国 际 电 信 联 盟

ITU-T H.235.1

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：基线安全概要

ITU-T H.235.1 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.235.1 建议书

H.323 安全性：基线安全概要

摘　要

本建议书通过使用安全的基于口令的密码技术，使用 H.225.0 RAS 和呼叫信令消息的基于口令的 HMAC-SHA1-96 散列保护，提供 H.225.0 RAS 和呼叫信令、H.225.0 及隧道传送的 H.245 的认证和完整性保护。安全概要适用于 H.323 终端到网守、网守到网守、H.323 网关到网守，适用于在具有对称分配的密钥/密码的管理环境下的其他 H.323 实体。

在 H.235 子系列的较早版本中，该概要被包含在附件 D/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.235.1 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.235.1 建议书

H.323 安全性：基线安全概要

1 范围

本建议书通过使用安全的基于口令的密码技术，使用 H.225.0 RAS 和呼叫信令消息的基于口令的 HMAC-SHA1-96 散列保护，提供 H.225.0 RAS 和呼叫信令、H.225.0 及隧道传送的 H.245 的认证和完整性保护。安全概要适用于 H.323 终端到网守、网守到网守、H.323 网关到网守以及其他 H.323 实体。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

— ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*

— ITU-T Recommendation H.235 version 1 (1998), *Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals.*

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

— ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems.*

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

— ITU-T Recommendation H.235.4 (2005), *H.323 security: Direct and selective routed call security.*

— 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 version 10 (2003), *Control protocol for multimedia communication.*

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

— ITU-T Recommendation H.323 Annex F (1999), *Simple endpoint types.*

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

2.2 资料性参考文献

[FIPSPUB180-2] 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.

[OIW] Stable Implementation – Agreements for Open Systems Interconnection Protocols: Part 12 – OS Security; Output from the December 1994 Open Systems Environment Implementors' Workshop (OIW); http://nemo.ncsl.nist.gov/oiw/agreements/stable/OSI/12s_9412.txt.

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

[WEBOIDs] http://www.alvestrand.no/objectid/top.html.

3 术语和定义

出于本建议书的目的，第 3 节/H.323、第 3 节/H.225.0 和第 3 节/H.245 中给出的定义与本节中给出的定义适用。本建议书中使用的一些术语也在 ITU-T X.800 建议书| ISO/IEC 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。

为提供安全性业务，本建议书使用以下术语。

3.1 authentication and integrity 认证和完整性：该术语是支持消息完整性并连带用户认证一起的基线概要的组合安全性业务部分。用户能够在正确应用共享密钥时进行认证。这两种安全性业务由同样的安全性机制提供。

3.2 authentication-only 仅认证：该安全性业务由基线安全概要作为仅支持所选区域的认证的一个选择提供，但不提供完全的消息完整性。仅认证的安全概要适用于穿越 NAT/防火墙设备的信令信息。用户可以通过直接应用一个共享的秘密密钥程序确保认证。

当使用对称密钥技术时，该安全性业务认证/完整性仅在逐段转接的基础上采用。

4 符号和缩写

本建议书采用下列缩写：

ASN.1 抽象句法记法 1

EP 端点

EPID 端点标识符

GK	网守
GKID	网守标识符
GRQ	网守请求
HMAC	散列消息认证码
ICV	完整性校验值
ITU	国际电信联盟
LRQ	定位请求
MAC	消息认证码
NAT	网络地址解析
OID	对象标识符
RAS	注册、认可和状态
RTP	实时协议
SHA	安全散列算法
TCP	传输控制协议
UTC	协调世界时
VoIP	网际协议上的话音

5 惯例

本建议书中使用下列惯例：

— “须（Shall）”表明是强制性要求。

— “应（Should）”表明是推荐采取的非强制性措施。

— “可（May）”表明是非强制性措施，但并未建议采取这种措施。

本建议书定义 **baseline security profile（基线安全概要）**。基线安全概要通过简单手段使用基于安全口令的密码技术提供基本的安全性。基线安全概要可与诸如 H.235.3、H.235.4、H.235.5、H.235.6 和 H.235.7 之类的安全概要一起使用。

本建议书使用在 H.323 信令消息上提供认证/完整性安全性业务的 H.235 字段。不同的对象标识符（见第 15 节）确定实际选择哪种安全性业务以及正在使用哪种本建议书的协议版本。规程 I 指定如何通过某种安全性机制诸如对称（加密散列）技术来实施安全性业务。正文中通过符号参考符（例如“A”）引用对象标识符，也见第 5 节/H.235.0。

虽然消息完整性业务也始终提供消息认证，但反过来却不一定正确。事实上，组合的认证和完整性业务利用同样的密钥资料而未导致安全性弱点。

更进一步，所有逐段转接的安全性信息被放入 **CryptoHashedToken** 单元中。该信息在每个分段转接中重新计算。

出于认证和完整性的目的，本建议书采用某些对称加密技术。当应用对称技术时，该文本使用术语口令和共享秘密。

一般而言，口令、对话密钥及共享秘密的共同点是可以在两个（或更多）实体之间以对称密码的方式使用。口令和对话密钥/共享秘密之间的区别在于该密钥如何实际使用，例如认证与授权的口令、加密的对话密钥。当共享秘密实际上不涉及任何特定的应用时，术语共享秘密有几分中性。

当该术语可由用户输入时，**password（口令）**（也可视为共享秘密）可供 RAS 和 H.225.0 的认证/完整性使用。口令通常具备长期的使用期限；口令事先已知，并且可以规定作为整个用户预订处理的一部分。为在协议中更为方便地处理起见，一些算法（例如传送口令通过散列算法）可以对口令进行变换以便导致定长口令。

很明显，使用口令务必谨慎设置。口令只能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，使用本建议书的安全概要时，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）

这一 H.235 **ClearToken** 提供掌握 32 比特整数的被称为 **random** 的字段。该字段蕴涵以下意义：**random** 实际上是从任意值起始的单调递增数，并伴随每个出局消息而增加。在几个消息相继不久发布而仍传送同一时间标记的情况下，作为附加的“随机化”值 **random** 字段供输入到加密的散列函数中使用。当 UTC 时钟不能提供充分的时钟分辨率时，该情形也能出现。本质上，生成的散列值或完整性检测值由于变化的 **random** 值而显得不同。这可以抵御重放攻击。为使设施简便易行，在此真实的 **random** 序列上推荐选择递增计数器。在由当地时间窗定义的持续时间周期内，接收者可以保留接收的 **timeStamp/random** 对。当同样的 **timestamp/random** 对发生两次时，可以标识受到重放攻击。

注 — 该时间窗补偿同步时间变化和网络传输延迟。

该概要规定“在 **ClearToken** 中设置 **generalID** 为该接收者的标识符”。这实际上意味着对于发送到网守的 RAS 消息来说，这是 GK 标识符；对于发送到端点的 RAS 消息来说，这是端点标识符；对于发送到网守的 H.225.0 呼叫信令消息来说，这是 GK 标识符；对于发送到端点定义的 H.225.0 呼叫信令消息来说，这是端点标识符，也见第 14 节。

这一 **sendersID** 必须设置成发送者的标识字符串。这实际上意味着对于发送到网守的 RAS 消息来说，这是端点标识符；对于发送到端点的 RAS 消息来说，这是网守标识符；对于发送到网守的 H.225.0 呼叫信令消息来说，这是 GK 标识符；对于发送到端点的 H.225.0 呼叫信令消息来说，这是端点标识符，也见第 14 节。

本建议书可应用跨越整个消息的消息完整性保护。对于 H.225.0 RAS 来说，完整性保护包括整个 RAS 消息；对于呼叫信令来说，这包括整个 H.225.0 呼叫信令消息，包括 Q.931 头。

本建议书使用众所周知的安全性术语如密钥、密钥管理和 SET，它们在其他语境中具有其他不同的含义（例如，按键键盘、Q.931/Q.932 特性的密钥管理以及安全电子交易协议）。

6 概述

本建议书通过使用安全的基于口令的密码技术，使用 H.225.0 RAS 和呼叫信令消息的基于口令的 HMAC-SHA1-96 散列保护，提供 H.225.0 RAS 和呼叫信令、H.225.0 及隧道传送的 H.245 的认证和完整性保护。安全概要适用于 H.323 终端到网守、网守到网守、H.323 网关到网守，适用于在具有对称分配的密钥/密码的管理环境下的其他 H.323 实体。

6.1 安全性特征概括

由这些概要所提供的特征包括：

— 对于 RAS，H.225.0 和隧道传送 H.245 消息：

- 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 — 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。

- 信令消息自身的完整性包括到达实体的消息的核心部分（字段）不考虑该消息所历经的应用等级分段转接个数。

- 应用等级逐段转接的信令消息认证、完整性对整个消息提供这些安全性业务。

通过以合适方式提供上述安全性业务可以对抗若干种攻击，它们包括：

- 拒绝服务攻击：快速检测的密码散列值可以防止此类攻击。
- 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。
- 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。

简单安全概要的其他突出的部分包括：

- 使用基于 IMTC/ETSI/IETF 资料的稳健的、众所周知的和广泛采用的算法。
- 根据商业模型的安全性需求按阶段配置能力。
- 适用于各种不同的配置方案，诸如在闭合用户群内和可调节环境的和在多点会议中。

- 当提供某些穿越 NAT/防火墙的安全时，仅包含认证的安全概要应适用。

表 1 概括本建议书中由安全概要所规定的所有规程用于处理不同的安全性需求。任选的仅认证安全概要用斜纹阴影区示出 — 电子版中为蓝色填充区。

表 1/H.235.1－安全概要一览

安全性业务	呼叫功能			
	RAS	H.225.0	H.245（注）	RTP
认证	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	
仅认证	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	
不可否认				
完整性	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	口令 HMAC-SHA1-96	
机密性				
接入控制				
密钥管理	基于预订的口令分配			
注 — 在 H.225.0 快速连接内部隧道传送的 H.245 或嵌入的 H.245。				

对于认证，用户必须使用基于口令方案。由于基于口令方案的简单性和易于实现，强烈推荐该方案用于认证。H.225.0 RAS 和呼叫信令消息中的所有字段是消息完整性的推荐方法（也可使用口令方案）。

采用该安全概要的安全 H.323 实体使用同样的公共安全性机制与完整性一起实现认证。

接入控制手段未明确描述；它们可以在 H.235 信令字段内（ClearToken，CryptoToken）所传送的接收信息上局部实施。

就运行和管理而言，本建议书未描述基于预订的口令/密钥分配规程。此规程通过不属于本建议书范围的手段实施。

涉及的通信实体能够隐含地确定或基线安全概要或签名安全概要的用法，通过估算该消息中签署的安全性对象标识符（**tokenOID** 和 **algorithmOID**；也见第 15 节）。

6.2 基线安全概要的适用性

基线安全概要可在预订的口令/对称密钥能够被指派给安全的 H.323 实体（终端）和网络单元（GK，代理服务器）的场合环境中应用。如规程 I 所指定的，使用基于口令的 HMAC-SHA1-96 散列，它提供 H.225.0 RAS 和呼叫信令、H.225.0 和隧道传送的 H.245 的认证和完整性。使用 FastStart（GK 到 GK 或终端到终端）的 H.225.0 呼叫建立包括完整的采用 Diffie-Hellman 的密钥管理。

基线安全概要强制使用快速连接规程，建议使用 H.225.0 消息内隧道传送的 H.245。

6.3 H.323 需求

假定实施该基线安全概要的 H.323 实体支持以下 H.323 特性：

- 快速连接；
- GK 选路模型。

6.4 规程的概述

本子节描述在此概要中使用的以下规程。

规程 I 是根据两个实体（例如网守和 H.323 端点）之间的共享口令，基于简单对称密钥的信令消息认证机制。该规程提供 RAS、Q.931 和 H.245 消息的认证和完整性（见第 7 节）。

规程 IA 是根据两个实体（例如网守和 H.323 端点）之间的共享口令，基于简单对称密钥的信令消息仅认证机制。该规程仅提供认证，但不提供完全的消息完整性。仅认证选项在 H.323 消息穿越 NAT/防火墙的情况下适用。

依据安全性政策，认证同样可以是单方的或相互的采用相反方向的认证/完整性并由此提供更高的安全性。网守同样可以决定是否采用反方向的认证/完整性。

从安全端点或对等的网守所接收的 RAS 或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 **securityDenial** 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 信令指示使用规程 I 和基于对象标识符值的应用安全性机制（也见第 15 节）以及填充的消息字段。

该概要不使用 H.235 ICV 字段；确切地密码完整性检测值作为密码散列值来对待，并置入 **CryptoToken** 的散列字段中。

7 基于对称密钥的信令消息认证详情（规程 I）

采用规程 I 时必须遵从以下规程：

- 12 字节（96 比特）散列值与 HMAC-SHA1-96 算法一起供生成认证码使用。若密钥从口令中生成，则必须使用 8.2.4/H.235.0 中描述的机制从口令中计算密钥。

  注 1 — 当该密钥从用户输入的口令中衍生时，应留心确保足够充分的随机性。例如推荐使用真正随机加密的密钥或确信随机口令足够长。

- 每个 RAS/H.225.0 消息中 **CryptoH323Token** 必须包含下列字段：

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

- **tokenOID** 设置为“A”指示认证/完整性计算包括 RAS/H.225.0 消息中的所有字段。
- **hashedVals** 包含与下列字段一起使用的 **ClearToken** 字段：
  - — **tokenOID** 设置为“T”指示 **ClearToken** 正在供消息认证/完整性和重放保护所使用，也任选地供 8.5/H.235.6 中描述的 Diffie-Hellman 密钥管理使用。替代地，其他具有 OID 的 ClearToken 可替代基线 ClearToken 使用。
  - — **timeStamp** 包含时间标记。
  - — **random** 包含单调递增的序列号。该数允许使两个消息具有惟一相同的时间标记（时钟分辨率之内）。
  - — **generalID** 包含接收者的标识符（仅单播消息的情形中）。
  - — **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 2 — 当使用无话音加密安全概要的基线安全概要时，无任何 Diffie-Hellman 参数需要发送，**dhkey** 应不存在；为了简化，可以设置为{'0'B,'0'B,'0'B}来替代 **halfkey**、**modsize** 和 **generator** 字段。

— **token** 包含具有以下字段的 **HASHED**：

- **algorithmOID** 设置成“U”指示使用 HMAC-SHA1-96。
- **params** 设置为 NULL。
- **hash** 包含使用 HMAC-SHA1-96 计算的认证码。该认证码可在以下字段上计算：
  - — 只要 **CryptoHashedToken** 中 **tokenOID** 设置为“A”（指示认证和完整性），就应包含该消息的所有 H.225.0 RAS 和呼叫信令。

tokenOID“A”用于保护包括所有 H.245 消息内容的隧道传送 H323-UU-PDU；依照 7.3 中所描述的规程，该散列计算将在具有全部字段的整个 **H.225.0** 呼叫信令消息上实施。

- 在终止分段路径的每个信道端点（情况可能是 EP1-GK1、GK1-GK2、GK2-EP2、EP1-GK2、GK1-EP2 或 EP1-EP2）核实认证码，并在该后续分段路径外发送该消息之前重新计算。

注 3 — 认证码基于每个消息计算。

注 4 — 必须使用 SHA1 标准 [ISO/IEC 10118-3]内的填充方法。

注 5 — 当正在使用组合的认证和完整性时，认证码在整个消息上计算。

注 6 — 为了防止可能的重放攻击，强烈建议实施必须确保在单调递增序列编号周转结束之前（或循环完成之前）更改口令（密钥）。

注 7 — 接收者能够通过估算散列的 **EncodedGeneralToken** 内的 **tokenOID** 来检测规程 I 的使用（检测“A”的存在）。

7.1 基于口令的散列计算

受到保护的认证/完整性消息的发送端和接收端双方在所有的 ASN.1 编码的消息字段上计算加了密钥的散列（使用 OID“A”）。对于仅认证概要，发送端和接收端在所有的 ASN.1 编码的 ClearToken 上计算加了密钥的散列（使用 OID“B”）。

7.2 HMAC-SHA1-96

HMAC-SHA1-96 为 160 比特 SHA1 计算的截短的 96 比特密码散列值。该散列值网络字节序表示的最左 96 比特必须作为该结果使用。RFC 2104 描述具有设置成共享秘密（= SHA1-散列口令）的密钥 *K* 以及设置成消息缓存的正文的规程。

7.3 认证和完整性的计算和验证

对于认证与消息完整性（在 OID“A”的情形中采用），其规程如下。

消息的发送者应如下计算散列值：

1） 将散列值设置成具有长度为 96 比特的特定缺省模式。这里精确的比特模式并不重要，重要的是好的选择是在剩余消息中不出现的惟一比特样式。

2） ASN.1— 编码整个消息，对于 RAS，这必须包括整个 H.225.0 RAS 消息；对于呼叫信令，这必须包括整个 H.225.0 呼叫信令消息。

3） 在编码消息中定位该缺省模式；采用 96 个全零比特重写所出现的比特模式。

注 1 — 在缺省模式在该消息中多次发生的极少数情形下，这可以包含某些逐次逼近的步骤。

4） 在 ASN.1 编码消息上使用 HMAC-SHA1-96 计算该加密散列值（见第 7.2 节）。

5） 在编码消息中采用计算的散列值替代缺省模式。

接收者接收消息后处理如下：

1） ASN.1 — 译码该消息。

2） 抽取接收的散列值并在局部变量 RV 中保存。

3） 在接收的编码消息中搜索并定位该散列值 RV。

注 2 — 在整个消息中散列值子字符串可能发生若干次的极少数情况下，步骤 3-6 必须伴随不同的起始搜索位置连续重复。

4） 在编码消息中采用 96 个全零重写该比特模式；

5） 在编码消息上使用 HMAC-SHA1-96 计算该加密散列值（见第 7.2 节）；

6） 将 RV 与计算的散列值相比较。仅当两个散列值相等时该消息才被认为未讹误；在此情形，认证是成功的并且该规程终止；

7） 否则重复步骤 3-7 通过恢复原先位置上的 RV 并搜寻另一次的匹配。若没有任何一次匹配生成可与准确的散列值相比，则该认证失败并且运行期间该消息已（有意或无意的）被变更。

8 仅认证（规程 IA）

终端可选择实施仅认证（用 OID“B”，见第 20 节/H.235.2）。在这一情况下，就在 RAS/H.225.0 消息的子集（**CryptoToken** 内的 **ClearToken**）上计算认证码。仅认证对于在 H.323 有效载荷内改变 IP 地址/端口穿越 NAT/防火墙可能有用。

由于认证仅跨越消息的非常有限的端口，仅认证不提供规程 I 所表征的消息完整性。因此，仅认证提供较低的安全性。

对于仅认证，必须在保护消息中使用下列字段：

- 每个 RAS/H.225.0 消息中的 **CryptoH323Token** 字段必须包含下列字段：
  - — 包含 **CryptoToken** 的 **nestedCryptoToken**，其自身包含的 **cryptoHashedToken** 包含下列字段：
    - **tokenOID** 设置为：
      - — “B”（见第 20 节/H.235.2）指示仅认证计算包括所有 **ClearToken** 中的所有字段。
    - **hashedVals** 包含与下列字段一起使用的 **ClearToken** 字段：
      - — **tokenOID** 设置为：
        - “T”（作为基线 ClearToken 例子用于 ClearToken 内容的余数）或用于其他目的的适当的 OID。
      - — **timeStamp** 包含时间标记；
      - — **random** 包含单调递增的序列数。该数允许使两个消息具有惟一相同的时间标记（时钟分辨率之内）；
      - — **generalID** 包含接收者的标识符（仅单播消息的情形中）；
      - — **sendersID** 包含发送者的标识符；
      - — **dhkey** 在 **Setup** 到 **Connect** 期间，如 ITU-T H.235.0 建议书中所指定的用于传送该 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 — 当使用无话音加密安全概要的基线安全概要时无任何 Diffie-Hellman 参数需要发送；为了简化，可以设置为{'0'B，'0'B，'0'B}的二进制表示来替代 **halfkey**、**modsize** 和 **generator** 字段。
  - — **token** 包含具有以下字段的 **HASHED**：
    - **algorithmOID** 设置为“U”指示使用 HMAC-SHA1-96；
    - **params** 设置为 NULL；
    - **hash** 包含使用 HMAC-SHA1-96 计算的认证码。该认证码可在以下字段上计算：
      - — 只要 **CryptoHashedToken** 中的 **tokenOID** 设置为“B”（指示仅认证），就应当包含 **ClearToken** 的所有字段。
- 在终止分段路径的每个信道端点（情况可能是 EP1-GK1、GK1-GK2、GK2-EP2、EP1-GK2、GK1-EP2 或 EP1-EP2）核实认证码，并在该后续分段路径外发送该消息之前重新计算。

注 2 — 认证码基于每个 **ClearToken** 计算。

注 3 — 必须使用 SHA1 标准 [ISO/IEC 10118-3]内的填充方法。

注 4 — 为了防止可能的重放攻击，强烈建议实施必须确保在单调递增序列编号周转结束之前（或循环完成之前）更改口令（密钥）。

注 5 — 接收者能够通过估算 **tokenOID** 内的 **OID**“B”来检测规程 IA 的使用。

认证码必须就在 **cryptoHashedToken** 的 **token** 的 **CryptoH323Token**（即 **ClearToken**）内的 **ClearToken** 上计算。用密码写的散列必须在 **ClearToken** 的 ASN.1 编码比特串上计算。

H.235 第 1 版和第 2 版端点可使用仅认证，在这一情况下，对于“B”，必须使用对应的 OID。H.235 第 1 版端点必须坚持第 11 节中描述的规程。

9 规程 I 的用法说明

在网守和直接选路的 H.225.0 信道不同组合所构成的通信信道端点上，图 1 到图 3 解释共享密钥的存在。不考虑呼叫模型，为了向 RAS 消息提供认证和完整性，共享密钥自始至终在 EP 和其 GK 之间存在。在相同的两个节点之间，当 RAS 信道和 H.225.0 信道终止时，可以使用相同的密钥为 RAS 和 H.225.0 消息提供认证和完整性。

图 1 显示最易调节的方案，其中两个端点在采用 GK 选路模型的分区内。所有涉及的 GK 均互相共享密钥。为了使之可调节，推荐图 1 中解释的方案。

注 1 — 该方案不能提供真正的端点之间的端到端安全性；所有的安全性取决于可信的中间网守。

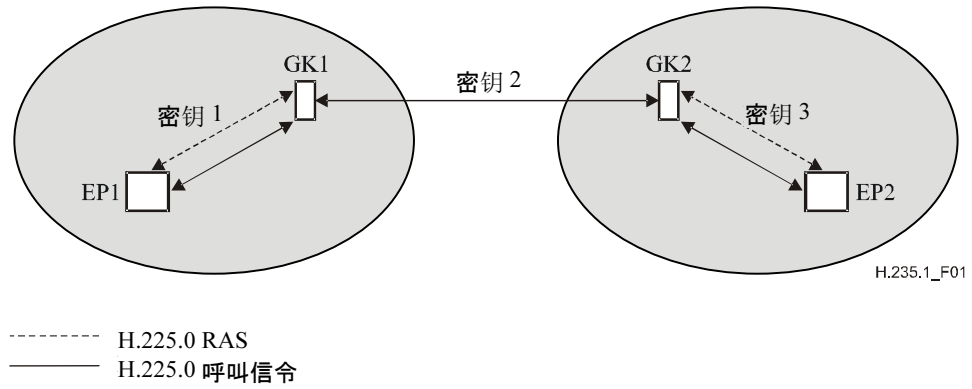
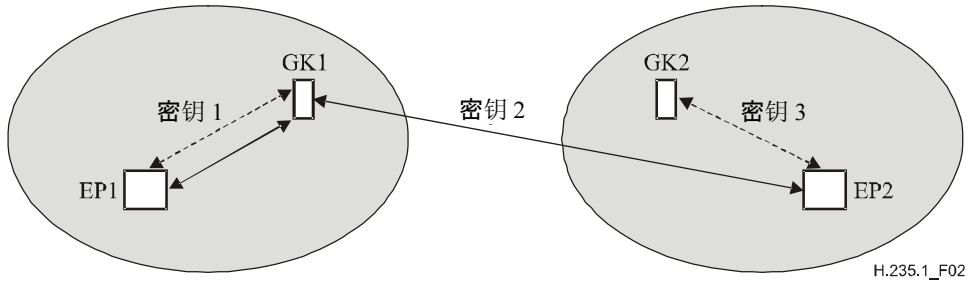


图 1/H.235.1－在GK选路分区内具有两个EP的GK-GK方案的规程I用法说明

图 2 显示一个混合方案，其中一个 EP 在采用 GK 选路模型的分区内，而另一个 EP 在采用直接选路模型的分区内。该方案可能在 EP2 和 GK1 的数量受限的闭合环境中出现。

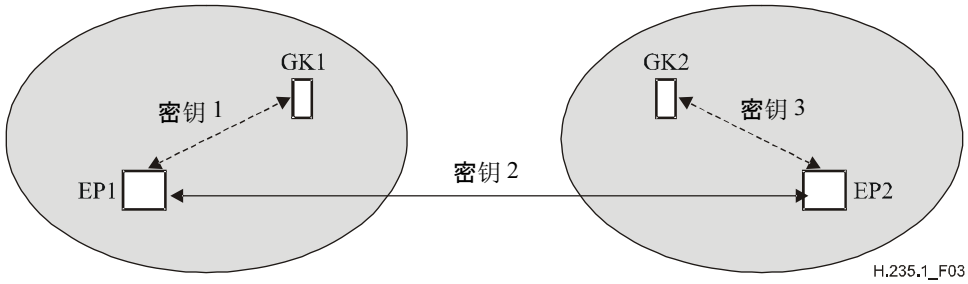


--------- H.225.0 RAS
———— H.225.0 呼叫信令

图 2/H.235.1－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

图 3 显示两个 EP 均在采用直接选路 GK 模型分区内的方案。在涉及多个 EP 时，该方案不是真正可调节的。原则上，作为替代，推荐使用 H.235.2 的规程 II/III。对于该特定方案以及规程 I、II 或 III 附加的安全性测量而言例如，在 H.323 网关依靠具有接入令牌的呼叫授权防止呼叫欺诈和误用，它们虽然未在本建议书中描述但同样是必要的；这一点有待进一步研究。

注 2 — 该方案提供端点之间真正的端到端安全性而无需依赖可信的中间节点。



--------- H.225.0 RAS
———— H.225.0 呼叫信令

图3/H.235.1－两个EP均在使用直接选路GK的分区内的方案的规程I用法说明

考虑到图 1 中的情形，其中 3 个口令分别在 EP1-GK1、GK1-GK2 以及 GK2-EP2 之间两两共享。根据 8.2.4/H.235.0 中描述的规程，从这些口令生成 3 个 20 字节密钥 *Key1*、*Key2* 和 *Key3*。为了更大的安全性，推荐使三个随机口令/密钥之间互不相关。

以下说明 RAS、H.225.0 和 H.245 消息认证和完整性的规程详情。描述实例解释 GK 选路模型中的特定参数；不同方案中其他有用和有效的对象标识符组合同样也是可能的。

注 3 — GK 之间（图 1）、GK 与远程 EP 之间（图 2）或 EP 之间（图 3）共享对称密钥（口令）的数量太多的情形中，上图中所示的各种方案均不能很好地调节。

9.1 RAS消息认证和完整性

考虑 EP1 希望向 GK1 发送 RAS 消息 — 即 **ARQ** 消息 — 的情形。EP1 生成时间标记和序列号，并与 **generalID** 字段中的 GK1 的化名和 **sendersID** 字段中的 EP 的 ID 一起分别包含在 **timeStamp** 和 **random** 字段中。这些字段在 **ARQ** 消息的 **cryptoH323Token** 的 **CryptoToken** 字段的 **cryptoHashedToken** 中存在的 **hashedVals** 的 **ClearToken** 字段中出现。

cryptoHashedToken 内 **tokenOID** 设置为“A”指示 **ARQ** 消息中的所有字段被散列。在 **cryptoHashedToken** 中 **token** 内 **HASHED** 将 **algorithmOID** 设置为“U”指示使用 HMAC-SHA1-96 而且 **params** 设置为空。然后 EP1 根据 HMAC-SHA1-96 使用 20 字节密钥 *Key1* 计算认证码。认证码在整个 RAS 消息上计算。

在 **ARQ** 消息的 **cryptoH323Token** 中存在的 **CryptoToken** 的 **cryptoHashedToken** 字段的 **token** 字段中的 **hash** 内 EP1 包含计算的认证码。然后向 GK1 发送 **ARQ** 消息。

一旦接收 **ARQ** 消息，GK1 根据以下几种准则核实认证码，这些准则包括：

- **timeStamp** 的存活性，**random** 的惟一性；
- **generalID** 与其自身标识符的一致性；
- **ARQ** 消息中认证码与由 GK1 计算的认证码之间的匹配。

9.2 H.225.0消息认证和完整性

考虑 EP1 希望向 EP2 发送 H.225.0 消息 — 即 **Setup** 消息 — 的情形。EP1 生成时间标记和序列号，并与 **generalID** 字段中的 GK1 的化名和 **sendersID** 字段中 EP 的 ID 一起分别包含在 **timeStamp** 和 **random** 字段中，EP1 也计算 Diffie-Hellman 半密钥并将 Diffie-Hellman 参数 **halfkey**、**modsize** 和 **generator** 包含在 **ClearToken** 的 **dhkey** 密钥字段中。这些字段在 **Setup** 消息的 **cryptoH323Token** 的 **CryptoToken** 字段的 **cryptoHashedToken** 中存在的 **hashedVals** 的 **ClearToken** 字段中出现。

cryptoHashedToken 内 **tokenOID** 设置为“A”指示 H.225.0 呼叫信令消息中的所有字段被散列。在 **cryptoHashedToken** 中的 **token** 内 **HASHED** 将 **algorithmOID** 设置为“U”指示使用 HMAC-SHA1-96 而且将 **params** 设置为空。然后 EP1 根据 HMAC-SHA1 算法使用 12 比特密钥 *Key1* 计算认证码。认证码依照选择的散列方法（A）考虑在整个 H.225.0 消息上计算。

在 **Setup** 消息的 **cryptoH323Token** 中存在的 **CryptoToken** 的 **cryptoHashedToken** 字段的 **token** 字段中的 **hash** 内 EP1 包含计算的认证码。然后向 GK1 发送 **Setup** 消息。

一旦接收 **Setup** 消息，GK1 根据以下几种准则核实认证码，这些准则包括：

- **timestamp** 的存活性，**random** 的惟一性。
- **generalID** 与其自身标识符的一致性。
- 核实 Diffie-Hellman 参数，例如，测试 1024 比特基集和生成码是否正确。测试 DH-参数是否安全是消耗时间的处理，因此仅当本地政策要求时才进行。
- **Setup** 消息中认证码与通过 GK1 计算的认证码之间的匹配。

若认证码成功核实，则如下向 GK2 转发该认证码之前 GK1 计算新的认证码，并将其插入（代替）到 **Setup** 消息中。GK1 使用与 GK1-GK2 分段路径有关的值来代替 **hashedVals** 的 **ClearToken** 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 GK1-GK2 分段路径的下一个单调递增的序列编号，**generalID** 字段包含 GK2 的化名，而 **sendersID** 字段包含 GK1 的化名。GK1 将在 **ClearToken** 的 **dhkey** 字段中包括接收的 Diffie-Hellman 参数。

然后 GK1 使用密钥 *Key2* 和 HMAC-SHA1-96 算法（**algorithmOID**=“U”）计算该 **Setup** 消息的新的认证码，将它插入到 **token** 内的 **hash** 中并向 GK2 端传送该 **Setup** 消息。

一旦接收该 **Setup** 消息，GK2 就核实认证码，适当修改 **hashedVals** 中的 **ClearToken** 字段之后，计算新的认证码，插入到 **hash** 字段中并向 EP2 端传送 **Setup** 消息。

9.3 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。

EP1 生成 H.225.0 消息的 **CryptoToken**，设置 **tokenOID** 为“A”指示认证和完整性，并在 **hashedVals** 的 **ClearToken** 中设置 **timeStamp**、**random**、**sendersID**、**generalID** 字段以及 **tokenOID** 为“T”，设置 **algorithmOID** 为“U”指示使用 HMAC-SHA1-96 以及设置 **hash** 为在 H.225.0 呼叫信令消息的所有字段上所计算的散列认证码。

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** 消息中隧道传送 H.245 消息。**h323-UserInformation** 消息中 **h323-uu-pdu** 具有如下的字段设置：

- **h323-message-body** 字段设置成 **facility** 包含下列字段：
  - — **reason** 设置成 **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。

如上所述，EP1 生成作为 H.225.0 **facility** 消息一部分的 **CryptoToken**。然后由 EP1 向 GK1 传输 **facility** 消息。

在任一种情况中（无论 H.225.0 消息传输将发生或使用特别的 H.225.0 **facility** 消息），GK1 在接收的该消息上核实认证码。然后，若 H.225.0 消息传输对于 GK1-GK2 分段路径将要发生，则该 H.245 消息在那个消息中隧道传送；否则，它在特定的 H.225.0 **facility** 消息中隧道传送。作为任何 H.225.0 消息传输的情形，在 H.225.0 消息从 GK1 向 GK2 传输之前应计算该 H.225.0 消息的新的认证码。该处理在 GK2-EP2 分段路径上重复。

9.4 直接选路方案

如本建议书所概述的安全 H.323 实体不仅可以在 GK 选路环境中通信，而且也可以配置直接选路模型。该直接选路模型要求在简单 GK 选路环境中不必要的那些附加的安全性测量（接入令牌）。因此如何保护直接选路模型在 ITU-T H.235.4 建议书中描述。

10 后端业务支持

安全 H.323 实体可以依据 I.1.6/H.235.0 中描述的规程使用后端业务。

11 H.235 第 1 版的兼容性

尽管据了解这些安全概要伴随 ITU-T H.235 建议书第 2 版[ITU-T H.235 建议书（2000）]而开发，但稍作改动将该安全概要适用于 ITU-T H.235 建议书第 1 版[ITU-T H.235 建议书（1998）]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 15 节）。

ITU-T H.235 建议书第 1 版[ITU-T H.235 建议书（1998）]实施：

- 在 **ClearToken** 中不设置或估计 **sendersID**。
- 不能使用第 10 节中那样的后端业务。

12 组播特性

依据规程 I，H.225.0 组播消息诸如 GRQ 或 LRQ 不得包含 CryptoToken。当此类消息单播发送时，该消息必须包含 CryptoToken。

13 安全信令消息一览

本节提供本建议书如何以及通过哪些手段来保护多种的 H.323 信令消息的概括。

13.1 H.225.0 RAS

H.225.0 RAS消息	H.235信令字段	认证和完整性
任意	CryptoToken	规程 I

13.2 H.225.0 呼叫信令

H.225.0呼叫信令消息	H.235信令字段	认证和完整性
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 I

13.3 H.245呼叫控制

发往和来自安全 H.323 实体的 H.245 消息必须作为安全快速连接的一部分被级联或者使用安全的 H.225.0 **facility-UUIE** 隧道传送。

14 sendersID与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.235.1－所使用的对象标识符

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 **RRQ**	若生效，为 **EPID**，否则 **NULL**	**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**
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。空格指示丢弃或空的标识串。		

15 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 [H.235v1]和 H.235v2 [H.235v2]的对象标识符。

表 3/H.235.1－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
“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 I 中使用，指示散列包括 RAS/H.225.0 消息中的所有字段（认证和完整性）。
“E”	{itu-t（0）recommendation（0）h（8）235 version（0）3 9} {itu-t（0）recommendation（0）h（8）235 version（0）2 9}	对于在接收者一侧的确认，携载 sendersID 端到端 ClearToken。
“T”	{itu-t（0）recommendation（0）h（8）235 version（0）2 5} {itu-t（0）recommendation（0）h（8）235 version（0）1 5}	在消息认证的基线 ClearToken 的规程 I 和 IA 中使用，重放保护，任选地也用于 Diffie-Hellman 密钥管理，如 8.5/H235.6 中所描述的。
“U”	{itu-t（0）recommendation（0）h（8）235 version（0）2 6} {itu-t（0）recommendation（0）h（8）235 version（0）1 6}	在算法 OID 的规程 I 中使用，指示使用 HMAC-SHA1-96。

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