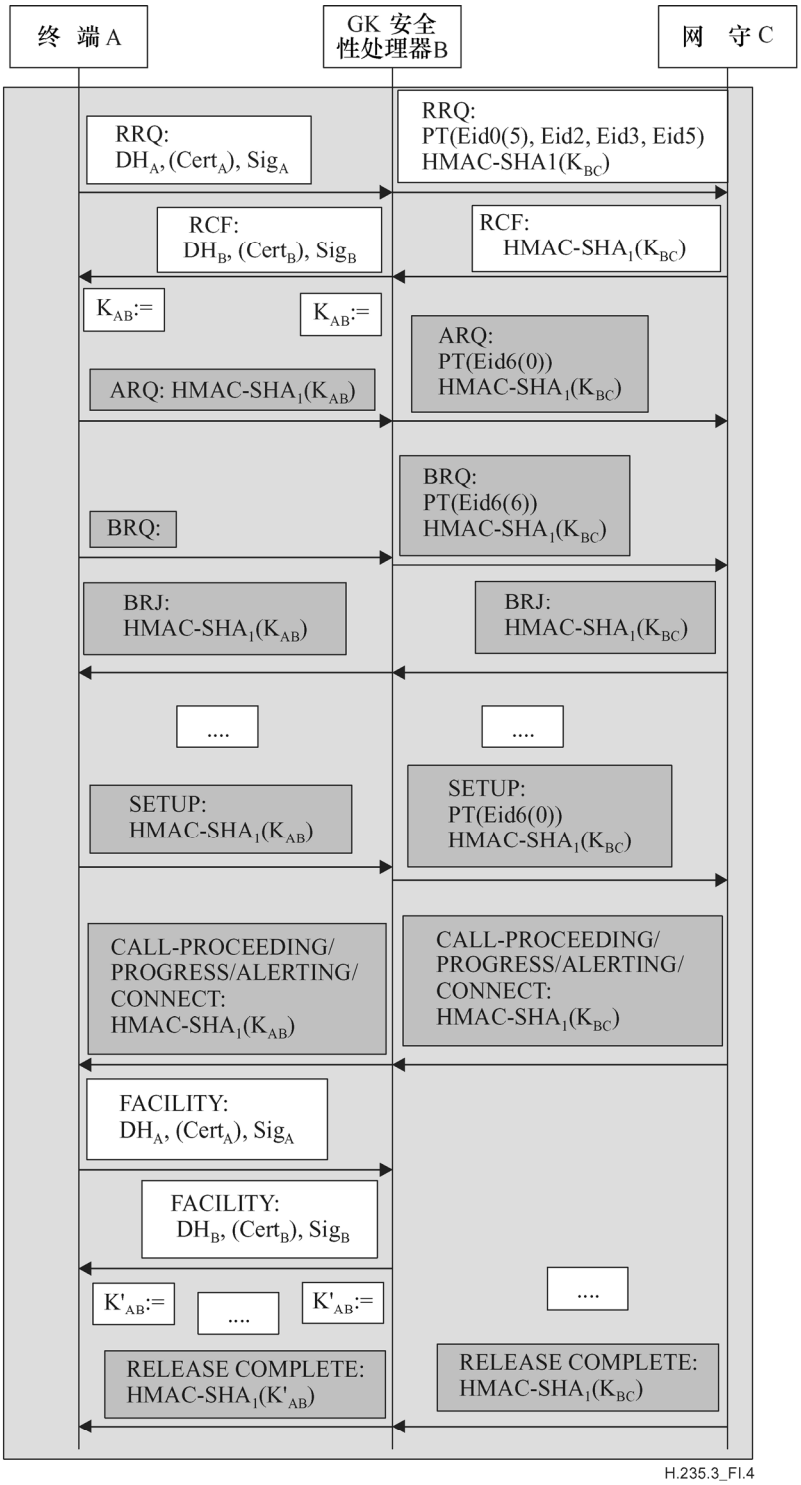
在 GKSP B 成功地认证和授权给终端 A 的情况下, GKSP B 和终端 A 计算动态共享秘密 K_{AB}。这一动态共享秘密表示确定终端 A 和 GKSP B 之间的信任关系。否则，在 GK C 不授权给终端 A 的情况下，GKSP B 通过计算和包含其 DH 半密钥 DH_B、其证书（任选）发送 **RCF** 给终端 A，用其私钥标注 **RRQ**（完整地或部分地）。由于终端 A 未经授权，GKSP B 不再能保持 K_{AB}。GKSP B 可将失败的 **RCF** 保留在一个日志文件中。

终端 A 和 GKSP B 使用这一动态共享秘密 K_{AB} 来进一步保护使用 H.235.1 基线安全概要的 H.225.0 RAS 和呼叫信令消息。GKSP B 和 GK C 使用 H.235.1 基线安全概要来保护所有的 H.225.0 RAS 和呼叫信令消息。

在终端 A 收到一个 **RCF** 的情况下, 终端 A 不继续使用呼叫建立。

图 I.4 也示出了终端 A（或其他某个终端）发送一个未保护的 **BRQ** 消息给 GKSP 的错误情况；该消息也可能已归因于一个攻击，即攻击者不知何故移除或折中 H.235.1 安全性保护。GKSP 察觉到失败的完整性验证，发送包括处理器令牌的 **BRQ** 消息给 GK,而安全概要单元指示 securityMessageIntegrityFailed（6）。GK 认识到安全性受到妨碍，通过用 **BRJ** 回答拒绝，不批准带宽请求。

在呼叫已经确定之后的某一点，对于具有 GKSP B 的 K_{AB}，终端 A 决定通过执行密钥更新规程更新密钥 K_{AB}；K'_{AB} 表示新更新的密钥。在呼叫结束时，它由 GK C 终止。



Cert 用户证书
DH_A Diffie-Hellman令牌g^a除以p
DH_B Diffie-Hellman令牌g^b除以p
Eid*n* 值为*n*的安全概要ElementID
EP 端点（终端）
GK 网守
GKSP 网守安全性处理器
HMAC-SHAI 计算的完整性校验值
K,K' 对称链路密钥
PT 处理器令牌
Sig 数字签名

图 I.4/H.235.3－具有GK安全性处理器和H.235.1消息保护的呼叫流（GKSP到GK）

在图 I.5 中,GKSP 和 GK 采用 H.235.3 混合安全概要来保护 H.225.0 RAS 和呼叫信令消息。K_{BC} 表示 GKSP 和 GK 最初协商然后进一步在 H.235.2 基线安全概要中用于保护 H.225.0 RAS 和呼叫信令消息的动态共享秘密。图 I.5 也示出了与其 GKSP B 共享静态共享秘密 K_{DB} 的 H.235.1 允许的 H.323 终端 D。

图 I.5 示出终端 A 通过 GKSP B 和 GK C 的整个呼叫流。该呼叫是 GK 选路的。在图 I.5 中，假定终端 A 实际上是在 GK 通过 GKSP 注册的第一个端点。

终端 A 和 GKSP B 使用这一动态共享秘密 K_{AB} 来保护更多的使用 H.235.1 基线安全概要的 H.225.0 RAS 和呼叫信令消息。GKSP B 和 GK C 使用 H.235.1 基线安全概要来保护更多的使用动态共享秘密 K_{BC} 的 H.225.0 RAS 和呼叫信令消息。

开始时，终端 A 和 GKSP B 按照 H.235.3 协商一个动态链接密钥 K_{AB}。两个实体都确定一个动态共享密钥 K_{AB} 时，在终端 A 和 GKSP 之间的第一次握手 **RRQ**/**RCF** 期间，GKSP 和 GK 也采用 H.235.3 来确定动态共享秘密 K_{BC}。

GKSP 发送从终端 A 接收的 **RRQ** 消息，增加一个包括 3 个安全概要单元的处理器令牌：

— 0 指示 H.235.3（5）；

— 3 指示 A 的证书序列号；

— 6 指示无差错（0），

并采用 H.235.3 混合安全概要。因为 GKSP B 和 GK C 还未共享任何共享秘密，GKSP 和 GK 运行 H.235.3 协议并确定一个动态共享秘密 K_{BC}。

之后某一时候，终端 D 使用 H.235.1 安全 **RRQ** 在 GKSP B 注册。GKSP B 发送这一 **RRQ** 给 GK C 并包括处理器令牌。处理器令牌传送 3 个安全概要单元：

— 0 指示 H.235.1（3）；

— 5 提供 D 的端点标识符；

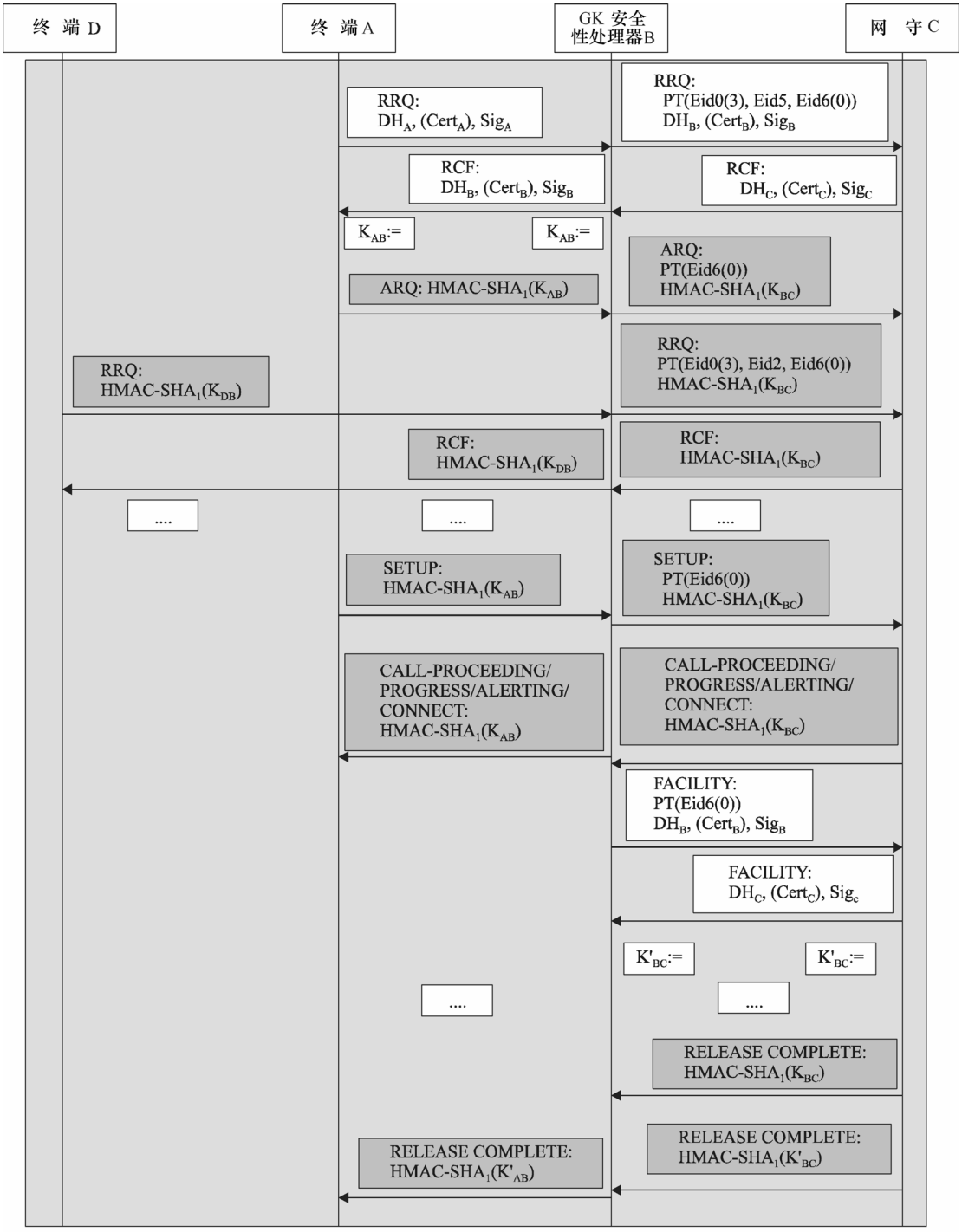
— 6 指示无差错（0），

并采用 H.235.3 混合安全概要。因为 H.235.3 动态共享秘密 K_{BC} 在之前已经被确定，所以 GKSP 通过采用 K_{BC} 保护使用 H.235.1 的 **RRQ** 消息。GK C 授权给终端 D 并用 GKSP 发送给终端 D 的 **RCF** 回答。

在来自终端 A 的呼叫已经通过 GK C 被确定的时间后的某一点，GKSP B 决定通过执行具有 GK C 的 K_{BC} 的密钥更新规程，更新密钥 K_{BC}，K'_{BC} 表示新更新的密钥。

图 I.5 也示出 GKSP 接收到来自 GK 的一个 RELEASE-COMPLETE 消息的错误情况。GKSP B 察觉到完整性验证失败；该消息不使用当前密钥。消息已经被攻击者重放或控制，或 GK 使用一个旧的、过期的密钥。GKSP B 记录安全时间并丢弃未将其发送给终端 A 的消息。

在呼叫末端，它由 GK C 终止。



Cert	用户证书	GK	网守
DH_A	Diffie-Hellman 令牌 g^a 除以 p	GKSP	网守安全性处理器
DH_B	Diffie-Hellman 令牌 g^b 除以 p	HMAC-SHAI	计算的完整性校验值
DH_C	Diffie-Hellman 令牌 g^c 除以 p	K,K'	对称链路密钥
Eid*n*	值为 *n* 的安全概要 ElementID	PT	处理器令牌
EP	端点（终端）	Sig	数字签名

图 I.5/H.235.3－具有GK安全性处理器和H.235.3消息保护的呼叫流（GKSP到GK）

I.5 对象标识符一览

表 I.2 列出将与表 I.1 一起使用的参考 OID。

表 I.2/H.235.3－附录I使用的对象标识符

对象标识符参考	对象标识符值	描　　述
"PT"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 15}	用于指示从 GKSP 到 GK 的通信的 GK 处理器清晰令牌。

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