国 际 电 信 联 盟

ITU-T H.235.5

国际电信联盟
电信标准化部门

(09/2005)

H系列：视听和多媒体系统

视听业务的基础设施 — 系统概况

H.323安全性：使用弱共享秘密在RAS中的安全认证框架

ITU-T H.235.5建议书

国际电信联盟

ITU-T 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.235.5建议书

H.235安全性：使用弱共享秘密在RAS中的安全认证框架

摘　要

本建议书为处于 H.225.0 RAS 交换中的双方相互认证提供了框架。本文描述的“拥有证据”的方法允许共享秘密如口令的安全使用，而如果它们单独使用，不可能提供足够的安全性。

本建议书也描述了对本框架的扩展以允许传输层安全参数同时协商，以保护后续的呼叫信令信道。

在 H.235 子系列的较早版本中，该概要被包含在 H.235 附件 H 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.235.5 建议书。

关键词

认证, 口令, 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

引言

在很多应用场合，端点（或它的用户）和它的网守之间仅共享一个“小”秘密，如口令或个人识别号码（PIN），这样一个秘密（此后我们必须称之为“口令”），及所有由它衍生出来的加密密钥，其密码性是很弱的。如第 10 节所述的查询/应答认证方案，提供了明文以及相应的密文的示例，因此，如果认证是采用简单口令加密，则可能遭受来自某个事务的旁观者的强力攻击。这样，这个旁观者可能重获口令或PIN，其后佯装成端点来获取服务。

一个类属标题为加密密钥交换的协议族，是使用一个共享的秘密来“遮掩”一个 Diffie-Hellman 密钥交换，它采取的方式是使攻击者必须先解决一系列有限对数问题，才能对这个共享的秘密形成有效的强力攻击。在 Bellovin and Merritt [B&M]的加密密钥交换(EKE)中，这个共享的秘密是用来在对称算法下对 Diffie-Hellman 公钥进行加密。在 Jablon [Jab]简单口令指数密钥交换(SPEKE)方法中，这个共享的秘密用来选择 Diffie-Hellman 组的不同的生成程序。这些协议将一个强有力的 Diffie-Hellman 密钥交换的安全性与共享的秘密的使用结合在一起，它采取的方式是攻击者在对秘密的攻击中，如果无法解决 Diffie-Hellman 的有限对数问题，就无法获得已知的明文。这些协议的优点是它们通过秘密—密钥加密的力量增加了 Diffie-Hellman 问题的力量（或反之）。一个潜在的不利条件则是这些协议通常都受到专利保护。

ITU-T H.235.5建议书

H.235安全性：使用弱共享秘密在RAS中的安全认证框架

1 范围

任何采用 H.225.0 RAS 协议的网守和端点都可使用本建议书。

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.245 (2005), *Control protocol for multimedia communication*.

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

– Federal Information Processing Standard FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 August 2002.

– NIST Special Publication 800-38A 2001, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

2.2 资料性参考文献

[AES] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security*.

[B&M] BELLOVIN (S.), MERRITT (M.): U.S. Patent 5,241,599, August 31, 1993, originally assigned to AT&T Bell Laboratories, now assigned to Lucent Technologies.

[Jab] JABLON (D.): Strong Password-Only Authenticated Key Exchange, *Computer Communication Review*, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-26, October 1996.

[NIST SP 800-57] NIST Draft Special Publication 800-57 (2005), *Recommendation for Key Management, Part 1: General Guideline*. http://www.csrc.nist.gov/publications/drafts/draft-800-57-Part1-April2005.pdf

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[RFC2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[RFC3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

3 定义

无。

4 缩写

本建议书使用以下缩写：

ACF 接入确认

AES 高级加密标准

ARJ 接入拒绝

ARQ 接入请求

CBC 密码块链接

CTR 计数器模式(见 NIST SP 800-38A)

D-H Diffie-Hellman

EKE 加密的密钥交换

GCF 网守确认

GK 网守

GRJ 网守拒绝

GRQ 网守请求

HMAC 散列消息验证码

ICV 完整性校验值

ID 标识符

LCF 定位确认

LRJ 拒绝定位

LRQ 定位请求

MIM 中间人

OID 对象标识符

PIN 个人识别号码

PRF 伪随机函数

RAS 注册、许可和状态协议

RCF 注册确认

RFC 请求注解

RRJ 注册拒绝

RRQ 注册请求

SHA1 安全散列算法 1

SPEKE　简单口令指数密钥交换

TLS　传输层安全性

UDP　用户数据报协议

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。

更多的惯例，可参见 H.235.0 的第 5 节。

6　基本框架

6.1　H.235.0中的协商能力改进

ITU-T H.235.0 建议书通过将以下通用单元加入到 **ClearToken** 的方式来提供对本安全框架的支持。

- **profileInfo** 是一个指定概要单元序列，每个单元由指定概要定义的完整值所标识，指定概要的 **OID** 由 **ClearToken.tokenOID** 所携带。

在以下的叙述中，有几个单元在 **profileInfo** 中传递；为便于讨论，每个单元除了识别值以外，还有一个名称。

6.2　端点和网守之间的应用

本基本框架是采用直通的方式进行的，在该框架中，请求者是希望与网守注册的端点，而响应者是网守。在下文中，隐含假定了所提到每一 **ClearToken**，均以认证概要中的 **tokenOID** 标识。**Random** 单元和/或 **random2** 单元可以通过以下两种方式中的任意一种为概要所使用：它们可以包括在认证密钥的计算中和/或包括在后续 RAS 信息（如 RRQ/RCF）中概要 **ClearToken** 中以防止重放。端点注册交换处理如下：

1)　端点通过将与希望的概要相适应的对象 ID 包含在 GatekeeperReQuest 的 **authenticationCapability** 单元的 **authenticationMechanism.keyExch** 单元中，宣布它加入一个或多个密钥协商和认证方案的意愿。假定在公钥系统（如 Diffie-Hellman 或椭圆曲线）和特定组别（如 RFC 2412 中的某一个 OAKLEY 组），密钥衍生函数（如通过 H.235.0 第 10 节中的伪随机函数）、消息认证码（如 HMAC-SHA1-96 [RFC2104]）以及它们所使用的序列方面，每个特定的 OID 完全定义了一个认证程序。端点还在 GRQ 中以以下形式包括一个或多个概要 **ClearToken**，每个又都携带以下列形式的提供的特定概要的 OID 以及必要的（加密）公钥资料：

   a)　**tokenOID** 携带着由已封装的 **GRQ** 的 **authenticationCapability** 所提供的概要 OID。

   b)　**timeStamp** 可以用于确保流通时间并防止重放。

c) **password** 不得用于实际的口令。

d) 如果使用，则 **dhkey** 携带 Diffie-Hellman 密钥参数。密封的 **halfkey** 单元采用选定概要所指定的方式加密。

e) **challenge** 未做要求。

f) **random** 由发起者提供，用于防止重放攻击。

g) 如果证书交换是概要中的一部分，也可能会用到 **certificate**。

h) 如果概要需要，也可能使用 **generalID**。

i) 如果概要需要，**eckasdhkey** 携带椭圆曲线密钥参数。密封的 **public-key** 单元采用选定概要所指定的方式加密。

j) 如果概要需要，也可能使用 **g sendersID**。

k) 如果概要为了解密而需要一个初始化矢量， **profileInfo** 单元 ，**initVect**, 可能会与（加密）公钥资料（**dhkey** 或 **eckasdhkey**）一起提供**。**

l) 如果发起者希望使用由一个早期交换衍生而来的密钥资料，它必须包括一个 **profileInfo** 单元，已标记 **sessionID**，包含着早期交换时指派的的标识符。此时，**dhkey**、**eckasdhkey** 与/或 **initVect** 不应包括在内。

m) 如果发起者希望为呼叫信令连接建立一个 TLS 对话，它可以包括一个或多个包含 TLS 密码组的 **profileInfo** 单元；如果出现 **sessionID**，则信息必须仅包含一个密码组（之前已协商的那一个）。

n) 如果发起者希望为呼叫信令连接建立一个 TLS 对话，它可以包括一个或多个包含压缩方法列表的 **profileInfo** 单元；如果出现 **sessionID**，则信息必须仅包含一个压缩方法列表（之前已协商的那一个）。

o) 为了提供概要程序下的任何额外的参数，可能需使用更多的 **profileInfo** 单元。

2) 当收到 GRQ，网守从所提供的列表中选择一个 **AuthenticationMechanism** 概要，生成一个合适的私钥，计算对应的公钥，如果需要为使用口令的对称加密生成一个初始化矢量，加密公钥，生成一个惟一的对话 ID，并生成一个随机量，所有这些都被编码进入 **ClearToken**。根据概要，ClearToken 单元有以下的使用方式：

a) **tokenOID** 携带从已封装的 GCF 的 **authenticationMethod** 中所选择的概要 OID。

b) **timeStamp** 可以用于确保流通时间并防止重放。

c) **password** 不得用于实际的口令。

d) 如果要使用，则 **dhkey** 携带 Diffie-Hellman 密钥参数。密封的 **halfkey** 单元采用选定概要所指定的方式加密。

e) 如果概要指定的密钥加密需要，**challenge** 可用于携带初始化矢量，或它也可能用于携带一个由端点发回的随机串以防止重放攻击。

f) **random** 可以包含由请求者提供的无法预测的、惟一的值以防止重放攻击。

g) 如果证书交换是概要中的一部分，也可能使用 **certificate**。

h) 如果概要需要，也可能使用 **generalID**。

i) 如果概要需要，**eckasdhkey** 携带椭圆曲线密钥参数。密封的 **public-key** 单元应采用选定概要所指定的方式加密。

j) 如果概要需要，也可能会使用 **sendersID**。

k) **random** (或一个额外 **profileInfo** 单元, 标记为 **random2**, 如果概要要求两个随机号码都保持在信息交换中) 应包含由响应者提供的无法预测的、惟一的值以防止重放攻击。

l) 如果概要为了解密而需要一个初始化矢量，**initVect** 可能会与（加密）公钥资料（**dhkey** 或 **eckasdhkey**）一起提供。

m) **sessionID** 是一个惟一(对网守而言)的标识符，用于表示此注册对话。在某些概要下，为了迅速建立一个保护的 TLS 呼叫信令信道，它也可以作为 TLS 对话 ID 使用。

n) 为了提供概要程序下的任何额外的参数，可能需使用 **profileInfo**。

然后网守根据概要，使用它的私钥、从 GCF 而来的（解密）公钥对共享秘密或主密钥进行计算，并从主密钥衍生出必需的加密密钥、认证密钥或其他资料。以上所述的 **ClearToken** 放置在 GatekeeperConfirm 消息内。必须使用衍生出的认证密钥对 GCF 的进行完整性检查/认证，然后发送到端点。认证/完整性检查可以通过好几种概要所指定的途径中的一种返回，如：通过概要指定的 **profileInfo** 单元，或通过 ITU-T H.235.1 建议书指定的程序。

3) 端点对从 GCF 而来的选定的 **authenticationMechanism.keyExch** 进行检查，并从由相应的 **tokenOID** 所标识的 **ClearToke** 中提取参数。然后端点选择它的私钥，计算对应的公钥，并选择概要要求的所有其他参数。端点再根据概要，使用自己的私钥及从 GCF 而来的（解密）公钥对共享秘密或主密钥进行计算，衍生出必需的解密密钥、认证密钥或由它而来的其他资料。接着端点必须检验 GCF 的完整性。如果 GCF 检验不正确，端点必须将它以及所有由它衍生而来的密钥资料一起丢弃，并继续等待有效的 GRQ 消息。标准的 RAS 恢复功能将使 GRQ 重新发送，并可能受到未被损坏的 GCF。如果几次重发都无法产生成功的应答，端点必须停止尝试注册，并通知它的用户出现错误。注意每次发送 GRQ，都会给网关的冒名顶替者多一次机会去猜测用户口令，并通过 GRQ 是否接受来确认它的猜测。如果 GCF 通过了完整性检查，端点确认了网守，那就可以进行注册，并在这个过程中将自己交给网守认证。

4) 然后端点用类似于上述的网守的方式，在概要 **tokenOID** 中增加 **ClearToken**。所有从 GCF 清晰令牌而来、被认为是概要的查询的字段都必须包括在 **ClearToken** 中。如果为了避免重放，概要指定 **ClearToken** 必须包括由上面接受到的 GCF 的 **random** 和 **random2**。这样 **ClearToken** 就放置在 **R**egistration**R**e**Q**uest 中发送回网守。端点应认证整个 RRQ 信息并将它发送给网守。从这个点向前，端点既不应接收也不应发送没有通过认证的 RAS 消息，认证是通过达成一致的概要使用从共享密钥资料衍生而来的认证密钥来进行的。

5) 网守接收到 RRQ，必须用共享密钥资料对已包括的认证和完整性检查去检验 RRQ 的完整性。如果完整性检查失败，网守必须忽略已接收到的 RRQ 并等待一个可核实的 RRQ。如果什么也没有，端点最终将放弃尝试注册并返回到搜寻网守的状态。如果完整性检查通过，网守将准备一个 Registration ConFirm 消息发回给端点。根据概要，此 RCF 可能包含了 **ClearToken**，它可以包括由 RRQ 提供的认证概要 **ClearToken** 而来的 **random**、**random2** 与/或 **challenge** 单元。RCF 以及所有后续的 RAS 消息，必须包含一个采用协商验证密钥和算法计算的可检验的认证和完整性检查。

6) 当端点收到 RCF 消息，它通过包括在内的认证和完整性检查单元对完整性进行检验。如果检验未通过，RCF 必须被丢弃，如果甚至再重新发送 RRQ 后也还是没有收到有效的 RCF 的话，对话必需取消，端点必须返回寻找新的网守。如果 RCF 通过检验，可以在建立安全呼叫信令信道时从它的 **ClearToken** 中提取对话 ID 和选定的密码组（如有的话），以备以后使用。

6.3 网守之间概要的应用

在网守之间的 LRQ/LCF 交换中，基本上要采用同样的程序。在此情况下，还不可能有明确的概要选择；始发的网守必须通过包括合适的 **ClearToken** 来为 GRQ 消息提供一个或多个概要。响应网守可以选择一个概要，并应如前所述为 GCF 消息返回相应的 **ClearToken**。注意，在这种情况下，呼叫的网守直到建立呼叫信令信道还没有将让响应网守对自己进行认证。

如果一群网守共享一个用于此目的秘密，则在组播模式下也可采用本程序。组播 LRQ 将基于此秘密；那些用 LCF 应答的网守将使用那个密钥来对提供的 Diffie-Hellman 公钥进行解码，还将各自选择它们自己的 **nonce** 和 Diffie-Hellman 私钥来应答。作为结果产生的对话密钥对于最后一对网守而言将是惟一的。

6.4 信令信道加密和认证

如果网守路由为网守所支持，可使用一个新协商的主密钥资料和已标识的密码参数来认证和保护呼叫信令信道，如为呼叫信令建立 TLS 对话。如果没有使用 TLS，网守必须在发回的概要 **ClearToken** 中包括已选定的 **cipherSuite** 和 **compress** 单元。

7 指定安全概要（SP1）

本节提供了一个标准安全概要，预期它能提供大约等同于一个 80 位的随机数字的共享秘密(参见[NIST SP 800-57])。本概要由以下几个部分所组成：

- 本概要（标记为“SP1“）的对象 ID 将为{itu-t (0) recommendation (0) h (8) 235 version (0) 3 60}。
- 主密钥, K_m, 协商：采用 OAKLEY 著名群 2 [RFC 2412]的 Diffie-Hellman 密钥交换，接着是 Diffie-Hellman 秘密的 SHA1 [FIPS PUB 180-1] 散列缩减， K_m = SHA1 (Diffie-Hellman 共享秘密)。
- 对称加密算法：必须是 2 八比特组用户鉴别器的 AES-128 区段计数器模式，D, 一个 12 个八比特组的初始化矢量, IV, 以及一个 2 个八比特组的计数器字段, C, 此计数器= D || IV || C, 且 C = 0 初始。CTR 模式的描述可参见[NIST SP 800-38A]。用户鉴别器, D, 当 IV 由发出 GRQ/RRQ 或 LRQ 的那一方所生成时设置为 0x3636；当由用 GCF/RCF 或 LCF 做出响应的那一方所生成时设置为 0x5c5c。每一方都必须确保它生成的每个 IV 是惟一的，它可以使用它自己的方法来确保惟一性。

- Diffie-Hellman 密钥加密：必须使用 AES-128 区段计数器模式来对 Diffie-Hellman 公钥进行加密（用一个采用网络字节顺序的八比特组串来代表）；初始化矢量携带在 **ClearToken.initVect** 中，16 个八比特组密钥，K_p，必须构造成一个高阶 128 位的用户口令的 SHA1 散列 1：K_p = Trunc(SHA1(用户口令), 16), 当 Trunc(x,y) 截短八位字节串 x 至 y 八比特。注意通常这被认为是一个弱密钥。
- 重放预防：每方都必须提供一个 32 位“随机”数字（可能包含一个计数器字段以确保惟一）；随机数字明确地用在对衍生密钥的计算上，因此它们各自都只需要传送一遍。
- 认证密钥, K_a, 衍生: H.235.0 第 10 节所定义的 PRF，我们将它标记为 PRF(*in_key*, *label*, *outkey_len*) 与 *in_key* = K_m, 以及 *label* = "auth_key" || R_e || R_g, R_e 是从 GRQ **中 ProfileElement** 而来的 **nonce**，R_g 是从 GCF **中 ProfileElement** 而来的 **nonce**, 同时 *outkey_len* = 128。
- 消息认证和完整性函数：使用 **tokenOID** 设置为“SP1”的 **ClearToken**，**ProfileElement.octets** 设置为在整个 ITU-T H.225.0 建议书描述的消息上计算出的 HMAC-SHA1-96 散列值；本程序应该适用于所有 RAS 和呼叫信令消息（除了 GRQ 或 LRQ，它们不包含 **sessionID**）。
- 单元加密密钥，K_e：呼叫信令消息的已选单元（或单元在哪里隧穿过）可以采用密钥 K_e = PRF(K_m, "encrypt_key" || R_e || R_g, 128)的 AES-128 区段计数器模式来加密。例如，此密钥可用于加密媒体对话密钥在 **h235Key** 单元的分发，就像在快速连接与/或 H.245 使用的那样。如果用这种方式来使用，“SP1”作为加密算法 OID 来使用。

本概要使用表 1 所定义的 **ProfileElement**。这些单元由如 ITU-T H.235.0 建议书所定义的 **ClearToken.profileInfo** 单元序列所携带。

表 1/H.235.5－概要单元

单元名称 (文中使用)	ElementID值	单元选择 (长度)	单元描述
initVect	1	八比特组 (12)	EKE加密的初始化矢量
nonce	2	八比特组(any)	一个无法预计的惟一值
cipherSuite	3	八比特组(2)	TLS密码组
compression	4	八比特组(1)	TLS压缩算法
sessionID	5	八比特组(1..)	惟一，可以与TLS对话ID相对应
integrityCheck	6	八比特组(12)	加密后的检查值

注册序列包含：

— 端点必须发送一个带有 **authenticationCapability** 单元的 GRQ，该单元包含一个带有 OID“SP1”的 **AuthenticationMechanism.keyExch**，以及相应的 **tokenID** = “SP1”的 **ClearToken**； 包含采用 **initVect** 作为 IV、密钥由用户口令衍生而来的 1024 位公钥加密的 **dhkey**；以及 **nonce** =一个端点选定的 32 位随机数字 。

— 网守必须回复一个包含 **authenticationMode** 单元的 GCF，该单元等同于一个带有 OID “SP1”的 **AuthenticationMechanism.keyExch**，以及相应的 **tokenID** = “SP1”的 **ClearToken**； 包含采用未加密 1024 位公钥的 **dhkey**；以及 **nonce** =一个网守选定的 32 位随机数字，伴随着包含用衍生认证密钥 K_a 计算的认证散列值的 **integrityCheck**。应注意的是，对于网守而言，对本概要的 GCF 中的 Diffie-Hellman 半密钥进行加密并不是必需的，因为它是使用衍生认证密钥通过展示自己的能力来自我认证和对 GCF 认证的第一方。此模式允许网守和多个端点一起重新使用 Diffie-Hellman 密钥。具体见第 10.5 节。

— 端点必须回复一个包含 **ProfileElement** 的 RRQ，该单元包含认证和完整性校验值，该单元的 **elementID** 设为 **integrityCheck**，且 **element** 设为采用衍生认证密钥 K_a 计算出的值。

— 后续的 RAS 消息，包括 RCF，必须使用同样的步骤和密钥进行认证和完整性检查。H.225.0 呼叫信令消息（以及隧道传送的 H.245 消息，如有的话）必须使用 **ClearToken** 来认证，其 **tokenOID** 设为“SP1”，包含 **elementID** 设为 **integrityCheck** 以及 **element** 设为计算值的 **profileInfo ProfileElement**。

— 网守和端点应采用加密密钥 K_e 以及区段计数器模式的加密算法 AES-128，来对已选定的 RAS 上的信息传输、呼叫信令与/或 H.245 来进行加密。例如，网守可分发媒体加密密钥，并用 K_e 和概要加密算法来保证安全。

— 如果端点被要求注册，而它还保留有原来的对话 ID 和主秘密，它应尝试用原来的对话 ID 和主秘密来注册，包括将 GRQ 中明确的对话 ID（且不包括 Diffie-Hellman 半密钥）放入它的 GRQ。

— 此概要必须能在两个网守之间使用（见第 6.3 节）。

8 改进的安全概要（SP2）

本节定义了一个以原来的概要 SP1 为基础的新的安全概要。它被非正式地称为 SP2，而它正式的标识为 OID {itu-t (0) recommendation (0) h (8) 235 version (0) 4 62}。除了以下小标题列出的以外，本概要基本与 SP1 一样。对 SP1 的改进主要包括：

— 呼叫信令序列的编号改进以防止重放攻击。

— 使用端点别名来进行基于口令的加密密钥的生成的补白，以防止字典式攻击。

— nonce 的长度增大了，且可变。

— 一个为加密初始化矢量而衍生的补白密钥。

— 使用 **genericData** 提供了一个更有效的概要 **ClearToken** 传输。

SP2 使用表 1 中的概要单元以及表 2 中的额外概要单元。

表 2/H.235.5－SP2的额外概要单元

单元名称 (文中使用)	ElementID值	单元选择 (长度)	单元描述
seqNumber	7	八比特组(4)	按网络字节顺序排列的32位序列数字
connectID	8	八比特组(2)	信号连接标识符 (可选项，默认= 0)
endpointID	9	八比特组(可变)	与端点及其口令关联的ASN.1已编码的AliasAddress (可选项)

8.1 呼叫信令序列号码

H.225.0 呼叫信令消息未包含一个序列号码，因为它们是在可靠连接（TCP）上传输的。除此之外，在应用层惟一信息标识符的缺乏，使呼叫信令处于重放和反射攻击的危险之下。此问题可通过给每个呼叫信令消息增加一个序列号码，一个可选的连接标识符来解决。注意此技术并不能完全防止重放和反射攻击，但它极大地降低了攻击成功的几率。

序列号码必须在每个方向上都是惟一的以防止反射攻击。这在现实条件的限制下是可以实现的，可通过要求 GRQ 的发出者（端点）或 LRQ 消息的发出者（网守）从数字 0 开始它的呼叫信令传输信令序列，以数字 2^{31} 开始它的接收序列来实现。这提供了一个在任何交叠可能发生前的非常长的时间（在非常少见的每毫秒一条信息的速率下几乎有 600 小时）。后续使用同一 SessionID 的进行的呼叫应在每个方向上均采用下一个未用的序列号码传输。（为了允许在连接发生故障的情况下出现信息遗失，接收者应采用一个最后一次接受的序列号码之后的小(如 5-10)窗口来接受信息，并从那里开始进行）。能对使用同样的对话 ID 进行多路同时呼叫信令连接提供支持的设备，可以使用一个可选的 **connectID** 来标识不同呼叫的单独的序列号码。如果没有特别说明，就假定 **connectID** 为 0。

8.2 从口令生成弱加密密钥

为了防止字典式攻击，用别名自己来“补白”加密密钥是十分理想的；该攻击先猜测 PIN，再用它加密一个 D-H 公钥，然后持续应用到所有已知的端点别名上。特别地，基于口令的密钥 K_p 必须由口令的串接和所提供的 **endpointID** 计算而来：

$$K_p = \text{Trunc}(\text{SHA1}(\text{用户口令} \,||\, \textbf{endpointID}), 16)$$

通常，在 **endpointID** 内的 **AliasAddress** 将是包含在 GRQ 中的 **endpointAlias** 单元中的其中一个别名，但这并不是必需的。例如，**endpointID** 可以识别一个同时支持很多端点的网关，这些端点的别名都列在 **endpointType** 上。

8.3 Nonce长度

安全概要 1 要求各方都提供一个 4 八比特组（32 位）的 nonce，以作为密钥协商协议的一部分。当是在初始密钥协商中提供时，在响应网守重复使用同样的 Diffie-Hellman 公钥但请求者却生成了一个新的密钥的请况下，32 位可能也已足以确保是最新的。不过，当在一个已协商好的主密钥上协商新的对话密钥时，64 个独立数位可能还不能为每对衍生密钥提供足够的差值。因此建议 nonce 的长度是可变的，从最小 4 个八比特组到最大 16 个八比特组。

8.4 初始化矢量补白

作为一个增加的模糊措施，一个 112 位对话补白密钥，K_s，是从协商主密钥衍生而来：

$$K_s = \text{PRF}(K_m, \text{"salting\_key"} \,||\, R_e \,||\, R_g, 112)$$

用于加密和解密的初始 AES-128-CM 计数器以下述的方式建立：

Counter = (K_s ^ (D || IV)) || C, 其中 C 为 16 位计数器字段，初始值为 0。

8.5 ClearToken编码

安全概要 1 利用 **clearToken** 序列来携带概要的参数。每个 H.225.0 消息包含一个 **ClearTokens** 序列，除非 **h323-message-body** 选择 **empty**；所有的消息均携带 **genericData**。SP1 程序的结构使得 **ClearToken** 的结构相当有规律，它允许提前用 ASN.1 进行编码，并且作为一个原始参数携带，该参数用 SP2 OID 标识，其 **GenericData** 单元中的 **id.standard** 设为 1。这种形式也使 **clearToken** 可用"null" OID {0,0}来标识。最重要的是，由于 **ClearToken** 单独的编码形式已成为可用的常规的编码和解码过程，所以 token 的定位和其中的检查值变得容易。这样，在已编码的 clear token 中定位 integrityCheck 单元比在整个编码消息中去定位要快一些。

9 框架的扩展（资料性参考）

在本框架内，下述单元可以被引入到安全概要中。

9.1 经由TLS使用主密钥来保护呼叫信令信道

为了在 TLS 传输协议([RFC 2246], [RFC 3546])下对呼叫信令信道进行保护，RAS 交换期间的密钥资料协商可以用来衍生对话密钥。实际上，RAS 协商替代了初始 TLS 握手协议。当然只有呼叫信令为网守选路的才有意义。这对于网守间的认证和采用 LRQ/LCF 交换的信令特别有用。在这种情况下，没有第三个 RAS 消息使用协商后的密钥资料，通过此 RAS 消息可以用来向被叫的网守来认证自己，但是被叫方也可以通过它自身的能力来与正确的 TLS 对话参数建立呼叫信令信道来进行隐含认证。图 1 显示了相关的信息流：RAS 用来协商对话主密钥，对话 ID 和相应的预主秘密分发到 TLS 软件，且呼叫信令层在 TLS 上使用对话 ID 建立呼叫信令信道。由于完成秘密传输的方法是独立执行的，这已超出本建议书的范围。应注意的是本建议书指定了端口 1300 作为缺省的呼叫信令 TLS 监听端口。不过端点必须使用其中一个由网守提供的呼叫信令传输地址。

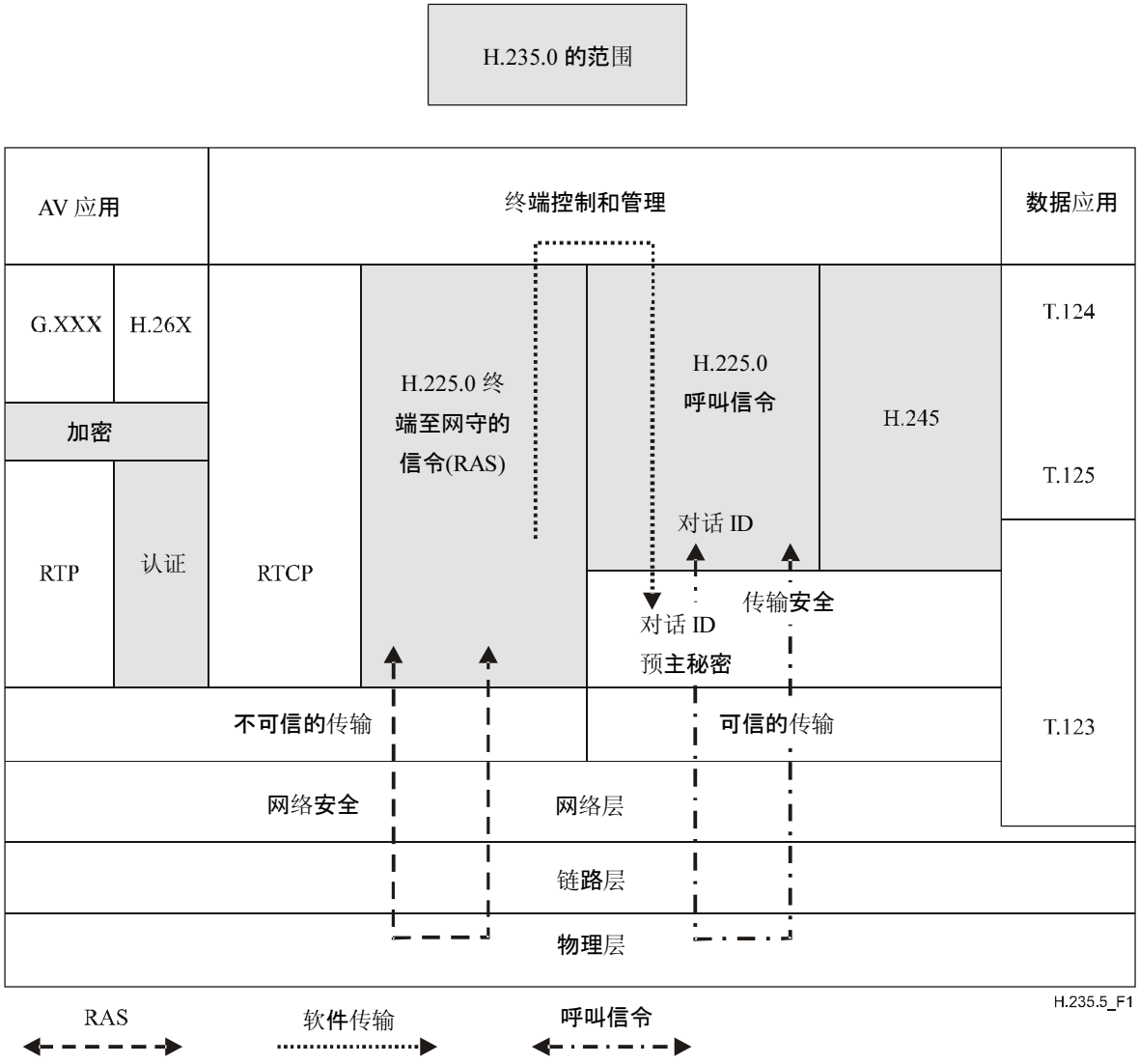

图 1/H.235.5－安全概要和TLS的信息流

以下描述为图 1 中的基础网络的各步骤提供参考。

9.1.1 端点注册

端点可以通过在概要 **ClearToken** 中包括一个或多个 **cipherSuite** 单元以及一个或多个 **compression** 单元，来测试网守的能力来支持被保护的 TLS 呼叫信令，该 **ClearToken** 包含在 GRQ 消息内，GRQ 消息则在前述的步骤 1 中发出。如果端点希望使用预先协商的对话，它还必须将 **sessionID** 包括在 **ClearToken** 中（必须指明只有与要求的对话相配的单个密码组和单个压缩方法）。如果协商是基于一个已经存在的 TLS 对话，除了 **nonce** 之外，概要 **ClearToken** 也不需要密码材料。

如果不存在一个请求的对话，则网守必须选择另一个认证概要（如有提供）或它必须回复一个包含 **GatekeeperRejectReason.resourceUnavailable** 的 GRJ。如果请求的对话确实已存在，主密钥资料是由 TLS 对话而获得，并被用来（伴随着由 GRQ 而来 **random** 的和网守生成的 **random2**）为 RAS 交换计算认证密钥。**sessionID**、**cipherSuite**, **compress** 方法以及网守的 **nonce** 必须在 GCF 中的概要 **ClearToken** 送回。

如果网守支持 TLS 对话协商，它必须按照概要所指定的方式来计算主密钥资料，指派一个新的对话 ID 并把它放在 **sessionID** 的概要 **ClearToken** 中发回。概要 **ClearToken** 还必须包含上面步骤 2 所要求的安全参数，伴随着一个单个的已选定的 **cipherSuite**，一个单个的已选定的 **compress** 方法以及非零的 **sessionID**。注意，已选定的密码组的密钥交换方法并不重要。如果网守同意呼叫信令的 TLS 保护，所有的在后续的 RRQ/RCF 或 ARQ/ACF 消息中交换的呼叫信令传输地址必须由 TLS 激活。

如果网守不支持 TLS 协商与/或网守选路，那么就不得有 TLS 参数传回，但是认证程序还是可以由上文所述的步骤 3 继续进行。端点必须决定它是否已准备好在呼叫信令没有 TLS 保护的情况下继续，它可以选择这样做也可以再利用认证概要。在注册序列成功完成时，TLS 对话已快速建立一个或多个与网守的呼叫信令连接，并已可使用，而不需要再通过公钥方法重新协商密钥资料。

TLS 对话的存续期是有限的。因此，端点有必要重新协商对话参数并获取新的对话 ID。这可以通过上文所述的在一个较轻便（保持活跃）的注册序列中交换必要的 **ClearToken** 单元来达成。此序列不得影响 RAS 认证密钥。

9.2 使用证书进行网守认证

虽然在 RAS 中交换可检验的证书链是不切实际的（由于 UDP 包的容量限制），但如果端点可以通过其他途径获取一个服务器公钥的可信版本，可以让服务器对端点进行自我认证。服务器可以在 GCF 消息中简单地包括一个 **CryptoH323Token.cryptoGKCert** 单元，并将其中的 **ClearToken.tokenOID** 设置为选定的安全概要 OID。

9.3 另一信令安全机制的应用

作为本建议书下的安全概要中的一部分的协商后的参数，可以为传输与/或应用层安全机制所使用，具体由特定的概要决定。在需要时加入到 H.235 **ClearToken** 中的 **profileInfo** 序列，就是为上述应用而提供的。

10 威胁（资料性参考）

10.1 被动攻击

目前，上文所述的方案不易遭到被动攻击，因为 Diffie-Hellman 协商不易遭到被动攻击。

10.2 拒绝服务攻击

本方案可能会遭受拒绝服务攻击，在此攻击中一个第三方对初始 GRQ 发出一个伪造的 GRJ 的响应。此类攻击可能可以也可能不可以用以下的方式识别：如果拒绝的网守是合法的，且知道共享秘密（如网守是端点的网守且 **rejectReason** 拒绝原因是 **resourceUnavailable** 资源无法提供），这样网守可以完成密钥协商并通过在 GRJ 中回复一个描述 GCF 的相同单元（例外情况是在 GCF **authenticationMode** 中回复的 OID，它回复到 GRJ 后将在 **ClearToken.profileInfo** 单元内）来对 GRJ 进行认证。这将留做一个特定概要的定义中的一部分。

如果 GRJ 没有认证，那么这可能来自于攻击者。在对 GRJ 做出反应之前（如寻找替代的网守），端点应等待可能接收的其他 GRJ，或从正当的网守发出的认证过的 GCF。否则，端点应对接收到的所有 GRJ（推测这些中的一个是合法的）中任一 **altGKInfo** 建议的网守进行尝试。不管在何种情况下，只有正当的网守（它知道共享秘密）可以回复认证过的 GCF。

10.3 中间人攻击

考虑采用未加密的 Diffie-Hellman 密钥交换，而使用口令或 PIN 从 Diffie-Hellman 秘密衍生对话密钥的交换方式是很吸引人的。不过，这种交换格式可能会遭受中间人攻击，它可使用完整性校验值，通过 GCF 消息提供的合法网守用强力攻击来发现“小”共享秘密。

当然，任一 MIM 能够操作任何认证过的 RAS 消息以确保消息将因为完整性检查失败而被丢弃。如果所有的消息都能被操作，服务也能被拒绝。

10.4 猜测攻击

攻击者可能佯装成合法的端点或合法的网守，或同时两者（中间人），且试图通过尝试和错误来猜测共享秘密。例如攻击者（假定它知道认证概要但不知道共享秘密的细节）可以猜测共享秘密并将这个猜测通过发送 GRQ 的方式来试图注册。通常，网守将对这个尝试给一个包含 GK 公钥（采用真正的共享秘密加密）的 GCF，以及一个采用取决于 GK 对攻击者的加密公钥的解密的衍生密钥计算的 ICV，作为响应。攻击者可以使用此信息来检验它对共享秘密的猜测。如果这个猜测证实了 GCF 的 ICV，那它很可能就等同于实际的共享秘密；这也可通过持续不断的注册序列来得到证实。如果这个猜想不能用来重现 GCF 中的 ICV，那么攻击者务必另做猜测并再次尝试。由于共享秘密的密钥空间较小，对于强力攻击搜索而言猜测的次数可能并不是禁止的。此攻击需要网守（或端点，如果攻击者佯装为网守的话）的积极参与。对于这样的攻击，传统的方法是监控未成功的尝试的次数，当达到门限阀值时，认为所有的后续尝试都是无效的（至少在某一特定时期）并发出警告，但上述过程是独立完成的。

10.5 未加密的网守半密钥

如上提到的，如果响应网守没有给它的Diffie-Hellman半密钥加密，EKE交换仍可在特定条件下保持安全。特别地，网守务必是经ICV展示自己对共享秘密（PIN）的了解的第一方。如果不是，那么网守（或是佯装为网守的闯入者）可以很简便地通过尝试所有可能的PIN来对端点的D-H半密钥进行解密，计算作为结果的D-H秘密、衍生认证密钥，并用它与端点提供的ICV进行测试。如果端点能首先检查网守提供的ICV，并在ICV和预期不一致时拒绝继续登记，这也就不可能发生了。

未加密的半密钥的使用对于网守的优越性在于它能够对不同的端点重复使用它自己相应的私钥。如果同一密钥在多方共享秘密或PIN下被加密分发的话，这也就不可能发生了。假如说一个第三方的旁观者可以收集两种不同PIN下的加密半密钥的实例，那它就可以在两个PIN的可能组合中搜索，看哪一对解密后能产生同样的半密钥。如果可能存在的PIN假如说有10^8个，那么需要尝试的可能组合也只有10^{16}个。这是一个相当于搜索54位随机数的问题，而它并不是完全办不到的。即使找到的可能答案不止一个，通过采用第三方观测也就能很快确定正确的答案。

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