国 际 电 信 联 盟

ITU-T H.235.0

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：H系列（H.323和其他基于H.245的）多媒体系统的安全性框架

ITU-T H.235.0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.235.0建议书

H.323安全性：H系列（H.323和其他基于H.245的）多媒体系统的安全性框架

摘　要

本建议书描述为纳入诸如认证和保密（数据加密）等安全性业务在 H.3xx 系列建议书框架内所做的改进。提出的方案适用于利用 ITU-T H.245 建议书作为控制协议的那些简单端到端和多点会议的任何终端；也适用于 H.225.0 RAS 和/或呼叫信令协议的 H.323 系统。

例如，H.323 系统是在不提供服务质量保证的分组网上运行的。由于同样的技术原因，基础网络也不提供 QoS，因此该网络不提供安全业务。非安全网络上的安全实时通信通常包括两个主要的有关领域 — 认证和保密。

本建议书描述由 H.3xx 系列多媒体终端所使用的安全性基础设施及专用的保密技术。本建议书将适用于有关的交互式会议范畴。这些范畴包括将在会议中交换的所有实时媒体流的认证和保密，但不完全局限于此。本建议书提供 H.323 实体间所必需的协议和算法。

本建议书利用 ITU-T H.245 建议书中所支持的通用设施，并且在这种情况下与该控制协议一起操作的任何标准均可使用该安全性框架。可以预料，在任何可能的情况下，其他的 H 系列终端可以交互操作并直接使用本建议书中所描述的方法。本建议书不会一开始就在所有方面规定全面实施，而将特别强调端点的认证与媒体保密。

本建议书包括一般的协商业务的能力和一般的功能以及对所用密码技术和能力的选择性。使用它们的具体方式与系统能力、应用需求及具体的安全性政策限制有关。本建议书支持多样化的密码算法，对不同的用途采用不同的算法；例如各种密钥长度。某些密码算法可指派给特定的安全性业务（例如，一个算法可指派给快速媒体流加密，而另一个算法可指派给信令加密）。

还应注意，某些有效的密码算法或机制可以预留供输出或其他国内用途（例如受限的密钥长度）。本建议书除了支持采用非标准化的或专利的密码算法的信令外，也支持采用常见算法的信令。不存在任何特定的强制性算法；但是强烈推荐端点必须尽可能多地支持可用的算法，以实现端点间的交互操作。这与支持 ITU-T H.245 建议书并不能确保两个实体的编译码器之间的交互操作能力的概念类似。

ITU-T H.235 第 4 版将原来的 ITU-T H.235v3 分成一套 H.235.x 子系列建议书，并重新组织子系列建议书。新的 ITU-T H.235.8 和 H.235.9 建议书已经被加入到系列中；其他的子系列建议书已被扩展赋予了新的功能性（ITU-T H.235.3 和 H.235.5 建议书）。ITU-T H.235.0 建议书具有共用内容的 H.323 安全性框架和对所有 H.235.x 子系列建议书都有用的一般信息。

新的 H.235.0 附录 IV、V 和 VI 提供 ITU-T H.235 第 3 版（2003），包括随后的勘误 1 和修正案，与新的建议书结构对应的文本、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.235.0 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，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

页

ITU-T H.235.0建议书

H.323安全性：H系列（H.323和其他基于H.245的）多媒体系统的安全性框架

1 范围

本建议书的主要目的是在当前的 H 系列协议框架内提供认证、保密以及完整性。本建议书的当前文本（2000）同 ITU-T H.323 建议书一道提供实施详情。预期本框架与采用 ITU-T H.245 建议书作为其控制协议的其他 H 系列协议一起和/或使用 H.225.0 RAS 和/或呼叫信令协议操作。

本建议书中包括的其他目标为：

1） 应将安全性体系结构开发成实施 H 系列终端安全性系统的可扩展的和灵活的框架。这必须通过由这些终端提供灵活的与独立的业务和功能来完成。这包括协商的能力以及对所用密码技术和能力的选择性及使用它们的方式。

2） 由于使用 H.3xx 协议而必须对所有通信提供安全性保障。这包括所有实体之间的连接建立、呼叫控制和媒体交换的各个方面。该要求包括使用机密通信（保密），并且可能利用对等认证和保护用户环境免受攻击的功能。

3） 本建议书将不排除 H.3xx 实体中可以保护它们不遭受来自网络攻击的其他的安全功能的集成。

4） 本建议书不应限制任何 H.3xx 系列建议书适当调节的能力。该调节可以包括安全用户的数目以及提供的安全性等级。

5） 在适当的条件下，无论基础传输或布局如何，都应提供所有的手段和设备。可以要求本建议书范围以外的其他手段来抵御这种威胁。

6） 制定有助于在混合环境中操作的规则（安全的和非安全的实体环境）。

7） 本建议书应提供分发与所用密码有关的对话密钥的设施。（这不意味着基于公钥的证书管理务必是本建议书的一部分。）

8） 本建议书提供了两种易于交互的安全概要。H.235.1 描述一个简单而安全的基于口令的安全概要，同时，H.235.2 克服了 H.235.1 的局限性，它是配置数字签名、证书和公钥基础设施的签名安全概要。

本建议书中描述的安全性体系未假定参与方彼此熟悉。但假定已采取适当的防范措施以便实际保护 H 系列端点。由此，对通信的主要安全性威胁假定为来自网络上的窃听或改道传输媒体流的一些其他方法。

ITU-T H.323 建议书提供在两个或多个同线用户之间进行音频、视频和数据会议的方法，但未提供允许每个参与方鉴别其他参与方身份的机制，也未提供使通信保密（即加密该流）的方法。

ITU-T H.323、H.324 和 H.310 建议书利用 ITU-T H.245 建议书的逻辑信道信令规程，该规程描述信道开放时每个逻辑信道的内容。对接收者和传输方能力的表示规程做了规定，传输限于接收者所能译码的范围内，并且接收者可以请求来自传输方的特殊理想模式。每个端点的安全能力采用与任何其他通信能力相同的方式通信。

某些 H 系列（H.323）终端可用于多点配置。本建议书中描述的安全性机制将考虑在这些环境中的安全性操作，包括集中式和分散式 MCU 操作。

1.1 H.235.x子系列建议书的结构

这一安全性框架建议书包含下列 H.235.x 子系列建议书中的结构，如图 1 所示。本建议书包含公共内容和对于所有 H.235.x 子系列建议书都有用的一般消息。

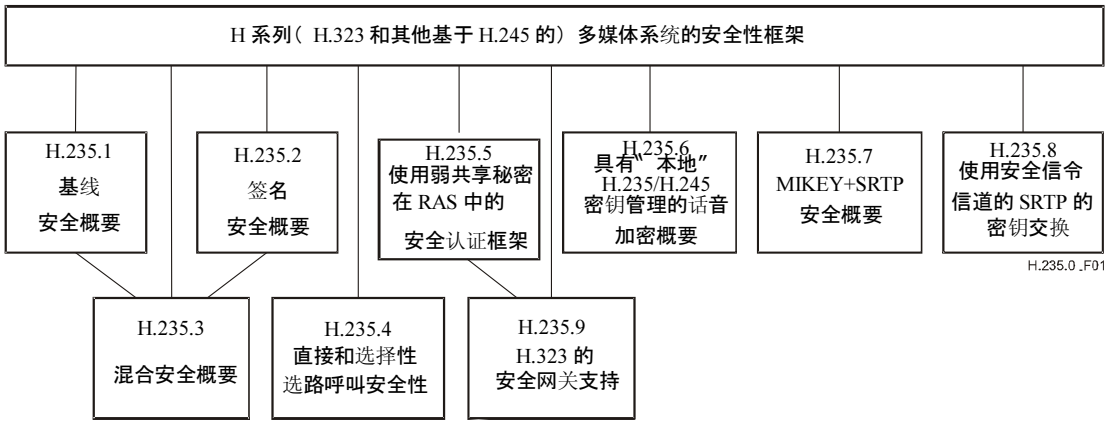


图 1/H.235.0－H.235.x子系列建议书的结构

图 1 中的垂直线指示直接从属于 H.235.0 正文；也可以较间接地从属于其他 H.235.x 建议书。有几个建议书可以一起补充使用，也见第 6.9 节。

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* plus Amendment 1 (2004), plus Corrigendum 1 (2005).

– 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.235.3 (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.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.

– 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.235.7 (2005), *H.323 security: Usage of the MIKEY key management protocol for the Secure Real Time Transport Protocol (SRTP) within H.235*.

– ITU-T Recommendation H.235.8 (2005), *H.323 security: Key exchange for SRTP using secure signalling channels*.

– ITU-T Recommendation H.235.9 (2005), *H.323 security: Security gateway support for H.323*.

– 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 H.530 (2002), *Symmetric security procedures for H.323 mobility in H.510,* plus Corrigendum 1 (2003).

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

– 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*.

– ISO/IEC 9798-2:1999, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*.

– ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanism using digital signature techniques*.

– ISO/IEC 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.*

– ISO/IEC 15946-1:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

– ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

– ATM Forum: af-sec-0100.002 (2001), *ATM Security Specification Version 1.1*.

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

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

– IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP.*

– IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP).*

– IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*

– IETF RFC 3546 (2003), Transport Layer Security Protocol (TLS) Extensions.

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

2.2 资料性参考文献

[Daemon] DAEMON (J.), *Cipher and Hash function design*, Ph.D. Thesis, Katholieke Universiteit Leuven, March 1995.

[ESP] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*.

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

[IKE] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

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

[J.170] ITU-T Recommendation J.170 (2005), *IPCablecom security specification*.

[RTP] IETF RFC 3550 (2003), *RTP: A transport Protocol for Real-Time Applications*.

[Schneier] SCHNEIER (B.), *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, Inc., 1995.

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

3 术语和定义

出于本建议书的目的，除本节中的定义适用外，第 3 节/H.323、第 3 节/H.225.0 和第 3 节/H.245 中给出的定义也适用。本建议书中使用的一些术语也在 ITU-T X.800 建议书 | ISO 7498-2 和 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 中定义。

3.1 access control 接入控制：防止资源的未授权使用，包括防止以未授权的方式使用资源（ITU-T X.800 建议书）。

3.2 authentication 认证：对实体具有的身份提供保证（ITU-T X.811 建议书 | ISO/IEC 10181-2）。

3.3 authorization 授权：根据已认证的身份授予许可权。

3.4 attack 攻击：为绕过系统的安全机制或利用其不足所采取的行动。对系统的直接攻击利用的是安全机制的基础算法、原理或特性的缺陷。非直接攻击是指绕过安全机制或使系统错误地使用安全机制。

3.5 certificate 证书：由安全机构或可信的第三方发布的一系列与安全性有关的数据以及为数据提供完整性和数据源认证业务的安全性信息（ITU-T X.810 建议书 | ISO/IEC 10181-1）。本建议书中该术语指的是“公钥”证书，也就是由可信机构以不可伪造的格式所核实和签署的所有者公钥赋值（以及其他任选信息）。

3.6 cipher 密码：一种密码算法，一种数学变换。

3.7 confidentiality 机密性：防止将信息泄露给非授权的个体、实体或过程的特性。

3.8 cryptographic algorithm 密码算法：从一个或几个输入值计算结果的数学函数。

3.8 *bis* EC-GDSA：带有附录的椭圆曲线数字签名，与 NIST 数字签名算法（DSA）类似（也见 ISO/IEC 15946-2，第 5 章）。

3.8 *ter* elliptic Curve Cryptosystem 椭圆曲线密码系统：公钥加密系统（见 ATM 论坛安全规范第 1.1 版的第 8.7 节）。

3.8 *quat* elliptic Curve Key Agreement Scheme 椭圆曲线密钥协议机制 — Diffie-Hellman：使用椭圆曲线加密的 Diffie-Hellman 密钥协议方案。

3.9 encipherment 加密：加密（加扰）是通过运行密码算法（加密算法）使数据对于非授权实体变得不可解读的过程。解密（去扰）是相反的操作，通过该操作将密文变换成明文。

3.10 integrity 完整性：数据未曾以非授权方式变更的特性。

3.11 key management 密钥管理：按照安全性对策的密钥生成、存储、分发、删除、存档和使用（ITU-T X.800 建议书）。

3.12 media stream 媒体流：媒体流可以分成音频、视频、数据或它们任意类型的组合。媒体流数据传送用户数据或应用数据（有效载荷），但不传送控制数据。

3.13 non-repudiation 不可否认：防止参与通信的某个实体否认曾参与了整个或部分通信。

3.14 privacy 保密：通信的一种方式，以此方式只有明确授权的同线用户才可以解释该通信。这通常可以通过加密和密码的共享密钥来实现。

3.15 private channel 专用信道：对本建议书而言，专用信道是在安全信道上事先协商确定的一个信道。就此而言，它可用于处理媒体流。

3.16 public key cryptography 公钥密码：利用非对称密钥（供加密/解密）的加密系统，系统中密钥间有一种彼此之间不能合理计算的数学关系。

3.17 security profile 安全概要：出自 ITU-T H.235 建议书的一致的、可交互操作的规程和特性（子）集，它对于保证特定通信配置中参与通信的各实体间的 H.323 多媒体通信的安全是有用的。

3.18 spamming 滥发：向系统过度发送非授权数据的拒绝服务攻击。一种特定的情况是 UDP 端口上发送 RTP 分组的媒体滥发。通常该系统被分组溢满；要消耗宝贵的系统资源进行处理。

3.19 symmetric（secret-key based）cryptographic algorithm 对称（基于密钥的）密码算法：实施加密的一种算法，或实施解密的相应算法；对于加密和解密均要求同样的密钥（ITU-T X.810 建议书 | ISO/IEC 10181-1）。

3.20 threat 威胁：安全性的潜在侵害（ITU-T X.800 建议书 | ISO 7498-2）。

4 符号和缩写

本建议书使用下列缩写：

X || Y	X 和 Y 并置
3DES	三倍 DES
AES	高级加密算法
ALG	应用层网关
ASN.1	抽象句法记法 1
BES	后端服务器
CA	认证机构
CBC	密码块链接
CFB	密码反馈模式
CRL	证书撤销一览表
DES	数据加密标准
DH	Diffie-Hellman
DNS	域名系统
DSS	数字签名标准
DTMF	双音多频
ECB	电子代码本
ECC 和 EC	椭圆曲线密码系统（见“*ATM 论坛安全规范第 1.1 版*”第 8.7 节）。一种公钥密码系统。
EC-GDSA	带有附录的椭圆曲线数字签名，与 NIST 数字签名算法（DSA）类似（也见[ISO/IEC 15946-2，第 5 章]）
ECKAS-DH	椭圆曲线密钥协议方案 — Diffie-Hellman。使用椭圆曲线加密的 Diffie-Hellman 密钥协议方案
EOFB	增强型 OFB 模式
EP	端点
GK	网守
GW	网关
ICV	完整性检验值
ID	标识符
IETF	互联网工程任务组
IPsec	网际协议安全性
ISAKMP	互联网安全协会密钥管理协议

ISO	国际标准化组织
IV	初始化矢量
LDAP	轻便式号码簿接入协议
MAC	消息认证码
MC	组播控制器
MCU	多点控制单元
MPS	多个有效载荷流
NAT	网络地址解析
OCSP	在线证书状态协议
OFB	输出反馈模式
OID	对象标识符
PDU	协议数据单位
PKI	公钥基础设施
POTS	普通老式电话业务
PRF	伪随机函数
Q&A	问题与答案
QoS	服务质量
RAS	注册、认可和状态
RSA	Rivest、Shamir 和 Adleman（公钥算法）
RTCP	实时传输控制协议
RTP	实时传输协议
SASET	安全音频简单端点类型
SDU	业务数据单元
SHA1	安全散列算法 1
SRTP	安全实时传输协议
SSL	安全套接字层
TLS	传输层安全性
TSAP	传输业务接入点
TTP	可信的第三方
UDP	用户数据报协议
XOR，⊕	异运算

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。

引用的节、子节、附件和附录指的都是本建议书的内容，除非明确列出另一个建议书。例如，“1.4”是指本建议书的第 1.4 节；“6.4/H.245”是指 ITU-T H.245 建议书的第 6.4 节。

本建议书描述“n”种不同消息类型的使用：H.245、RAS、Q.931 等。为区分不同的消息类型，采用以下惯例。H.245 消息和参数名称由多个串接的黑体字组成（**maximumDelayJitter**）。RAS 消息名称表示为 3 个字母的缩写（**ARQ**）。Q.931 消息名称由一个或两个首字母大写的单词组成（**Call Proceeding**）。

本建议书使用设置一个复合的 ASN.1 数据结构为 NULL 的符号；例如，“**paramS** 设置为 NULL”（见第 7 节/H.235.1、第 8 节/H.235.1、9.1/H.235.1、 9.2/H.235.1、第 7 节/H.235.2、第 9 节/H.235.2、15.1/H.235.2 和 15.2/H.235.2）。这必须意味着在特定 SEQUENCE（即 **Params**）中所有任选的元素都缺省。

本建议书定义了信令安全性能、程序或安全算法的各种对象标识符（OID）。这些 OID 与指定值的序列树相关，这些值可能来自外部源或是 ITU-T 保持的 OID 树的一部分。特别地，与 ITU-T H.235 建议书相关的那些 OID 在文本中有下列表述：

“OID” = {itu-t（0）recommendation（0）h（8）235 version（0）**V N**}，其中 **V** 象征性地代表一个十进制的数字，它指示 ITU-T H.235 建议书的对应版本；如 1、2、3 或 4。**N** 象征性地代表一个十进制的数字，它惟一地标识 OID 实例，因而标识程序、算法或安全性能。

因此，ASN.1 编码 OID 由数字序列组成。为方便起见，每个 OID 的电文助记速写串符号在报文中使用，如“OID”。给出每个 OID 串与 ASN.1 数字序列相关的映射。遵循 ITU-T H.235 建议书的实施必须仅使用 ASN.1 编码数字。

6 系统引言

图 2 给出 ITU-T H.323 建议书内的本建议书的范围的概述。

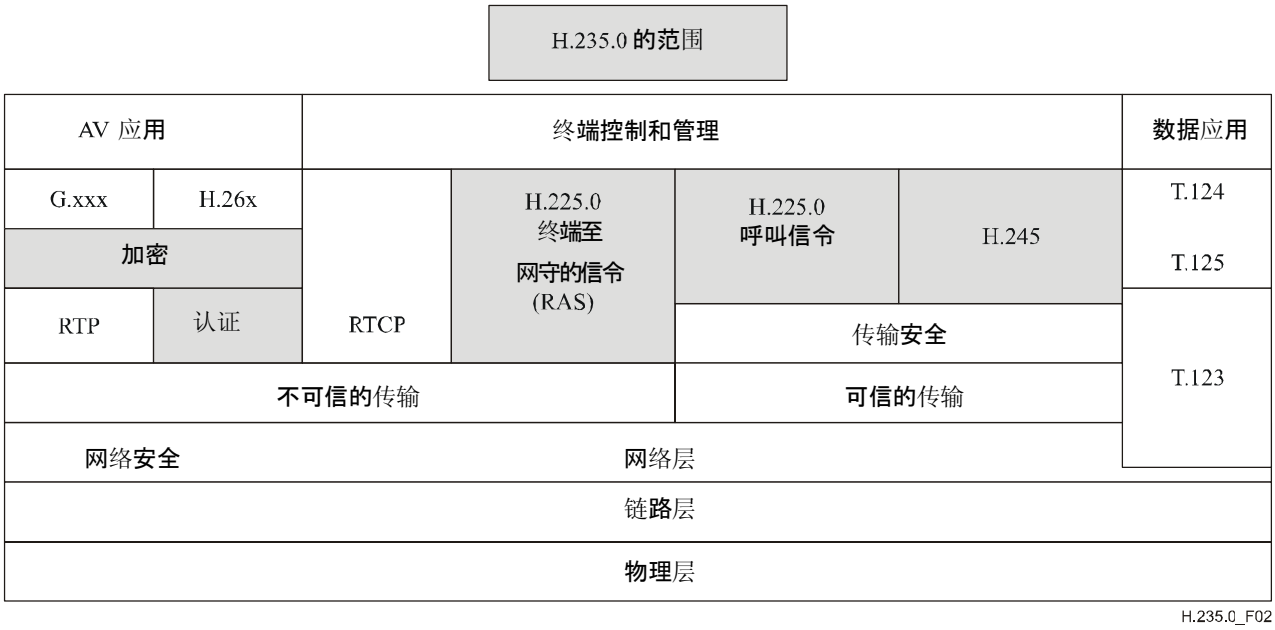


图 2/H.235.0－概述

对于 ITU-T H.323 建议书，TLS（RFC 2246，RFC 3546）使用的信令、IPsec 或有关 H.245 控制信道的所有权机制必须在初始 Q.931 消息交换期间在安全或不安全的 H.225.0 信道上发生。

6.1 摘要

1） 在众所周知的安全端口（ITU-T H.225.0 建议书），呼叫信令信道可以使用 TLS（RFC 2246，RFC 3546）或 IPsec（RFC 2401，[ESP]）保证安全。

2） 用户的认证可以在初始呼叫连接期间，在使 H.245 信道安全的处理中进行和/或可以通过在 H.245 信道上交换证书来完成。

3） 媒体信道的加密能力通过扩展现有的能力协商机制来确定。

4） 来自主控方密钥资料的初始分配由 H.245 **OpenLogicalChannel** 或 **OpenLogicalChannelAck**。

5） 重置密钥可通过 H.245 指令：**EncryptionUpdateCommand**、**EncryptionUpdateRequest**、**EncryptionUpdate** 和 **EncryptionUpdateAck** 来完成。

6） 保护密钥资料分配或者通过做为专用信道来运行 H.245 信道，或者通过使用选择的交换证书对密钥资料加以精心的保护。

7） 提出的安全性协议或者符合 ISO 出版的标准，或者符合 IETF 提出的标准。

6.2 认证

认证就是核实应答者是否确实是自称的身份的过程。认证可以与基于公钥的证书的交换一起完成。认证也可通过利用参与的实体间交换共享的秘密来实现。该秘密可以是静态的口令，也可以是一些其他先验的信息。

本建议书描述交换证书的协议，但未规定互相核实和接受证书所使用的准则。通常，证书向校验方保证该证书提供者确为其人。交换证书背后隐含的意图是鉴别该端点的用户，而不仅仅是实际端点。认证协议使用数字证书证实响应方拥有与包含在该证书中的公钥相对应的私钥。该认证可以保护免受中间人攻击，但不能自动证实所谓的响应方。要做到这一点，一般要求存在某种考虑该证书其他内容的方针。例如，对于授权证书来说，证书通常会包含服务提供商的标识以及由服务提供商给出的某种格式的用户记账标识。

除证书协议所要求的范围外，本建议书中认证框架未规定证书的内容（即未指定证书政策）。然而使用该框架的应用可以施加高层政策要求，如把证书交给用户批准。高层政策或者可以在应用中自动生成或者需要人工交互。

对于不使用数字证书的认证而言，本建议书提供信令来完成各种不同的查询/响应方案。这种认证的方法要求通过通信实体的先期协调以可获得共享的秘密。该方法的一个实例是基于预订业务的用户。

作为第三种选择，认证可以在单独的安全性协议环境范围内实现，诸如 TLS[RFC 2246，RFC 3546]或 RFC 2409[IKE]。

双向的或单向的认证均可以由对等的实体支持。该认证可在某些或全部的通信信道上发生。

本建议书中所描述的所有特定的认证机制等同于或来源于如在 ISO/IEC 9798 的第 2、3 部分中所指定的 ISO 制定的算法，或以 IETF 协议为根据。

6.2.1 证书

证书的标准化，包括它们的生成、管理和分配超出本建议书的范围。用于建立安全信道（呼叫信令和/或呼叫控制）的证书必须遵从曾经协商用来保护该信道安全的那些协议所规定的那些条款。

应予注意，对于使用公钥证书的认证，要求端点使用有关的私钥赋值来提供数字签名。公钥证书交换本身不能抵御中间人攻击。H.235 协议符合此要求。

6.3 呼叫建立安全性

至少存在两个理由来激发保护呼叫建立信道的安全（例如使用 Q.931 的 H.323）。第一个理由是受理呼叫之前的简单认证要求。第二个理由是容许呼叫授权。如果 H 系列终端中需要此功能，在呼叫连接消息交换之前，应使用安全的通信方式（例如 H.323 的 TLS/IPsec）。另外，可以根据业务特定的认证提供授权。业务特定的认证政策的限制超出本建议书的范围。

6.4 呼叫控制（H.245）安全性

呼叫控制信道（H.245）也应以某种方式保证其安全以提供后续媒体的保密。H.245 信道必须使用任何商定的保密机制来保证其安全（这包括“无任何保护”的选项）。利用 H.245 消息表明该共享的、专用的媒体信道中所使用的加密算法和密钥。在逐个逻辑信道上做到这一点的能力使不同的媒体信道能由不同的体制加密。例如，集中式多点会议中，对于到每个端点的流可以使用不同的密钥。因此，对会议中的每个端点而言，媒体流都是保密的。为了以安全的方式利用 H.245 消息，整个 H.245 信道（逻辑信道 0）应以商定的安全方式开放。

保护 H.245 安全的机制取决于所用的 H 系列终端。对采用这种安全结构的所有系统的惟一的要求是每个系统均必须具备某种方式，用于在 H.245 信道实际启动之前协商和/或表明 H.245 信道运行所用的特殊安全方式。例如，H.323 将使用 H.225.0 连接信令消息实现这一点。

6.5 媒体流保密

本建议书描述基于分组传输所携载的媒体流的媒体保密。相对于 H.245 逻辑信道特性，这些信道可以为单向。在物理层或传输层不要求信道为单向。

获取媒体保密的第一步应为提供专用控制信道，在该专用控制信道上建立密码加密资料和/或建立将携载加密媒体流的逻辑信道。为达此目的，当在安全会议中运行时，任何参与端点均可使用加密的 H.245 信道。以此方式，在 H.245 **OpenLogicalChannel** 指令中传送的密码算法选择和加密密钥受到保护。

只要 H.245 安全信道提供相互可接受的保密等级，H.245 安全信道就可以采用有别于其他专用媒体信道中的那些特性来运行。这就使媒体流及任何以完全独立的方式运行的控制信道得到安全措施强度和复杂度完全不同的保护。

若要求 H.245 信道以非加密的方式运行，则特定的媒体加密密钥可以通过参与方协商一致认可并签署的方式单个加密。**h235Control** 类型的逻辑信道可用于提供资料以保护媒体加密密钥。该逻辑信道可以任何适当的协商方式运行。

逻辑信道中携载的数据保密（加密）必须采用 **OpenLogicalChannel** 所指定的格式。与传输有关的头信息应不加密。数据的保密将依据端到端加密。

6.6 可信单元

认证（信任）和保密的基础由通信信道的终端定义。对于连接建立信道，它可以处在主叫方和主网络部件之间。例如，电话机“相信”网络交换机将会把它连至它所拨叫的电话机。由于这个原因，终接一个加密的 H.245 控制信道或终接任何 **encryptedData** 类型逻辑信道的任何实体均必须看做该连接的可信单元；这可以包括 MC（U）和网关。信任一个单元的结果是有信心向该单元泄露保密机制（算法和密钥）。

根据以上给定的假设，鉴别任意的和所有的“可信”单元是通信路径上参与方义不容辞的职责。如对“标准的”端到端认证所发生的上述行为，通常将通过证书交换来完成。除推荐对使用该可信单元的所有实体该证书为可接受的之外，本建议书将不要求任何特定级别的认证。信任模型和证书政策的详情有待进一步研究。

只有证明可信单元间的连接可以抵御中间人攻击时，才能确保两个端点之间的保密。

6.6.1 密钥托管

尽管没有特定的操作要求，本建议书包含实体使用 H.235 协议支持信令单元内被称为可信的第三方（TTP）设施的规定。

恢复丢失的媒体加密密钥的能力在最好有该功能或请求有该功能的设备中应得到支持。

密钥托管这种设施常常被称做可信的第三方（TTP）。该设施有待进一步研究。

6.7 不可否认

有待进一步研究。

6.8 移动安全性

按照 ITU-T H.510 建议书，基于 H.323 的系统可能在移动的环境中采用。这样的系统的安全性规程和协议在 ITU-T H.530 建议书中描述。ITU-T H.530 建议书采用本建议书中的协议和规程。

6.9 安全概要

本建议书参考一套 H.235 安全概要（即 H.235.1、H.235.2、H.235.3、H.235.4、H.235.5、H.235.6、H.235.7、H.235.8 和 H.235.9）。安全概要规定了完好定义的环境和范围应用性下的 H.235 或 H.235 功能性子集的具体使用。

依据环境和应用，安全概要可以选择性地实施或一起实施。通常，允许 H.235 的系统在作为信令消息的一部分的对象标识符内标识采用哪一个安全概要。允许 H.235 的系统必须依据其需要选择安全概要。

任选地，最初端点可以就在 **RRQ/GRQ** 消息中同时提供多个安全概要，让网守在 **RCF/GCF** 消息中回答它以选择一个最充分的概要。在网守间的 **LRQ/LCF** 处理也可以携载几个安全概要。当计算数字签名或散列值以提供消息完整性时，首先必须在消息的字节子集和字节集上计算不提供消息完整性的散列值和数字签名，提供消息完整性的所有数字签名和散列值应在消息缓存器中置 0，然后应使用这个缓存器计算所有的数字签名和散列值，然后在消息中置数。

子系列建议书中的每一个都是作为 H.235.0 的安全概要编写的。H.235.0 安全概要典型地在特定的情形中包含一个 H.235.0 的使用情况特定实例和/或有一个特定的安全性特征规范或安全性机制/安全概要的组合。

所有的安全概要在 H.235.0 内是可选的。

图 3 显示安全概要的某些典型和可能的组合。直线指示成对的安全概要组合被定义，是可能的。虚线指示组合通常是可能的，然而这样的组合可能不是很有用。没有连线指示特定的组合还未定义。

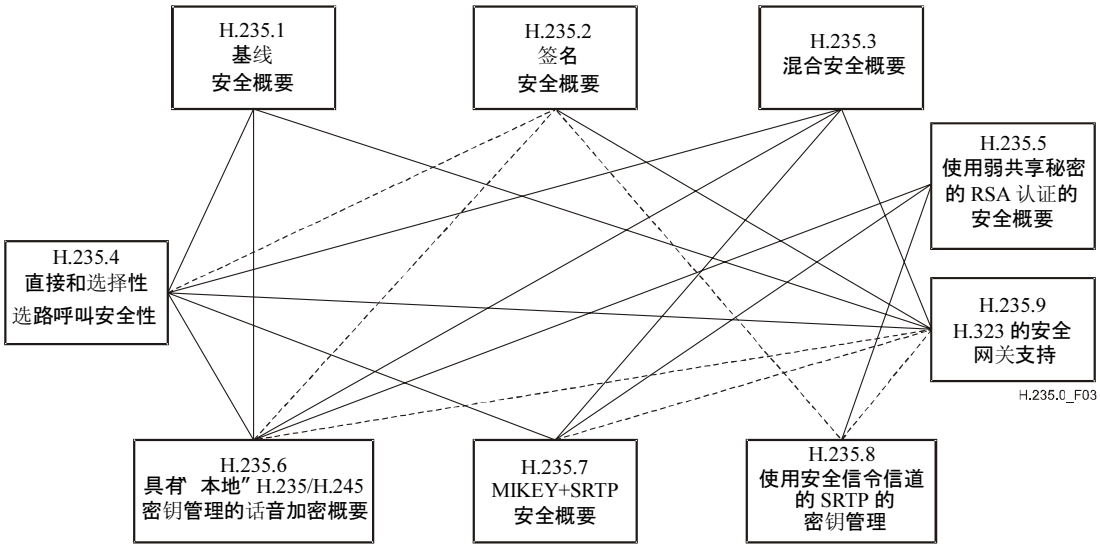


图 3/H.235.0－安全概要组合图示

6.10 安全的NAT/防火墙遍历

ITU-T H.235.9 建议书规定为了保留信令完整性和保密，如何在 H.323 实体之间在 H.225.0 RAS 信令通路内探索安全网关（如 ALG）的存在，以及网守和安全网关是如何共享安全性信息的。

ITU-T H.235.1 建议书（规程 IA）和 H.235.2 建议书（仅认证规程）提供了对特定规程的补充，以允许 H.225.0 RAS 和呼叫信令协议的基于 H.235 的消息认证能够遍历 NAT/防火墙设备。

7 连接建立规程

如系统引言子节中所阐述的，呼叫连接信道（H.323 系列的 H.225.0）和呼叫控制（H.245）信道必须以商定的安全方式或非安全方式从首次交换开始起操作。对于呼叫连接信道，这是预先完成的（对于 H.323，TLS 安全的 TSAP（端口 1300）必须供 Q.931 消息使用）。对于呼叫控制信道，安全方式由 H 系列终端所用的初始连接建立协议中所传送的信息来确定。

在不存在任何重叠安全能力的情况下，被叫端可以拒绝该连接。返还的误差不应传递任何有关安全性失配的信息；主叫端将不得不通过某些其他手段来确定原因。主叫端如收到不具备充分的安全性能力的连接确认消息，应终止该呼叫。

若主叫端和被叫端有相互兼容的安全能力，双方必须假定 H.245 信道以商定的安全方式操作。采用此处确定的安全方式而未能建立 H.245 信道应被认为是协议错误并应终止连接。

ITU-T H.235.6 建议书提供了更进一步的安全性连接确定规程，包括密钥管理；见第 7 节和第 8 节/H.235.6。

8 认证信令和规程

通常，认证或者依据使用共享的秘密（只要知道该秘密就正确地完成了认证）或依据采用证书的基于公钥的方法（通过拥有正确的私钥来证明其身份）。共享秘密以及后续使用的对称密码要求通信实体之间事先接触。事先的面对面或安全接触能够采用根据公钥密码的方法通过生成或交换共享密钥来替代，例如通过 Diffie-Hellman 密钥交换。在密钥生成和交换中通信各用户方不得不通过使用数字签名消息等进行认证；否则，通信各方无法确信它们与谁共享秘密。

本建议书描述基于预订的认证方法，即为了共享秘密务必事先接触的认证方法以及在认证中直接使用公钥密码或者用公钥生成共享秘密的认证方法。

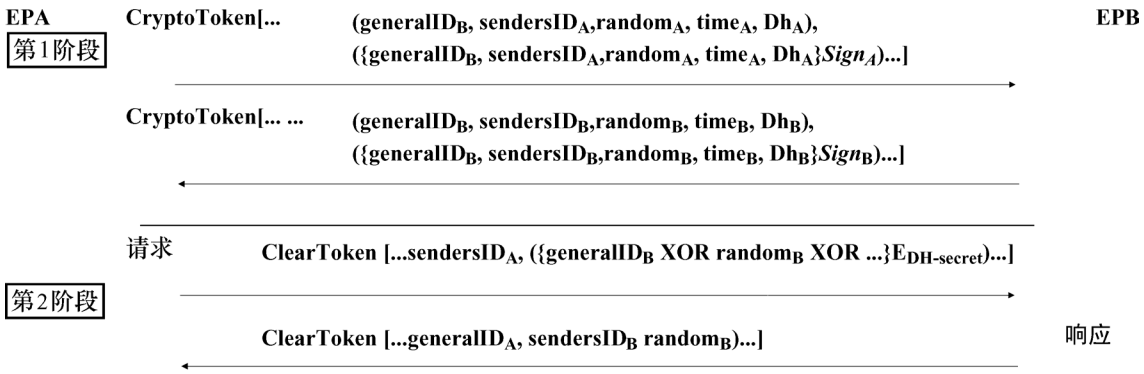
8.1 采用任选认证的Diffie-Hellman

本子节的目的不是提供绝对的、用户级认证。此方法提供信令以生成双方实体间可以导致专用通信加密资料的共享秘密。

在该交换结束时，双方实体都会拥有共享的秘密密钥和使用该密钥所用的算法。此时该共享的秘密密钥才可以在任何后续的请求/响应交换中使用。应予注意在极少数情况下，对特殊算法 Diffie-Hellman 交换或许产生众所周知的弱密钥。在此种情形下，任何一方的实体均应中断并再次连接以建立新的密钥集。

图 4 的第 1 阶段说明 Diffie-Hellman 期间的数据交换。第 2 阶段容许特定应用或特定协议请求消息由响应方予以认证。注意伴随每次响应均会返还一个新的随机值。

注 — 若在非安全信道上交换消息，则为了对共享秘密的各方用户进行认证，务必使用数字签名（或其他消息源认证方法）。也可提供一个任选的签名单元；以下这些用**黑斜体字**说明。



[... ...] 表示令牌序列。

() 表示特殊令牌，可以包含多个单元。

{}$E_{DH\text{-}secret}$ 表示所包含的数值被采用 Diffie-Hellman 秘密算法加密。

EPB 知道使用哪个共享密钥通过与 **generalID$_A$** 联合来解密 **generalID$_B$** 标识符，**generalID$_A$** 也应作为 **sendersID$_A$** 在消息中传送。应注意的是，为简化编码第 2 阶段的加密值在 **ClearToken** 的 **generalID** 字段中通过。

图 4/H.235.0－采用任选认证的Diffie-Hellman

8.2 基于预订的认证

尽管此处概述的规程（以及产生它们的 ISO 算法）在性质上是双向的，但是若认证仅在某个方向上需求，则规程也可以仅只在一个方向上使用。对二次扫描和三次扫描规程做了描述。当源自反向的消息不需要认证时，可仅在一个方向上实施相互的二次扫描认证。这些交换假定每个端点拥有某个惟一标识它的熟知的标识符（如文本标识符）。对于二次扫描规程而言，还要进一步假设存在相互可接受的时间基准（由此衍生时间标记）。可接受的时间偏移容限为本地实施事务。作为来自认证方的一次查询，三次扫描规程使用随机生成的、不可预测的查询编号（可由顺序计数器“随机”增加）。该随机数拟用于防止重放攻击。不同于二次扫描规程，三次扫描规程对包含启动方查询的第一个初始消息不做认证。

依据需求，存在 3 种可以实施的不同变种：

1） 具有对称加密的基于口令的认证；

2） 具有散列的基于口令的认证；

3） 具有签名的基于证书的认证。

在所有的情形中依据所选择的变种，令牌将包含以下子节中所描述的信息。注意，在所有的情形中，该 **generalID** 可以通过配置或目录查寻已知而绝非在频带协议交换中已知。为了简化接收者处理，发送者应在 **sendersID** 中包含其标识符，并将 **generalID** 设置为接收者的标识。

注 1 — 在时间标记作为安全性交换的一部分被生成和通过的所有情形中，实施者应采取以下预防措施。时间标记的分段应足够细致，以担保伴随每个消息而增加。若此点不能担保，则有可能遭受重放攻击。（例如，若时间标记仅按分钟增加，则在端点“A”向端点“B”发送消息之后一分钟的持续时间内端点“C”能够欺骗端点“A”）。

注 2 — 若该消息为组播，则消息不安全。

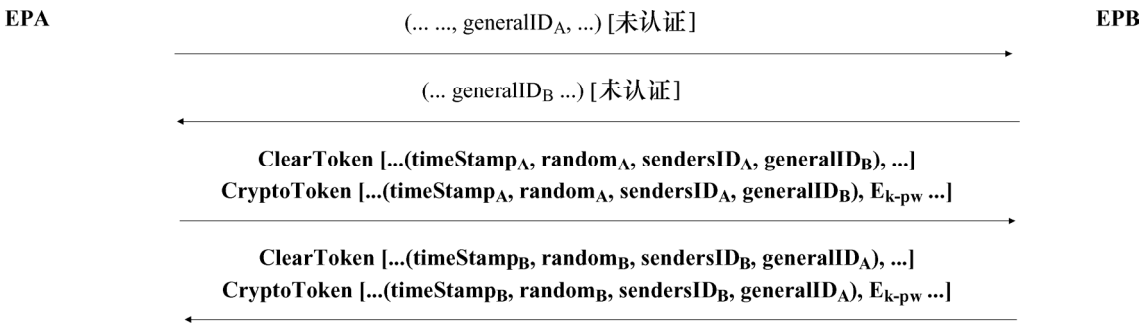
8.2.1 具有对称加密的口令

图 5 和图 6 分别显示在二次扫描或三次扫描中实施此类认证所要求的令牌格式与消息交换。本协议依据 ISO/IEC 9798-2 的 5.2.1（二次扫描）和 5.2.2（三次扫描）；假定标识符和相关口令在预订时交换。加密密钥为 N 个八比特组长（如算法 ID 所指出的），并构成如下：

— 若口令长度=N，则密钥＝口令；

— 若口令长度<N，则密钥填充 0；

— 若口令长度>N，则头 N 个八比特组指派给密钥，然后该口令的第 N+M 个八比特组与第 Mmod（N）个八比特组异或（对所有超过 N 的八比特组）（即所有“多余”的口令八比特组通过异或反复在密钥上合并）。



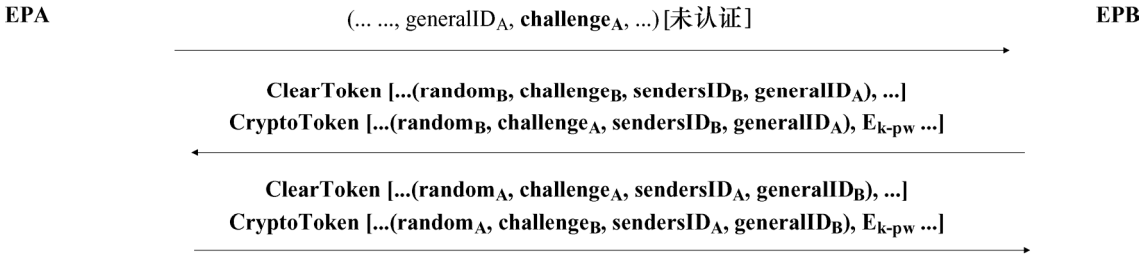
注 1 — 来自 EPB 的该返还令牌为任选；若省略，则仅实现单向认证。

注 2 — **E$_{k-pw}$** 表示使用从口令“pw”衍生的密钥“k”所加密的赋值。

注 3 — **random** 为单调递增计数器，使多路消息具有惟一相同的时间标记。

注 4 — 在第 3 消息中，EPA 提供单独的 **ClearToken**，通过与 **CryptoToken** 中同样的 OID 来标识；对第 4 消息类似，反之亦然。

图 5/H.235.0－具有对称加密的口令，二次扫描



注 1 — 若希望单向认证，则 **challenge$_A$** 和从 B 到 A 的返还加密的 **CryptoToken** 不是必要的。

注 2 — **E$_{k-pw}$** 表示使用从口令“pw”衍生的密钥“k”进行加密的加密操作。

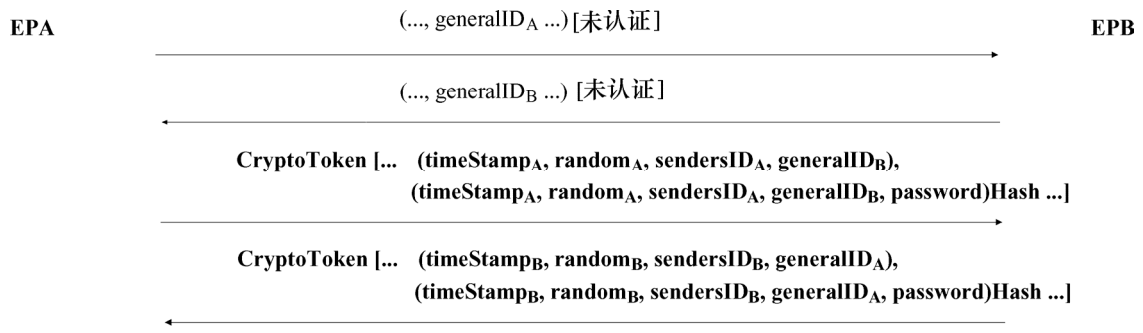
注 3 — 在第 3 消息中，EPA 在嵌入的编码的 **GeneralToken** 中以明文方式提供一个新的 **challenge$_A$**。作为响应，EPA 也返还 **challenge$_B$**；对第 2 消息类似，反之亦然。

注 4 — 对于多路未完成消息，**random**（即单调递增计数器）必须使查询成为惟一的。

图 6/H.235.0－具有对称加密的口令，三次扫描

8.2.2 具有散列的口令

图 7 和图 8 分别显示在二次扫描或三次扫描中实施此类认证所要求的令牌格式与消息交换。本协议依据 ISO/IEC 9798-4 的第 5.2.1 和 5.2.2 节；假定标识符和相关口令在预订时交换。ITU-T H.235.1 建议书提供二次扫描散列规程的详细描述。

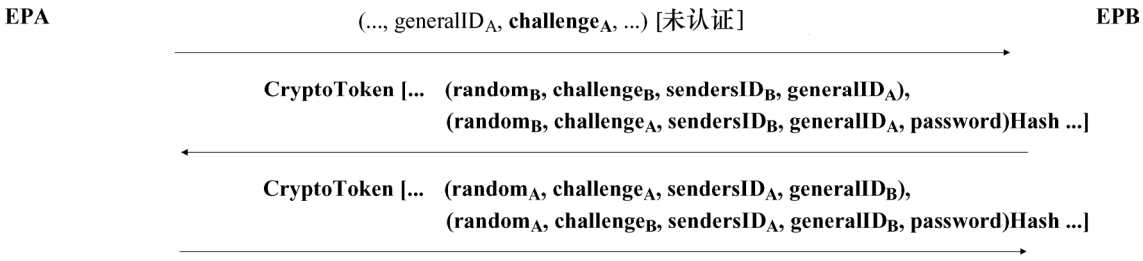


注 1 — 来自 EPB 的返还令牌为任选；若省略，则仅实现单向认证。

注 2 — **Hash** 表示对所包含的值进行运算的散列函数。

注 3 — **random** 为单调递增计数器，以区分具有同一时间标记的多路消息。

图 7/H.235.0－具有hash的口令，二次扫描



注 1 — 来自 EPB 的返还令牌为任选；若省略，则仅实现单向认证。

注 2 — Hash 表示对所包含的值进行运算的散列函数。

注 3 — 在第 3 消息中，EPA 在嵌入的编码的 **GeneralToken** 中以明文方式提供一个新的 **challenge$_A$**。作为响应，EPA 也返还 **challenge$_B$**；对第 2 消息类似，反之亦然。

注 4 — 对于多路未完成消息，**random**（即单调递增计数器）必须使查询成为惟一的。

图 8/H.235.0－具有hash的口令，三次扫描

注 1 — **cryptoHashedToken** 结构用于传送在该交换中所使用的参数。在此结构中所包含的是计算该散列值所必需的参数的“透明”版本。实施者必须在 **hashedVals** 中包括时间标记，而不得包括口令。（例如，口令和“**generalID**”均应事先为接收者所知；而前者可以省略。）

注 2 — 散列函数必须适用于至少包含 ID、时间标记和口令字段的 **EncodedGeneralToken** 结构；口令值绝不能在 **ClearToken** 中传送。

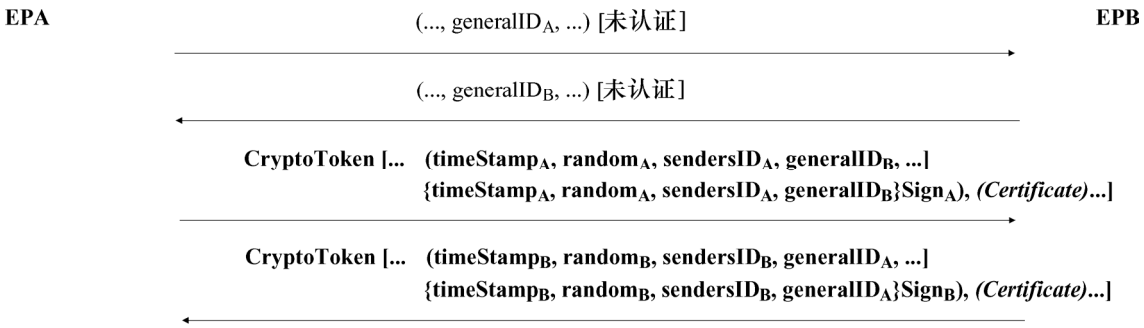
注 3 — 设施应确保用户输入的口令传递足够多的熵。应拒绝过短的或易受字典攻击的口令。在某些情况下，输送用户输入的通行短语通过密码散列函数并使用该输出比特或许是极有益处的。

8.2.3 具有签名的基于证书的认证

图 9 和图 10 显示实施此类认证所要求的令牌格式与消息交换。本协议依据 ISO/IEC 9798-3 的第 5.2.1 节；假定标识符和相关证书在预订时被指派/交换。ITU-T H.235.2 建议书提供二次扫描签名规程的详细描述。

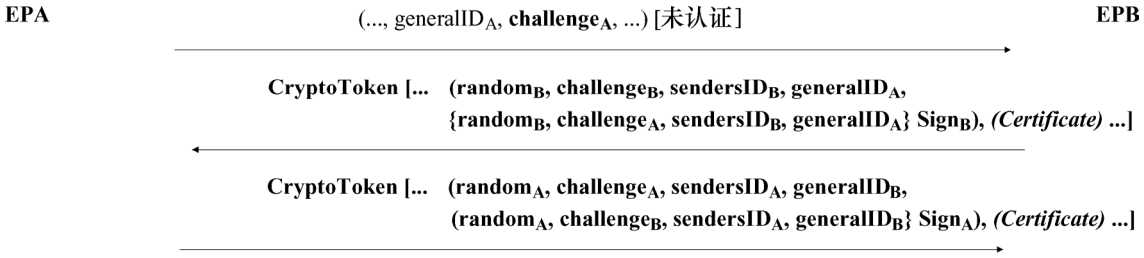
注 1 — 也可提供任选的证书单元；这些单元以**黑斜体字**表示如下。

注 2 — 若消息为组播，则对象标识符（对于 A 处源起的消息为 **generalID$_B$** 并且反之亦然）不应包含在 **ClearToken** 中。



注 1 — 来自 EPB 的返还令牌为任选；若省略，则仅实现单向认证。
注 2 — 一种“付费”类证书可由 EPA 始发方任选包含。
注 3 — **Sign** 表示对所含的值执行签字操作（来自相关证书）。
注 4 — **random** 为单调递增计数器使多路消息具有相同的时间标记。

图 9/H.235.0－具有签名的基于证书的认证，二次扫描



注 1 — 来自 EPB 的返还令牌为任选；若省略，则仅实现单向认证。
注 2 — 一种“付费”类证书可由 EPA 始发方任选包含。
注 3 — **Sign** 表示对所含的值执行签字操作（来自相关证书）。
注 4 — 在第 3 消息中，EPA 在嵌入的编码的 **GeneralToken** 中以明文方式提供一个新的 **challenge$_A$**。作为响应，EPA 也返还 **challenge$_B$**；对第 2 消息类似，反之亦然。
注 5 — 对于多路未完成消息，**random**（即单调递增计数器）必须使查询成为惟一的。

图 10/H.235.0－具有签名的基于证书的认证，三次扫描

8.2.4 共享秘密和口令的使用

为了认证、完整性与机密性，本建议书采用某种对称的密码技术。采用对称技术时本文使用术语口令和共享秘密。共享秘密被理解为标识任意比特串的通用的术语。共享秘密可以被指派或配置作为用户的预订处理的一部分或者可以是带内计算的一部分，诸如 Diffie-Hellman 衍生的共享秘密。

口令可以视为用户可记忆的文字与数字的字符串。很明显，使用口令务必谨慎设置：口令只有从相当大的范围内随机选择，并且不可预测和定期更换以携带足够的信息量，才能保证足够的安全。设置并维护口令的规则不在本建议书的范围内。

从口令和共享秘密中获得益处的最好方法是使用密码级强度的单向散列函数将用户口令字符串变换成为固定的比特串作为共享秘密。

作为推荐的实例，使用 H.235.1 的安全概要时，SHA1 散列函数适用于将口令字符串变换成为 20 字节的共享秘密。它的优点在于散列后的结果不仅没有暴露真实的口令，而且在确实没有牺牲信息熵的条件下规定了定长比特串格式。

因此，

共享秘密：＝SHA1（口令）

8.3 认证的RAS信令/规程

本建议书将不明确提供网守和端点之间的任何消息保密格式。存在两种类型的认证可以使用。第一种类型是不要求端点与网守之间任何事先接触的基于对称加密的类型。第二种类型是基于预订类型，并有两种格式：口令或证书。所有这些格式均可以从第 8、8.2.1、8.2.2 和 8.2.3 节中所示的规程衍生。本附件中，前面提到的子节中所示的通用标签（EPA 和 EPB）分别代表端点和网守。

8.3.1 端点—网守的认证（基于非预订的）

该机制可以为网守提供一个密码链接，到事先注册的特殊端点的网守，该端点是发布后续 RAS 消息的同一个端点。应予注意，该机制可以不向端点提供网守的任何认证，除非包含任选的签名单元。一致性关系的建立在终端发布 **GRQ** 时发生，如 7.2.1/H.323 中所概述的。Diffie-Hellman 交换将与 **GRQ** 和 **GCF** 消息一起发生，如第 8 节的第 1 阶段中所显示的。现在该共享密钥将从终端到网守在任何后续的 **RRQ/URQ** 上使用。若网守以此方式操作并且接收 **GRQ** 而没有包含 *DHset* 或可接受的算法值的令牌，则它必须按照第 11.1 节在 **DRJ** 中返还 **securityDenial** 理由代码。

作为 **GRQ/GCF** 交换期间所生成的 Diffie-Hellman 共享密钥可以用于后续 **xRQ** 消息上的认证。以下规程将用于完成该方式的认证。

终端（**xRQ**）：

1） 如 ITU-T H.225.0 建议书适当子节中所描述的该终端必须提供在此消息中所有的信息。

2） 此终端必须使用协商的共享密钥对 **GatekeeperIdentifier**（作为在 **GCF** 中返还的）加密。作为 **generalID**，它务必在 **clearToken** 中传送（见 8.1）。

16 比特 **random** 字段和 **requestSeqNum**（请求序列编号）字段务必先后与 **GatekeeperIdentifier** 的每个 16 比特异或。若 **GatekeeperIdentifier** 未在偶数个 16 的边界上结束，则 **GatekeeperIdentifier** 的最后 8 比特必须与该随机值及 **requestSeqNum** 字段的最低有效字节先后异或。**GatekeeperIdentifier** 必须使用 **GCF** 中所选择的算法加密（algorithmOID）并利用整个共享秘密。

下例说明该规程：

RND16： 随机值的 16 比特值

SQN16： 请求序列编号字段的 16 比特值

BMPX： 网守标识符的第 X 个 BMP 字符

BMP1′=（BMP1）XOR（RND16）XOR（SQN16）

BMP2′=（BMP2）XOR（RND16）XOR（SQN16）

BMP3′=（BMP3）XOR（RND16）XOR（SQN16）

BMP4′=（BMP4）XOR（RND16）XOR（SQN16）

BMP5′=（BMP5）XOR（RND16）XOR（SQN16）

：

：

BMPn′=（BMPn）XOR（RND16）XOR（SQN16）

为了密码化地链接该终端和具有原始注册端（发布 **RRQ** 的端点）的后续消息必须利用最近所返还的 **random** 值（该值可能会比 **RCF** 中返还的值更新 — 来自最后的 **xCF** 消息）。

网守（**xCF/xRJ**）：

1） 网守必须加密其 **GatekeeperIdentifier**（遵从以上规程），采用与该端点化名有关的共享密钥并将它与 **xRQ** 中的值进行比较。

2） 只要两个加密值不匹配，网守就必须返还 **xRJ**。

3） 只要 **GatekeeperIdentifier** 匹配，网守就必须使用任何本地逻辑信道并采用 **xCF** 或 **xRJ** 来响应。

4） 若该网守发送 **xCF**，则它应包含指派的 **EndpointIdentifier** 以及在 **clearToken** 的 **random** 字段中的新的随机值。

该交换的图示表示可参考图 4 的第 2 阶段。该网守知道使用那些共享密钥来解密由该消息中的化名所命名的网守标识符。

8.3.2 端点—网守的认证（基于预订的）

除 **GRQ/GCF** 外的所有 RAS 消息应包含由特定操作方式所请求的认证令牌。依据需求和环境，存在 3 种可以实施的不同变种：

1） 具有对称加密的基于口令的认证；

2） 具有散列的基于口令的认证；

3） 具有签名的基于证书的认证。

在所有情形中依据所选择的变种，令牌将包含以下若干子节中所描述的信息。若网守以安全方式操作并接收 RAS 消息而没有任何可接受的令牌值，则它必须按照第 11.1 节在 reject 消息中返还 **securityDenial** 理由代码。在所有情形中，来自 GK 的返还令牌为任选；若省略，仅只实现单向认证。

8.3.2.1 具有对称加密的口令

网守发现阶段（**GRQ、GCF** 和 **GRJ**）或许未被保护，如图 11 所示，或者可以使用 **cryptoToken** 来保护。

图 11/H.235.0－具有对称加密的口令

8.3.2.2 具有散列的口令

网守发现阶段（**GRQ、GCF** 和 **GRJ**）或许未被保护，如图 12 所示，或者依照 ITU-T H.235.1 建议书使用 **cryptoToken** 来保护。

图 12/H.235.0－具有hash的口令

8.3.2.3 具有签名的基于证书的认证

网守发现阶段（**GRQ**、**GCF** 和 **GRJ**）或许未被保护，如图 13 所示，或者依照 ITU-T H.235.2 建议书使用 **cryptoToken** 来保护。

图 13/H.235.0－具有签名的基于证书的认证

8.4 在RAS信道上的密钥管理

在某些环境下，期望由网守在其控制下向一个或多个端点分配（RAS）对话密钥，或从一个端点向另一个端点分配。提议的机制假定网守和端点共享一个强壮的、秘密的密钥或知道彼此的公钥。对于选路网守，这样的情况的一个例子是向 RAS 消息中的一个端点发送一个对话密钥，如 **RCF** 或 **ACF**，在加密选路的网守信令信道上使用。另一个例子可能是网守发送一个对话密钥，在成功的 RAS 通信中使用（例如 **RRQ** 或 **ARQ**）。

这一机制与用于媒体对话密钥的分配的机制类似。它在某些情况下可用于避免密钥协商的开销。

对于密钥传送，**ClearToken** 的任选的 **h235Key** 字节应在 H.235v3 中使用。**H235Key** 元素的灵活性将允许使用以下所述传送加密密钥资料：

- 安全信道（**secureChannel** 选项）假定 RAS 或呼叫信令信道通过其他方式是安全的（IPsec/SSL，等等）；
- 在广播信道上共享的加密密码（**sharedSecret** 选择），或类似的但更适宜的 **secureSharedSecret** 选择；
- 在广播信道上的公钥加密和认证（**certProtectedKey** 选项）。

交换的 RAS 对话密钥的使用及其对 RAS、呼叫信令消息和/或传输信道的应用有待进一步研究。

9 使用椭圆曲线加密系统的非对称认证和密钥交换

本建议书提供适用于签名、密钥管理和加密的完善椭圆曲线技术。相对于“传统”的非对称技术如RSA，它的一个基本优势在于：

- 缩短的密码密钥生成可匹敌 RSA 的安全性。椭圆曲线加密系统的典型的密钥长度为 160 比特；即相当于 1024 比特 RSA 密钥的安全性。缩短的密钥消耗更少的存储器内存并使椭圆曲线加密系统对于智能卡式设备以及在任何其他采用低存储器要求的设施中特别地有吸引力。在 H.323 环境中，伴随低价格要求的基于附件 J/H.323 的安全式音频简单端点类型（SASET）很适合于采用椭圆曲线技术。
- 在软件和硬件设施中实现改进的处理速度。缩短的密钥有助于处理速度的提高。这导致更快的交互式（用户）响应。

椭圆曲线密码的所有背景信息、说明和处理规程参见[“ATM 安全性规范”第 1.1 版，第 8.7 节]。推荐

以其仿射的、非压缩符号对椭圆点进行编码，而不使用点压缩/点解压缩方法。本论题的进一步信息可在 ISO/IEC 15946-1 和 ISO/IEC 15946-2 中得到。

9.1 密钥管理

基于椭圆曲线的 Diffie-Hellman 密钥协议方案同样与本建议书中规定的传统的 mod-p 情况类似。分两种情况：

- 基本字段上的椭圆曲线：**eckasdhp** 掌握椭圆曲线与 Diffie-Hellman 参数。
- 特征 2 的椭圆曲线：**eckasdh2** 掌握椭圆曲线与 Diffie-Hellman 参数。

ECKASDH 结构掌握任一种情况。一些椭圆曲线的实例在 ISO/IEC 15946-1 中列出。同样可以使用任何其他适合与恰当的椭圆曲线。

由于 **ClearToken** 的有效的序列结构，信令 **dhkey** 和 **eckasdhkey** 不应同时出现。采用 Diffie-Hellman 密钥交换时，仅其中一个信令出现。

注 — 不要混淆由用户 A 随机选择的秘密参数 ***a*** 或由用户 B 随机选择的秘密参数 ***b*** 与公共 Weierstrass（威尔斯特拉斯）系数 ***a***，***b*** 之间的含义。

9.2 数字签名

ECGDSAsignature 字段携载所计算的基于椭圆曲线的数字签名值 **r** 和 **s**。“ATM 安全性规范”第 1.1 版的第 8.7.3 节和 ISO/IEC 15946-2 的第 5 章提供签名算法 EC-GDSA 的进一步信息。

基于椭圆曲线的数字签名 **ECGDSA** 必须由 ASN.1 编码并放入 **SIGNED** 宏字段中的 **signature** 字段中。对于数字签名，发送者必须在 **algorithmOID** 中包含对象标识符，通过它，接收者能够确定椭圆曲线数字签名的用法。

10 伪随机函数（PRF）

出于从静态密钥资料中衍生出动态密钥，本节定义了一个伪随机函数和一个随机值。

注 — 此 PRF 与 MIKEY PRF 是同样的（见 RFC 3830 第 4.1.2 节）。

密钥衍生方法有下列输入参数：

- *inkey*： 衍生函数的输入密钥。
- *inkey_len*： 输入密钥的比特长度。
- *label*： 特殊的标签，视被衍生的密钥类型和随机 **challenge** 值而定。
- *outkey_len*： 输出密钥的比特长度。

伪随机函数有下列输出：

- *outkey*： 期望长度的输出密钥。

这一 PRF 必须使用 PRF，正如在 RFC 3830 第 4.1.2 节中定义的那样。

11 安全性误差纠正

本建议书未指定或推荐可用于端点监视其自身绝对保密的任何方法。然而它确实推荐检测到失密时所应采取的行动。

若任何一方端点在呼叫连接信道（例如 H.323 的 H.225.0）的安全性中检测到缺陷，则它必须遵循适用于该特殊端点的协议规程立即关闭该连接（见 8.5/H.323（除步骤 B-5 外））。

若任何一方端点在 H.245 信道或安全数据（**h235Control**）逻辑信道的安全性中检测到缺陷，则它必须遵循适用于该特殊端点的协议规程立即关闭该连接（见 8.5/H.323（除步骤 B-5 外））。

若任何一方端点在某个逻辑信道中检测到失密，则它应立即请求新的密钥（**encryptionUpdate Request**）和/或关闭该逻辑信道。听凭 MC（U）的处置，一个逻辑信道上的失密可能导致所有其他逻辑信道被关闭和/或听凭 MC（U）的处置重置密钥。MC（U）必须前送 **encryptionUpdateRequest**、**encryptionUpdate** 消息给受影响的任何端点及所有端点。

听凭 MC（U）的处置，个别信道上的安全性误差可能会导致所有会议端点的连接关闭，并因此终止会议。

11.1 错误信令

具有安全能力的网守或其他安全的增强型 H.225.0 实体必须提供错误应用。安全性错误指示实体不能正确地处理接收到的消息。无论何时只要可能，必须提供详细的错误编码。

- **securityWrongSyncTime** 必须指示发送者发现一个具有不适当的时间标记的安全问题。这可能是由时间服务器的问题、丢失同步或过多的网络延迟造成的。
- **securityReplay** 必须指示已经面临重放攻击。这是在一个给定的时间标记中不止一次发生同一序列号时的情况。
- **securityWrongGeneralID** 必须指示在消息中通用 ID 的不匹配。
- **securityWrongSendersID** 必须指示在消息中 sendersID 的不匹配。这可能由使用者错误进入造成。
- **securityIntegrityFailed** 必须指示完整性/签名检验失效。对于 H.235.1，这可能由在初始化请求过程中的错误或不适合类型的密码或面临的主动攻击造成。对于 H.235.2 和 H.235.3，这必须指示在消息上的数字签名失效。这可能由采用了错误的私钥/公钥或面临的主动攻击造成。

- **securityWrongOID** 必须指示在令牌 OID（透明或加密 Token）或加密 algorithmOID 中的任何不匹配。这指示实施的不同安全性算法/概要。
- **securityDHmismatch** 必须指示在交换的 Diffie-Hellman 参数中的任何不匹配。这可能指示不同的 DH 参数集或甚至是采用的不同话音加密算法。
- **securityCertificateExpired** 必须指示期满的证书。
- **securityCertificateDateInvalid** 必须指示至今不再有效的证书。
- **securityCertificateRevoked** 必须指示被发现已撤销的证书。
- **securityCertificateNotReadable** 必须指示证书不能正确地 ASN.1 编码或在其他坏形态下。
- **securityCertificateSignatureInvalid** 必须指示证书中的签名不正确。
- **securityCertificateMissing** 必须指示不期望但发现证书丢失或证书不能另外定位。
- **securityCertificateIncomplete** 必须指示某些期望的证书扩展不存在。
- **securityUnsupportedCertificateAlgOID** 必须指示确定的加密算法（如在证书中使用的散列或数字签名）不被理解或不被支持。作为返回响应的一部分，为了方便接收者选择一个适当的响应，发送者可以提供在单独的令牌中提供可接受的证书的清单。
- **securityUnknownCA** 必须指示没有发现 CA/根证书或证书与信赖的 CA 不匹配。

在任何 H.235 安全性失效的情况下，H.225.0 RAS 的 **securityDenial**（或 H.225.0 呼叫信令的 **securityDenied**）必须被返回。

注 1 — securityWrongSyncTime、securityReplay、securityWrongGeneralID、securityWrongSendersID、SecurityIntegrityFailed、securityDHmismatch 和 securityWrongOID 可能在 H.235.1、H.235.2 或 H.235.3 安全概要中发生。

注 2 — securityCertificateExpired、securityCertificateDateInvalid、securityCertificateRevoked、securityCertificateNotReadable、securityCertificateSignatureInvalid、securityCertificateMissing，securityCertificateIncomplete、securityUnsupportedCertificateAlgOID 和 securityUnknownCA 可能在 H.235.2 或 H.235.3 安全概要中发生。

附 件 A

H.235 ASN.1

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- 输出全部的

ChallengeString            ::= OCTET STRING (SIZE(8..128))
TimeStamp                  ::= INTEGER(1..4294967295)      -- 自 00:00
                                                           -- 1/1/1970 UTC 后的秒数
RandomVal                  ::= INTEGER -- 32 比特整数
Password                   ::= BMPString (SIZE (1..128))
Identifier                 ::= BMPString (SIZE (1..128))
KeyMaterial                ::= BIT STRING(SIZE(1..2048))

NonStandardParameter ::= SEQUENCE
{
     nonStandardIdentifier    OBJECT IDENTIFIER,
     data                     OCTET STRING
}
-- 若使用这些比特串的局部字节表示，它们必须
-- 利用标准的网络字节顺序（例如高字节先传）
DHset ::= SEQUENCE
{
    halfkey        BIT STRING (SIZE(0..2048)), -- = g^x mod n
    modSize        BIT STRING (SIZE(0..2048)), --  n
    generator      BIT STRING (SIZE(0..2048)), -- g
    ...
}

ECpoint ::= SEQUENCE -- 椭圆曲线点非压缩的（x,y）仿射坐标表示
{
     x         BIT STRING (SIZE(0..511)) OPTIONAL,
     y         BIT STRING (SIZE(0..511)) OPTIONAL,
    ...
}

ECKASDH::= CHOICE -- 椭圆曲线密钥协议方案 Diffie-Hellman 的参数
{
     eckasdhp SEQUENCE -- 椭圆曲线的基本字段参数
     {
          public-key      ECpoint, -- 该字段包含 ECKAS-DHp 公钥值表示
                -- 若该信息元从发送者向接收者发送，该字段包含启动方的 ECKAS-DHp 公钥值（aP）表示。
                -- 若该信息元从接收者回送发送者，该字段包含响应方的 ECKAS-DHp 公钥值（bP）表示。
          modulus          BIT STRING (SIZE(0..511)),--该字段包含 ECKAS-DHp 公钥模数值
                -- (p)表示。
          base             ECpoint, -- 该字段包含 ECKAS-DHp 公共基表示(P)。
          weierstrassA     BIT STRING (SIZE(0..511)), -- 该字段包含 ECKAS-DHp
                -- Weierstrass 系数(a)表示。
          weierstrassB     BIT STRING (SIZE(0..511)) - 该字段包含 ECKAS-DHp
                -- Weierstrass 系数(b)表示。
     },
```

```
    eckasdh2 SEQUENCE -- 椭圆曲线特征 2 参数
    {
        public-key      ECpoint, -- 该字段包含 ECKAS-DH2 公钥值表示。
            -- 若该信息元从发送者向接收者发送，该字段包含启动方的 ECKAS-DH2 公钥值（aP）。
            -- 若该信息元从接收者回送发送者，该字段包含响应方的 ECKAS-DH2 公钥值（bP）。
        fieldSize       BIT STRING (SIZE(0..511)), -- 该字段包含 ECKAS-DH2
            --字段尺寸值(m)表示。
        Base            ECpoint, -- 该字段包含 ECKAS-DH2 公共基(P)表示。
        WeierstrassA    BIT STRING (SIZE(0..511)), -- 该字段包含 ECKAS-DH2
            -- Weierstrass 系数(a)表示。
        WeierstrassB    BIT STRING (SIZE(0..511)) -- 该字段包含 ECKAS-DH2
            -- Weierstrass 系数(b)表示。
    },
    ...
}
ECGDSASignature::= SEQUENCE -- 椭圆曲线数字签名算法参数
{
    r       BIT STRING (SIZE(0..511)), -- 该字段包含 ECGDSA 数字签名的 r 分量表示。
    s       BIT STRING (SIZE(0..511)) -- 该字段包含 ECGDSA 数字签名的 s 分量表示。
}

TypedCertificate ::= SEQUENCE
{
    type          OBJECT IDENTIFIER,
    certificate   OCTET STRING,
    ...
}

AuthenticationBES ::= CHOICE
{
    default       NULL, -- 加密的 ClearToken
    radius        NULL, -- RADIUS-challenge/响应
    ...
}

AuthenticationMechanism  ::= CHOICE
{
    dhExch        NULL, -- Diffie-Hellman
    pwdSymEnc     NULL, -- 具有对称加密的口令
    pwdHash       NULL, -- 具有散列变换的口令
    certSign      NULL, -- 具有签名的证书
    ipsec         NULL, -- 基于 IPsec 的连接
    tls           NULL,
    nonStandard   NonStandardParameter, -- 其他。
    ...,
    authenticationBES  AuthenticationBES,-- 对 BES 的用户认证
    keyExch  OBJECT IDENTIFIER            -- 密钥交换概要

}
```

```
ClearToken              ::= SEQUENCE  -- 一个“令牌”可以包含多种值类型。
{
     tokenOID           OBJECT IDENTIFIER,
     timeStamp          TimeStamp OPTIONAL,
     password           Password OPTIONAL,
     dhkey              DHset OPTIONAL,
     challenge          ChallengeString OPTIONAL,
     random             RandomVal OPTIONAL,
     certificate        TypedCertificate OPTIONAL,
     generalID          Identifier OPTIONAL,
     nonStandard        NonStandardParameter OPTIONAL,
     ...,
     eckasdhkey         ECKASDH OPTIONAL,    -- 椭圆曲线密钥协议方案-Diffie
                                             -- Hellman 模拟(ECKAS-DH)
     sendersID          Identifier OPTIONAL,
     h235Key            H235Key OPTIONAL -- V3 中的集中分布密钥
     profileInfo        SEQUENCE OF ProfileElement OPTIONAL  -- 特定概要

}

--  消息（与加密相反）中直接包含 ClearToken 时，一个对象标识符应被放置在 tokenOID
--  字段中
--  在所有其他的情形中，应该使用对象标识符{ 0 0 }指示 tokenOID 值不存在。
--  此处开始所有的密码参数类型...
--
ProfileElement      ::= SEQUENCE
{
     elementID      INTEGER (0..255), -- 元素标识符，如由概要定义的
     paramS         Params OPTIONAL,  -- 任何特定元素的参数
     element        Element OPTIONAL, -- 以要求模式表示的值
     …
}

Element ::= CHOICE
{
     octets             OCTET STRING,
     integer            INTEGER,
     bits               BIT STRING,
     name               BMPString,
     flag               BOOLEAN,
     …
}


SIGNED { ToBeSigned } ::= SEQUENCE {
     toBeSigned         ToBeSigned,
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,    -- 任何“运转时间”参数
     signature          BIT STRING -- 可以是 RSA 或 ASN.1 编码的 ECGDSA 签名
} ( CONSTRAINED BY { -- 校验或符号证书 -- } )


ENCRYPTED { ToBeEncrypted } ::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,    -- 任何“运转时间”参数
     encryptedData      OCTET STRING
} ( CONSTRAINED BY { -- 加密或解密 -- ToBeEncrypted } )
```

```
HASHED { ToBeHashed } ::= SEQUENCE {
     algorithmOID       OBJECT IDENTIFIER,
     paramS             Params,  -- 任何“运转时间”参数
     hash               BIT STRING
} ( CONSTRAINED BY { -- 散列 -- ToBeHashed } )

IV8 ::= OCTET STRING (SIZE(8)) – 64 比特块密文初始值
IV16 ::= OCTET STRING (SIZE(16)) – 128 比特块密文初始值

-- 所使用的签名算法务必选择签名接收端所必需的这些参数类型之一。

Params ::= SEQUENCE {
     ranInt         INTEGER OPTIONAL, -- 某个整数值
     iv8            IV8 OPTIONAL,  -- 8 个八比特组初始化矢量
     ...,
     iv16           IV16 OPTIONAL,  -- 16 字节初始化矢量
     iv             OCTET STRING OPTIONAL, -- 随机长度初始化矢量
     clearSalt      OCTET STRING OPTIONAL -- 用于加密的非加密密钥
}

EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- 通用用法令牌 -- )
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStamp PRESENT, generalID
PRESENT})
EncodedPwdCertToken ::= TYPE-IDENTIFIER.&Type (PwdCertToken)

CryptoToken::= CHOICE
{

     cryptoEncryptedToken SEQUENCE -- 一般用途/特定应用令牌
     {
          tokenOID      OBJECT IDENTIFIER,
          token         ENCRYPTED { EncodedGeneralToken }
     },
     cryptoSignedToken  SEQUENCE -- 一般用途/特定应用令牌
     {
          tokenOID      OBJECT IDENTIFIER,
          token         SIGNED { EncodedGeneralToken }
     },
     cryptoHashedToken SEQUENCE -- 一般用途/特定应用令牌
     {
          tokenOID      OBJECT IDENTIFIER,
          hashedVals    ClearToken,
          token HASHED { EncodedGeneralToken }
     },
     cryptoPwdEncr      ENCRYPTED { EncodedPwdCertToken },
     ...
}

-- 在 H.245 OLC 结构内这些字段允许对话密钥的传送。
-- 它们作为独立模式 ASN.1 并根据 H.245 内的 OCTET STRING 编码。
H235Key     ::=CHOICE  -- 此字段在 H.245“h235Key”字段中使用。
{
     secureChannel         KeyMaterial,
     sharedSecret          ENCRYPTED {EncodedKeySyncMaterial},
     certProtectedKey      SIGNED {EncodedKeySignedMaterial },
     ...,
     secureSharedSecret    V3KeySyncMaterial -- 用于 H.235 V3 端点
}
```

```
KeySignedMaterial ::= SEQUENCE {
     generalId      Identifier, -- 从属方的化名
     mrandom        RandomVal, -- 主叫方的随机值
     srandom        RandomVal OPTIONAL, -- 从属方的随机值
     timeStamp      TimeStamp OPTIONAL, -- 主动提供的 EU 的主叫方时间标记
     encrptval      ENCRYPTED { EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial ::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature       ::= SEQUENCE
{
     certificate               TypedCertificate,
     responseRandom            RandomVal,
     requesterRandom           RandomVal OPTIONAL,
     signature                 SIGNED { EncodedReturnSig },
     ...
}

ReturnSig ::= SEQUENCE {
     generalId                 Identifier, -- 从属方化名
     responseRandom            RandomVal,
     requestRandom             RandomVal OPTIONAL,
     certificate               TypedCertificate OPTIONAL -- 请求的证书
}

EncodedReturnSig ::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial    ::= SEQUENCE
{
     generalID      Identifier,
     keyMaterial    KeyMaterial,
     ...
}
EncodedKeySyncMaterial  ::=TYPE-IDENTIFIER.&Type (KeySyncMaterial)



V3KeySyncMaterial ::= SEQUENCE
{
     generalID                 Identifier OPTIONAL, -- 对等终接 ID
     algorithmOID              OBJECT IDENTIFIER OPTIONAL, -- 加密算法
     paramS                    Params, -- IV
     encryptedSessionKey       OCTET STRING OPTIONAL, -- 加密的对话密钥
     encryptedSaltingKey       OCTET STRING OPTIONAL, -- 加密的媒体补白密钥
     clearSaltingKey           OCTET STRING OPTIONAL, -- 未加密的媒体补白密钥
     paramSsalt                Params OPTIONAL, -- 补白密钥加密 IV（和透明的补白）
     keyDerivationOID          OBJECT IDENTIFIER OPTIONAL, -- 密钥衍生方法
     ...,
     generickeyMaterial        OCTET STRING OPTIONAL--—ASN.1 编码的密钥材料形式
                               --取决于相关的媒体加密标记
}


END    -- H235 安全性消息定义结束
```

附 件 B

H.324特定问题

有待进一步研究。

附 录 I

H.323实施详情

I.1 实施实例

以下子节描述在 H.235 框架内可以开发的实施实例。这些实例并不打算限制本建议书内众多其他可能有效的实例，而是要给出 ITU-T H.323 建议书内更为具体的用法实例。

I.1.1 令牌

本子节将描述不可见的或隐藏目标寻址信息的安全令牌用法。在例举的方案中，一个端点希望用另一个端点众所周知的化名呼叫该端点。更具体地，这涉及 H.323 端点、网守、POTS 网关和电话，如图 I.1 所示。

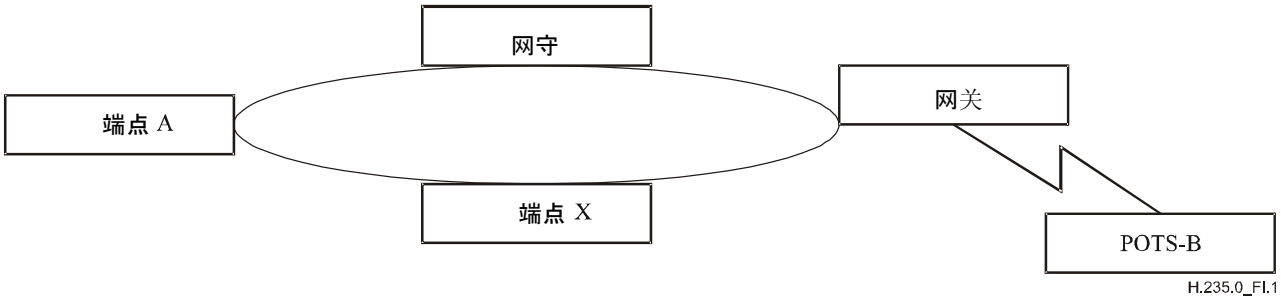


图 I.1/H.235.0－令牌

目前，H.323 可以类似于采用主叫方 ID 的电话网络的方式操作。这种方案要说明的情况是，主叫方不想暴露其实际地址，但仍想完成呼叫。这在目标电话号码需要维持保密的 POTS-H.323 网关中是重要的。

假定 EPA 试图呼叫 POTS-B，并且 POTS-B 不想向 EPA 暴露其 E.164 电话号码。（如何建立该政策超出本例范围）。

- EPA 将向它的网守发送 ARQ 以解决由其化名/GW 所表示的 POTS 电话的地址。网守将其标识成“专用”化名，知道为了完成该连接它务必返还 POTS 网关地址（类似于若 H.320 端点被一个 H.323 端点呼叫，则必须返还 H.320 网关地址的情形）。
- 在返还的 ACF 中，如所期望的网守返还 POTS 网关的地址。请求向端点电话拨号的寻址信息（即电话号码）将在 ACF 中所包含的 CryptoToken 中返还。该 CryptoToken 包括电话的实际 E.164（电话号码），它既不能被主叫方（即 EPA）解密也不能被其所理解。

- 端点向网关设备发布 SETUP 消息（它的呼叫信令地址在 ACF 中返还）包含与 ACF 一起接收的 opaque 令牌。
- 一旦接收 SETUP 消息，网关向其网守发布其 ARQ，包括在 SETUP 消息中接收的任何令牌。
- 网守可以解密该令牌并在 **ACF** 中返还电话号码。

以下显示一个令牌结构实例的部分 ASN.1，对字段的内容加以说明。假定利用 **cryptoEncoded-GeneralToken** 来包含加密的电话号码。

实施可以选择 **tokenOID** 并将该令牌表示成包含 E.164 电话号码。用于加密该电话号码的特殊方法（例如，56 比特 DES），将包括在“ENCRYPT”定义 **algorithmOID** 中。

```
CryptoToken::= CHOICE
{
     cryptoEncodedGeneralToken SEQUENCE    -- 一般用途/特定应用的令牌
     {
         tokenOID  OBJECT IDENTIFIER,
         ENCRYPTED { EncodedGeneralToken }
     },
.
.
. [abbreviated text]
.

}
```

如上所述，**CryptoToken** 可以在 SETUP 消息（从 EPA 到 GW）和 **ARQ**（从 GW 到网守）消息中传送。网守解密令牌（电话号码）后，它将在 **ClearToken** 中以其透明形式传送。

I.1.2 H.323系统中令牌用法

作为在 RAS 中传送的单个 **CryptoH323Token** 的用法曾存在一些混淆。存在两种主要的 **CryptoH323Token** 类型：H.235 规程使用的和以特定应用方式使用的 **CryptoH323Token**。这些令牌的使用应依据以下规则：

- 所有 H.235 规定的令牌（即 **CryptoEPPwdHash**，**CryptoGKPwdHash**，**cryptoEPPwdEncr**，**CryptoGKPwdEncr**，**CryptoGKCert** 和 **cryptoFastStart**）必须与本建议书所描述的规程和算法一起使用。
- 特定应用的或专门使用的令牌必须利用 **nestedCryptoToken** 供其交换。
- 任何使用的 **nestedCryptoToken** 应有明确标识它的 **tokenOID**（对象标识符）。

I.1.3 H.323系统中H.235随机值用法

端点与网守之间在 xRQ/xCF 序列中传送的随机值可以由该网守更新。如第 8.3.1 节所述，该随机值可以在任何 xCF 消息中更新这些消息，由来自端点的后续 xRQ 消息使用。由于 RAS 消息或许丢失（包括 xCF/xRJ）的实际情况，更新的随机值也可能丢失。从此种情况恢复可以是该安全环境的重新初始化，但属于本地实施问题。

要求使用多种未定的 RAS 请求的实施通过在任何认证中使用的随机值更新来限制。若该值更新在请求的每个响应上发生，则不可能有并行请求。一个可能的解决方案是采用逻辑“窗”，在逻辑“窗”期间随机值保持常量。该问题是本地实施事务。

I.1.4 口令

本例中，假定用户是网守的预订方（即用户在网守的分区内），并且具有相关的预订 ID 和口令。用户将与网守一起使用预订 ID（在化名中传送 — H323ID）注册并且加密由网守所提出的查询串。这假定网守也知道与预订 ID 有关的口令。网守通过核实查询串是否正确加密来鉴别用户。

采用网守认证的实例注册规程如下：

1） 若端点使用 **GRQ** 发现网守，消息中的一个化名将为预订 ID（作为一个 **H323ID**）。**authenticationcapability** 将包含 **pwdSymEnc** 的 **AuthenticationMechanism**，而且 **algorithmOID** 将设置成指示由端点所支持的整个加密算法集合（例如，其中之一是 EBC 方式的 56 比特 DES）。

2） 网守将采用 **GCF** 响应（假定它识别该化名）携载包含一个 **ClearToken** 的 **token** 单元。该 **ClearToken** 将包含 **challenge** 和 **timeStamp** 单元。该 **challenge** 将包括 16 个字节（为防止重放攻击，**ClearToken** 应包含 **timeStamp**）。**authenticationmode** 应设置成 **pwdSymEnc** 并且 **algorithmOID** 应设置指示该网守所要求的加密算法（例如，ECB 方式的 56 比特 DES）。

若网守不支持 GRQ 中所指示的任何 **algorithmOID**，则它将采用 **GRJ** 响应包含 **resourceUnavailable** 的 **GatekeeperRejectReason**。

3） 然后通过在 **CryptoToken** 中发送包含 **cryptoEPPwdEncr** 的 **RRQ** 该端点应用将试图与采用 **GCF** 响应的该 GK（之一）一起注册。该 **cryptoEPPwdEncr** 将具有在 **GRQ/GCF** 交换中承认的加密算法的 **algorithmOID**。

加密密钥使用第 8.2.1 节中所描述的规程根据用户的口令构造。生成的字节“串”用作为 DES 密钥来加密 **challenge**。

4） 当网守接收 **RRQ** 中的加密查询时，通过将它与一个同样生成的加密查询相比较可以鉴别该注册用户。若两个加密串不匹配，则网守将以 **RRJ** 响应具有 **RegistrationRejectReason** 设置为 **securityDenial**。若它们匹配，则网守向端点发送 **RCF**。

5） 网守若收到包含不可接受的 **CryptoToken** 单元的 **RRQ**，则应采用 **GatekeeperRejectReason** 为 **discoveryRequired** 的 **RRJ** 加以响应。一旦接收到此 **RRJ**，端点就可实施将允许网守/端点交换新查询的发现。注意，**GRQ** 消息可以单播到网守。

I.1.5 IPsec

通常，对于无论何种（应用）协议在其上运行均为透明的 IP 层而言，可以使用 IPsec[RFC 2401]、RFC 2406[ESP]和 RFC 2409[IKE]来提供认证以及任选的机密性（即加密）。为允许这一点，该应用协议不需要更新；仅在每个端点的安全政策需要更新。

例如，对于简单的端到端呼叫，为了最大的利用 IPsec，可遵循以下方案：

1） 主叫端及其网守将设置方针请求在 RAS 协议上使用 IPsec（认证，任选地，以及机密性）。这样，在从端点向网守发送第一个 RAS 消息之前，端点上的 ISAKMP/Oakley 规程将在发往和来自 RAS 信道的众所周知端口的分组上协商即将使用的安全性业务。一旦协商完成，RAS 信道将完全类似于它似乎未被保护时的那样操作。使用该安全信道，网守将把被叫端中的呼叫信令信道的地址及端口号通告给该端点。

2） 获得呼叫信令信道地址和端口号后，主叫端将动态的更新它的安全性政策以在该地址和协议/端口对上请求所需要的 IPsec 安全。现在，当主叫端试图接触该地址/端口时，分组将会排队同时一个 ISAKMP（RFC 2407）/Oakley（RFC 2412）协商在端点之间进行。一旦该协商完成，地址/端口的 IPsec 安全性契约（SA）将存在并且 Q.931 信令可以开始。

3） 在 Q.931 SETUP 和 CONNECT 交换上，端点可以协商 H.245 信道的 IPsec 的使用。这将允许端点再次动态更新它们的 IPsec 法规数据库以强制在该连接上的 IPsec 使用。

4） 正如呼叫信令信道的情形一样，透明的 ISAKMP（RFC 2407）/Oakley（RFC 2412）协商将在传输任何 H.245 分组之前发生。由该 ISAKMP（RFC 2407）/Oakley（RFC 2412）交换所实施的认证将是用户到用户认证上的初始尝试，并且将在两个用户中间建立（可能的）安全信道，在其上协商音频信道的特征。某些人对人 Q&A 后，若任何一方的用户对认证不满意，可以选择不同的证书并重复 ISAKMP（RFC 2407）/Oakley（RFC 2412）交换。

5） 每个 H.245 ISAKMP（RFC 2407）/Oakley（RFC 2412）认证后，交换 RTP 音频信道的新的加锁资料。该加锁资料由主控方在安全的 H.245 信道上分发。由于 H.245 协议是为主控方在 H.245 信道上分发媒体加锁资料而定义的（允许供多点通信），因此不推荐供 RTP 信道所使用的 IPsec。

由于 H.245 协议中携载动态分配的端口号，对于代理服务器或 NAT 防火墙，加密的 H.245 信道是一个潜在的问题。这样的防火墙不得不解密、修改以及再加密协议以正确操作。出于这个原因，在 ITU-T H.245 建议书中引入“安全性”逻辑信道。若使用该信道，则 H.245 信道可以保持非安全；认证和密钥生成采用“安全性”逻辑信道完成。逻辑信道信令将允许该信道采用 IPsec 保护，并且该“安全性”逻辑信道上所使用的加密密钥将用于保护由主控方在 H.245 信道上所分发的 **EncryptionSync**。

I.1.6 后端业务支持

后端服务器（BES）是整个基于 H.323 多媒体环境中的一个重要辅助功能。例如，BES 提供用户认证、业务授权、以及核算、计费、记账业务及其他业务。在简单模型中，网守可以提供此类业务。在分散配置中，GK 或许始终不提供此类业务；或者由于它不能访问 BES 数据库或它可能是不同管理域的一部分。同样地，终端或用户一般也不知道它们的 BES。

图 I.2 显示采用多媒体终端（例如 SASET）、网守和链接的 BES 方案。如何准确地与 GK 进行 BES 通信不在 ITU-T H.323 建议书的范围内。若干方法和协议可以采用：RADIUS（见 RFC 2865）被认为是最重要的方法和协议之一，它被服务提供商广泛使用。

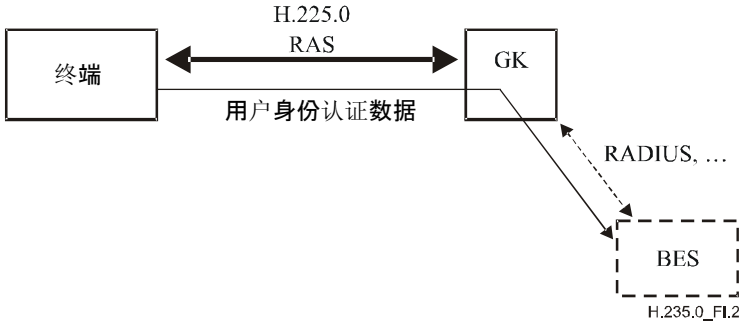


图 I.2/H.235.0－后端业务方案

提供 BES 支持的 GK 至少应支持以下两种方式：

1） **缺省方式**，其中终端不知道该 BES，并且要求与该 GK 建立信任关系。终端向 GK 发送加密格式的用户认证数据（**cryptoEncryptedToken**），GK 解密该数据，提取用户认证信息并对 BES 使用它。**ClearToken** 的基于口令加密通过向 **CryptoToken** 使用该终端与该 GK 之间共享的一个截然不同的秘密来实现。加密密钥可以从该终端在 GK 上所采用的安全注册的口令中衍生。

CryptoToken 携载 **cryptoEncryptedToken**，其中 **tokenOID** 设置为“M”指示 BES 缺省方式；并且 **token** 掌握：

- 表明加密算法的 **algorithmOID**；“Y”（DES56-CBC），“Z”（3DES-OCBC）；见第 11 节/H.235.6；
- 不使用的 **paramS**；
- 加密的 **ClearToken** 设置为字节表示的 **encryptedData**。

ClearToken 掌握如 **password** 的用户认证数据。保护的 **ClearToken** 信息可以是口令/PIN、用户标识符、预先付费呼叫卡号和信用卡号。**timeStamp** 设置为终端的当前时间，**random** 包括一个单调递增的序列号，**sendersID** 设置为终端 ID 以及 **generalID** 设置为 GK 标识符。加密算法的初始值（IV）必须保持为常量；它可以是终端预订秘密的一部分。

注 — **ClearToken** 不传输。

2） **RADIUS 方式**，其中 BES 和终端用户共享公共的秘密，并且 GK 也不应是 BES RADIUS 认证的可信方。GK 简单地向终端转发来自 *Access-Challenge* 内的 BES 所接收的 RADIUS 查询，并在相反方向上的 *Access-Request* 内作为 RADIUS 响应发送该用户的应答。网守发现期间终端和 GK 在 **AuthenticationMechanism** 内的 **AuthenticationBES**（认证 **BES**）中协商该 RADIUS 查询/响应能力。

一旦收到传送查询的 RADIUS *Access-Challenge* 消息，当采用 **GCF** 或任何其他 RAS 消息质疑终端时，GK 就应将 16 字节查询放入 **ClearToken** 的 **challenge** 字段中。**ClearToken** 中的 **tokenOID** “K”指示一个 RADIUS 查询。

然后终端可以向用户提出查询并且等待响应输入。终端必须采用 RAS 消息应答，其中该响应放入 **ClearToken 的 challenge** 字段中。**ClearToken** 中的 **tokenOID**“L”指示一个 RADIUS 响应。

以下表 I.1 列出所有引用的 OID。

表 I.1/H.235.0－I.1.6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
“K”	{itu-t（0）recommendation（0）h（8）235 version（0）2 31}	在 **ClearToken** 中指示一个 RADIUS 查询
“L”	{itu-t（0）recommendation（0）h（8）235 version（0）2 32}	在 **ClearToken** 中指示一个 RADIUS 响应（在查询字段中传送）
“M”	{itu-t（0）recommendation（0）h（8）235 version（0）2 33}	与 **ClearToken** 中受保护的口令一起指示 BES 缺省方式

附　录　II

H.324实施详情

有待进一步研究。

附　录　III

其他H系列实施详情

有待进一步研究。

附 录 IV

H.235v3修正案1勘误1与H.235v4子系列建议书对应的章节

这一资料性附录示出在 H.235v4 子系列建议书中的 H.235v3 修正案 1 勘误 1 的所有章节的布置。

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标 题	H.235v4.x 子系列建议书	章 节
正文	–	–	–
1	范围	H.235.0	1
2	参考文献	H.235.0 H.235.1 H.235.2 H.235.3	2 2 2 2
3	术语和定义	H.235.0 H.235.2 H.235.6	3 3 3
4	符号和缩写	H.235.0 H.235.3 H.235.6	4 4 4
5	惯例	H.235.0 H.235.2 H.235.6	5 5 5
6	系统引言	H.235.0	6
6.1	摘要	H.235.0	6.1
6.2	认证	H.235.0	6.2
6.2.1	证书	H.235.0	6.2.1
6.3	呼叫建立安全性	H.235.0	6.3
6.4	呼叫控制（H.245）安全性	H.235.0	6.4
6.5	媒体流保密	H.235.0	6.5
6.6	可信单元	H.235.0	6.6
6.6.1	密钥托管	H.235.0	6.6.1
6.7	不可否认	H.235.0	6.7
6.8	移动安全性	H.235.0	6.8
6.9	安全概要	H.235.0	6.9
7	连接建立规程	H.235.0	7
7.1	引言	H.235.0	–
8	H.245 信令和规程	H.235.6	7

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标　　题	H.235v4.x 子系列建议书	章　　节
8.1	安全 H.245 信道操作	H.235.6	7.1
8.2	非安全 H.245 信道操作	H.235.6	7.2
8.3	能力交换	H.235.6	7.3
8.4	主控方角色	H.235.6	7.4
8.5	逻辑信道信令	H.235.6	7.5
8.6	快速连接安全性	H.235.6	7.6
8.6.1	单向快速启动安全性	H.235.6	7.6.1
8.6.1.1	在快速连接中使用多重加密算法	H.235.6	7.6.1.1
8.6.2	双向快速启动安全性	H.235.6	7.6.2
8.7	加密 H.245 DTMF	H.235.6	7.7
8.7.1	加密的基串	H.235.6	7.7.1
8.7.2	加密的 iA5 串	H.235.6	7.7.2
8.7.3	加密的通用串	H.235.6	7.7.3
8.7.4	对象标识符一览	H.235.6	7.7.4
8.8	Diffie-Hellman 操作	H.235.6	7.8
9	多点规程	H.235.6	8.8
9.1	认证	H.235.6	8.8.1
9.2	保密	H.235.6	8.8.2
10	认证信令和规程	H.235.0	8
10.1	引言	H.235.0	---
10.2	采用任选认证的 Diffie-Hellman	H.235.0	8.1
10.3	基于预订的认证	H.235.0	8.2
10.3.1	引言	H.235.0	–
10.3.2	具有对称加密的口令	H.235.0	8.2.1
10.3.3	具有散列的口令	H.235.0	8.2.2
10.3.4	具有签名的基于证书的认证	H.235.0	8.2.3
10.3.5	共享秘密和口令的使用	H.235.0	8.2.4
11	媒体流加密规程	H.235.6	9
11.1	媒体对话密钥	H.235.6	9.1
11.2	媒体反滥发	H.235.6	9.2
11.2.1	对象标识符一览	H.235.6	9.2.1
12	安全性误差纠正	H.235.0	11
13	使用椭圆曲线加密系统的非对称认证和密钥交换	H.235.0	9
13.1	密钥管理	H.235.0	9.1

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标　　题	H.235v4.x 子系列建议书	章　　节
13.2	数字签名	H.235.0	9.2
附录 I	H.323 实施详情	H.235.0	附录 I
I.1	密文填充方法	H.235.6	I.1
I.2	新密钥	H.235.6	8.7.2
I.3	H.323 可信单元	H.235.6	8.7.3
I.4	实施实例	H.235.0	I.1
I.4.1	令牌	H.235.0	I.1.1
I.4.2	H.323 系统中令牌用法	H.235.0	I.1.2
I.4.3	H.323 系统中 H.235 随机值用法	H.235.0	I.1.3
I.4.4	口令	H.235.0	I.1.4
I.4.5	IPsec	H.235.0	I.1.5
I.4.6	后端业务支持	H.235.0	I.1.6
附录 II	H.324 实施详情	H.235.0	附录 II
附录 III	其他 H 系列实施详情	H.235.0	附录 III
附录 IV	参考资料	H.235.0	2.2
附件 A	**H.235 ASN.1**	**H.235.0**	**附件 A**
附件 B	**H.323 特定问题**	**H.235.6**	–
B.1	背景	H.235.0	6
B.2	信令和规程	H.235.6	8
B.2.1	修订版 1 的兼容性	H.235.6	8.1
B.2.2	误差信令	H.235.0	11.1
B.2.3	第 3 版的特性指示	H.235.6	8.2
B.2.4	密钥传送	H.235.6	8.3
B.2.4.1	在 H.235 第 3 版中改进的密钥传输	H.235.6	8.3.1
B.2.5	增强型 OFB 模式	H.235.6	8.4
B.2.6	密钥更新和同步	H.235.6	8.6
B.2.6.1	未确认的密钥更新	H.235.6	8.6.1
B.2.6.2	改进的密钥更新	H.235.6	8.6.2
B.2.6.3	基于有效载荷类型的密钥更新和同步	H.235.6	8.6.3
B.3	RTP/RTCP 问题	H.235.6	9.3
B.3.1	初始化矢量	H.235.6	9.3.1
B.3.1.1	CBC 初始化矢量	H.235.6	9.3.1.1
B.3.1.2	EOFB 初始化矢量	H.235.6	9.3.1.2
B.3.2	填充	H.235.6	9.3.2
B.3.3	RTCP 保护	H.235.6	9.3.3

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1 章节	标　　题	H.235v4.x 子系列建议书	章　　节
B.3.4	安全有效载荷流	H.235.6	9.3.4
B.3.5	与 J.170 的相互作用	H.235.6	9.3.5
B.4	认证的 RAS 信令/规程	H.235.0	8.3
B.4.1	引言	H.235.0	–
B.4.2	端点—网守的认证（基于非预订的）	H.235.0	8.3.1
B.4.3	端点—网守的认证（基于预订的）	H.235.0	8.3.2
B.4.3.1	具有对称加密的口令	H.235.0	8.3.2.1
B.4.3.2	具有散列的口令	H.235.0	8.3.2.2
B.4.3.3	具有签名的基于证书的认证	H.235.0	8.3.3.3
B.5	非终端交互	H.235.6	8.7
B.5.1	网关	H.235.6	8.7.1
B.6	在 RAS 信道上的密钥管理	H.235.0	8.4
B.7	伪随机函数（PRF）	H.235.0	10
附件 C	**H.324 特定问题**	**H.235.0**	**附件 B**
附件 D	**基线安全概要**	**H.235.1**	
D.1	引言	H.235.1	
D.2	惯例	H.235.1	5
D.3	范围	H.235.1	1
D.4	符号和缩写	H.235.1	4
D.5	规范性参考文献	H.235.1	2.1
D.6	基线安全概要	H.235.1	
D.6.1	概述	H.235.1	6.1
D.6.1.1	基线安全概要	H.235.1	6.2
D.6.1.2	话音加密安全概要	H.235.6	6.1
D.6.2	认证和完整性	H.235.1	3.1
D.6.3	H.323 需求	H.235.1	6.3
D.6.3.1	概述	H.235.1	6.4
D.6.3.2	基于对称密钥的信令消息认证详情（规程 I）	H.235.1	7
D.6.3.3	基于口令的散列计算	H.235.1	7.1
D.6.3.3.1	HMAC-SHA1-96	H.235.1	7.2
D.6.3.3.2	认证和完整性	H.235.1	7.3
D.6.3.3.3	仅认证（规程 IA）	H.235.1	8
D.6.3.4	规程 I 的用法说明	H.235.1	9

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1 章节	标　　题	H.235v4.x 子系列建议书	章　　节
D.6.3.4.1	RAS 消息认证和完整性	H.235.1	9.1
D.6.3.4.2	H.225.0 消息认证和完整性	H.235.1	9.2
D.6.3.4.3	H.245 消息认证和完整性	H.235.1	9.3
D.6.4	直接选路方案	H.235.1	9.4
D.6.5	后端业务支持	H.235.1	10
D.6.6	H.235 第 1 版的兼容性	H.235.1	11
D.6.7	组播特性	H.235.1	12
D.7	话音加密安全概要	H.235.6	6.1
D.7.1	密钥管理	H.235.6	8.5
D.7.2	密钥更新和同步	H.235.6	8.6
D.7.3	外 CBC 方式的三倍 DES	H.235.6	9.4
D.7.4	在 EOFB 方式内操作的 DES 算法	H.235.6	9.5
D.7.5	外 EOFB 方式的三倍 DES	H.235.6	9.6
D.8	合法拦截	H.235.6	10
D.9	安全信令消息一览	H.235.1	13
D.9.1	H.225.0 RAS	H.235.1	13.1
D.9.2	H.225.0 呼叫信令	H.235.1	13.2
D.9.3	H.245 呼叫控制	H.235.1	13.3
D.10	sendersID 与 generalID 用法	H.235.1	14
D.11	对象标识符一览	H.235.1 H.235.6	15 11
D.12	参考资料	H.235.1 H.235.6	2.2 2.2
附件 E	**签名概要**	**H.235.2**	
E.1	概述	H.235.2	6
E.2	惯例	H.235.2	5
E.3	H.323 需求	H.235.2	6.1
E.4	安全性业务	H.235.2	5
E.5	采用公钥/私钥对的数字签名详情（规程 II）	H.235.2	7
E.6	多点会议规程	H.235.2	8
E.7	端到端认证（规程 III）	H.235.2	9
E.8	仅认证	H.235.2	10
E.9	认证和完整性	H.235.2	11
E.10	数字签名计算	H.235.2	12

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标　　题	H.235v4.x 子系列建议书	章　　节
E.11	数字签名核实	H.235.2	13
E.12	证书处理	H.235.2	14
E.13	规程 II 用法说明	H.235.2	15
E.13.1	RAS 消息认证、完整性和不可否认	H.235.2	15.1
E.13.2	RAS 仅认证	H.235.2	15.2
E.13.3	H.225.0 消息认证、完整性和不可否认	H.235.2	15.3
E.13.4	H.245 消息认证和完整性	H.235.2	15.4
E.14	H.235 第 1 版的兼容性	H.235.2	16
E.15	组播特性	H.235.2	17
E.16	安全信令消息一览	H.235.2	18
E.16.1	H.225.0 RAS	H.235.2	18.1
E.16.2	H.225.0 呼叫信令	H.235.2	18.2
E.17	sendersID 和 generalID 用法	H.235.2	19
E.18	对象标识符一览	H.235.2	20
附录 IV（附件 E）	参考资料	H.235.2	2.2
附件 F	**混合安全概要**	**H.235.3**	
F.1	概述	H.235.3	6
F.2	规范性参考文献	H.235.3	2.1
F.3	首字母缩略语	H.235.3	4
F.4	规范惯例	H.235.3	5
F.5	H.323 需求	H.235.3	6.1
F.6	认证和完整性	H.235.3	6.2
F.7	规程 IV	H.235.3	7
F.8	并发呼叫的安全性关联	H.235.3	8
F.9	密钥更新	H.235.3	9
F.10	图解实例	H.235.3	11
F.11	组播特性	H.235.3	12
F.12	安全信令消息一览	H.235.3	13
F.12.1	H.225.0 RAS	H.235.3	13.1
F.12.2	H.225.0 呼叫信令（单个管理域）	H.235.3	13.2
F.12.3	H.225.0 呼叫信令（多个管理域）	H.235.3	13.3
F.13	对象标识符一览	H.235.3	14
附录 IV	参考资料	H.235.3	2.2

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标　　题	H.235v4.x 子系列建议书	章　　节
附件 G	安全实时传输协议（SRTP）与 MIKEY 密钥管理协议在 H.235 内的使用	**H.235.7**	
G.1	范围	H.235.7	1
G.2	参考资料	H.235.7	2
G.2.1	规范性参考文献	H.235.7	2.1
G.2.2	资料性参考文献	H.235.7	2.2
G.3	定义	H.235.7	3
G.4	符号和缩写	H.235.7	4
G.5	规范惯例	H.235.7	5
G.6	引言	H.235.7	6
G.7	概述和情形	H.235.7	7
G.7.1	在“会话层”MIKEY 的操作	H.235.7	7.1
G.7.2	在“媒体层”MIKEY 的操作	H.235.7	7.2
G.7.3	MIKEY 能力的协商	H.235.7	7.3
G.8	使用对称安全技术的安全概要	H.235.7	8
G.8.1	终止一个 H.323 呼叫	H.235.7	8.1
G.8.2	TGK 密钥重置和 CSB 更新	H.235.7	8.2
G.8.3	H.245 隧道传送的支持	H.235.7	8.3
G.8.4	SRTP 算法	H.235.7	8.4
G.8.5	对象标识符一览	H.235.7	8.5
G.9	使用不对称安全技术的安全概要	H.235.7	9
G.9.1	终止一个 H.323 呼叫	H.235.7	9.1
G.9.2	TGK 密钥重置和 CSB 更新	H.235.7	9.2
G.9.3	H.245 隧道传送的支持	H.235.7	9.3
G.9.4	SRTP 算法	H.235.7	9.4
G.9.5	对象标识符一览	H.235.7	9.5
G.I	MIKEY-DHHMAC 选项	H.235.7	附录 I
G.I.1	终止一个 H.323 呼叫	H.235.7	I.1
G.I.2	TGK 密钥重置和 CSB 更新	H.235.7	I.2
G.II	使用 H.235 附件 I 来建立预共享的秘密	H.235.7	附录 II
G.II.1	终止一个 H.323 呼叫	H.235.7	II.1
G.II.2	TGK 密钥重置和 CSB 更新	H.235.7	II.2

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1 章节	标　　题	H.235v4.x 子系列建议书	章　　节
附件 H	**RAS 密钥管理**	**H.235.5**	
H.1	引言	H.235.5	–
H.2	范围	H.235.5	1
H.3	参考文献	H.235.5	2
H.3.1	规范性参考文献	H.235.5	2.1
H.3.2	资料性参考文献	H.235.5	2.2
H.4	定义	H.235.5	3
H.5	缩写	H.235.5	4
H.6	基本框架	H.235.5	6
H.6.1	H.235v3 中的协商能力改进	H.235.5	6.1
H.6.2	在端点和网守之间的应用	H.235.5	6.2
H.6.3	网守之间概要的使用	H.235.5	6.3
H.6.4	信令信道加密合认证	H.235.5	6.4
H.7	指定的安全概要（SP1）	H.235.5	7
H.8	框架的扩展（资料性参考）	H.235.5	9
H.8.1	经由 TLS 使用主密钥保护呼叫信令信道	H.235.5	9.1
H.8.1.1	端点注册	H.235.5	9.1.1
H.8.2	使用证书进行网守认证	H.235.5	9.2
H.8.3	另一信令安全性机制的应用	H.235.5	9.3
H.9	威胁（资料性参考）	H.235.5	10
H.9.1	被动攻击	H.235.5	10.1
H.9.2	拒绝服务攻击	H.235.5	10.2
H.9.3	中间人攻击	H.235.5	10.3
H.9.4	猜测攻击	H.235.5	10.4
H.9.5	未加密的网守半密钥	H.235.5	10.5
附件 I	**直接选路呼叫的支持**	**H.235.4**	
I.1	范围	H.235.4	1
I.2	引言	H.235.4	6
I.3	规范惯例	H.235.4	5
I.4	术语和定义	H.235.4	3
I.5	符号和缩写	H.235.4	4
I.6	规范性参考文献	H.235.4	2
I.7	概述	H.235.4	7

表 IV.1/H.235.0－对应章节

H.235v3修正案1勘误1章节	标　　题	H.235v4.x 子系列建议书	章　　节
I.8	限制	H.235.4	8
I.9	规程 DRC	H.235.4	9
I.10	基于 PRF 的密钥衍生规程	H.235.4	12
I.11	基于 FIPS-140 的密钥衍生规程	H.235.4	13
I.12	对象标识符一览	H.235.4	14
附录 I（附件 I）	参考资料	H.235.4	2.2

附　录　V

H.235v3修正案1勘误1与H.235v4子系列建议书对应的图

这一资料性附录示出在 H.235v4 子系列建议书中的 H.235v3 修正案 1 勘误 1 的所有图的布置。

表 V.1/H.235.0－对应的图

H.235v3修正案1勘误1图	标　　题	H.235v4.x 子系列建议书	图
图 1	采用任选认证的 Diffie-Hellman	H.235.0	4
图 2a	具有对称加密的口令，二次扫描	H.235.0	5
图 2b	具有对称加密的口令，三次扫描	H.235.0	6
图 3a	具有 hash 的口令，二次扫描	H.235.0	7
图 3b	具有 hash 的口令，三次扫描	H.230.0	8
图 4a	具有签名的基于证书，二次扫描	H.235.0	9
图 4b	具有签名的基于证书的认证，三次扫描	H.235.0	10
图 5	媒体加密	H.235.6	7
图 6	媒体解密	H.235.6	8
图 7	媒体反滥发的 RTP 分组格式	H.235.6	9
图 I.1	ECB 方式的密文侵占	H.235.6	I.1
图 I.2	CBC 方式的密文侵占	H.235.6	I.2
图 I.2a	CBC 方式的零填充	H.235.6	I.3
图 I.3	CFB 方式的零填充	H.235.6	I.4
图 I.4	OFB 方式的零填充	H.235.6	I.5

表 V.1/H.235.0－对应的图

H.235v3修正案1勘误1图	标　　题	H.235v4.x 子系列建议书	图
图 I.4.1	EOFB 方式的零填充	H.235.6	I.6
图 I.5	RTP 所规定的填充	H.235.6	I.7
图 I.6	令牌	H.235.0	I.1
图 I.7	后端业务方案	H.235.0	I.2
图 B.1	概述	H.235.0	2
图 B.1.1	从主控方到从属方的未确认的对话密钥分配/密钥更新	H.235.6	4
图 B.1.2	从属方逻辑信道上的对话密钥更新	H.235.6	5
图 B.1.3	主控方逻辑信道上的对话密钥更新	H.235.6	6
图 B.2	具有对称加密的口令	H.235.0	11
图 B.3	具有 hash 的口令	H.235.0	12
图 B.4	具有签名的基于证书的认证	H.235.0	13
图 D.1	在 GK 选路分区内具有两个 EP 的 GK-GK 方案的规程 I 用法说明	H.235.1	1
图 D.2	在 GK 选路分区内具有 EP1 而 EP2 在直接选路分区内的混合方案的规程 I 用法说明	H.235.1	2
图 D.3	具有两个 EP 均在使用直接选路 GK 分区内的方案的规程 I 用法说明	H.235.1	3
图 D.4	外 CBC 方式的三倍 DES 加密	H.235.6	10
图 D.5	外 EOFB 方式的三倍 DES 加密	H.235.6	11
图 E.1	逐段转接安全性和端到端认证的同步使用	H.235.2	1
图 E.2	GK-GK 选路模型中公钥用法说明	H.235.2	2
图 F.1	并发呼叫的安全性关联	H.235.3	1
图 F.2	单一管理域中的流程图	H.235.3	2
图 F.3	多个管理域中的流程图	H.235.3	3
图 G.1	情形	H.235.7	1
图 G.2	使用 MIKEY 和 SRTP 的安全情形	H.235.7	2
图 G.3	仅是逐段转接地具有共享秘密的情形	H.235.7	3

表 V.1/H.235.0－对应的图

H.235v3修正案1勘误1图	标　　题	H.235v4.x 子系列建议书	图
图 G.4	端点 B 用 MIKEY 预共享秘密呼叫端点 A 的例子（GK 选路）	H.235.7	4
图 G.5	EP B 对 MIKEY 预共享秘密的处理	H.235.7	5
图 G.6	EP A 对 MIKEY 预共享秘密的处理	H.235.7	6
图 G.7	端点 B 终止一个呼叫的例子	H.235.7	7
图 G.8	端点 B 更新一个密钥的例子	H.237.7	8
图 G.9	端到端采用 PKI 的情形（多 GK）	H.235.7	9
图 G.10	EP B 用 MIKEY-PK-SIGN 呼叫 EP A 的例子（多 GK 选路）	H.235.7	10
图 G.11	EP B 对 MIKEY-PK-SIGN 的处理	H.235.7	11
图 G.12	EP A 对 MIKEY-PK-SIGN 的处理	H.235.7	12
图 G.13	端点 B 终止一个呼叫的例子	H.235.7	13
图 G.14	EP B（发起方）发起 TGK 密钥重置和密钥更新的例子	H.235.7	14
图 G.I-1	端点 B 用 MIKEY-DHHMAC 呼叫端点 A 的例子（GK 选路）	H.235.7	I.1
图 G.I-2	端点 B 终止一个呼叫的例子	H.235.7	I.2
图 G.I-3	端点 B 更新一个密钥的例子	H.235.7	I.3
图 G.II-1	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）	H.235.7	II.1
图 H.1	安全概要和 TLS 的信息流	H.235.5	1
图 I.1	直接选路呼叫情形	H.235.4	1
图 I.2	基本通信流	H.235.4	2

附 录 VI

H.235v3修正案1勘误1与H.235v4子系列建议书对应的表

这一资料性附录示出在 H.235v4 子系列建议书中的 H.235v3 修正案 1 勘误 1 的所有表的布置。

表 VI.1/H.235.0－对应的表

H.235v3修正案1勘误1表	标　　题	H.235v4.x 子系列建议书	表
表 1	NULL 加密的对象标识符	H.235.6	2
表 2	H.245 DTMF 加密的对象标识符	H.235.6	3
表 3	供反滥发所使用的对象标识符	H.235.6	5
表 I.1	I.4.6 使用的对象标识符	H.235.0	I.1
表 D.1	附件 D 安全概要一览	----	---
表 D.2	基线安全概要	H.235.1	1
表 D.3	话音加密概要	H.235.6	1
表 D.4	Diffie-Hellman 群	H.235.6	4
表 D.5	sendersID 和 generalID 用法	H.235.1	2
表 D.6	附件 D 所使用的对象标识符	H.235.1 H.235.6	3 6
表 E.1	签名安全概要	H.235.2	1
表 E.2	sendersID 和 generalID 用法	H.235.2	2
表 E.3	附件 E 所使用的对象标识符	H.235.2	3
表 F.1	混合安全概要概述	H.235.3	1
表 F.2	附件 F 所使用的对象标识符	H.235.3	2
表 G.1	MIKEY 密钥管理协议	H.235.7	1
表 H.1	概要单元	H.235.5	1
表 I.0	从共享秘密中计算加密和补白密钥	H.235.4	1
表 I.1	H.235.4 所使用的对象标识符	H.235.4	2

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