国 际 电 信 联 盟

ITU-T H.235.2

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：签名安全概要

ITU-T H.235.2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.235.2建议书

H.323安全性：签名安全概要

摘　要

本建议书描述采用数字签名来保护 H.225.0 信令的任选的安全概要。

在 H.235 子系列的较早版本中，该概要被包含在附件 E/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.235.2 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

ITU-T H.235.2建议书

H.323安全性：签名安全概要

1 范围

本建议书描述采用数字签名来保护 H.225.0 信令的任选的安全概要。

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 (1998), *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.235.6 (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*.

– 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 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

– 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.*

[RFC3447] IETF RFC 3447 (2003), *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

3 术语和定义

出于本建议书的目的，除了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、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 certification authorities 证书核发机构：证书核发机构（CA），在有关电子签名的环境中使用时，通过发布“证书”验证公共核实密钥。

3.2 certificate repositories 证书库：证书库（例如一个 X.500 号码簿）掌握用户证书和证书撤销一览表（CRL）。通过访问证书库可获得该信息，但信息库不对从 CA 或 RA 所接收的信息内容和准确性负责。

3.3 digital signature 数字签名：它是数据消息的密码变换（使用非对称的密码技术）的数字化表示，以致任何具有该签署消息和该相关公钥的个人能够确定：

i） 使用与相关公钥相对应的私钥生成该变换；且

ii） 自该密码变换以来所签署的消息未曾变更。

3.4 on-line certificate Status Providers 联机证书状态供应方：联机证书状态协议（OCSP）使应用能够确定标识证书的撤销状态。OCSP 可用于满足使用比采用 CRL 可能更为及时方式提供撤销信息的某些操作需求。联机证书状态提供方可以视为使用脱机 CRL 的一种选择。

3.5 proxy 代理服务器：代理服务器是类似于网守的中间 H.323 实体。代理服务器可以是单个的网络节点或者可以同功能性的 H.323 实体一起配置诸如网守一类的实体。代理服务器可以实施安全任务诸如签名和证书核实以及接入控制。

3.6 registration authorities 注册机构：注册机构充当用户和 CA 之间中间媒体的角色。它们接收来自用户的请求并以适当的格式向 CA 传输这些请求。

3.7 time stamping authorities 时间标记机构：在密钥丢失或密钥泄露的情形中，不可否认的时间标记机构是强制的。事实上，在散列或散列标识符上它们向任何人提供对抗签名，其中包括可靠的时间。

3.8 trust service provider 信任服务提供方：实体，能够被其他实体在通信或证书过程中作为可信的中间媒体所使用的，或者作为可信的信息服务提供方所使用的实体。

本建议书使用以下术语以提供安全性业务。

3.9 authentication-only 仅认证：此签名安全概要的安全性业务支持这样的用户认证，即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。注意该安全性业务不提供对策来抵御任意的剪辑与粘贴、消息人为操纵或窜改攻击。当转发消息到另一个目标时（例如网守），对于核实该消息认证（数据源认证）的安全代理服务器而言，仅认证或许有用。

注 — 转发通常改变消息的某些部分，因此端到端安全性不能实现。

不仅如此，仅认证同样能够在逐段转接的基础上使用。规程 III 说明端到端方案的该安全性业务同时规程 II 说明逐段转接情形的该安全性业务。

3.10 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，可以保护消息防止窜改。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。规程 II 说明此安全性业务。

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）。

4 符号和缩写

本建议书采用下列缩写：

ARQ	接入请求
ASN.1	抽象句法记法 1
CA	认证机构
CRL	证书撤销一览表
DH	Diffie-Hellman
DNS	域名服务
EP	端点
EPID	端点标识符
GK	网守
GKID	网守标识符
GRQ	网守需求
ICV	完整性校验值
IP	网际协议
ITU	国际电信联盟

LDAP 轻便式号码簿接入协议

LRQ 位置请求

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

OCSP 在线证书状态协议

PKCS 公钥加密系统

RA 注册机构

RAS 注册、认可和状态

RSA Rivest、Shamir 和 Adleman

RTP 实时协议

SHA 安全散列算法

URL 通用资源定位器

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。

如果必要，为了实现话音机密性，签名安全概要可以使用 H.235.1 的**话音加密安全概要**。

伴随不同的安全性机制诸如非对称密码（数字签名）技术，规程 II 和 III 详细说明如何实施作为逐段转接和端到端不同方案的安全性业务。

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。

更进一步，所有逐段转接安全性信息放置到 **CryptoSignedToken** 单元中。该信息在每个分段转接上依照规程 II 重新计算。

另一方面端到端安全性信息 — 仅在使用 H.323 代理服务器和规程 III 时才可能 — 基本上计算类似于放置到 **CryptoSignedToken** 中的信息，但将此安全性信息存储在该消息的单独的 **CryptoToken** 中。传输中该信息不改变。单独的对象标识符就可以区分逐段转接和端到端 **CryptoToken** 之间的差别。

使用数字签名的非对称技术可在逐段转接和/或端到端基础上使用。

6 概述

本建议书描述采用数字签名作为选项推荐的安全概要。为改进安全性或每当需求时，H.323 安全实体（终端、网守、网关、MCU 等）可以实施该签名安全概要。

签名安全概要要求 GK 选路模型并基于 H.245 隧道传送技术；对于非 GK 选路模型的支持有待进一步研究。

签名安全概要适用于可升级的“全球”IP 电话；该安全概要克服 H.235.1 的简单、基线安全概要的局限。例如，签名安全概要不取决于不同域内分段转接的互相共享秘密的管理。对 H.245 消息完整性它提供了 H.245 消息的隧道传送并且也提供不可否认消息。伴随 H.235 代理服务器或中间网守的同步使用作为真正端到端认证、签名安全概要同样支持的逐段转接的安全性。

对于 RAS、H.225.0 和 H.245 消息，由这些概要所提供的特征包括：

- 对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。
- 也能够提供两个实体之间交换的消息不可否认，它与该消息所历经的应用等级分段转接的数目无关。特别地，对该消息核心分段（字段）提供不可否认。例如，可以是这样的情形，即 EP 向其 GK 发送 SETUP 消息时，这两个实体（EP 和 GK）可以被一个或多个代理服务器分隔。

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：

- 拒绝服务攻击：快速检测的数字签名可以防止此类攻击。
- 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。当中间人为输入处于应用等级实体之间时，对于该消息所选择的分段通过端到端用户认证和完整性的存在可以防止此类攻击。
- 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。

推荐签名安全概要作为选项。该安全概要在具有潜在多个终端的环境中使用，在那里口令/对称密钥指派是不适宜的，例如在大规模或整体规模方案中。对于使用数字签名和证书的不可否认，签名安全概要提供另外的安全性业务。数字签名能够使用 SHA1 或 MD5 散列并提供认证和/或完整性（见规程 II 和 III）。

在逐段转接基础上使用认证和完整性或仅认证的 H.323 实体必须使用规程 II。只使用仅认证的 H.323 实体将不实施完整性。对于真正端到端认证该仅认证的 H.323 实体必须使用规程 III。

本建议书可以应用跨越整个消息的消息完整性保护。对于 H.225.0 RAS 而言，完整性保护覆盖了整个 RAS 消息；对于呼叫信令而言，完整性保护则覆盖整个 H.225.0 呼叫信令消息，包括 Q.931 头。

在 H.225.0 性能消息内签名安全概要允许安全地隧道传送 H.245 呼叫控制 PDU。H.245 密钥更新和同步机制要求隧道传送，例如对甚长持续时间呼叫有用。

注 2 — 安全 G.711 语音编码的密钥更新最迟应在传输 2^{30} 个 64 比特块后发生，即多于 12 整天的连续对话。

表 1 中垂直阴影区（电子版为蓝色填充区）表示签名安全概要的范围。当省略由水平阴影区（电子版为绿色填充区）指示的完整性时，仅认证安全概要产生。签名安全概要内选项是在 RSA-SHA1 或 RSA-MD5 数字签名之间做出选择。H.235.6 的话音加密安全概要（见 6.1/H.235.6）能够任选地与签名安全概要一起使用。

表 1/H.235.2－签名安全概要

安全性业务	呼叫功能			
	RAS	H.225.0	H.245 (Note)	RTP
认证	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	数字签名	数字签名	数字签名	
不可否认	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	数字签名	数字签名	数字签名	
完整性	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	数字签名	数字签名	数字签名	
机密性				
接入控制				
密钥管理	证书分配	证书分配		
注 — 在H.225.0快速连接内部隧道传送的H.245或嵌入的H.245。				

注 3 — 签名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 4 — 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）。

对于认证，用户将使用公钥/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、证书和证书分配以及私钥/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 20 节）所涉及的通信实体能够隐含地确定或者 H.235.1 基线安全概要或者该签名安全概要的用法。

使用的下列规程在该概要中描述：

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 II 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先进的完整性，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在相反方向上使用认证/完整性，并由此提供更高的安全性。终端的安全性政策可以允许“仅认证”而无必须计算密码完整性（见第 9 节）。

从安全端点/对等的网守所接收的 RAS/呼叫信令消息中检测到故障认证和/或失效的完整性有效性的网守采用相应的通过设置为 **securityDenial** 的拒绝理由或依据 11.1/H.235.0 采用其他适当的安全误差编码来指示安全性失效的拒绝消息响应。依据识别攻击的性能和与其反应的最适当的方法，接收具有未定义的对象标识符（**tokenOID**、**algorithmOID**）的安全的 **xRQ** 的网守可以用非安全的 **xRJ** 响应，设置理由为 **securityDenia** 拒绝，或它可以丢弃那个信息。遭遇的安全性事件应记入日志。另一方面，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。类似地，遭遇的安全性事件应记入日志。

存在隐含的 H.235 信令，表明使用了规程 II，并根据对象标识符的值表明采用的安全性机制（也见第 20 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；而是在 **CryptoSignedToken** 中 **token** 的 **signature** 字段中放置密码完整性检测值。

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；
- GK 选路模型。

7 采用公钥/私钥对的数字签名详情（规程II）

只要规程 II 从事于逐段转接的安全性就必须依从以下规程：

- SHA1 或 MD5 应与 RSA 算法一道用于生成数字签名。在这方面依从 PKCS 1 和 PKCS 7 将有助于实现互操作。

  每个 RAS/H.225.0 消息中 **CrytoH323token** 字段必须包含以下字段：

  — 包含 **CryptoToken** 的 **nestedCryptoToken**，该 **CryptoToken** 自身包含的 **cryptoSignedToken** 包含下列字段：

  - **tokenOID** 设置为：
    - — “A”指示认证/完整性计算包括 H.225.0 RAS 消息中的所有字段（见第 11 节）；
    - — “B”指示认证/完整性计算仅包括 RAS/H.225.0 消息中仅认证的子集字段（见第 10 节）。
  - **token** 包含以下字段：
    - — **toBeSigned** 包括 **EncodedGeneralToken**，它实际上是伴随以下字段设置的 **ClearToken**：
      - **tokenOID** 设置为“S”，指示供消息认证/完整性/不可否认使用的 **ClearToken**。
      - **timeStamp** 包含时间标记。
      - **random** 包含单调递增的序列号。
      - **generalID** 包含接收者的标识符（仅在单播的情形中）。
      - **sendersID** 包含发送者的标识符。
      - **dhKey**，在 **Setup** 和 **connect** 期间，如本建议书中所指定的用于传送 Diffie-Hellman 参数：
        - — **halfkey** 包含一个同线用户方的随机公钥；
        - — **modsize** 包含 DH 基集（见表 4/H.235.6）；
        - — **generator** 包含 DH 群（见表 4/H.235.6）。

        注 1 — 当使用签名安全概要而无话音加密安全概要时，无任何 Diffie-Hellman 参数需要发送；**dhkey** 应缺省，可以设置{'0'B，'0'B，'0'B}表示替代 **halfkey**、**modsize** 和 **generator**。
      - **certificate** 包含发送者的数字证书，其中 **type** 标识证书类型（“V”指示使用 MD5-RSA 证书，“W”指示使用 SHA1-RSA 证书），**certificate** 携载实际的证书（见第 14 节）。
      - **algorithmOID** 设置为：
        - — “V”指示使用 MD5-RSA 签名；
        - — “W”指示使用 SHA1-RSA 签名。
      - **paramS** 设置为 NULL。
      - **signature** 包含在 H.225.0 RAS 消息或呼叫信令消息的所有字段上使用 SHA1 或 MD5 RSA 所计算的签名（只要 **tokenOID** 为“A”，见第 11 节）或者在

H.225.0 RAS 消息或呼叫信令消息的某些核心字段使用 SHA1 或 MD5 RSA 所计算的签名（如果 **tokenOID** 为“B”，见第 10 节）。

当 **tokenOID**“A”供保护包括所有 H.245 消息内容的隧道传送的 H323-UU-PDU 所使用时，签名计算必须依据第 11 节描述的规程在具有全部字段的整个 H.225.0 呼叫信令消息上完成。在使用 **tokenOID**“B”的情形中，当采用规程 III 时实现 **CryptoToken** 的仅认证（见第 10 节）。

- 该签名所意指的实体（可能位于一个或多个应用转接分段之外）核实该签名。

注 2 — 接收者能够通过估计 **CryptoSignedToken** 的令牌内的 **algorithmOID** 检测规程 II 的使用（检测“V”或“W”的存在）。

8 多点会议规程

MCU 必须通过隧道传送的 H.245 **ConferenceRequest** 和 **ConferenceResponse** 指令如 8.8.1/H.235.6 中所述支持来自终端请求的证书的安全分配。在多点会议环境中，这允许终端请求来自其他终端的证书并因此获得有关会议其他参与方的一致性确认。

ConferenceRequest 传递 **requestTerminalCertificate**，其字段设置如下：

- **terminalLabel**：作为通过 MCU 的远程终端的寻址手段使用；
- **certSelectionCriteria**：发送者可以请求仅特定类型的证书；
- **sRandom**：由请求发送者所生成的随机查询。

ConferenceResponse 传送 **terminalCertificateResponse**，其字段设置如下：

- **terminalLabel**：允许将返还的证书同该终端联系起来。
- **certificateResponse**：传送来自 MCU 的响应，具有字段设置如下：
  - **terminalLabel**：远程终端标识；
  - **certificateResponse**：这实际上是来自 **EncodedReturnSi**ASN.1 编码的八比特组串，如：
    - **generalID**：目标终端标识；
    - **responseRandom**：由 MCU 生成的随机查询值；
    - **requestRandom**：重放的 **sRrandom**；
    - **certificate**：传递该返还的证书，其中 **type** 指示作为 OID 的该证书类型，并且 **certificate** 携载数字证书（见第 14 节）。

9 端到端认证（规程III）

图 1 显示采用代理服务器分隔 GK 和 EP 的方案，其中两种不同的 **CryptoToken** 分别用于逐段转接认证以及端到端认证和/或逐段转接完整性。逐段转接认证的 **CryptoToken** 仅适用于两个实体之间的分段路径并且在每个其他的分段路径上不得不重新计算。在另一方面，端到端认证的 **CryptoToken** 只由发送端点一次生成并在传输中不被中间节点所变更。中间节点可以确认端到端 **CryptoToken** 中所传送的签名和证书并应在传输中转发该 **CryptoToken**。

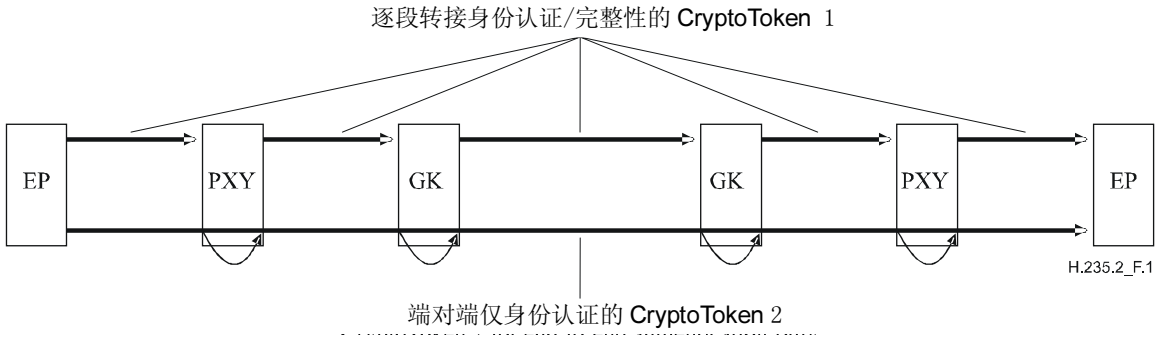

图 1/H.235.2－逐段转接安全性和端到端认证的同步使用

注 1 — 如图 1 所示的代理服务器可以是单独的网络节点或者可以与功能性的 H.323 实体一起配置，例如作为 GK 的一部分。

注 2 — 取决于所签署的 **tokenOID**，代理服务器能够确定接收的 **CryptoToken** 是否预订传输到代理服务器（“S”）或某些其他的接收者（“R”）。

注 3 — 由于在每个分段路径上中间实体变更信令消息内容的事实，端到端完整性是不可能的。

对于跨越 H.323 代理服务器或中间网络单元的真正的端到端认证而言，发送端点/终端必须如下计算数字签名。

每个 RAS/H.225.0 消息中 **CryptoH323Token** 字段必须包含以下字段：

- 包含 **CryptoToken** 的 **nestedCryptoToken**，该 **CryptoToken** 自身包含的 **cryptoSignedToken** 包含下列字段：
  - — **tokenOID** 设置为：
    - “A”指示逐段转接认证/完整性计算包括 RAS/H.225.0 消息中的所有字段（见第 11 节）；
    - “B”指示仅认证计算，包括 H.225.0 RAS 消息字段中的仅认证的子集字段（见第 10 节）。
- **token** 包括以下字段：
  - － **toBeSigned** 包括所使用的 **ClearToken** 字段具有以下字段：
    - **tokenOID** 设置为“R”，指示在端到端基础上即将用于仅认证/不可否认的 **ClearToken**；

      注 4 — 实际上正在采用哪些安全性业务也依赖于证书中的密钥使用比特。
    - **random** 包含单调递增的序列号；
    - **timeStamp** 仅当该终结结束实体被时间同步时供增强的安全性任选；
    - **generalID** 包含接收者的端点标识符（仅在单播的情形中）。在逐段转接的情形中，此为下一个分段转接的标识符；在端到端的情形中，此为远端端点标识符；
    - **sendersID** 包含端点发送者；
    - **certificate** 包含发送者的数字证书，其中 **type** 指示该证书类型（“V”指示使用 MD5-RSA 证书，“W”指示使用 SHA1-RSA 证书），**certificate** 携载实际的证书（见第 14 节）；

- **dhKey**，在 **Setup** 和 **connect** 期间，如本建议书中所指定的用于传送 Diffie-Hellman 参数：
  - — **halfkey** 包含一个同线用户方的随机公钥；
  - — **modsize** 包含 DH 基集（见表 4/H.235.6）；
  - — **generator** 包含 DH 群（见表 4/H.235.6）。

注 5 — 当使用签名安全概要而无话音加密安全概要时，无任何 Diffie-Hellman 参数需要发送；**dhkey** 应缺省，可以设置{'0'B,'0'B,'0'B}表示替代 **halfkey**、**modsize** 和 **generator**。

- — **algorithmOID** 设置为：
  - “V”指示使用 MD5-RSA 签名；
  - “W”指示使用 SHA1-RSA 签名。
- — **paramS** 设置为 NULL。
- — **signature** 包含在 H.225.0 RAS 消息或呼叫信令消息的所有字段上使用 SHA1 或 MD5 RSA 所计算的签名（只要 **tokenOID** 为“A”）或者在 H.225.0 RAS 消息或呼叫信令消息的某些核心字段上所计算的签名（只要 **tokenOID** 为“B”）。

代理服务器可以核实任何获得的数字签名和/或证书并且依照本地法规只要认为不适合就可抛弃该消息，或代理服务器前送转发接收的 **CryptoToken**。为了逐段转接的安全性，代理服务器务必依据规程 II 或 III 生成新的 H.235 信令信息单元。

终结分段路径的实体 — 可以是终端 — 应核实 **CryptoToken** 中所接收的安全性信息，并依赖于端到端安全性单元的存在可以另外地估计端到端 **CryptoToken** 信息的赋值。终端或中间 H.323 实体中确切的核实规程可以依照本地法规有所变化。

10 仅认证

终端可以选择实施仅认证（使用 OID“B”）。在此情形，认证码只在 RAS/H.225.0 消息的子集（**CryptoToken** 内的 **ClearToken**）上计算。仅认证对于真正的端到端认证有用（见第 9 节）。**ClearToken** 结构中以下字段将作为该子集使用：

- **tokenOID**：对于仅认证设施存在单独的令牌对象标识符（tokenOID“B”）。
- **random**：单调递增的序列号。
- **timeStamp**：时间标记。
- **generalID**：接收者的标识符（仅在单播消息的情形中）。在逐段转接的情形中，此为下一个分段转接的标识符；在端到端的情形中，此为远程端端点标识符。
- **sendersID**：发送者的标识符。
- **dhkey**：Diffie-Hellman 参数。仅在 **Setup** 和 **connect** 消息期间使用该字段和子字段。

认证码在 **cryptoSignedToken** 的 **token** 的 **EncodedGeneralToken**（即 **ClearToken**）内的 **ClearToken** 上计算。数字签名必须在 **ClearToken** 的 ASN.1 编码的比特串上计算。在计算数字签名前，**ClearToken** 中 **tokenOID** 必须设置为{0 0}。

11 认证和完整性

对于所有 ASN.1 编码消息字段上的认证和消息的完整性而言（使用 OID“A”），规程如下。

消息的发送者必须计算该签名如下：

1） 设置签名值为采用固定长度的特定缺省模式（例如 1024 比特）。该步骤必须为数字签名的最大长度预留空间，对于某个给定的证书这完全是可能的。这里精确的比特模式并不重要，重要的是好的选择在于剩余消息中不出现惟一的比特模式。

2） ASN.1 编码整个消息。

3） 在编码的消息中定位该缺省模式；所出现的比特模式采用全零比特重写。

注 1 — 在消息中缺省模式出现多次的极少数情况下，这可以包含某些逐次逼近步骤。

4） 使用由 **algorithmOID**“V”或“W”指示的方法在 ASN.1 编码消息上计算数字签名（见第 12 节）。

5） 采用计算的数字签名值替代编码消息中的缺省模式。在数字签名长度小于预留空间长度的情形时，前导零必须放置在该签名值的最高有效比特之前。

接收者接收消息并且处理如下：

1） ASN.1 译码该消息。

2） 提取所接收的数字签名值并在局部变量 SV 中保持。

3） 在接收的编码消息中搜索并定位该签名值 SV。

注 2 — 在整个消息中签名值子字符串发生若干次的极少数情况下，伴随不同的起始搜索位置不得不持续重复步骤 3-6。

4） 采用全零重写编码消息中的比特模式。

5） 使用 **algorithmOID**“V”或“W”（见第 12 节）指示的方法在编码消息上计算数字签名。

6） 将 SV 与计算的签名值比较。仅当两个签名值相等时该消息才认为未被讹误并且可靠；在此情况下，认证成功并终止规程。

7） 否则，重复步骤 3-7 通过重新存储 SV 到先前的位置并搜索另一次匹配。若无任何一个生成的匹配可与正确的签名值相比，则认证失败并在传输期间或由于某些其他原因该消息被（无意或有意地）变更。

12 数字签名计算

该数字签名生成处理的输入为 ASN.1 编码比特串，它包括消息汇编计算处理的结果和签署方的私钥。数字签名生成细节取决于所采用的签名算法；该证书确定所使用的签名算法；当证书中存在密钥用法扩展时，对于符合签署条件的密钥务必设置 **digitalSignature** 比特。由签署方生成的签名值编码成比特串并在 **signature** 字段中携载。

为了计算采用附录（RSASSA-PKCS1-v1_5-SIGN）的基于 RSA 的数字签名，PKCS #1（见 E.8.1.1）中所描述的方法与 OS2IP、RSASP1、I2OSP 规程以及 EMSA-PKCS1-v1_5 的编码方法一起必须使用。

13 数字签名核实

该签名的核实处理的输入包括消息汇编计算处理的结果和签署方的公钥。接收者可以通过任何手段获得正确的签署方公钥，但更为优先选择的方法是来自从 **certificate** 字段所获得的证书并使用散列的签署方的证书使之生效。签署方的公钥生效可以根据证书路径处理（RFC 3280）进行。签名核实的细节取决于所采用的签名算法。

为了核实采用附录（RSASSA-PKCS1-v1_5-VERIFY）的基于 RSA 的数字签名，PKCS #1（见 E.8.1.2）中所描述的方法与 OS2IP、RSASP1、I2OSP 规程以及 EMSA-PKCS1-v1_5-ENCODE 方法一起必须使用。

14 证书处理

对于数字签名的核实，接收实体务必曾经对由认可的认证机构（CA）所签署的发送者的证书进行访问。接收者如何能够访问发送者的证书存在若干种可能性：

- 该证书包含在消息交换中，如规程 II 和 III 所描述的；在这一情况下，**certificate** 具有实际的证书，**type** 特有 OID“V”或 OID“W”。
- 接收者知晓该证书；或许来自较早交换的本地存储。
- 发送者提供能够找到该证书的 URL，而不是证书本身。为此，**certificate** 包括 URL 而 **type** 设置为 OID“P”。
- 接收者通过本建议书以外的其他手段获得证书（例如 LDAP 号码簿查询）。

无论何时，数字证书在消息中传送，接收实体（网守，端点）必须对着证书的标识符检验发送者的标识符（网守，端点）以防止中间人攻击。

对于从网守到端点的数位符号消息，一个端点检验网守标识符存在不同的可能性：

— 例如，如果可以获得主机名，在主体字段或证书中的 subjectAltName 的通用名称属性中，端点可对照网守标识符检验主机名。另外，端点可使用 DNS 质询相关的 IP 地址，并对照在响应消息标志的网守中存在的网守的 IP 地址检验它。

— 例如，网守标识符可由 IP 地址（在网络字节顺序中的 4 字节值表示）与网守标识符的其他标识信息连接构造，截短至携载网守标识符的 sendersID 字段的最大长度。另外端点可对照网守的响应的 IP 头中存在的 IP 地址检验属于主机名的 IP 地址。

注 — 当涉及网络地址解析（NAT）设备时，这一方法不会如期望地工作。

— 如果在证书中不能获得主机名，作为证书（*iPAddress subjectAltName*）一部分的 IP 地址必须直接用来执行上述规定的检验。

用户应仔细检查由网守出示的证书以确定它是否满足期望。如果端点有关于期望的网守标识符的外部信息，则主机名可省略。例如，一个端点可连接到一个网守，这个网守的地址和主机名是动态的，但是端点知道网守会出示证书。在这样的情况下，为了阻止中间人攻击，重要的是尽可能地缩小可接收的证书的范围。在特定的情况下，端点可以适当地仅忽略网守标识符，但务必理解这会让连接开放而受到积极的攻击。

如果主机名与证书中的标识符不匹配，以用户为导向的端点必须通知用户（端点可给用户在任何情况下继续连接的机会）或用一个坏证书错误终止连接。自动的端点必须将错误记录到一个适当的检查记录中（如果可以的话），且应（用一个坏证书错误）终止连接。

自动的端点可提供不允许该检验的一个配置背景，但必须提供一个允许检验的背景。

另外，建议网守对任何从端点发送到网守的数字符号消息执行身份检验。网守执行这样一个检验有多确切被认为是本地事务，应受网守的安全性政策实施的制约。例如，可设想在证书中传送的用户名也可能是 H.323 标识符的一部分。更进一步地，网守可用本地管理的/配置的用户数据（如果可以的话）核对这样的标识符信息，也可在其上基于政策决策。

如果网守有关于期望的网守标识符的外部信息，主机名检验可以省略。例如，一个端点可连接到一个网守，这个网守的地址和主机名是动态的，但是端点知道网守会出示证书。在这样的情况下，为了阻止中间人攻击，重要的是尽可能地缩小可接收的证书的范围。在特定的情况下，端点可以适当地仅忽略网守标识符，但务必理解这会让连接开放而受到积极的攻击。

如果主机名与证书中的标识符不匹配，网守必须将错误记录到一个适当的检查记录中（如果可以的话），且应（用一个坏证书错误）终止连接。

如果 dNSName 类型存在 subjectAltName 扩展，它必须被作为标识符使用。否则，必须使用证书的 Subject 字段中的（最特有的）通用名字段。尽管通用名的使用仍在实践中，但请求和鼓励认证机构用 dNSName 代替。

匹配必须使用 RFC 3280 规定的匹配规则执行。如果在证书中有不止一个给定类型的标识符（例如不止一个 dNSName 名），则认为在任何一个设备中的匹配可接受。名字可包含通配符*，它被看做是匹配任何单个域名成分或成分残片。例如，*.a.com 匹配 foo.a.com 但不匹配 bar.foo.a.com。f*com 匹配 foo.com 但不匹配 bar.com。

规程 II 和 III 提供携载数字证书的手段。为了更有效率，若通过本建议书以外的其他手段数字证书未曾在实体中生效，则该实体的数字证书最多仅需要传输一次。这样证书交换应仅在通信建立起始时发生；对于 RAS，它可以或在网守发现期间发生或若该阶段被省略则在网守注册期间发生。类似的，对于快速连接，证书可以包含在初始呼叫信令消息中并可在以后的呼叫信令消息中安全地被省略。

对于此安全概要，必须使用 X.509v3（1997）证书。其他证书格式有待进一步研究。

15 规程II用法说明

考虑图 2 的情形，其中每个实体具有其自己的私钥—公钥对/证书。实体也可拥有多个密钥对。图中，H.323 代理服务器将 EP1 和 GK1 分隔。

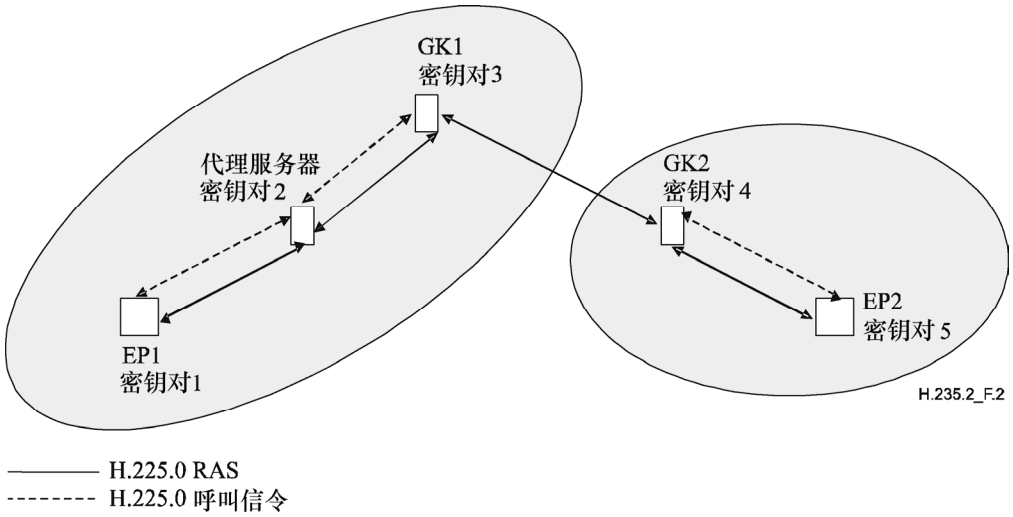

图 2/H.235.2－GK-GK选路模型中公钥用法说明

H.323 代理服务器以双重身份动作：一方面，代理服务器在它的每个分段路径上终止认证和完整性。代理服务器在出局 RAS 消息中以类似于附件 D 的规程 I 中描述的方式主动地包括更新计算的认证/完整性信息。另一方面，代理服务器使端到端安全性信息无更改地通过。然而代理服务器可以在传输中核实接收的证书/或数字签名。

下面说明 RAS、H.225.0 和 H.245 消息的认证、完整性和不可否认的规程详情。

15.1 RAS消息认证、完整性和不可否认

考虑逐段转接通信的情况，其中 EP1 希望向 GK1 发送 RAS 消息，即 **ARQ** 消息。EP1 生成时间标记和序列号，并分别包含在 **timeStamp** 和 **random** 字段中，同 **generalID** 字段中包含代理服务器的化名和 **sendersID** 字段中包含 EP1 的标识符一道。这些字段在 **ARQ** 消息的 **CryptoH323Token** 的 **CryptoToken** 字段的 **CryptoSignedToken** 的 **token** 中出现的 **EncodedGeneralToken** 的 **ClearToken** 字段中存在。该 **CryptoH323Token** 是 **CryptoToken** 序列中最小的几个 **token** 之一。**CryptoSignedToken** 内 **tokenOID** 设置为“A”指示 **ARQ** 消息中的所有字段被签署。**cryptoSignedToken** 中 **token** 具有 **algorithmOID** 设置为“V”指示使用 MD5-RSA 算法或 **algorithmOID** 为“W”指示使用 SHA1-RSA 算法并且 **paramS** 设置为空。然后 EP1 根据给定的签名算法使用它的私钥计算签名。当 **tokenOID** 设置为“A”时，签名在 **ARQ** 消息的所有字段上计算。在 **ARQ** 消息的 **CryptoH323token** 中出现的 **CryptoToken** 的 **CryptoSignedToken** 字段的 **token** 字段中的 **signature** 内，EP1 包括计算的签名并在 **certificate** 字段中包含证书。

类似的，对于通过代理服务器的端到端通信，EP1 生成另一个包含数字签名的 **CryptoToken**，该数字签名覆盖 **ARQ** 消息的 **ClearToken** 中的某些核心字段（见第 9 节）。**CryptoSignedToken** 中 **tokenOID** 设置为“B”指示其 **ClearToken** 的仅认证；**ClearToken** 中的 **tokenOID** 设置为“R”指示端到端认证，还设置 **timeStamp**、**random**、**sendersID**、**generalID** 字段并在 **SETUP/CONNECT** 情况下还设置 **dhkey**，在 **token** 中设置以下字段：**algorithmOID** 设置为“V”或“W”指示该签名算法，**paramS** 为空，并且 **signature** 为在 **ClearToken** 字段上所计算的数字签名。**certificate** 携带 EP1 的数字证书，然后向代理服务器发送 **ARQ** 消息。

一旦接收 **ARQ** 消息，代理服务器就要核实那些向其寻址的令牌的签名（在此情形，即采用 **tokenOID** “A”）。这将基于若干准则，包括：

- timestamp 的存活性，**random** 的惟一性；
- **generalID** 与自身的标识符的一致性；
- **sendersID** 的接入许可；
- **ARQ** 消息中的签名与由 GK1 计算的签名匹配；
- 核实 Diffie-Hellman 参数，例如，检测 1024 比特基集和生成码是否正确。检测 DH 参数是否安全是消耗时间的处理，并仅当在本地政策要求时才进行；
- 核实该接收的证书。

若签名成功核实，则代理服务器计算新的签名，并在向 GK1 如下转发 **ARQ** 之前在 **ARQ** 消息中插入（代替）。代理服务器使用与代理服务器－GK1 分段路径有关的值替代 **ClearToken**（**toBeSigned**）字段中的 **timeStamp**、**random**、**sendersID** 和 **generalID** 字段。**timeStamp** 字段包含当前的时间标记，**random** 字段包含代理服务器－GK1 分段路径的下一个单调递增的序列号，**sendersID** 字段包含代理服务器的化名以及 **generalID** 字段包含 GK1 的化名。然后代理服务器使用其私钥和签名算法计算该 **ARQ** 消息的新的签名，并插入 **token** 内的 **signature** 字段中，并添加其 **certificate** 字段。代理服务器也在新的出局消息中同它的 **ClearToken** 一起包括接收的端到端 **CryptoToken**，并向 GK1 传送 **ARQ** 消息。根据 **ARQ** 消息的选择字段（**tokenOID**“B”）以及未指定给代理服务器的由 EP1 所计算的签名也在 **ARQ** 消息中原封不动地向 GK1 传送。

一旦接收 **ARQ** 消息，GK1 就将核实签名。在适当修正 **toBeSigned** 中的 **ClearToken** 字段后，计算新的签名，并将其插入到 **certificate** 字段，添加其 **certificate** 字段，并向 EP2 继续传送 **Setup** 消息。再次，GK1 将向对等的 GK2 向转发任何在单个 **CryptoToken** 中所接收的端到端信息，通过包括该信息进入未修正的 **CryptoToken** 中。

15.2 RAS仅认证

考虑逐段转接通信的情形，其中 EP1 希望向 GK1 发送 RAS 消息 — 即 **ARQ** 消息。EP1 生成时间标记和序列号，并分别包含它们在 **timeStamp** 和 **random** 字段中，与 **generalID** 字段中包含代理服务器的化名和 **sendersID** 字段中包含 EP1 的标识符一道。这些字段在 **ARQ** 消息的 **CryptoH323Token** 的 **CryptoToken** 字段的 **CryptoSignedToken** 的 **token** 中出现的 **toBeSigned** 的 **ClearToken** 字段中存在。**CryptoSignedToken** 内 **tokenOID** 设置为“B”指示仅 **ClearToken** 字段中特定的子集字段被签署。**CryptoSignedToken** 中 **token** 具有 **algorithmOID** 设置为“V”指示使用 MD5-RSA 或 **algorithmOID** 设置为“W”指示使用 SHA1-RSA 并且 **params** 设置为 NULL。然后 EP1 根据给定的签名算法使用其私钥计算签名。签名在 **ARQ** 消息的特定的 **ClearToken** 字段上计算。在 **ARQ** 消息的 **cryptoH323Token** 中出现的 **CryptoToken** 的 **cryptoSignedToken** 字段的 **token** 字段中的 **signature** 内，EP1 包含该计算的签名并添加其 **certificate** 字段。

类似的，EP1 生成端到端认证的另一个数字签名，它覆盖 **ARQ** 消息中单个 **CryptoToken** 中的某些 **ClearToken** 字段。包括该数字签名（由 “V”或“W”**tokenOID** 所标识的）。然后向代理服务器发送 **ARQ** 消息。

一旦接收 **ARQ** 消息，代理服务器就应核实那些向它寻址的令牌的签名（在此情形中，即采用 **tokenOID**“B”），这将根据若干准则，包括：

- timestamp 的存活性，**random** 的惟一性；
- **generalID** 与自身的标识符的一致性；
- **sendersID** 的接入许可；
- **ARQ** 消息中的签名与由 GK1 计算的签名匹配；
- 核实该接收的证书。

若签名成功核实，代理服务器计算新的签名，并在向 GK1 如下转发 **ARQ** 消息之前将其插入（代替）到 **ARQ** 消息中。代理服务器使用代理服务器－GK1 分段路径有关的值替代 **toBeSigned** 字段的 **ClearToken** 中的 **timeStamp**、**random**、**sendersID** 和 **generalID**。**timeStamp** 字段包含当前的时间标记，**random** 字段包含代理服务器－GK1 分段路径的下一个单调递增的序列号，并且 **generalID** 字段包含 GK1 的化名。然后代理服务器使用其私钥及签名算法 MD5-RSA 或 SHA1-RSA（**algorithmOID**=“V”或“W”）计算该 **ClearToken** 的新的签名，并将其插入到 **cryptoSignedToken** 的 **token** 内的 **signature** 字段中，添加其 **certificate** 字段并向 GK1 传送 **ARQ** 消息。根据 **ARQ** 消息的选择的 **ClearToken** 字段以及未指给代理服务器的由 EP1 所计算的签名也在 **ARQ** 消息中原封不动地向 GK1 传送。

一旦接收 **ARQ** 消息，GK1 就将核实该签名，在适当修正 **toBeSigned** 中的 **ClearToken** 字段之后，计算新的签名，将其插入到 **certificate** 字段中，并向 EP2 传送 **Setup** 消息。来自 EP1 的端到端签名信息原封不动地包含在 **Setup** 消息中。

15.3 H.225.0消息认证、完整性和不可否认

H.225.0 消息规程与 RAS 消息的规程相同。区别仅在于在 **tokenOID** 被设置为“B”时，必须对每个 H.225.0 消息标识需要签署的字段集合。

15.4 H.245消息认证和完整性

考虑 EP1 希望向 EP2 传送 H.245 消息 — 即 **TerminalCapabilitySet** 消息 — 的情形。EP1 核查看 H.225.0 消息是否需要向 GK1 发送。若需要，则在那个 H.225.0 消息内隧道传送该 H.245 消息。H.225.0 消息内字段设置与早先对 H.225.0 消息传输所描述的字段设置相同。由于 H.245 消息被隧道传送，因此 **h323-UserInformation** 消息中 **h323-uu-pdu** 如下设置其字段：

- **h323-message-body** 字段设置为即将传输的 H.225.0 消息类型。
- **h245Tunnelling** 设置为 TRUE。
- **h245Control** 包含 H.245 PDU 八比特组串。

然而，若无任何 H.225.0 消息传输将发生，则在特定的 H.225.0 **facility** 消息内隧道传送 H.245 消息。**h323-UserInformation** 消息中 **h323-uu-pdu** 具有如下的字段设置：

- **h323-message-body** 字段设置为包含以下字段的 **facility**：
  - — **reason** 设置为 **undefinedReason**；
  - — **token** 和 **CryptoToken** 设置成如对任何 H.225.0 消息那样。
- **h245Tunnelling** 设置为 TRUE。
- **h245Control** 包含 H.245 PDU 八比特组串。

然后从 EP1 向代理服务器传输 **facility** 消息。

在任一种情况下（无论是 H.225.0 消息传输将发生还是使用特定的 H.225.0 **facility** 消息），一旦接收该消息代理服务器就将核实指定给它的签名（在此情况下，通过 **tokenOID**“A”描绘）。然后，若代理服务器—GK1 分段路径 H.225.0 消息传输将发生，则 H.245 消息在该消息内隧道传送；否则，在特定的 H.225.0 **facility** 消息内隧道传送。在任何 H.225.0 消息传输的情形中，在其从代理服务器向 GK1 传输之前计算该 H.225.0 消息的新的签名。从 EP1 向代理服务器发送的以及未指定给该代理服务器的签名部分原封不动的通过代理服务器向 GK1 传送。

本节提供签名安全概要如何以及通过那些手段保护多样化的 H.323 信令消息的概括一览。

16 H.235第1版的兼容性

尽管据了解这些安全概要伴随 H.235 第 2 版[ITU-T H.235 建议书 v2]而开发，但稍作改动将该安全概要适用于 H.235 第 1 版[ITU-T H.235 建议书 v1]也是可能的。接收者能够通过估计安全概要对象标识符来检测发送者的 H.235 协议版本的存在（见第 20 节）。

H.235 第 1 版[ITU-T H.235 建议书 v1]实施：

- 在 **ClearToken** 中不设置或估计 **sendersID**。

17 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 和 II，必须包括 **CryptoToken**。当此类消息单播发送时，该消息也必须包括 **CryptoToken**。

18 安全信令消息一览

18.1 H.225.0 RAS

H.225.0 RAS 消息	H.235 信令字段	仅认证	认证 和完整性	不可否认
任意	CryptoToken	规程 II/III	规程 II/III	规程 II/III

注 — 对于单播消息，规程 II 或 III 必须与所用 **CryptoToken** 中的与安全性字段一起采用。

18.2 H.225.0呼叫信令

H.225.0 呼叫信令消息	H.235 信令字段	仅认证	认证和完整性	不可否认
Alerting-UUIE, CallProceeding-UUIE, Connect-UUIE, Setup-UUIE, Facility-UUIE, Progress-UUIE, Information-UUIE, ReleaseComplete-UUIE, Status-UUIE, StatusInquiry-UUIE, SetupAcknowledge-UUIE, Notify-UUIE	CryptoToken	规程 II/III	规程 II/III	规程 II/III

19 sendersID和generalID用法

ClearToken 掌握 **sendersID** 和 **generalID** 字段。当标识信息生效时，对于网守启动的消息，该 **sendersID** 必须被设置为网守标识符（GKID），而对于端点启动的消息，该 **sendersID** 必须被设置为端点标识符（EPID）。当标识信息生效时，对于端点启动的消息，该 **generalID** 必须被设置为 GKID，而对于网守启动的消息，该 **generalID** 必须被设置为 EPID。当标识信息未生效或广播/组播涵义不明确的情形时，该字段可被丢弃或将包含空字符串。表 2 概括此种情况。

表 2/H.235.2－sendersID和GeneralID的使用

消　息	sendersID	generalID
单播 **GRQ**	若生效，为 **EPID**，否则 **NULL**	**GKID**
组播 **GRQ**	若生效，为 **EPID**，否则 **NULL**	
GCF，GRJ	**GKID**	若生效，为 **EPID**，否则 **NULL**
初始化 **RRQ**		**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ， UCF， URJ， BRQ， BCF， BRJ， DRQ， DCF， DRJ， NSM， RIP，SCI，SCR，XRS（EP 到 GK）	**EPID**	**GKID**
URQ， UCF， URJ， BRQ， BCF， BRJ， DRQ， DCF， DRJ， NSM， RIP，SCI，SCR，XRS（GK 到 EP）	**GKID**	**EPID**
ARQ，IRQ，RAI	**EPID**	**GKID**
ACF，ARJ，BCF，LCF，LRJ，IRR，IRQ， RAC， LCF， LRJ， IACK， INAK	**GKID**	**EPID**

表 2/H.235.2－sendersID和GeneralID的使用

消　息	sendersID	generalID
消　息	sendersID	generalID
单播 **LRQ**（EP 到 GK）	**EPID**	**GKID**
单播 **LRQ**（GK 到 GK）	**GKID**	**GKID**
组播 **LRQ**	**EPID**	
注 — GKID 表示网守标识符，EPID 表示端点标识符。空格指示丢弃的或空的标识串。		

20　对象标识符一览

表 3 列出所有引用的 OID（也见[OIW]和[WEBOID]）。包括用于 H.235v1 和 H.235v2 的对象标识符。

表 3/H.235.2－对象标识符

对象标识符参考符	对象标识符值	描　述
“A”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	在 CryptoToken-tokenOID 的规程 II 中使用，指示签名包括 H.225.0 RAS 消息的**所有**字段（认证和完整性）。
“B”	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 2}	在 CryptoToken-tokenOID 的规程 II 中使用，指示签名包括仅认证而无完整性终端的 RAS/ H.225.0 消息（ClearToken）的字段的**子集**。 在 CryptoToken-tokenOID 的 H.235.1 的规程 IA 中使用，指示散列包括仅认证而无完整性终端的 RAS/H.225.0 消息（ClearToken）的字段的**子集**。
“P”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 4} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 4}	在规程 II 或 III 中使用，指示 **certificate** 携载 URL。
“R”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 3} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 3}	在 CryptoToken-tokenOID 的规程 II 中使用，指示端到端认证/完整性的 ClearToken 正在使用。
“S”	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 7} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 7}	在规程 II 中使用。此 tokenOID 指示消息认证、完整性和不可否认。

表 3/H.235.2－对象标识符

对象标识符参考符	对象标识符值	描　述
“V”	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}	在规程 II 中作为 algorithmOID 使用，指示使用 MD5 RSA 数字签名。
“W”	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	在规程 II 中作为 algorithmOID 使用，指示使用 SHA1 RSA 数字签名。

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