国　　际　　电　　信　　联　　盟

电信和信息技术安全

关于电信安全的若干议题综述及相关ITU-T建议书应用简介

2003年12月

ITU-T 电信标准化部门

ITU 国际电信联盟

电信和信息技术安全

关于电信安全的若干议题综述

及相关ITU-T建议书应用简介

致 谢

很多作者为编写本手册做出了贡献,他们或者参与制定了相关 ITU-T 建议书，或者参与了 ITU-T 研究组的会议、讲习班和研讨会。特别要归功于下列人员：Lakshmi Raman 女士贡献了第 6.4 节及第 2 章的部分文字，后一部分还经过了 Messrs Herb Bertine 和 Rao Vasireddy 审校；第 3 章威胁和风险的资料既来自 ITU-T 的工作，也来自[Shannon]的表述；第 5 章和第 6.5 节的文字基于[Wisekey] 的一般资料和 David Chadwick 教授的大力支持，尤其是对第 6.5.2 节 Salford 的 E 处方应用 (以及[Policy]资料)的描述；第 6.1 节关于 VoIP 和 ITU-T H.323 系统的文字来源于 [Packetizer]和[Euchner]，以及 Martin Euchner 先生的贡献；第 6.2 节文字来自于 ITU-T J.169，Eric Rosenfeld 先生在第 6.1.2 节对其还作了述评；第 6.3 节文字基于 ITU-T T.30 和 T.36 中的资料。还要感谢众多不知名的审评人员。附件 C 中的资料来自回复 ITU-T 第 17 工作组安全调查问卷的不同 ITU-T 研究组的众多专家，附件 B 基于 ITU-T 课题 10/17 专家尤其是 Sándor Mazgon 先生维护的安全相关建议书纲要。

目录

前 言

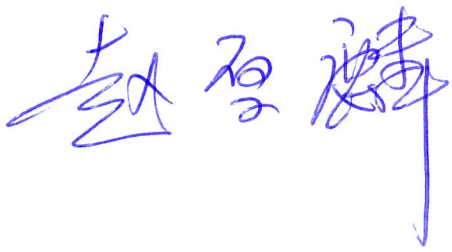
长期以来一直局限于银行、航空或军事应用等领域的数字安全的问题现在已逐渐变成人民群众每个人的事。

数字安全问题日渐受到重视的现象可能受到电子邮件传播病毒或黑客窃取信用卡信息等新闻标题的影响。但这种影响并非问题的全部答案。随着计算和联网已如水和电一样成为日常生活的重要组成部分，数字安全不仅被专家们议论，还越来越多地被政府、公司和消费者谈论。此外，如果我们的商务活动和个人生活的众多方面越来越依赖计算机和网络，毫无疑问，人们会要求这些系统应该安全运行。

同样，人们应该把安全作为一个深思熟虑的过程，应用于从系统设想和系统布署设计到制订系统的安装、运营及使用的政策和实际操作规程的全过程。在制定标准时，对安全的考虑必须始终是初始工作的一部分，而不应作为事后的补救措施 - 否则，系统的易受攻击的弱点就会由此产生。标准化委员会的角色就是认真听取那些市场及经验中已知的问题，尽可能地提供对它们的解决办法，颁布规范或指南，以帮助运用者和用户使各项通信系统和各种服务能够足够牢靠地运行和使用。

多年来，国际电信联盟的标准化部门 ITU-T 一直积极参与电信和信息技术安全研究。但是， 鉴于各种信息繁多，人们并不总是很容易弄清楚哪些已被研究，以及到哪里去找相关资料。本手册尝试将所有已知的信息综合在一起，以方便人们的检索。我向 ITU 电信标准化局的工程师们表示赞赏，他们在来自 ITU 成员的有关专家们的支持下完成了本手册的大部分章节，任务艰巨，成绩显著。本手册旨在为技术人员、中层管理人员以及负责制订和执行电信规则的相关人员提供一份指南，帮助他们实际运用安全功能。本手册通过几个应用实例，提供了对安全问题一些事项的解释，偏重强调 ITU-T 建议书是如何处理这些事项的。

我相信，本手册将成为关注安全事项人士的有用指南，我们欢迎读者对本手册提出意见和建议，以便改进我们今后的版本的编辑。



国际电信联盟
电信标准化局主任
赵厚麟
2003 年 12 月，日内瓦

概 要

通信产业适应日了越来越全球化的商务环境的需要，在几乎所有的产业部门促进了生产率的提高，并成为促进全球沟通的桥梁。这一通信基础设施如此高效主要归因于ITU-T 等标准化组织制定的标准。标准不仅保证了现有的网络高效而且为下一代网络打下了基础。但是，尽管标准在继续满足终端用户和产业的需要，随着开放界面和协议日益增长的使用、新角色的多元化、应用和平台的不断分化、未经充分测试的实现导致对网络恶意使用的机会不断增长。近年来，全球网络上都观察到安全侵害（诸如病毒、存储数据机密性被破坏）泛滥，经常造成巨大的损失效果。问题是，如何在支持开放的通信基础设施的同时不牺牲其上交换的信息。答案在于标准组织在各个通信基础设施领域中与安全威胁的斗争的努力。这种规定体现在从协议规范和应用的细节直到网络管理。本安全手册的目的在于突出并提供对 ITU-T – 有时与其他标准组织共同 — 制定的众多的建议书鸟瞰的视角，以保障通信基础设施及相关服务和应用的安全。

为涵盖安全问题的多个方面，必须建立一个框架体系以形成一个讨论这些概念用的统一的词汇表。

第 2 章总结了在 ITU-T 建议书 X.805 中定义的体系要素以及已被定义的涵盖网络应用端到端安全的 8 个尺度 – 保密、数据机密性、认证、完整性、不可抵赖性、访问控制、通信安全及可用性。这些通用原则用于指导和理解其他章节的具体问题。主要要素包括安全层、安全层面和用于任何层和层面结合的尺度。

第 3 章介绍了讨论安全的三个关键术语：脆弱性、威胁和风险，描述了三个术语不同的特性，并给出了一些例证。本章的关键是注意安全风险如何来自于脆弱性和威胁的结合。

第 4 章在前几章的基础上定义了基础要求以形成安全框架。战胜威胁实现安全的关键要素是制定认证、访问控制、数据加密等机制、算法及安全措施。第 5 章定义了公共密钥概念相关的机制和权限管理基础设施，这些机制和基础设施可用于很多不同的终端用户应用。

在这个框架、体系和机制之外，ITU-T 在其建议书中制定了几个系统和服务的安全规定。因此，本手册重要的焦点在于应用，如第 6 章所见。在这第一版中包括一组应用，包括 IP (H.323 和 IP 同轴通信系统)上的语音和多媒体应用、健康保护和传真。在布署体系以及如何制定协议满足安全需求方面对这些应用进行了描述。在提供应用信息的安全之外，还需要保障网络和网络服务管理的安全。针对网络管理方面的安全规定的标准示例也在第 6 章。

此外，此手册版本含有与安全及其他本文档涉及的话题相关的，从 ITU-T 相关建议书及其他来源例如 ITU-T SANCHO 数据库和 ITU-T 第 17 研究组制定的通信系统安全概略)中抽取的缩写词和定义的列表，在附件 A 里。本手册还提供了最新版本的 ITU-T 安

全方面的建议书目录，附件 B 广泛且更进一步展示了 ITU-T 安全方面工作的幅度。在附件 C 中我们总结了 ITU-T 每个研究组所做的安全相关工作，这些资料不断更新并可在 www.itu.int/ITU-T 查到。

总之， ITU-T 不仅积极参与了 IP 相关技术研究，而且积极满足安全需求极其多变的众多工业部门的需求。本手册显示了 ITU-T 建议书如何提供了在一般性的框架体系和特定系统和应用方面 – 已在全球为网络和服务提供所实施的解决方案。

1 手册范围

本手册概述了通信和信息技术中的安全问题，描述了实践问题并指明了 ITU-T 如何处理当前应用中安全的不同方面。手册具有教材的性质：它把 ITU-T 建议书中与安全相关的材料收集在一起并分别解释其相互关系。在这第一版中，手册并未涵盖安全所有的方面，尤其是与可用性有关的部分 – 尽管 ITU-T 有许多可提供，以及 ITU-T 也很积极参与的环境性损害方面。而且，所选问题以已经完成的工作为基础，而不是以正在进行的工作为基础，本手册以后的版本再处理这部分问题。

本手册的目标读者是工程师、产品经理、学生、专业人员和希望更好理解实际应用中安全问题的管制机构。

2 基本安全体系结构和尺度

建议书 X.805 定义了分布式应用实现端到端安全的体系和尺度的框架。基本的原则及定义适用于所用应用，尽管诸如威胁、弱点的细节以及应对或防治的对策根据应用需求的不同而不同。

安全体系定义基于层和层面两个主要概念。安全层讨论对构成端到端网络的网络元素和系统的要求。为保证端到端的安全在各层实现，在区分跨不同层的要求时使用了分层的方法。这三层是：基础设施层、服务层和应用层。定义这些层的好处之一是在不同应用提供端到端安全时允许重复使用。每一层的弱点不同，因此针对性措施也根据每层需求来定义。基础设施层包括网络传输设施和单独的网络元素。属于基础设施层的成分的例子有单独的路由器、交换机和服务器以及其间的通信链路。服务层讨论提供给用户的网络服务的安全。这些服务从基础连接性服务例如租用线服务延伸到增值服务例如即时消息。应用层讨论用户使用的基于网络的应用的要求。这些应用可能简单如电子邮件，也可能复杂如用于石油勘探或汽车设计等的使用非常高端视频转换的综合视频实现。

这一框架的第二轴线是讨论网络中实施的活动的安全。本安全框架定义了三个安全层面表示三种网络中发生的受保护的活动。这些安全层面是： (1) 管理层面, (2) 控制层面和 (3) 终端用户层面。这些安全层面分别讨论与网络管理活动、网络控制或信令活动和终端用户活动相关的特定安全需求。在第 6.4 节中详细讨论的管理层面关注运行、管理、维护和提供服务(OAM&P)活动, 如向某个用户或网络提供服务。控制层面与独立于网络所用的媒介和技术的端到端通信的建立（和修改）方面的信令有关。终端用户层面讨论用户访问和使用网络的安全，也包括保护用户数据流。

利用安全层和安全层面两条轴线（3 个安全层面和 3 个安全层），本框架还定义了讨论网络安全的 8 个尺度。这些尺度在下一章定义。从层次的角度，这些安全尺度适用于由层和层面构成的 3*3 矩阵中的每一个单元以决定合适的防治措施。图 1 表示安全体系中的安全层面、层和尺度。关于管理层面的第 6.4 节表明了其他 ITU-T 建议书如何讨论 3*3 矩阵中管理层面的 3 个单元。

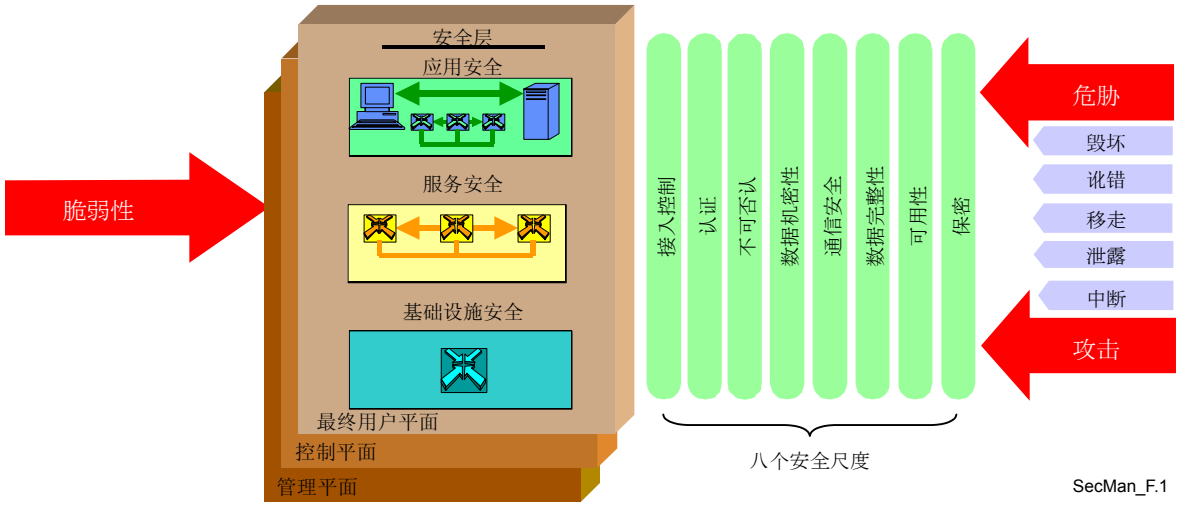


图 1

ITU-T X.805 中的安全体系成分

2.1 保密和数据机密性

保密概念是安全的基本驱动因素。通常理解保密是个人控制或影响与其相关的哪些信息可被收集和存储以及可能被谁、向谁披露的权利。延伸出来，保密还与某些保护其信息不向其同意的人士之外的任何人披露，所以只有明确地被授权的人士才能破译彼此之间交换的内容的技术手段（如加密）有关。

通常保密和机密性被用作同一个术语，但应注意 ITU-T X.805 区分了保密和数据机密性。前者与保护用户标识和其进行的活动（如在线购物习惯、访问过的网页等）的相关性有关，后者与反对未经授权访问数据内容的保护有关。加密、访问控制列表、文件许可是保护数据机密性常用的方法。

F.115、H.235、 J.160、Q.1531、 X.800 和 X.805 等多个 ITU-T 建议书中都提到保密一词。

2.2 认证

认证是对一实体声称的标识为真提供证明。这里的实体不仅包括人类用户，还包括设备、服务和应用。认证还证实一个实体未试图伪装或非经授权地重放一个先前的通信。有两种认证：数据来源认证（即在面向联接的关联中要求的认证）和对端实体认证（在无联接关联中的认证）。网络要保证与意向中的对等实体（而不是与一个试图伪装者或对前一连接的重放）建立数据交换，并且数据确实来源于声称的源头。认证通常在识别后进行。识别、认证和授权用的信息应由网络予以保护。

F.500、F.851、F.852、 H.235、 J.160、 J.93、J.95、 M.60、 X.217、 X.217-Bis、 X.509、X.800、X.805 和 X.811 等多个 ITU-T 建议书中都提到认证这一术语。

2.3 完整性

数据完整性是指数据未被未经授权就改变的性质。延伸出来，数据完整性也保证信息未被未经授权的修改、删除、重造和复制，并给出这些未经授权的活动的迹象。H.235、J.160、 J.93、 J.95、Q.1290、Q.1531、X.800 和 X.815 等多个 ITU-T 建议书中提到完整性这一术语。

2.4 不可抵赖性

不可抵赖性是防止用户事后否认其实施了某一行为的能力。这些行为包括制造、发源、收到和发送内容，例如发送或接收消息、发起或接受呼叫、参加语音和视频会议等等。

不可抵赖性要求提供对数据发送或接收的不可伪造的证明，防止发送者否认一个正确的消息或接收者否认接收。网络可提供下面两种或其中之一形式：数据接收者得到数据来源的证明以避免发送者不诚实地否认其发送了数据或其内容；或发送者得到数据传送的证明以免接收者事后否认接收了数据或其内容。

F.400、F.435、F.440、J.160、J.93、J.95、M.60、T.411、X.400、X.805、X.813 和 X.843 等多个 ITU-T 建议书中提到不可抵赖性这一术语。

2.5 X.805定义的其他尺度

除保密和数据机密性、认证、完整性和不可抵赖性之外，ITU-T X.805 还定义了其他 3 个安全尺度：访问控制、通信和可用性。

访问控制安全尺度防止未经授权使用网络资源。访问控制保证只允许被授权的个人或设备访问网络元素、存贮的信息、信息流、服务和应用。访问控制在的 ITU-T 建议书 X.810 和 X.812 中定义。它与认证有关，并超出了认证的范围。

通信安全尺度是 X.805 中定义的新的尺度，保证信息只在被授权的端点间流动。该尺度指为免通信转移和侦听而控制网络通信流的措施。

可用性尺度保证对网络元素、存贮数据、信息流、服务和应用的已经授权的访问不因网络中断而被拒绝。网络重建和灾难恢复措施也属于这个范畴。

3 脆弱性、威胁和风险

对实施最有利的ＩＴ方案和决定哪种最新最好的万维网应用、服务器和数据库最适应组织目标的巨大的关注使得保护资产中数据经常被放到第二位考虑。许多企业识认为：因为企业没被攻击，所以没有威胁。

标准组织具有应对协议中弱点的独特能力和责任。标准组织可采取一些立即和相对简单的行动提高所有现正被标准化的协议的安全。

*安全脆弱性*是系统设计、实现或运行中的、可被利用来破坏系统安全性的瑕疵或弱点(RFC 2828)。安全脆弱性不是风险、威胁或攻击。

弱点有四种类型。*威胁型*弱点来源于预测未来威胁（例如 7 号信令系统）的困难。*设计和规范型*弱点来源于协议设计中的错误或疏忽使其天生地不安全（例如 IEEE 802.11b 中的 WEP 也叫做 WiFi）。*实现型*弱点是协议实现中的错误产生的弱点。最后，*运行和配置型*弱点来源于实现时选项错误使用或软弱的布署政策（例如在网络中没有强制使用加密，或网络管理人员选择了软弱的流密码）。

根据 X.800，*安全威胁*是对安全潜在的侵害，可能是主动性的（当系统状态可被改变时），或被动性的（不改变系统状态但非法泄露信息）。伪装成合法主体和拒绝服务是主动性威胁的例子，窃听获取口令是被动性威胁的例子。威胁方可能是黑客、恐怖分子、破坏分子、有组织犯罪或政府发起的，但相当数量的威胁来自组织内部人员。

*安全风险*来源于安全脆弱性与安全威胁的结合。例如，操作系统应用的溢出漏洞（即脆弱性）加上黑客的知识、合适的工具和访问（即威胁）可产生万维网服务器攻击的风险。安全风险的后果是数据丢失、数据损坏、隐私失窃、诈骗、宕机及失去公共信任。

尽管威胁会改变，在协议的整个生命期安全弱点始终存在。由于使用标准化的协议，基于协议的安全风险在规模上可能是非常大的、全球性的。所以理解并识别协议中的弱点非常重要。

4 安全框架的要求

对通用网络安全框架的要求来自不同的源头：

- 顾客 / 客户需要对网络和所提供的服务的信心，包括大灾（含恐怖活动）发生时服务的可用性（尤其是应急业务）.
- 政府机构的法律法令中要求安全，以保证服务可用性、公平竞争和隐私保护。
- 网络运营者和服务提供商自身需要安全，以保护他们的运营和商业利益，承担他们对客户和公众的义务。

对通信网络和服务的安全要求最好应基于国际公认的安全标准，因为可以增加互操作性，并避免重复劳动和另起炉灶。与被保护的交易的价值相比，提供和使用安全服务和机制可能相当昂贵。在考虑安全措施的成本和安全缺口潜在的财务影响时应有平衡。因此，具备按被保护的服务要求将安全性按客户定制的能力非常重要。使用的安全服务和机制应允许这种客户化。由于安全特性可能的组合多种多样，最好有一个覆盖大范围电信网络服务的安全简表。

标准化有利于方案和产品的重复使用，意味着安全可以更快、更便宜地实现。

对制造商和系统用户等来说，为实现安全，标准化解决方案重要的好处是产品制造和电信网络成份间的互操作的规模经济性。

为电信网络或服务提供商提供的安全服务和机制与保护不受拒绝服务、侦听、哄骗、篡改消息（修改、延迟、删除、插入、重放、重选路由、错路由、改变消息顺序）、复制或伪造等恶意攻击有关。保护包括防止攻击、发现攻击、从攻击中恢复、防止服务因自然事件（气候等）损坏的措施和管理安全相关信息。提供安全时还必须实现由适当授权的合法当局要求的合法拦截。

5 X.509 的 PKI 和特权管理

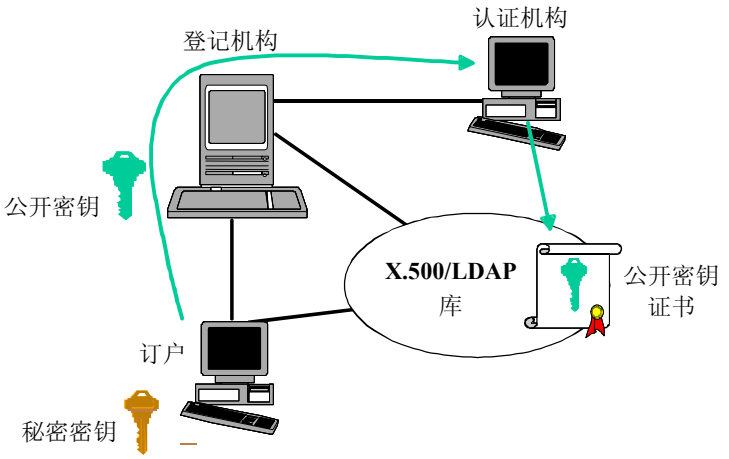
X.509 公共密钥基础设施(PKI)提供了基于公共密钥证书和证书管理机构的强认证标准。 PKI 提供了认证通信各方间消息的可升级的方法。PKI 的基础技术是公共密钥加密，所以先介绍它。除 PKI 之外，X.509 还提供了基于属性证书和属性机构、定义了强授权标准的权限管理基础设施 (PMI)。PMI 用于确定用户的权利和权限。 PKI 和 PMI 的构成如图 2 表示。

5.1 秘密和公共密钥加密

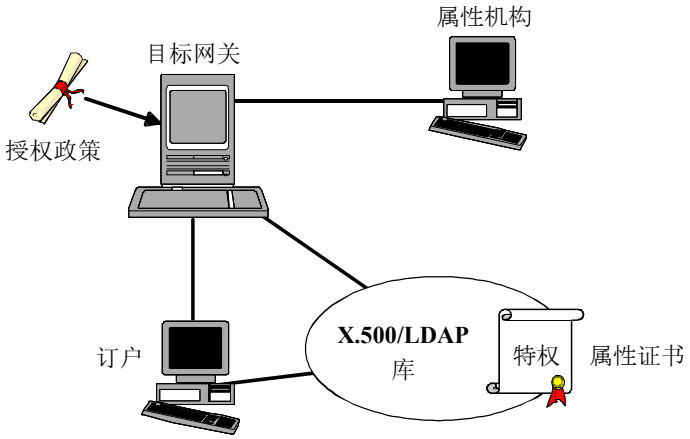
对称 (或秘密密钥) 加密是指加密和解密使用同一密钥的加密系统，如图 3(a) 所示。对称加密系统要求制定各方共享独特的秘密密钥的初始协定。由于获知加密密钥即获知解密密钥，反之亦然，密钥必须通过安全途径分发到各方。

非对称 (或公共密钥) 加密系统如图 3(b)所示使用一对密钥– 一个公共密钥和一个秘密密钥。其中之一公开，但另一个秘而不宣。公共密钥不同于秘密密钥。虽然数学上相关，但没有可行的办法从公共密钥获知秘密密钥。虽然公共密钥广为传播，但秘密密钥总保持秘密（例如在一个智能卡或令牌上，未来还可能在 PDA 或手机上）。总之，要发送加密的秘密数据给某人，这个人用接收者的公共密钥加密数据，接收到加密数据人人用他相应的秘密密钥解密数据。要发送认证数据给某人，发送者用他 / 她的秘密密钥加密数据，接收者用发送者的公共密钥来认证数据。但是，这样使用非对称加密有一些缺点。首先，公共密钥加密耗费计算时间，所以使用非对称加密法加密消息的全部是没效率的。其次，由于中间节点无法得知谁是接收方，把消息全部加密后无法将消息发送到接收端。因此，实际上非对称加密法只用于加密消息的小部分。 如果要求机密性，消息用传统的对称加密法加密，对称的密钥用接收方的公共密钥非对称加密。如果要求认证，消息用 SHA1 或 MD5 等安全的单向散列函数方法处理，产生的 160 或 128 位散列值用发送者的秘密密钥非对称加密，并在传送前附在消息（明文传送）之后。 这个附加的加密校验和叫做数字签名– 电子商务的重要特色。

公共密钥加密依赖于人们已知晓相应秘密密钥持有者正确的公共密钥。如果张三错误地相信自己拿到了李四的公共密钥，而实际上这个公共密钥属于王五的秘密密钥，那么张三会相信由王五数字化签署的消息实际来自李四（这得以让王五伪装成李四）。更有甚者，如果张三想送一个机密消息给李四，王五将能截获并破译这个消息，而李四可能读不到它。所以人们必须有办法验证一个公共密钥的真正主人。

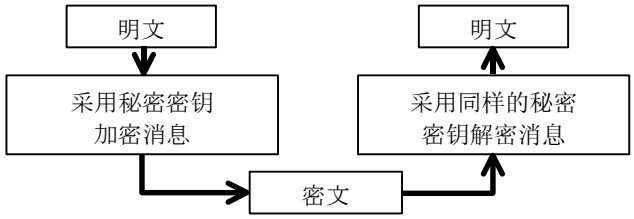


(a) 公开密钥基础设施的组成部分



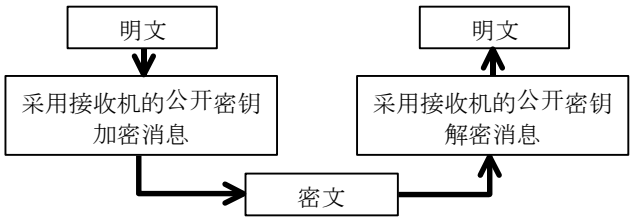
(b) 特权管理基础设施的组成部分 SecMan_F.2

图 2 PKI 和 PMI 的构成



- 双方共享一个单一的秘密密钥
- 问题：在完全保密的情况下交换密钥不易
- 最著名例子：DES(数据加密标准)

(a) (对称)秘密密钥加密



- 每一参与者都
  - 有一个自己专用的秘密密钥
  - 有一个众人皆知的公开密钥
- 问题：比秘密密钥加密慢
- 最著名例子：RSA

(b) (不对称)公开密钥加密 SecMan_F.3

图 3
对称（或秘密）和不对称（或公开）密钥加密处理和主要性能图示

5.2 公共密钥证书

公共密钥证书（有时被称作“数字证书”）是验证一对非对称密钥对的主人的方法。公共密钥证书将一个公共密钥与它主人的名字紧紧联系在一起，并经证明这一关联的受信任的机构数字签发。这一受信任的机构被称作证书机构 (CA)。国际认可的公共密钥证书格式在 X.509 标准中定义。简而言之，一个 X.509 公共密钥证书包含一个公共密钥、该密钥使用的非对称算法的标识、该密钥对的主人的名称、证明这一所有关系的ＣＡ的名称、证书的序列号和有效期、该证书符合的 X.509 版本号以及一组可选的包含该ＣＡ证书政策的扩展域。整个证书然后用该ＣＡ的秘密密钥数字签发。X.509 证书可以广泛公开在万维网站、LDAP 目录或附在电子邮件的Ｖ卡上，ＣＡ的签名保证它的内容不会在不知晓的情况下被篡改。

显然为验证一个用户的公共密钥证书，需要获得签发这个用户证书的ＣＡ的公共密钥，才能检查用户证书上的签名。一个 ＣＡ可以让另一个（高级）ＣＡ证明它的公共密钥，这样顺着证书链，验证公共密钥变成了一个叠代过程 ，最终这个链必须在某个“信任的根源”、一般碰到的是自我签发的ＣＡ证书（在其中该根ＣＡ证明这是它自己的公共密钥）处结束。签名允许我们验证密钥和ＣＡ名称自该证书发放以来未被篡改。但是，我们不能认定一个自签发的证书中的ＣＡ的名称，因为该ＣＡ自己加进了这个名称。因此，公共密钥基础设施中的关键成份是根ＣＡ公共密钥（作为自签发证书）以可说服我们相信该公共密钥确实属于自签发的证书中标明的ＣＡ方式的安全分发。否则，我们无法相信是否有人伪装成根ＣＡ。

5.3 公共密钥基础设施

PKI 的主要目的是发放和管理公共密钥证书，包括根ＣＡ的自签发证书。密钥管理包括生成密钥对、生成公共密钥证书、撤消公共密钥证书（例如当用户的秘密密钥暴露）、保存和记录密钥和证书以及它们到期后的销毁。每个ＣＡ根据一套政策运行，X.509 标准提供了在该ＣＡ发放的证书的扩展域中发布（部分）政策信息的机制。ＣＡ采用的政策规定和程序通常在该ＣＡ公开发布的证书政策 (CP)和证书使用声明(CPS)文件中定义。这些文件有助于保证通常的、评价我们对国际间或部门间ＣＡ发放的公共密钥证书的信任的质量基础。他们提供了建立机构间信任的（部分的）法律框架，也规范了使用这些发放的证书的限制。

应该注意，使用公共密钥证书的认证要求端点提供使用秘密密钥的数字签名。仅仅交换公共密钥证书并不能避免中间人的攻击。

5.4 权限管理基础设施

ITU-T 建议书 X.509 第一版定义了公共密钥基础设施的基本元素，包括公共密钥证书的定义。２０００年的修订版包括对属性证书和权限管理基础设施框架的重要增补。定义这些机制允许在多厂商和多应用的环境下设置用户访问权限。

在 PMI 和 PKI 之间有些概念相似，但前者关注授权，后者集中在认证。图 2 和表 1 表示了两者的相似之处。

表1 权限管理和公共密钥基础设施特性比较

权限管理基础设施	**公共密钥基础设施**
机构源(SoA)	根证书机构 (信任锚)
属性机构(AA)	证书机构
属性证书	公共密钥证书
属性证书撤消表	证书撤消表
PMI 机构撤消表	PKI 机构撤消表

为用户分配优先权的目的是保证他们服从机构源规定的安全政策。属性证书中政策相关信息与用户名称绑定在一起，还有一些成份如图 4 所示。

版本
持有者
发放者
签名 (算法标识)
证书序号
有效期
属性
发放者独特标识
扩展域

图 4 X.509 属性证书结构

建议书 X.509 中描述了 PMI 控制的 5 个部分：权限声明者、权限验证、目标方法 [1]、权限政策和环境变量（见图 5 ）。该技术使权限验证者能控制权限声明者按权限政策对目标方法的访问。

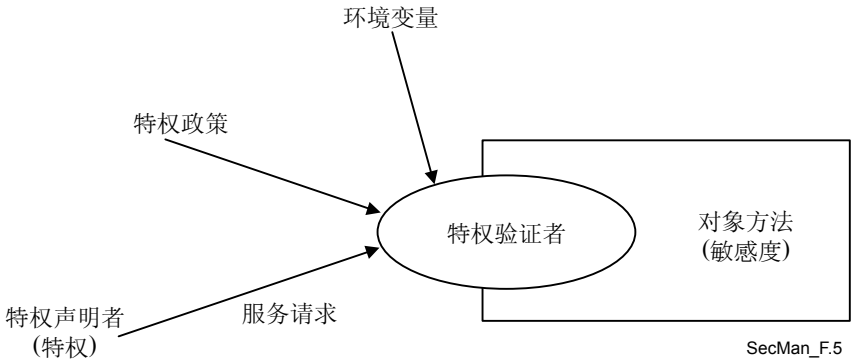


图 5 ITU-T X.509 PMI 控制模型

当实现中需要委托优先权时，建议书 X.509 考虑的 PMI 委托模型有四个部分：权限验证者、SoA、其他 AA 和权限声明者 (见图 6)。

[1] 目标方法被规定为可以调用某种资源的某种行动（如某个文件系统可能已经读取、写入或执行了目标方法。）

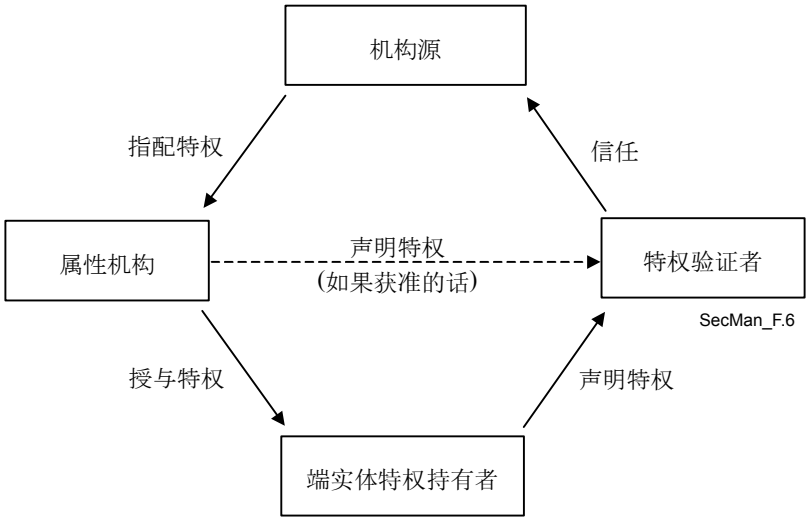


图 6 ITU-T X.509 PMI 委托模型

考虑到用户被赋予了角色，近来授权模式的实现采用了基于角色的访问控制 (RBAC)模型 。授权政策将一组许可与角色联系起来，用户按政策检查他的角色以便开展后续行动。第 6.5.2 节的 E 处方应用解释了 RBAC 系统的使用。

6 应用

本章介绍的应用属于两个完全不同的种类。第一类集中于终端用户应用。其中一个例子就是 VoIP，描述了用来提供这种终端用户应用的网络架构和网络元素。作为一个特别的案例，这里要从三个层面来论述用 VoIP 支撑多媒体应用的安全因素和解决方法。还有一种最终用户应用是 IPCablecom 系统，这种系统是在有线电视网络上提供基于 IP 的实时服务和传真传输服务。 这些应用不限于电信行业的服务，还包括 E 健康（电子健康)服务，特别是 E 处方（电子处方）系统。第二类集中在网络管理应用。安全性是服务商为确保其服务的质量和完整性而需要考虑的重要因素。因此，在网络管理中给予适当的特权和授权是非常有必要的。

6.1 使用H.323系统的VoIP

基于 IP 的话音(VoIP)，即 IP 电话，是用 IP 协议来提供哪些原来是由传统电路交换方式的 PSTN 网络提供的服务。这些服务包括最主要的话音业务和一些相关的补充业务，例如：电话会议、呼叫前转、呼叫等待、多线连选、呼叫转移、呼叫寄存与代容、呼叫保持和呼叫随我转移等，以及许多其他智能网络业务和一些语音频带数据。互联网话音业务是 VoIP 的一种特殊运用，它的语音流直接承载在公共互联网骨干网上。

H.323 是 ITU-T 一个总括性的建议书，它为在局域网（LANs）上或者通过包括互联网在内的那些不提供服务质量（QoS）保证的 IP 网上进行音频、视频和数据通信奠定了基础。这些网络包含目前的企业办公网络、分组交换的 TCP/IP 网、IPX 以太网、高速以太网和令牌环网等技术。遵守了 H.323 协议，多厂商的多媒体产品和应用就可以互操作，使得用户在通信时不用考虑产品间的兼容性。H.323 是第一个已经定义好的 VoIP 协议，也被认为是用户、商业企业、娱乐场所和专业应用的基于局域网产品的一个基础。H.323 系统的核心建议书部分是：

- H.323－“总括性”文件，描述 H.225.0、H.245 以及其他一些有关传送基于包交换的多媒体会议业务的文件的用法。
- H.225.0－描述了三个信令协议（RAS，呼叫信令和附件 G）。
- H.245－多媒体控制协议（与 H.310，H.323 和 H.324 相同）。
- H.235－基于 H.245 系统的安全性。
- H.246— 与 PSTN 的交互协议。
- H.450.x —补充业务。
- H.460.x — 各种 H.323 协议扩展。
- H.501— 移动性管理和网间/网内通信协议。
- H.510 — 用户、终端和业务的移动性。
- H.530—H.510 的安全说明。

ITU-T 在 1996 年批准了第一版 H.323 规范书，1998 年 1 月批准了第二版，现在的第五版了是在 2003 年 7 月获得批准的。这个标准涵盖的范围宽泛，既包括独立的设备和嵌入式个人电脑技术，同时还包括点对点和点对多点会议技术标准。H.323 也适用于呼叫控制、多媒体管理和带宽管理，以及局域网与其他网络的接口。

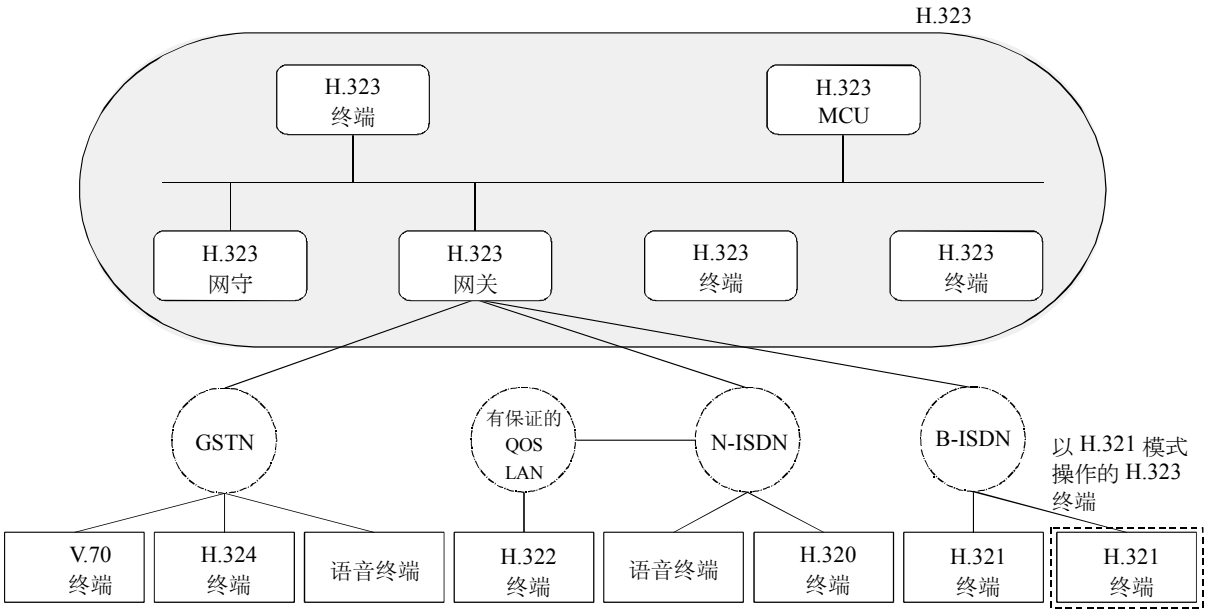
H.323 是一个比较大的通信标准系列的一部分，它使视频会议得以在网络上传输。这个系列称做 H.32X，包括 H.320 和 H.324，分别用于 ISDN 和 PSTN 通信。这里只是对 H.323 标准的优点、体系结构和应用做一个概述。

H.323 定义了网络通信系统的四个主要组成部分：终端、网关、网守和多点控制单元。此外，可能还有边界控制器和对等网络元素。以上网络元素见图 7。

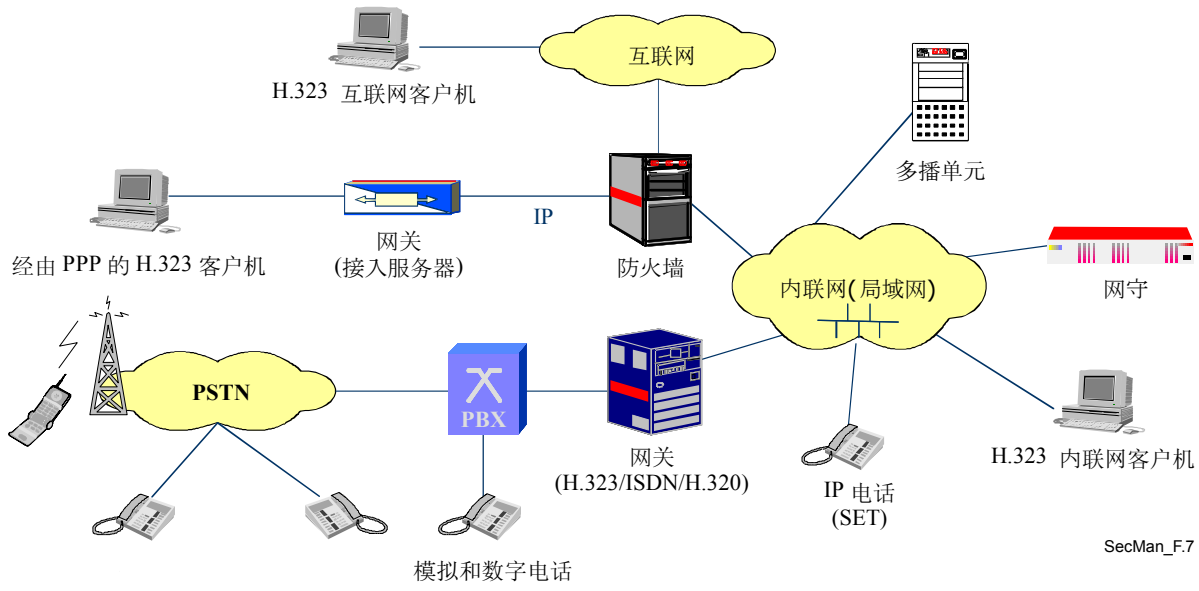
*终端（T）*位于提供双向通信的 IP 骨干网上的用户端点。H.323 终端必须支持语音通信，并且可以支持视频编码、T.120 数据会议协议簇以及 MCU 的兼容性，例如 IP 电话、视频电话、交互式语音应答设备（IVR devices）、语音邮件系统、“软电话”（如：NetMeeting）等。

网关（GW）在 H.323 会议系统中是一个可选网络元素。网管可以提供许多服务，最普通的就是在 H.323 会议系统终端与其他类型终端间的协议转换功能。这个功能包括传输格式间的协议转换（如：H.245 到 H.242 间的转换）和通信进程间的协议转换（如：H.225.0 到 H.221 间的转换）。此外，网关可以在音频编码与视频编码间进行转换和执行呼叫建立和清除局域网端和交换电路网端的呼叫。

网守（GK）是 H.323 网络中的一个最重要的组成部分，它在其区域范围内对所有的呼叫处理起着核心作用，并为注册端提供呼叫控制服务。许多情况下，H.323 网守的作用相当于一个虚拟交换机，它可以实现访问控制、地址解析，并且可以直接在用户终端间建立呼叫，或可以通过网守自身发送呼叫信令，实现例如跟踪/定位、忙时呼叫前转等功能。与网守关联的设备有**边界**（或对等的）设备元素（BE），用来在管理域内交换地址信息和参与呼叫授权。这样的功能性也将使不同的 H.323 “岛”或网络之间互相通信。这是通过交换一系列的信息实现的，如图 8 所示。



(a) H.323 系统及其组成部分[Packetizer]



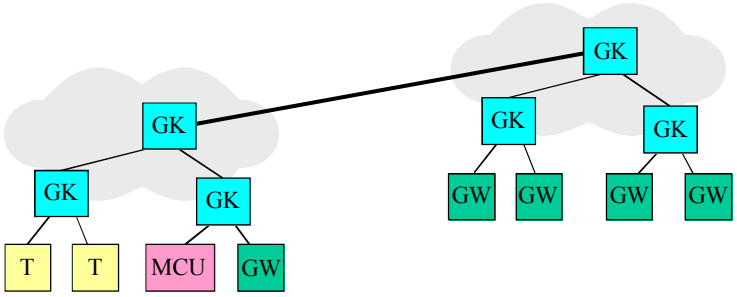
(b) H.323 构成方案 [Euchner]

图 7

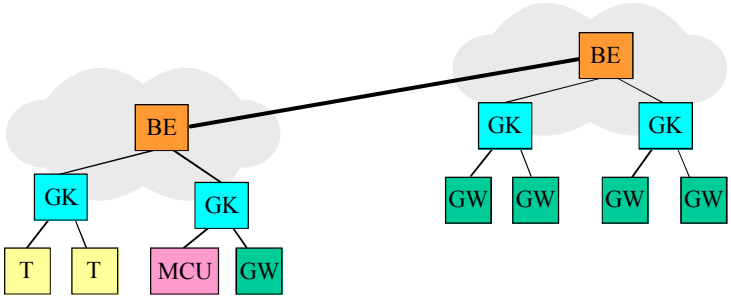
H.323 系统: 组成部分和配置方案

多点控制单元（MCU）支持三点或多点终端的会议。H.323 协议规定，MCU 应包括一个必备的多点控制器，零个或多个多点处理器。多点控制器负责管理呼叫信令但不能直接处理媒体流，而由多点处理器来处理媒体流，它能够混合、交换和处理音频、视频和/或数据比特。多点控制器和多点处理器的性能可以集成在一个特定的组件中或是其他 H.323 组件的一部分。

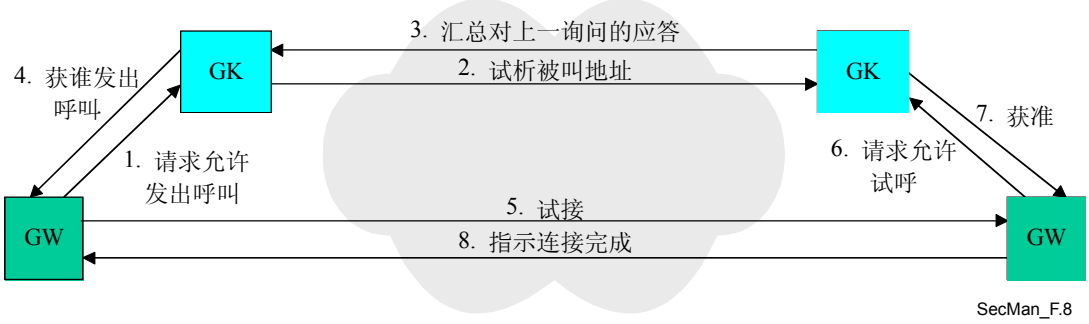
尽管 H.323 起初是作为一个多媒协议设计的，但它现在最主要是应用于 IP 语音市场。H.323 网络现在每月承载着数十亿分钟的话音和视频流量（仅指公网上的数量）；当今大部分的 VoIP 流量都是通过 H.323 协议传输的。据统计，目前 VoIP 的流量已占国际长途电话分钟数的百分之十，而且 H.323 视频流量也在稳步上升。其主要原因在于协议自身的成熟性和它的实施，再有就是 H.323 被证实为是一个极具扩展性的解决方案，H.323 产品链从组件和芯片到无线电话和视频会议硬件，可同时满足服务提供商和企业的需求。



(a) 采用 RAS[1] 的拓扑结构



(b) 采用附件 G/H.225.0 的拓扑结构



(c) 高层呼叫流程

图例：BE：边界元素　　GK：网守　　GW：网关　　MCU：多点控制单元　　T：终端

图 8
管理域之间的通信

以下是 H.323 系统提供的功能性列表：

- 话音、视频和数据会议性能；
- 不同类型终端间的通信，包括个人电脑（PC）到电话、传真到传真、电话到电话和网上通话；
- 支持 T.38 传真和 IP 调制解调；
- 大量补充业务（呼叫转移、呼叫代接等）；
- 与包括 H.320(ISDN)和 H.323M（3GPP 移动无线）在内的其他 H.32x 系统的强互操作性；
- 媒体网关分解规范（通过 H.248 网关控制协议）；
- 支持信令和媒体安全；
- 用户、终端和业务终端移动性；
- 支持应急业务信令；

应用 H.323 的例子包括被运营商批发转让的服务，特别是 VoIP 骨干网（话音业务四类交换机）和电话卡业务。在公众通信中 H.323 协议被用于 IP-PBX 交换机、IP 交换中心（IP-Centrex）、语音虚拟专网、语音和数据集成系统、WiFi 电话以及呼叫中心和移动业务的实施。在专业通信中，H.323 协议广泛应用于语音（或音频）和视频会议的语音/数据/视频集成和远程教育。在家庭环境中，应用包括宽带音频－视频接入、PC 到电话，定制新闻和信息的分发。

6.1.1 多媒体和 VoIP 中的安全问题

如图 9 所示，由于 IP 网络天然的开放性所致，H. 323 系统中的所有元素都能够在地理上被随处分配，因而出现了一些安全威胁。

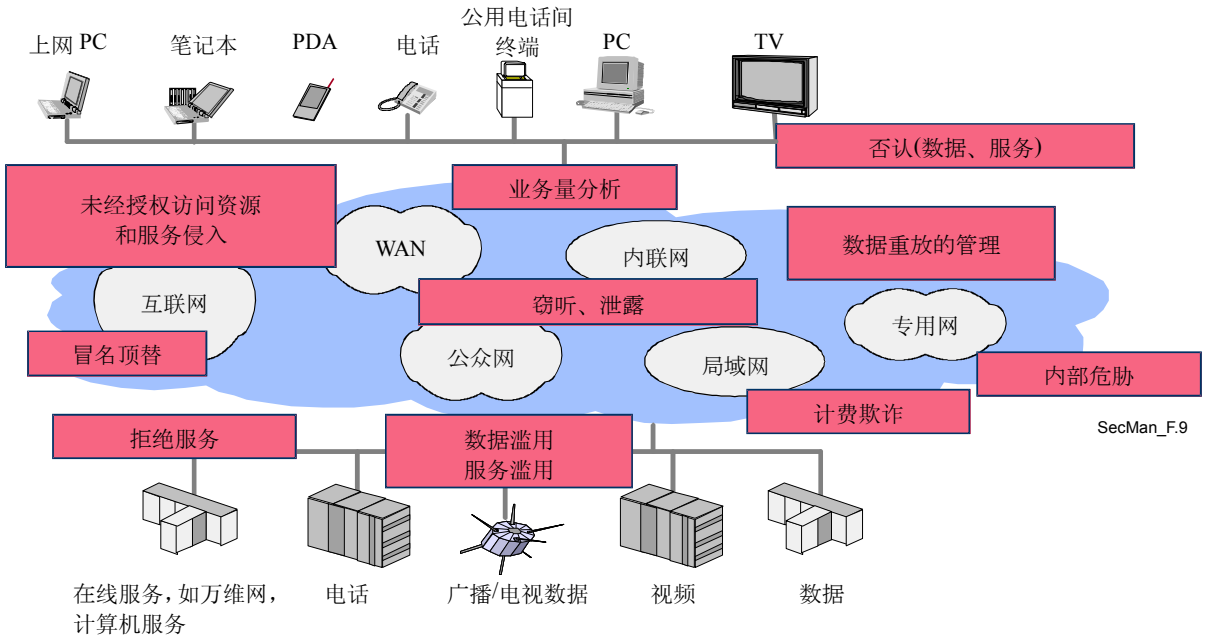


图9

多媒体通信中的安全威胁

多媒体通信和 IP 电话系统中的主要安全问题大体如下：

- 用户和终端认证：VoIP 服务提供商为了准确计费或计算业务使用量而需要知道谁正在使用他们的服务。作为认证的一个先决条件，用户和/或终端必须用某种标识来标定。而后，用户/终端必须证实其出示的标识是真实的。这种情形主要发生在通过强加密认证过程（例如受保护的密码或 X.509 数字签名）。同样，用户可能也想通过身份认证知道他们正在与谁通话。

- 服务器认证：VoIP 用户之间主要是通过包括服务器（网守、多播单元、网关）在内的一些 VoIP 基础设施实现互相通信，因此用户关心的是他们是否联接了正确的服务器和/或正确的服务提供商。这方面的问题涉及固定和移动用户。

- 用户/终端和服务器认证以应对安全威胁，例如伪装、中间者攻击、IP 地址欺骗和连接劫持。

- 呼叫认证是一个判断过程，以确定用户/终端是否真的被允许使用像服务特征（例如呼叫 PSTN）那样的服务资源或网络资源（QoS、带宽、编解码等）。通常是将认证和授权功能结合起来实现访问控制判断。认证和授权有助于阻止类似伪装、误用和欺骗、操控和拒绝服务等攻击。

- 信令安全保护解决的是保护信令协议免于操控、误用以及机密性和保密问题。信令协议主要通过密码加密方式以及完整性保护和重放来进行保护。应特别注意，为达到实时通信的临界性能要求，可以通过一些握手过程和短循环以避免过多的呼叫建立次数或由于安全处理造成的数据包延迟或颤抖而引起的语音质量的降低。

- 对语音的保密是通过加密语音数据包实现的，也就是 RTP（real-time transpert protocol）有效载荷和计数器对被窃语音数据的监听。通常，多媒体应用的媒体数据包（例如视频）也要被加密。进一步的媒体数据包的保护还包括有效负载的认证/完整性保护。

- 密钥管理不仅包括在用户和服务器中安全分发密钥介质的所有过程，还包括更新过期的密钥和遗失的密钥。密钥管理可以是独立于 VoIP 应用（密码规定）分离的一个过程，在动态协商表明安全能力的安全简表及发放基于会话的密钥时，也可以与信令综合在一起。

- 跨域安全涉及在不同环境中的系统根据不同的需求、不同的安全政策和不同的安全能力已经实施不同的安全特性，因而有必要能够动态地调整安全简表和安全能力，调整包括加密算法和算法的参数。在跨越边界以及涉及不同服务提供商和网络时，这一点尤为重要。跨域通信的一个重要安全要求是能够平滑地跨越防火墙和应对网络地址转换（NAT）设备的限制。

以上内容虽不全面，但属 H.323 安全的核心部分。实际上，我们可能要面对超过 H.323 考虑范围之外的安全问题（例如安全政策、网管安全、安全提供服务、实施安全、操作安全和安全事件处理）。

6.1.2 VoIP 安全是如何规定的

在 H.323 多媒体系统中，ITU-T 建议书 H.235 定义的安全简表包括 H.323 的安全机制和安全协议规范。1998 年 H.235 第一次被写入第二版 H.323 系统中。其后，随着时间的变迁通过巩固以上那些安全机制、增加更多成熟的安全算法（例如高安全性、高速 AES 加密算法），为一些特定用例和环境设计出有用并有效的安全简表，使 H.235 有了进一步的发展。第三版的 H.235 是目前 ITU-T 对基于 H.323 系统的安全建议书，这些系统可以为从小集团组织到企业和大型运营商提供不同的安全性。

简而言之，H.235 规定了密码保护的控制协议族（H.225.0 RAS、呼叫信令和 H.245）和加密保护的音频/视频媒体流数据。在 H.323 信令的不同进程中，H.235 规定了那些想要和必要调整的加密服务、加密算法和安全能力的方法。建立动态会话密钥的密钥管理功能完全可与信令握手协议整合在一起，这样将有助于减少呼叫建立的延迟时间。H.235 密钥管理支持“传统的”点到点通信，以及当多个多媒体终端在集团内通信时的带有多播单元（即 MCUs）的多点结构。

H.235 含有许多安全方案可以适用于不同的目标环境，如企业内/企业间和运营商间。依据假设可用到的安全设施、终端能力和平台等（简单终端或智能终端），H.235 提出了一系列个性化和具有互操作性的安全简表。这些可用的安全简表提供的安全技术从包括密码保护（H.235 认证和消息集成的附件 D）的简单共享密钥简表到使用数字签名和 X.509 PKI 认证（H.235 附件 E 和附件 F）的许多成熟的简表。这样就既可以用较简单但又无需升级的技术实施跳对跳保护，也可以用可升级的 PKI 技术实现点对点保护。H.235 附件 I 放松对由网守选路的、以服务器为核心架构的严格依赖，而转向采取点对点保护模式的安全方案。

H.235 利用如椭圆曲线加密算法和 AES 密码算法等特殊优化的安全技术以达到严格性能要求。通过加密 RTP 有效载荷在应用层实现语音加密。这样，在终端采用了数字信号处理器（DSP）和语音压缩编码器，而无需特殊操作系统平台，就可以通过紧密相互作用的方式使小足印（small footprint）技术得以有效实施。如果适用和匹配合理，现有的安全工具如目前应用中的互联网安全包和标准（IPSec，SSL/TLS）就能够在 H.235 中被（重新）用上。

图 10 给出了 H.235 的框架，包括了为建立呼叫（H.225.0 和 H.245 模块）和双边通信（包括音频和/或视频压缩的 RTP 有效载荷加密）的相关规定。这些功能包括认证、集成、私密和非判断机制。网守通过在终端进行访问控制和可能的非判断机制来实现认证。基于 IP 的传输层和更低层的安全性超越了 H.323 和 H.235 的范围，但通常可以用 IETF 的 IP 安全性（IPSec）和传输层安全（TLS）协议簇来实现。通常，IPSec 或 TLS 能够用来规定 IP 层的认证和随意规定机密性（如加密）功能，而无论上面运行的是什么样的（应用）协议，同时也不必升级应用协议和每一端点的安全策略。

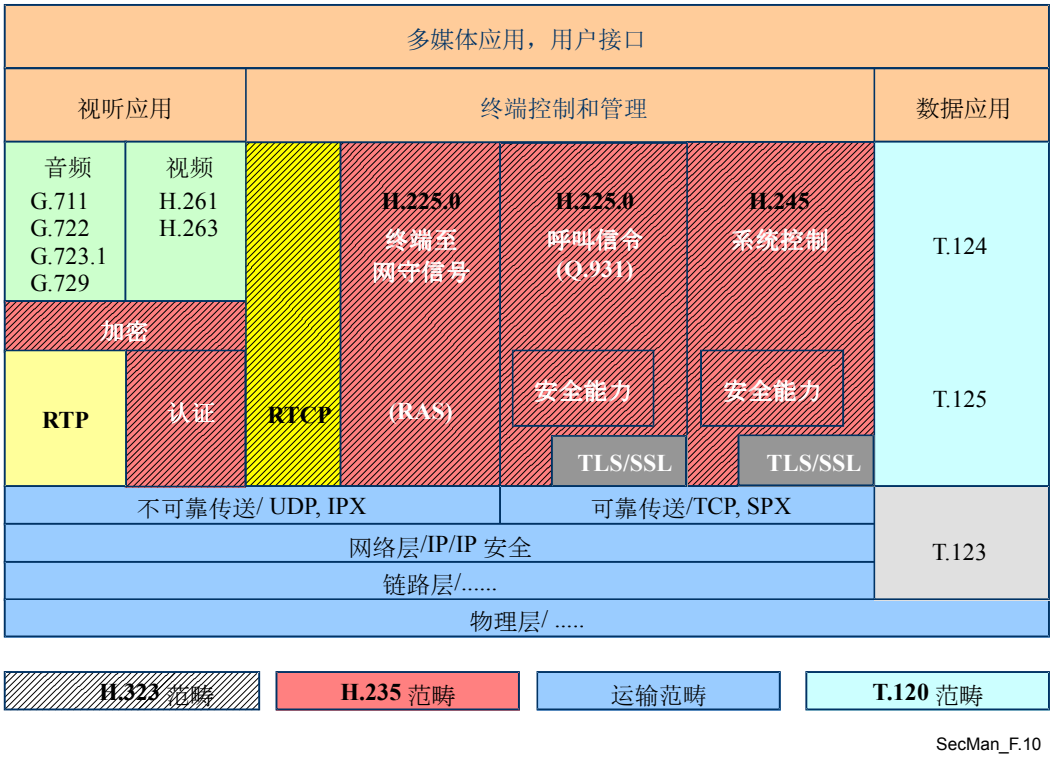


图 10
H.235 提供的在 H.323 中的安全简表

虽然 H.235 仅仅是通过有限移动性的规定来表述“静态”H.323 环境，但还是很有必要在分布式的 H.323 环境下给出安全用户和终端的移动性规定，这些移动性超出了域间的相互连接和有限的网守区域的移动性。ITU-T 建议书 H.530 通过表述以下这些安全问题涵盖上述安全性需求：

- 访问非本地域的移动终端/用户认证和授权。
- 访问域的认证。
- 安全密钥管理。
- 移动终端和访问域之间的信令数据保护。

除 H.235 外，H.350 和 H.350.2 采用 LDAP 和 SSL3 规定可升级的密钥管理。ITU-T 建议书 H.350.x 规定了一些重要的能力，这些能力使企业和运营商能安全地管理大量使用基于 IP 视频和语音的用户。H.350 规定了将 H.323、SIP、H.320 和通用消息服务联入号码簿服务的方法，致使现代的身份认证管理措施能被应用于多媒体通信。此外，这个体系结构还为存放这些协议相关的安全证书规定了标准位置。

H.350 没有改变任何协议的安全性结构。无论如何，H.350 提供了一个适合存储认证证书的标准地方。应该注意的是，H.323 和 SIP 都支持共享秘密认证（分别见 H.235 附件 D 和 HTTP 文摘）。而这些方法要求呼叫服务器拥有使用密码的权限。因此，如果呼叫服务器或 H.350 号码薄受威胁，密码也可能受到威胁。这些缺陷除了与其说谎是 H.350 本身的缺陷，不如说是因为系统（H.350 号码簿或呼叫服务器）及其操作方面的缺陷所致。

要极力提倡呼叫服务器和 H.350 在共享信息前的相互认证。此外，更要主张 H.350 号码薄和呼叫服务器或终端之间的通信应该像 SSL 或 TLS 那样建立在 SSL 和 TLS 等安全通信通道上。

因该注意，LDAP 服务器上的访问控制列表是安全策略的内容而不是标准的一部分。系统管理员应考虑用 H.350 属性的一般性理解来设置访问控制。例如，地址的属性可能是公开的，但密码属性只应由被认证的用户使用。

6.2 IPCablecom 系统

IPCablecom 系统可以使得有线电视运营商在它们已经改造成支持电缆调制解调器的网络上提供基于 IP 的实时服务（例如语音通信）。ITU-T 建议书 J.160 定义了 IPCablecom 系统的体系结构。在很高的层次上，可以将 IPCablecom 系统的体系结构看做三个网络：“J.112 HFC 接入网”、“可管理 IP 网络”和 PSTN。接入点（AN）提供“J.112 HFC 接入网络”与“可管理的 IP 网络”之间的连接。信令网关（SG）和媒体网关（MG）提供“可管理的 IP 网络”与 PSTN 之间的连接。IPCablecom 系统的体系结构如图 11 所示。

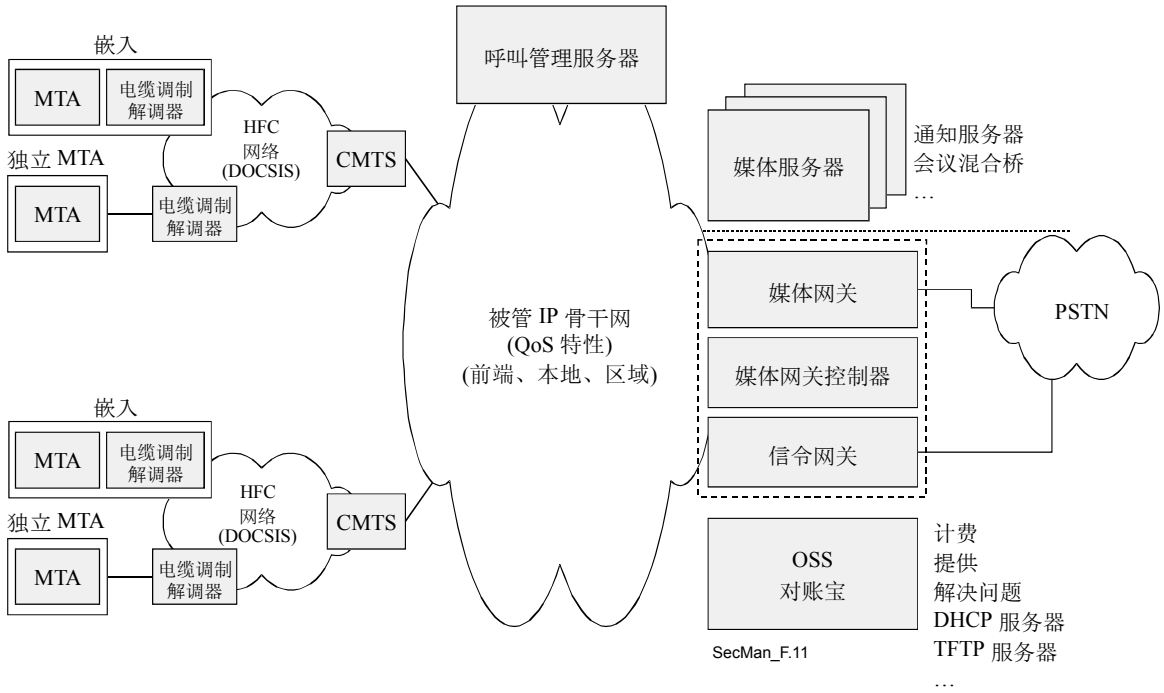


图 11
IPCablecom 推荐体系结构[J.165]

J.112 混合光纤同轴电缆（HFC）接入网提供住宅用户与电缆接入端之间高速、可靠和安全的传输。这个接入网可以提供 J.112 的所有性能，包括服务质量和通过电缆调制解调器终端系统（CMTS）实现的物理层接口。

被管IP网络具有多种功能。首先，它在负责信令、媒体、服务提供和服务质量的确立的IPCablecom系统基本功能功能元素之间建立互连。此外，可管理的 IP 网络在其他可管理的 IP 与 J.112HFC 网络间提供远程 IP 连接。可管理的 IP 网络包括以下功能元素：呼叫管理服务器、发布服务器、信令网关、媒体网关、媒体网关控制器和一些运营支撑系统(OSS)的后台服务器。

呼叫管理服务器（CMS）在IPCablecom网络中为媒体终端适配器（MTA）、接入节点和 PSTN 网关提供呼叫控制和信令相关的服务。CMS 是位于 IP 有线电缆网络中可管理 IP 部分的一个可信网络元素。**发布服务器**是逻辑网络元素，它根据网络中发生的事件播放信息音和消息。**信令网关**功能在 IPCablecom 网络边缘发送和接受电路交换网络的信令。对于 IPCablecom 系统，信令网关的功能只是用七号信令 SS7（多频语调的设备关联信令直接由媒体网关功能来支撑）的形式支撑非设备关联信令。媒体网关控制器（MGC）接收并中介 IPCablecom 网络与 PSTN 网络之间的呼叫信令信息，负责维护并控制请求与 PSTN 网络互联的呼叫的所有呼叫状态。媒体网关（MG）作为 PSTN 网络和 IPCablecomIP 网络之间的连接转换器。每一个转换器作为一个端点，根据媒体网关控制器的指令与 IPCablecom 网络上的其他端点建立并控制其媒体连接。同时，媒体网关控制器向媒体网关发出指令，要求其探测并生成与呼叫状态相关的事件和信号，而这些呼叫状态是媒体网关控制器已知的。**运营支撑系统后台**包括支撑核心商业流程中的商务、服务和网络管理组件。运营支撑系统的主功能区是故障管理、性能管理、安全管理、计费管理和认证管理。IPCablecom 系统定义了一个有限的运营支撑系统功能组件有限集合，支撑媒体终端适配器（MTA）设备的提供和载有记费信息的事件消息。

6.2.1 IP 有线电缆通信系统的安全问题

每个 IPCablecom 系统的协议接口常遭受对用户和服务提供商都构成安全风险的威胁。例如，媒体流通道可能穿越大量潜在未知的互联网业务和骨干服务提供商的线路。结果，媒体流将会很容易受到恶意窃听从而致使通信秘密受到损失。

6.2.2 IP 有线电缆通信系统的安全机制

IP 有线电缆系统的安全性是在底层堆栈基础上实现的，因此大部分使用 IETF 定义的机制。IPCablecom 系统架构详细介绍了这些威胁，对每一个已定义的协议接口，底层的安全机制（例如 IPSec）提供了安全服务要求的协议接口。在 X.805 体系结构中，IPCablecom 系统安全服务的整体概貌给出了如图 1 所示的三个位面和层次的所有九个单元。例如，IPSec 支持的控制层面的信令协议簇的服务。通过使用第三版的 SNMP 实现了管理框架的安全。

通过 IPCablecom 系统的核心服务层实现的安全服务是认证、访问控制、完整性、机密性和不可否认。IPCablecom 协议接口可以使用零、一种或多种这些服务来表述它们的特殊安全要求。

IPCablecom 系统的安全性通过以下每组协议接口的安全性要求来表述：

- 确定每组协议接口的威胁模型；
- 明确针对威胁所要求的安全服务（认证、授权、机密性、完整性和不可否认）；
- 详细说明提供指定安全服务的特殊安全机制。

这些安全机制既包括安全协议（例如，IPSsec、RTP 层安全和 SNMP 第三版安全性）也包括支持密钥管理协议（例如，IKE，PKINIT/Kerberos）。同样，IPCablecom 系统核心安全服务包括为提供端到端 RTP 媒体流加密的机制，这样可以充分减少对通信秘密的威胁。图 12 概括描绘了 IP 有线电视通信系统的所有安全接口。如果没有涉及密钥管理协议，这意味着此时它对于那个接口不是必需的了。IPCablecom 系统中没有安全性要求的接口在图 12 中没有给出。

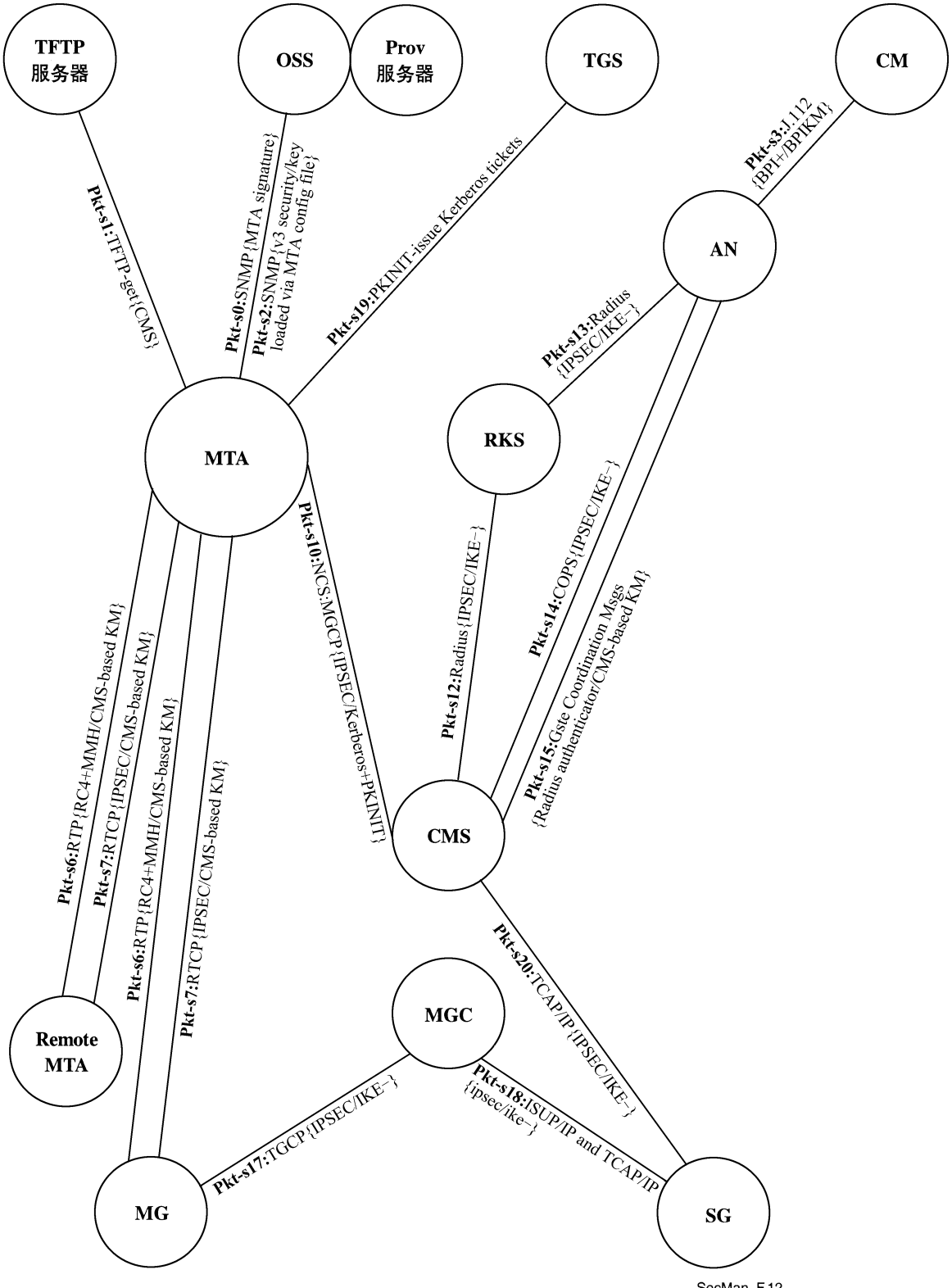
IP 有线电视通信系统安全体系结构把设备的提供分成三个不同的动作：用户登记、设备提供和设备认证。**用户登记**过程建立一个永久的用户计费帐户，这个帐户通过 MTA 的序列号或 MAC 地址独一无二的将 MTA 认证到 CMS。这个计费帐户同样被用来识别用户为 MTA 预定的服务。用户登记可以是在带内或是在带外（in-band or out-of-band）。用户登记过程的有效说明已超出了 IPCablecom 系统而且对每一个服务提供商都可能不一样。对于*设备提供*，MTA 设备验证通过第一次在自身和提供服务器间形成第三版 SNMP 安全性 5（使用 Kerberos 认证和密钥管理）下载配置文件的真实性。提供服务器提供附有本地配置文件的 MTA，和散列配置文件。MTA 找回配置文件、执行散列配置文件并且比较由备份服务器给出的结果。如果散列函数匹配，配置文件则被认证。为保证通信秘密（为了安全地将配置文件加密密钥传送到 MTA 必须启用第三版 SNMP 通信秘密），配置文件可能被选择性加密。*设备授权*提供的 MTA 设备向呼叫管理服务器、证明自己的身份，并在满负荷工作前与该服务器建立安全联系。设备授权使后发的呼叫信令在已建立安全连接的情况下得到保护。

信令的传送和媒体流都是受到保护的。对所有的信令传送来说，如 QoS 信令、呼叫信令以及 PSTN 网关接口信令，都受到 IPsec 协议的保护。与 IPsec 安全相关的管理可以通过采用两个密钥 Kerberos/PKINIT 和 IKE 的管理协议来实施。Kerberos/PKINIT 是用来在 MTA 客户端和其 CMS 服务器之间交换的两个密钥，而 IKE 则是用来管理所有其他信令的 IPsec SAs。至于媒体流，每个媒体的 RTP 包都要单独加密，并经过认证来核实其是否是完整和原始的包。尽管 AES 是目前最适用的加密算法，但所有的 MTA 都有能力成为特殊加密算法。每一个 RTP 包都含有随机的信息认证编码（MAC）。同样，尽管 MMH 是目前指定的加密算法，但 MAC 也将有机会被采用。MAC 计算覆盖包的无加密的字头段和加密负荷。

加密码和 MAC 算法的密钥均源自端到端密码和随机数，它们在传送和接收 MTA 之间作为呼叫信令的一部分进行交换。因此，媒体流密钥交换的安全是通过呼叫信令的安全性来保障自身安全的。

同样，运营支撑系统（OSS）和计费系统也规定了安全性要求。在 IPCablecom 设备里，SNMP 代理在运行 SNMP 第三版（SNMPv3）。SNMPv3 用户安全模型[RFC 2274]给出了针对 SNMP 流量的认证和加密服务。SNMPv3 基于浏览的访问控制[RFC 2275]可以用来对 MIB 对象实施访问控制。

IKE 密钥管理协议的作用是在记录保持服务器（RKS）和每个生成事件消息的 IPCablecom 网元之间，进行加密和密钥认证。网络 IPSec 安全联系建立后，这些密钥必须在每个 RKS（主要、次要，等等）与每个 CMS 和 AN 间生成。MGC 和 RKS 间的密钥交换可能存在，并且留给了 IPCablecom 第一阶段的厂商去解决。事件消息是通过 RADIUS 传输协议从 CMS 和 ANS 发送到 RKS 的，该协议本身由 IPsec 实施保护。



IKE−　　采用预先共享密钥的IKE
IKE+　　IKE要求公开密钥证书
CMS-based KM　　密钥采用CMS随机生成和分发

图 12
IPCablecom 安全性接口
(labelled as <label>: <protocol> { <security protocol> / <key management protocol> })

6.3 安全传真传送

传真是一种非常普遍的应用。最初规定是在 PSTN(ITU-T T.4)上传输，然后是在 ISDN(ITU-T T.6)上传输，最近它被扩展到在 IP 网络（含互联网）上利用 ITU-T T.37 进行非实时业务传输（邮件转发）和利用 ITU-T T.38 进行实时(用 RTP)业务传输。无论是 PSTN 还是 ISDN 或 IP 网络，传真传输面临的两个典型安全问题是一连接认证（有时候是不可否认性）和传输数据的机密性。由于 IP 网络的分布式特点，T.37 和 T.38 让上述问题变得更为重要了。

ITU-T T.36 定义了两个独立的技术解决方案，可以被用在安全传真传送的内容中实现对被交换文件的加密。这两个技术解决方案是基于 HKM/HFX40 算法（附件 A/T.36）和 RSA 算法(附件 B/T.36)。即使上述两种算法都限定会话密钥不能超过 40 位（源于 1997 年通过上述建议书时，国家法规中的规定），也应为需要较长密钥的算法规定一个产生冗余会话密钥的方法（在 40 位会话密钥的基础上）。附件 C/T.36 描述了通过实体 X 和 Y 间的注册方法或通过在实体 X 和 Y 之间安全密钥传输为传真终端提供安全密钥管理能力的 HKM 系统使用情况。附件 D/T.36 给出了利用 HFX40 传输密码系统为传真终端提供消息机密性的整个过程。最后，附件 E/T.36 描述了 HFX40-I 散列算法，使用散列算法，在传真终端间交换必要的计算和信息来实现传真消息的完整性，从而作为一种被选择的或提前设定的方法来实现消息的加密。

最后，附件 E/T.36 描述了为发送的传真报文提供完整性的 HFX40-I 散列算法，作为一种选定的或事先编程的替代报文加密算法，内容包括算法的使用、必要的计算和传真终端间要交换的信息。

此外，T.36 定义了以下安全服务：

- 相互认证（强制的）；
- 安全服务（可选的），包括相互认证、消息完整性和消息接收确认；
- 安全服务（可选的），包括相互认证、消息机密性（加密）和会话密钥设施。
- 安全服务（可选的），包括相互认证、消息完整性、消息接收确认、消息机密性（加密）和会话密钥设施。

基于以上这些安全服务定义了四个服务简表，如下表 2 所示。

表2

附件 H/T.30 中的安全简表

安全服务	安全简表			
	1	2	3	4
相互认证	X	X	X	X
• 消息完整性 • 消息接收确认		X		X
• 消息机密性（加密） • 会话密钥设施			X	X

6.3.1 使用 HKM 和 HFX 的传真安全

霍索恩密钥管理（HKM）和霍索恩传真密码（HFX）组合系统为实体间（终端或终端制造商）的安全文件通信提供如下能力：

- 实体相互认证；
- 秘密会话密钥设施；
- 文件机密性；
- 接收确认；；
- 文件完整性的确认和否认；

密钥管理是通过附件 B/T.36 中定义的 HKM 系统提供的。 B/T.36.定义了两个过程：第一个是注册，第二个是秘密密钥的安全传输。 注册建立了共有密钥和安全地提供了所有后续传输。在后续传输中，HKM 系统提供了相互认证、为保证文件机密性和完整性的秘密会话密钥、接收确认及文件完整性的确认和否认。

文件机密性通过附件 D/T.36 中定义的传输密码（carrier cipher）获得。传输密码使用 12 位的十进制数字密钥，这个密钥与 40 位会话密钥大致相同。

文件的完整性利用附件 E/T.36 中定义的系统获得，而建议书 T.36 中定义了散列算法，包括有关的算法和信息交换。

在注册模式中，两个终端交换唯一识别对方的信息。这是一次性秘密密钥用户间达成的协议。每个实体都存储着与其唯一相关 16 位数，该实体利用这个数字完成注册。

当需要安全传输一个文件时，传送端向接收端传送一个与接收端相关的 16 位秘密数字、一个随机数以及一个加密的会话密钥作为接收端的口令。接收端向传送端传送一个与传送端相关的 16 位数字钥、一个随机数以及传送端发出的口令再加密版本，同时它传送一个随机数和一个加密的会话密钥作为给传送端的口令。传送端回应一个随机数和从接收端返回口令的再加密版本。通过这个过程，两个实体间实现了相互认证。同时，传送端传输一个随机数和加密会话密钥来实现加密和散列编码。

文件传输后，传送端向接收端传送一个随机数和一个加密会话密钥作为接收端的口令。同时，传送一个随机数和加密的散列值，使得接收端能确保接收文件的完整性。接收端向传送端传送一个随机数和传送发出的口令的再加密版本，同时，传送一个随机数和加密的“完整性文件”信息作为传输文件完整性的确认或否认。散列算法在整个文件传输的过程中被用来保证文件的完整性。

还有一种不涉及实体间安全信号交换的超越模式。用户同意人工输入一次性秘密会话密钥。传送端利用这种方式完成对文件的加密，而接收端利用这种方式完成解密。

6.3.2 使用 RSA 的传真安全

附件 H/T.30 规定了给出了基于 RSA 加密机制安全特征的机制。Rivest, Shamir & Adleman (RSA) 算法详见[ApplCryp,466 至 474 页]。具有安全特征的传输文件的编码方案可以是建议书 T.4 和 T.30 中定义的任一种。（改进的 Huffman、MR、MMR，附件 D/T.4 定义的字符集、BFT、附件 C/T.4 中定义的其他文件传输模式）

数字签名（认证和完整类型业务）的基本算法是采用一对“公开密钥/秘密密钥”的 RSA 算法。

如果是提供任选的机密性服务的话，含有加密文件用会话密钥“Ks“的令牌也用 RSA 算法加密。在这种用途中，各密钥（“加密公开密钥”/“加密秘密密钥”）的关系不同于认证和完整性类型的服务所用的密钥。这两种用途要分清。

ISO/IEC 9796（具备消息恢复功能的数字签名方案）中描述了用在附件 H 中 RSA 的使用方法。

为加密包含会话密钥的令牌，处理 RSA 算法时的冗余规则与 ISO/IEC9697 的规定相同。值得注意的是一些主管部门除了需要 RSA 外，还需要采用*数字签名算法*（DSA）机制[ApplCryp, pp-483-502 页]。

在附件 H/T.30 的方案中，默认的方式不是使用*认证中心*。然而它们可以被用于保证传真消息发送者公钥的合法性。在这种情况下，公钥可以用建议书 X.509 中指定的方法来鉴定。附件 H 中描述了传送端传输公钥证书的方法，但是证书的精确格式被留在日后研究并且证书的实际传输在协议中进行协商。

作为一个强制特征，提供了一个*注册模式*。它允许发送者和接收者在两方间的任何安全传真通信之前信任地注册和存储对方的公钥 。注册模式能够避免用户在终端上人工输入通信另一方的公开密钥（公钥长 64 字节或更长）。

因为注册模式允许交换公钥并把它们存储在终端中，因此没有必要在传真通信中传输它们。

就像在该附件中描述的，一些签名要根据散列函数的结果上。

散列函数能被用在（SHA-1，*安全散列算法*）一个来自美国国家标准和技术学会的算法或 MD5（RFC 1321）。对 SHA-1，散列运算结果的长度超过 160 位，而对 MD-5，散列运算结果的长度超过 128 位。符合附件 H/T.30 的终端可以使用 SHA-1 或 MD-5 或两个算法共用。两个算法的使用将在协议中进行讨论（见后面内容）。

机密性服务的数据加密是可选的。附件 H/T.30 种记录了五个可选的加密方案：FEAL-30、SAFER K-64、RC5、IDEA 和 HFX40(就像建议书 T.36 中描述的)。在一些国家这些方案的使用可能要受国家法规的约束。

还有其他一些算法可以使用。它们是 ISO/IEC9979（注册加密算法的过程）中给出的。

终端处理这些算法之一的能力和在通信过程中一种特定算法的实际使用将在协议中进行讨论。利用会话密钥进行加密。会话密钥的基本长度是 40 位。对于使用 40 位会话密钥的算法(例如 HFX40)，会话密钥“Ks”实际上被用作加密算法中的密钥，对于要求密钥超过 40 位的加密算法（例如，FEAL-32，IDEA，SAFER K-64 分别要求：64 位，128 位和 64 位），可以利用冗余机制获取必要长度的密钥，最后生成的密钥被称为“冗余会话密钥”， “冗余会话密钥”是在加密算法中实际使用的密钥。

6.4 网络管理应用

在对安全框架的需求一章中已注表明，有必要保护用于监视和控制通信网络的管理流量。管理流量通常按照完成错误、配置、性能、审计和安全管理功能所需的信息进行分类。安全管理领域既涉及安全管理网络的建立，也涉及安全体系结构三个层面的相关信息的管理。本节描述的是后者。

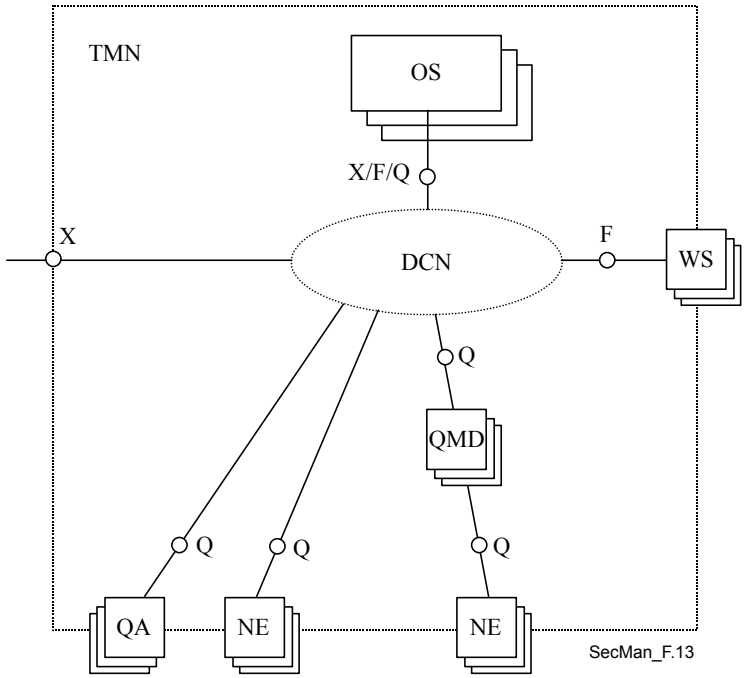
在传统通信网络中，管理流量通常是在一个只承载网络管理流量而没有用户流量的独立网络上传输。这个网络通常被称为是在 ITU-T 建议书 M.3010 中描述的电信管理网络（TMN）。 TMN 是被分隔和独立于公众网络基础设施，因此任何由于公众网络用户层面安全威胁的破坏不会扩散到 TMN。这种分离的结果是相对容易保护管理网络流量，因为接入这个层面是只限于授权网络管理员，服务也仅限于有效的管理活动。随着下一代网络的引入，用户应用的流量有时可能又会和管理流量混在一起。虽然这个方法只需要一个单一的综合网络基础设施，最大限度地降低了成本，但它也引入了许多新的安全挑战。用户层的这些威胁现在成为了管理和控制层的威胁。管理层现在成为多数用户都能访问的，同时多种恶意活动都成为可能。

为了提供一个完整的端到端解决方案，每一类型网络活动（例如管理平面活动、控制平面活动和用户平面活动）都要采取各种安全措施（例如访问控制、认证）对于网络结构、网络服务和网络应用。已经制定了若干 ITU-T 建议书，具体讨论管理平面的安全问题，涉及作为网络基础设施一部分的网元（NE）和管理系统（MS）。

6.4.1 网络管理体系结构

如下所述，维护电信基础设施所需的管理信息的保护标准已制定了不少，但管理不包括另外一个方面，就是与环境有关，不同的服务提供都要在这个环境中相互合作以提供端到端用户服务，好跨越地理边界给客房提供租用线，或者与支撑灾害恢复的管制体制或政府体制有关。

这个体系结构是用来定义了在建议书 M.3010 中被定义的通信网络网络管理和物理体系结构如图 13 所示。管理网络定义了决定在不同层次上执行 OAM&P 功能的交换的接口。



接口
DCN 数据通信网
NE 网元
OS 操作系统
WS 工作站

图 13
M.3010 中物理体系结构的例子

从安全的观点，对不同接口的需求不同。Q 接口在一个单独的管理域中，而 X 接口位于可能属于不同服务提供商的不同管理域。虽然 Q 接口和 X 接口都需要安全服务，但 X 接口要求的反制措施是更为稳固和必要的。ITU-T M.3016 概述了这些接口的安全危胁弱点和安全措施，而 ITU-T M.3320 则详细描述了 X 接口的具体问题。对不同通信层的协议问题在 ITU-T Q.811 和 Q.812 中进行了详细描述。

在管理范畴内讨论安全时涉及两方面。一是端到端活动的管理层（例如，VoIP 业务）。管理用户的管理活动必须用安全的方式来实现。这涉及到为部署端到端的应用在网络上交换的管理信息的安全。第二点是安全信息的管理。不论什么业务，例如 VoIP 或两个服务提供商间的故障报告活动，像加密密钥的使用这样的安全措施都应该被管理。这就是常说的安全信息的管理。前面定义的 PKI 就是这方面的一个例子。ITU-T M.3400 定义了若干与这两方面都相关的功能。

已经根据 X.805 的框架制定了若干建议书，涉及管理层面三个单元的管理功能。下面几节对这些建议书做了说明，并介绍这些建议书是如何讨论安全需求的。除了管理层三个层次的建议书外，还有其他建议书定义一般的或普通的服务，例如存在物理安全破坏时的报告警报、审计功能和为不同目标（例如，管理实体）定义保护等级的信息模型。

6.4.2 管理平面和基础设施的交叉

这个单元介绍了如何保护网络基础设施元素的管理活动，也就是传输和交换元素及连接这两种要素的链路，还有终端系统，如服务器。提供网络元素的活动必须由受权用户完成，就是一个例子。端到端的连通性可以按接入网和核心网未考虑。这些网络可能使用了不同的技术。已经制定了建议书，对接入和核心网都做了介绍。这里讨论的一个例子就是用于接入网的宽带无源光网络（BPON）。这种接入网络用户特权的管理是用在建议书 Q.834.3 中的统一模型方法学定义的，而采用 CORBA（公共对象请求代理体系结构）的管理交换则在 Q.834.4 中做了具体规定 。在这些建议书中描绘的接口就是图 13 中所示的 Q 接口。它应用在元素管理系统和网络管理系统之间。元素管理系统被用来管理单独的网络元素和由此知道由一个或多个供应商提供的硬件和软件体系结构的内部细节，然而网络管理系统是在端到端网络层面上执行活动并涉及多供应商管理系统。图 14 说明了为元素管理系统的用户创建、删除、分配和使用访问控制信息的各种对象。用户许可清单包含对每个受权用户的许可管理活动清单。访问控制管理器验证管理活动用户的用户标识符和密码并授权对许可清单中允许的功能的访问。

6.4.3 管理平面和服务层的交叉

管理层和服务层的交叉适合保护为提供商传输服务而提供的监视和控制网络资源。ITU-T 建议书为这个交叉点介绍了两方面。一方面是确保网络提供的服务有适当的安全措施。这方面的一个例子就是只有合法的用户允许执行与提供服务相关的操作。第二个方面就是定义了合法的管理和操作交换信息。这样的规定有助于检测安全破坏。当有安全破坏时，通常使用特定的管理系统来进行管理。

一个建议书介绍的第一个方面服务管理活动的例子，是关于连接管理的 ITU-T M.3208.2。拥有预先提供的链路服务客户使用这种服务来形成一个端到端的租用电路连接。这种连接管理服务允许用户在预先提供的资源的范围内建立/激活、修改和删除专用电路 。由于用户提供端到端的连接，有必要确保只有受权用户被允许执行这些操作。为与这个服务相关的管理活动定义的安全尺度是在 2.5 节中讨论的八个方面的一个子集，包括对等实体认证、数据完整性控制（防止在传输中非经授权修改数据）和访问控制（为确保一个订户不能恶意地或无意地访问另一订户的数据）。

ITU-T M.3210.1 是定义与无线服务管理层相关的管理活动建议书的一个例子。这相当于上面讨论的第二个方面。

在一个无线网络中，当用户从归属网络漫游到访问网络时，它们可以在不同的管理域间移动。在 ITU-T M.3210.1 中定义的这些服务描述了归属地的虚拟管理域如何在用户在被访问网络注册开就收集关于用户的适当信息。图 15 中的 a)和 b)项描述了在归属网络或在被访问网络中监视管理活动的产生。

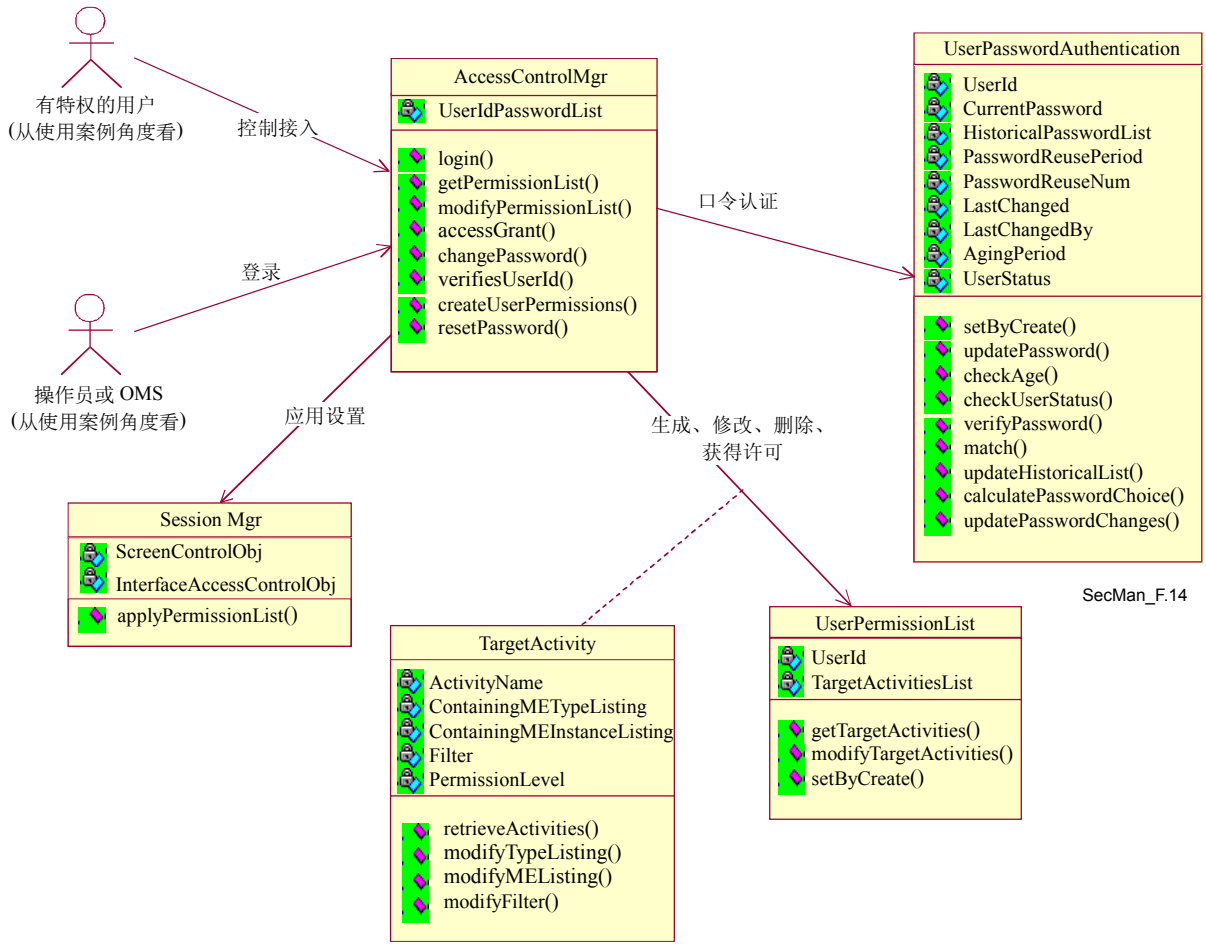


图 14
Q.834.3 中的用户特权管理

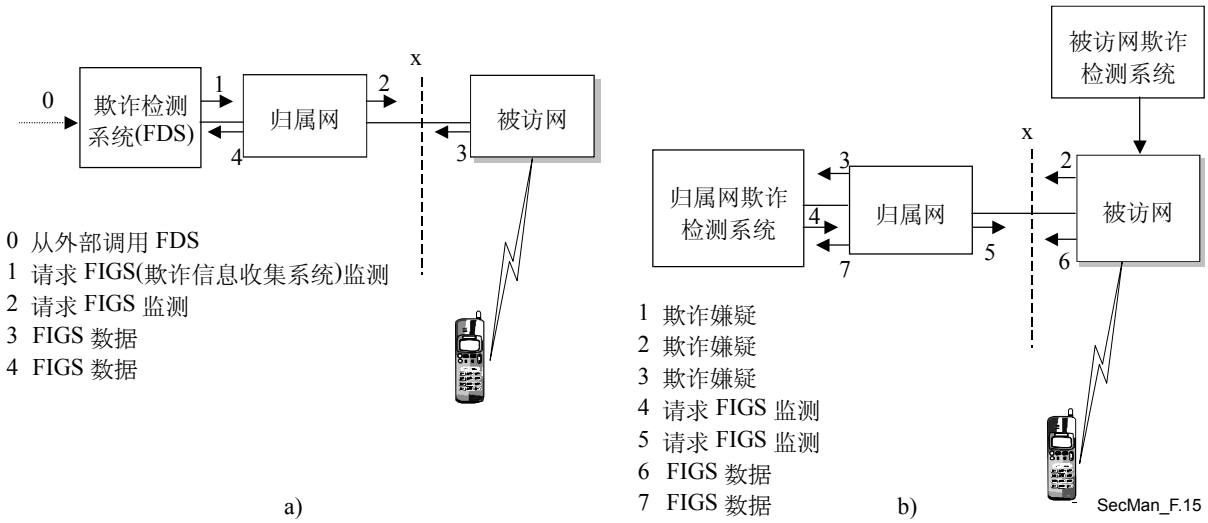


图 15
建议书 M.3210.1 中的无线服务虚拟管理

6.4.4 管理平面和应用层的交叉

管理平面和应用层的交叉是第三单元，与保护基于网络的端用户应用是一致的。例如报文消息和号码簿应用已经在 X.400 和 X.500 系列建议书中定义了。

另一类需要管理活动的应用是管理应用本身。这种表述有些繁琐，最好使用例子进行说明。这种应用的最终用户是服务提供商管理部门的管理（操作）人员。考虑一个服务提供商为了提供端到端的连接服务使用其他服务提供商的连接服务情况的情况。根据管制或市场环境，一些服务提供商可以提供接入服务，其他局间运营商可以提供长途连接。局间运营商从本地服务提供商那儿租来接入服务以提供跨地区的端到端连接。在出现业务损失时，采用叫做故障报告管理的管理应用在管理系统间报告故障。这些系统的用户和这个应用本身为了报告业务故障而要求授权。受权的系统和用户应该检索已报告的故障的状况。图 16 说明了必须用安全方式执行的相互作用。类似于电子邮件应用的邮箱管理，要对访问特权加以管理，防止未经授权访问的故障报告。一个服务提供商只允许报告其租用业务的故障而不是其他提供商租用的。

建议书 X.790 定义的这个管理应用和使用例如访问控制列表和双向认证的机制保护保护这些活动。这种应用和认证安全机制已经用这些建议书实现和部署了。

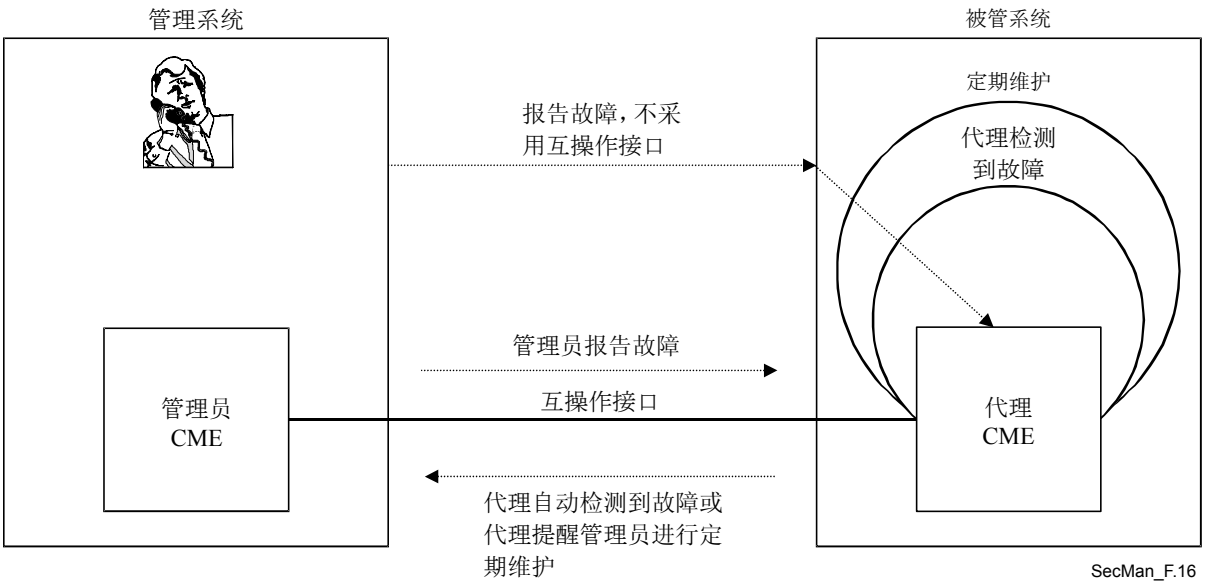


图 16
ITU-T X.790 规定的故障管理报告的产生

6.4.5 通用管理安全服务

建议书 X.736、X.740 和 X.741 定义了在公共管理信息协议（CMIP）用于接口时，适用于管理层所有三个单元的公共服务。X.736 定义了物理安全破坏等事件类型，这些事件类型的报警都被报告给管理系统。这是一种管理平面活动，能够在非授权用户获取完成网元的提供活动的权力和成为服务或邮箱的预订用户时，用来报告安全破坏事件。X.740 定义的审计功能描述了安全破坏事件日志记录并能被应用于所有三层。 X.741 定义了一个非常普遍和详尽地允许为独立于目标的管理活动而指定访问控制优先权的模型。该模型用非常精细的目标属性层次规定了分配特权的能力，因而特性非常丰富。

ITU-T 建议书 Q.816 也采用了在对象管理组织（OMG）论坛使用 CORBA 范例为管理活动定义的普通安全服务。

6.5 E处方

卫生保健的提供需要并产生了大量数据和信息。这些数据和信息需要安全地被收集、处理、分发、访问和使用，并遵守严格的道德和法律规则。这对临床和管理信息对例如流行病、文献和知识数据库信息等其他类型的信息也很重要。

这些类型的数据、信息的源头处在卫生保健基础设施内外，位于与各自用户远近不同的地方。实际上，用户需要和产生综合这些类型的信息和在不同阶段各自的功能，例如一个医生可以在检查一个患者时参考知识数据库和访问可以用于计费的病人的记录。

卫生保健就诊和处置是多面的。例如，它们发生在医患之间；在两个医生之间；在医生和一个专业咨询者之间；在一个患者和一个像测试实验室、制药机构和康复中心等健康机构之间。这种就诊可能发生在所在社区、在国家的另一地区或国外。所有这些遭遇都在实际开始前需要数据和信息，同时在就诊期间或其后产生同样的数据和信息。这样的数据和信息可能数量不同，时间不同，形式不同，如声音、数字、文本、图表和静态或动态的图像等不同的形式，同时经常是上述情况的有机结合。

这些数据和信息的原始资料和知识库可能坐落在不同的地方，也可能采用不同的形式，例如，完整的病历、手写的处方和医生、咨询者或实验室的报告。

传统上讲，所有这种就诊都是面对面的，口头和书面语言是交流和保存病案的主要形式。的词汇，运输时主要是使用公路、铁路和空运等公共和私人服务。随着电话业务网络的发展，这种网络成为了健康专家和机构国内及国际通信的网络，直到健康信息通信服务等现代工具发展和成长起来。

技术在卫生保健机构的临床/医学部分的应用越来越多，包括仪器和设备、特别是传感和测量设备、实验室业务、静态和动态成像。随着这些技术使用的增多以及这些技术的种类和复杂性的提高，这种技术服务从主流卫生保健机构中分离出去是不可避免的，不仅是从距离上分离出来，更明显地是从管理上分离出来。因此，这样以技术为基础的机构和主流卫生保健机构间的通信成为这类机构在效益和经济方面要考虑的重要问题。

卫生部门普遍使用信息通信技术（ICT）是从 25 年前使用简单的电子报文发送（电子邮件）传输纯字符的短信和报告开始的。正像语音通信是医生的诊所和卫生保健机构里安装电话的主要动力，电子邮件是最初安装现代通信链路最初的理由。同时，随着电子邮件服务的增长，对齐的性能和地理覆盖的需求也在增长：更多的地方以更快的速度用更多的带宽以适应不断增多的电子邮件附件。

在过去的十年，卫生部门对电子邮件，特别是经由互联网的电子邮件的使用量几何级数增长，在一国之内国家之间，甚至在最贫穷的国家，情况都是如此。例如，电子事务处理取代了并非确实需要当面就诊的那些功能，如书写和发送处方和报告，安排预约和服务日程，分诊，在电信服务性能许可时还要传输医学图像和与之相关的专家的书面或口头解释。

信息通信技术另一类复杂的用途是远程程序，就是“用视、听和数据通信提供医疗”，包括对远在外地的病人进行实际诊断、检查甚至治疗。远程医疗是一个正在增长的重要领域，预计会让传统的医疗卫生方式产生许多变化；实际上它开启了医疗的一种新模式。

另一方面是访问和使用以知识为基础的系统，相对而言这并不是新东西，但会随着远程信息处理支撑技术的发展而得到有益的扩展。这类系统也叫做专家系统和决策支持系统，是就医学科学问题和程序提供专家建议和指导的系统。例如，在得到病人的依从性和症状后，就可以提供诊断支持、建议进行额外的测试和给出治疗方案。

以上介绍的所有进展，还对卫生部门需要和使用的相关管理信息系统（MIS）产生了很大的影响，如医院的管理信息系统。这些系统不再是医院治疗病人的行政管理系统，而是包括了各种方便医疗人员的智能界面，如到临床决定支撑系统的界面，到远程医疗链路的界面，到门户网站的界面等。

关于医疗人员和患者，还有两个大家认识到的现实情况应该提一下：移动性和对解放双手的需求，这样就可以专心于治疗本身。移动性意味着他们能够从建筑物内或城内的任何其他地点，也包括整个国内和两国之间任何其他地点，获得其所需的医学资料，如电子病历，或获得一件工具或仪器，必要时经过其验证。而解放双手这个特性意味着必须找到不同医疗人员人工干预的识别和授权解决方案，如开门或敲击计算机键盘。

因此，卫生保健部门是一个信息高度密集型的部门，收集、传输、处理、显示和分发健康和与健康有关的数据和信息，是卫生保健服务在一国之内和各国之间运转和发展的交通、效率性和经济性的关键所在。

一个至关重要的要求是所有这类流程必须安全和机密地被执行，同时必须严格地遵守道德和法律规则和规定。

6.5.1 E 健康应用中 PKI 和 PMI 考虑

通过把各认证中心连在一起，PKI 再造了现实世界的分级结构，无论是地理上的层次（区域－国家－省（市）－行政区），还是按科目分给（卫生－药品－外科－专科手术－供应商等）。此外，由于这样的事实，即卫生部门普遍存在，分等级设置，影响广泛，跨境合作越来越多，用于卫生的标准化的 PKI/PMI 的定义变得不可或缺了。

卫生系统的技术互操作必须通过技术标准的切实贯彻来保证。大部分安全解决方案提供者已经实施了象 ITU-T X.509 的标准。由于用户认证是一个依靠本地信息的重要应用，自由地选择一个特定的 PKI/PMI 不应影响与卫生部门用其他 PKI/PMI 认证的人进行户操作的能力（这自然涉及到关于访问控制和卫生部门其他相关政策的一个起码的最小标准）。为了做到这一点，可以采用不同的战略，包括相互认可不同的基础设施或采用公共根。技术标准的实施，不同基础设施的技术互操作性和一些政策的标准化将为全球卫生事务保证提供一个十分有效和综合的环境。

6.5.2 索尔福德 E 处方系统

[策略]中描述的 E 处方系统是电子医疗中应用 PKI 和 PMI 的很好的例子。考虑到英国参与电子传输处方（ETP）项目的专业人员众多（34,500 个普通参与者，10,000 个有处方权的护士过几年将增长至 120,000 个，44,000 个注册药剂师和 22,000 个牙医），而真正需要授权的极少（例如，各种不开处方、配药、免费处方权的许可级别），基于角色的访问控制（RBAC）似乎是 ETP 最好的授权机制。如果把这种机制与英国潜在的病人数量（6 千万）和免费处方量达到了总处方量的 85%这个事实[FreePresc]一并考虑的话，则在可能的情况下 RBAC 也应该用于控制获得免费处方。考虑到需要获得授权/准许的人员数量巨大，把角色管理分散到各主管机构而非试图将某集中是特别重要的，否则这个系统就无法管理了。

每一个专业人士都有一个授予他们在此专业领域从业的主管部门。在英国，公共医学委员会负责医生资格注册和由于读职而取消其行医资格。公共牙科委员会对牙医、护理和妇产委员会对护士、皇家药剂学院对药剂师都有同样的管理权。由于这些部门的管理职责都执行的很好，因此上述 ETP 系统中的角色分配分别被赋予这些部门。

2001 年 7 月，成立了劳动和保障部（DWP）接管了上届政府中的社会安全部、教育和就业部的职责。它负责支付失业救济金和养老金并处方药价格管理局（PPA）一道，确定免费处方的准许权。许多人获准享受免费处方药，包括：60 岁及以上的人、16 岁以下的孩子、16 至 18 岁受全日制教育的青年人，领取生活保障金或失业津贴的人或它们的家庭，被发给通用国家健康系统(NHS)低收入计划完全救助证书（HC2）的人，孕妇，去年一年内生产的妇女和。因此这个权利的管理被分配给 DWP 和 PPA 的不同部门。

每一个专业人士被他们的专业管理部门授予了一个从业范围的证书，这个证书被存储在属于该专业管理部门的 LDAP 目录中。ETP 系统如果能够访问 LDAP 目录，将能决定对开处方和配药的授权。与此类似，如果 DWP 将角色属性证书授予给了有资格根据不同条件领取免费处方药的人并将证书存储在他们的 LDAP 目录（或目录簇）中，然后 ETP 系统将能通过访问这个 LDAP 目录来决定免费领取处方药的权利，药剂师不再需要向患者询问他们的权利。后者只是在患者是第一次被授予证书时才需要，例如当一个孕妇刚被全科医生诊断为怀孕，而 DWP 又不能及时颁发官方属性证书时。

这些角色后来都被授权决策引擎（例如 PERMIS，见网站 www.permis.org）用于根据 ETP 政策来决定是否医生能开处方、药剂师能配药和患者能享受免费处方药。在初始化时，每个 ETP 应用（处方系统、配药系统、PPA 系统）读入 ETP 策略，然后当特定专业人士请求开处方或配药等，授权决策引擎会从相应的 LDAP 目录中提取人员的角色，并根据政策作出决定。因此用户可以获得多种应用，而他们所需要具备的。只是一对 PKI 密钥。角色属性证书的分发可以在没有用户的情况下自动进行，他们不需要担心他们如何或在哪被系统存储和使用。

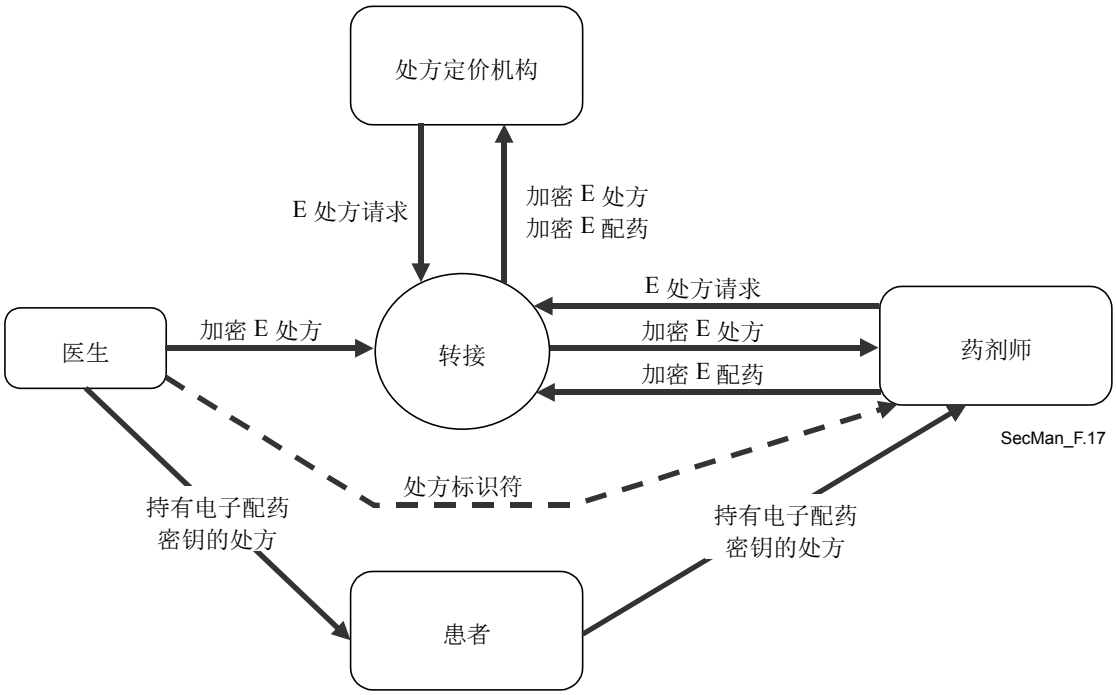


图 17
索尔福德 E 处方系统

图 17 显示了英国 E 处方系统的一个例子，它图示了系统实现中的几个关键安全问题。这个系统的核心是一个不仅提供强认证（例如，一个使用公钥证书的 PKI 系统）也提供强授权（例如，一个 PMI 系统）的安全基础设施，列出了医务专业人士被授予的权利的因为他们角色都储存在特征证书中。传统模型使用包含在每一个特定应用（例如病程记录、处方数据库、保险等）中的访问控制列表，要求用户（医生、药剂师、患者等）获取和管理几个不同的安全令牌（例如，用户名/密码，信用卡等）。在应用了 PKI 和 PMI 的新模型中，用户只需要一个令牌 — 用户的公共密钥证书 — 以便受益于地理上和/或拓扑分散的不同的服务和系统资源。用户属性证书由系统储存而不是由用户持有，而且只有授权的访问才能在使证书在两个组件中传输。由于属性证书是由签发者使用数字签名签发的，它们不可能在传输中被篡改。

在图 17 所示的例子中，E 处方由医生开出，数字签名（为了认证），使用一个随机会话密钥（为了机密性）对称加密，然后将 E 处方发送到一个存储中心。患者得到一个包含对称加密密钥条形码的纸质处方。然后患者选择一家药房，提交纸质处方，药剂师扫描条形码就得到了已解密的处方。与目前的纸质处方系统一样患者基本上控制有权按方抓药的人。但这还不够对谁有权开出何种药物及谁有权享受免费处方药进行控制也是必要的。

虽然上面的描述简要说明了一个紧密集成的系统，它可能实际上是分布式的，医生属性目录不同于认证药剂师或存储配药权和策略等的系统，该系统依赖于通过可信任的第三方来认证和授权不同的参与者。即使 PKI 和 PMI 专利解决方案是可用的，使用像 ITU-T X.509 这样的标准化解决方案使现在能更普遍和全球访问 E 处方。

7 结论

ITU-T 长久以来制定了一套关于安全的基础性建议书：X.800 是一个关于开放系统互联安全体系结构的参考文档，X.810-X.816 系列定义了一个安全框架，分别是开放系统的概述、认证、访问控制、不可否认性、机密性、完整性和安全性及审计警告。最近，ITU-T 建议书 X.805 描述了端到端通信系统的安全体系结构。X.805 提出的这种体系结构上的修订，修订考虑了随着多网络和多服务提供商环境的出现而增加的威胁和弱点。关于公钥和属性框架的建议书 X.509 的确是 ITU-T 在安全应用中引用最多的文本，其他以 X.509 原则为基础的标准或间接或直接地引用了该建议。

除了这些框架建议书外，ITU-T 已经通过它的建议书制定了几个系统和服务的安全管理规定。在本手册中，在第六章中已经描述了一些：使用 H.323 的 IP 语音业务或 IP 有线电视通信系统，安全传真传输和网络管理。还给出了公钥应用和 E 健康中特权管理的基础设施应用的例子。请注意，在 ITU-T 建议书还从更多的方面介绍了通信和信息技术的安全需求。这些问题以及在一些 ITU-T 研究组中还从更多的方面及例如欺骗预防、恢复和灾害恢复等方面的问题将在未来的版本中讨论。ITU-T 在安全方面的工作通过组织或参与国际安全研究会或讲习班、开发安全项目和在 ITU-T 中指定一个安全工作牵头研究组而得到加强 。

参考资料

本手册除了 ITU-T 建议书（在 www.itu.int/ITU-T/publications/recs.html 可以查到）外，还是用了下列资料。

[ApplCryp] B. Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] D. W. Chadwick; "The Use of X.509 in E-Healthcare", Workshop on Standardization in E-health; Geneva, 23-25 May 2003; PowerPoint at www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html and audio presentation at www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] M. Euchner, P-A. Probst; "Multimedia Security within Study Group 16: Past, Presence and Future", ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Free prescriptions statistics in the UK; www.doh.gov.uk/public/sb0119.htm

[Packetizer] "A Primer on the H.323 Series Standard" www.packetizer.com/iptel/h323/papers/primer/

[Policy] D. W. Chadwick, D. Mundy; "Policy Based Electronic Transmission of Prescriptions"; IEEE POLICY 2003, 4-6 June, Lake Como, Italy. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[SG17] ITU-T Study Group 17; "Lead Study Group on Communication System Security" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (*Section 2* on the Catalogue of ITU-T Recommendations related to Communications System Security; *Section 3* on Compendium of Security Definitions in ITU-T Recommendations)

[Shannon] G. Shannon; "Security Vulnerabilities in Protocols"; ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html

[Wisekey] S. Mandil, J. Darbellay; "Public Key Infrastructures in e-health"; written contribution to Workshop on Standardization in E-health; Geneva, 23-25 May 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

附件 A：安全术语

下列缩写和术语摘自相关的 ITU-T 建议书和其他外部资料，出处见下文中。附件 A.3 还给出了一些补充材料。

A.1 常用安全相关缩写

缩写	定义
3DES	[H.235] 三倍数据加密标准
A	[M.3010]代理
A/M	[M.3010]代理/管理员
AA	[X.509] 属性机构
AAA	[X.805] 认证认证、授权和计费
AARL	[X.509] 属性机构撤销列表
ACI	[X.810] 接入控制信息
ACRL	[X.509] 属性证书撤销列表
AE	[M.3010] 应用实体
AES	[H.235] [J.170] 高级加密标准算法
AH	[J.170] 认证报头是一种保证全部 IP 数据包消息完整性的 IPSec 安全协议，包括 IP 报头
ASCII	[T.36] 美国信息交换标准码
ASD	[J.170] 特定应用数据。IPSec 报头中的特定应用字段，和目标 IP 地址一起为每一个 SA 提供一个唯一的编号。
ASN.1	[H.680] 抽象句法记法一
ASP	[X.805] 应用服务提供商
ATM	[X.805] 异步传输模式
ATM	[M.3010] 异步传输模式
AuF	[H.530] 认证功能（参见 ITU-T 建议书 H.510 [6]）
B(n)	[T.36] 基值（n）
BE	[H.530] 边缘元素（参见 ITU-T 建议书. H.225.0 附件 G [2]）
BES	[H.235] 后台服务器
BML	[M.3010] 企业管理层
B-OSF	[M.3010] 企业管理层 — 操作系统功能
BPI+	[J.170] 基线保密接口+是运行在 MAC 层上的 J.112 标准的安全部分。
CA	[H.234] [H.235] [J.170] [X.509] 认证机构，即一个接受实体证书申请、认证申请、核发证书并保存与证书有关的状况信息的可信任组织。[J.170] 呼叫代理。CMS 中维护通信状态的部分，并控制通信中线路侧功能。
CARL	[X.509] 认证机构撤销列表
CBC	[H.235] [J.170] 密码模块链
CCA	[H.234] 国家认证机构
CFB	[H.235] 密码反馈模式
CH_n	[H.530] 质询数 n
CM	[J.170] 电缆调制解调器
CME	[X.790] 一致性管理实体
CMIP	[M.3010] 通用信息管理协议
CMIS	[X.790] 通用信息管理服务

缩写	定义
CMISE	[X.790] 通用信息管理服务要素
CMS	[J.170] 密码消息句法。[J.170] 呼叫管理服务器，用于控制语音通话链接。 在 MGCP/SGCP 术语中也称做呼叫代理(这是应用服务器的一个例子)。
CMTS	[J.112] 电缆调制解调器终接系统
CNM	[X.790] 客户网络管理
CORBA	[SANCHO] 通用对象请求代理体系结构
CRL	[H.235] [X.509] 证书撤销列表
DCF	[M.3010] 数据通信功能
DCN	[M.3010] 数据通信网
dCRL	[X.509] d-证书撤销列表
DES	[H.235] [J.170] 数据加密标准
DH	[H.235] [H.350] 迪菲—赫尔曼编码
DHCP	[J.170] [X.805] 动态主机配置协议
DIB	[X.509] 号码簿信息基
DIT	[X.509] 号码簿信息树
DN	[X.790] 著名的名字
DNS	[H.235] [J.170] [X.805] 域名服务器
DOCSIS	[J.170] 数据电缆传输服务接口规范
DoS	[X.805] 拒绝服务
DQoS	[J.170] 动态服务质量
DS-3	[X.805] 三级数字信号
DSA	[X.509] 号码簿系统代理
DSCP	[J.170] DiffServ 编码点。 每个 IP 包中用来确定 DiffServ 每跳性能 的一个字段。 在 IP v 4 中，TOS 字节被重新定义为 DSCP； 在 IPv6 中，服务类别八位字节用做 DSCP。参见 附件 C。
DSS	[H.235] 数字签名标准
DTMF	[H.235] [J.170] 双音多频
DUA	[X.509] 号码簿用户代理
EARL	[X.509]终端实体属性证书撤销列表
ECB	[H.235] 电子源码书模式
ECC, EC	[H.235] 椭圆曲线密码系统(参见 ATM 论坛安全标准 v1.1 中的 8.7 节)。一种公开密钥密码系统
EC-GDSA	[H.235] 与 NIST 数字签名算法 (DSA) 类似的带有附录的椭圆曲线数字签名(参见 [ISO/IEC 15946-2, 第五章])
ECKAS-DH	[H.235] 椭圆曲线密钥协议方案 — DH 。 使用椭圆曲线密码的 DH 密钥协议方案。
EML	[M.3010] 要素管理层
EOFB	[H.235] 增强 OFB 模式
E-OSF	[M.3010]要素管理层-操作系统函数
EP	[H.235] 终点
EP_{ID}	[H.530] MT 终点标识符, 参见 ITU-T 建议书 H.225.0 [1]
EPRL	[X.509]终端实体公开密钥证书撤销列表
ESH	[T.36]加密扰码普通散列值（24 位的十进制数）
ESIM	[T.36] 加密扰码完整性消息。一个 12 位的十进制数
ESP	[J.170] IPSec 封装安全
ESSK	[T.36] 加密扰码秘密密钥。一个 12 位的十进制数

缩写	定义
FDS	[M.3210.1] 欺诈探测系统
FEAL	[T.36] 快速数据加密算法。快速数据加密算法通过使用一个 64 位的秘密密钥把 64 位明文映射为 64 位的密文块，它与 DES 非常相似，但是功能要简单很多。简单快速的设计，使它非常适合于简单的微处理器（如智能卡）。 (A. Menezes 等, 应用密码技术手册，CRC Press, 1997)
FIGS	[M.3210.1] 欺诈信息收集系统
FQDN	[J.170] 完全合格域名。 详情参考 IETF RFC 821。
FTP	[X.805] 文件传输协议
FU	[X.790] 功能单位
GCA	[H.234]通用认证机构
GDMI	[M.3210.1] TMN 管理接口定义的指导方针
GDMO	[M.3010]管理对象定义的指导方针
GK	[H.235] [H.510] [H.530] 网守；网闸
GK_{ID}	[H.530] 被访问网守标识符，参见 ITU-T 建议书 H.225.0 [1]
GNM	[X.790] 通用网络模型
GRJ	[H.530] 网守拒绝
GRQ	[H.530] 网守请求
GW	[H.235] 网关
h[*]	[H.234]将***代入**函数 h 得到的结果
H-BE	[H.530] 归属 BE
HFC	[J.165]光纤/同轴混合缆
HFX	[T.30] [T.36] Hawthorne 传真密码
H-GK	[H.530] 归属 GK
HKM	[T.30] [T.36] Hawthorne 密钥管理算法
HKMD1	[T.36] HKM 算法双编加密
HLF	[H.530] 归属位置功能
HMAC	[J.170] 散列消息认证码。一种消息认证算法，基于 SHA-1 或 MD5 散列，在 RFC 2104 中定义.
HMAC-SHA1-96	[H.530]采用安全散列 算法 1 的散列消息认证码
$HMAC_Z$	[H.530] 散列消息认证码/用共享秘密 Z 来响应,，如果没有给出共享密秘 Z，则用下一跳的秘密。
iCRL	[X.509] 间接证书撤销列表
ICV	[H.235] 完整性检验值
ID	[H.235] 标识符
IDEA	[T.36] 国际数据加密算法，是 Xuejia Lai 和 James Massey 在 1992 年提出的一种加密算法，使用了 128 位密钥的块密码（64 位的块和 128 位密钥），被普遍认为安全性非常之高，是一种著名的算法。在它投入使用的几年中，除了几次尝试性的攻击，没有关于实质性攻击的报告 (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html)。
Idx	[T.36] X 的传真标识(传真电话号码) 的后六位
Idy	[T.36] Y 的传真标识(传真电话号码) 的后六位
IKE	[J.170] 互联网密钥交换，是用于协商并为 IPSec 的 SA 产生密钥的一种密钥管理机制。
IKE–	[J.170] 用来表示采用准共享密钥进行互联网密钥交换来实现认证的的规定的记法。

缩写	定义
IM	[T.36]完整性信息，用来确认或否认接收信息的完整性（12 位的十进制数字）
IMT-2000	[M.3210.1] 国际移动电信 2000
Imy	[T.36] Y 生成的完整性信息，用来确认或否认接收信息的完整性（12 位的十进制数字）
IN	[M.3010] 智能网
IP	[X.805] 网际协议
IPSec	[H.235] [H.530] [J.170] [X.805] 互联网安全协议
ISAKMP	[H.235] 互联网安全联系密钥管理协议
ISDN	[M.3010] 综合业务数字网
ISTP	[J.170] 互联网信令传送协议
IV	[H.235] 初始化向量
IVR	[J.170] 交互式语音应答系统
K	[H.530] 动态会话/链路密钥
KDC	[J.170] 密钥发布中心
LAN	[M.3010] 本地网
LDAP	[H.235] 轻量级号码簿访问协议
LLA	[M.3010] 逻辑分层体系结构
MAC	[H.235] [J.170] 消息认证码。与一条消息一同发送的固定长度的数据项目，用来确保消息的完整性，有时也记做 MIC。 [J.170]媒体接入控制，是数据链路层的子层，通常运行于物理层之上。
MAF	[M.3010] 管理应用功能
MAN	[M.3010] 城域网
MAPDU	[X.790] 管理应用协议数据单元
MCU	[H.235] 多点传送单元. [H.323] 多点控制单元
MD5	[H.235] [J.170] 五号消息摘要
MG	[J.170] 媒体网关
MGC	[J.170] 媒体网关控制器
MGCP	[J.170] 媒体网关控制协议
MIB	[J.170] [M.3010] 管理信息数据库
MIS	[M.3010]信息管理服务
MO	[M.3010] 被管理目标
mod n	[T.36] 以 n 为模数的模算法
MPS	[H.235] 多有效负载流
MPx	[T.36] X 的共有原语。一个只由 X 产生的 16 位的十进制数。X 的共有原语是采用 HKM 算法产生的，该算法使用了由 Unx、UCNx、Idx 和 Idy 形成的原语。
Mpy	[T.36] Y 的共有原语。
MRP	[H.530] 移动性选路代理
MS	[M.3210.1] 管理服务
MSB	[J.170] 最高有效位
MT	[H.530] 移动终端，参见 ITU-T 建议书 H.510 [6]
MTA	[J.170] 媒体终端适配器
NAT	[H.235] 网络地址转换
NCS	[J.170] 网络呼叫信令
NE	[M.3010] [X.790] 网元
NEF	[M.3010] 网元功能

缩写	定义
NEF-MAF	[M.3010] 网元功能 — 管理应用功能
NML	[M.3010] [M.3210.1] 网络管理层
NOC	[X.790] 网络运营中心
N-OSF	[M.3010] 网元功能 — 操作系统功能
NTP	[H.530] 网络时间协议
O	[M.3010] 可选的
OA&M	[M.3010] 运营、管理和维护
OAM&P	[SANCHO] 运营、管理、维护和提供服务
OCSP	[H.235] 在线认证状态协议
ODP	[X.810] 开放分布处理
OFB	[H.235] 输出反馈模式
OID	[H.235] [H.530] [J.170] [M.3010] 目标标识符
OS	[M.3010] [X.790] 操作系统
OSF	[M.3010] 操作系统功能
OSF-MAF	[M.3010] 操作系统功能 — 管理应用功能
OSI	[M.3010] [X.790] [X.805] [X.810] 开放系统互联
OSS	[J.170] 运营支援系统。用于配置、性能、故障、计费和安全管理的后台软件。
OT	[T.36] 一次性密钥。 两个用户都认可的一个 6-64 位的十进制数。
Otx	[T.36] 在 X 用 Y 注册的过程中 X 首次使用的一次性密钥
Oty	[T.36]Y 在为了完成相互注册而用 X 注册的过程中首次使用的一次性密钥，无论该密钥是否与 Otx 相同。
P(n)	[T.36] 相位值 (n)
PBX	[M.3010] 专用小交换机
PDU	[H.235] 协议数据单元
PH	[T.36] 消息的简单散列值 (24 位的十进制数字)
PKCROSS	[J.170] 利用 PKINIT 建立区间密钥和相关的区间政策，用于核发各区之间和各域之间的跨区业务许可证，以支持域内或域间的 CMS 到 CMS 信令（CMSS）。
PKCS	[H.235] [J.170] [X.509] 公开密钥密码标准
PKI	[H.235] [H.530] [X.509] [J.170] 公开密钥结构。一个下发公开密钥证书的过程，包括标准、认证机构以及用来管理证书的机构间的通信和协议。
PMI	[X.509] 特权管理基础设施
PRF	[H.235] 伪随机功能
Primitive	[T.36] 一个由 UIN 和 UCN 合成的 64 位数字
procREGxy	[T.36] X 和 Y 之间的注册过程
procSTKxy	[T.36] 从 X 向 Y 安全传送密钥的过程
PRS	[T.36] 伪随机函数
PSTN	[SANCHO] 公众交换电话网
PTO	[M.3010] 公众电信运营商
PTR	[X.790] 提供商故障报告
PVC	[X.805] 永久虚拟电路
PW	[H.530] 移动用户密码
QA	[M.3010] Q 接口适配器
QoS	[SANCHO] 服务质量

缩写	定义
R	[M.3010] 资源
R_1	[H.530] 随机数字
RADIUS	[J.170] 远端认证拨入用户业务
RBAC	[X.509] 基于角色的访问控制
RC4	[J.170] 在密码组中提供的一个可变长度密钥流，用于对 IPCable 的媒体业务加密。
RCN	[T.36] 注册密码.。一个 16 位的十进制数
RDN	[X.790] 相关显名
RIP	[H.530] 进程请求
RKS	[J.170] 记录保存服务器。 收集并关联不同事件消息的设备
RNCn	[T.36]与 SCn 关联的非秘密随机数。一个 4 位的十进制数
RNIM	[T.36] 与 IM 关联的非秘密随机。一个 4 位的十进制数
RNK	[T.36] 在加密一个 SK 时，用于使 MPx 产生的原语发生变化的非秘密随机数。一个 4 位的十进制数。
RNSRn	[T.36] 与 SRn 关联的非秘密随机数。一个 4 位的十进制数
RNSSn	[T.36] 与 SSn 关联的非秘密随机数。一个 4 位的十进制数
RRJ	[H.530] 注册拒绝
RRQ	[H.530] 注册请求
RSA	[H.235] [T.30] [T.36] Rivest, Shamir and Adleman (公开密钥算法)
RSVP	[J.170] 资源预留协议
RTCP	[H.235] [J.170] 实时传送控制协议
RTO	[J.170] 重发超时
RTP	[H.225.0] [H.235] [J.170] 实时协议
SA	[J.170] 安全联系
SAFER K-64	[T.36] 1993 年由 J. L. Massey 提出的采用 64 位密钥算法的安全快速加密程序，是一种采用 64 位明文和密文块的迭代块密码 (A. Menezes 等, 应用密码技术手册, CRC Press, 1997)。
SCn	[T.36] 秘密质询密钥。一个 12 位的十进制数
SDH	[M.3010] 同步数字体系
SDP	[J.170] 会话描述协议
SDU	[H.235] 服务数据单元
SG	[J.170] 信令网关，是在 IP 网络的边界发送/接收 SCN 本地信令的代理。在 7 号信令中，SG 的功能是把 SS7 国际网关中不同的 ISUP 和 TCAP 转换为通用的 ISUP 和 TCAP
SH	[T.36]进行扰频的简单散列值 (24 decimal digits)
SHA1	[H.235] 安全散列算法 No.1
SI	[X.810] 安全信息
SIP	[J.170] [X.805] 会话初始协议。 应用层的控制（信令）协议，用来创建、更改和终止与一个或多个参与者的会话
SIP+	[J.170] 会话初始协议扩展
SK	[T.36] 一种秘密密钥，可能是 SCn, SRn, SSn, 等.。一个 12 位的十进制数
SMAPM	[X.790] 系统管理应用协议机
SMK	[M.3010] 共享管理知识
SML	[M.3010] [M.3210.1] 服务管理层
SMO	[X.790] 系统管理概述
SMTP	[X.805] 简单邮件传输协议

缩写	定义
SNMP	[J.170] [X.805] 简单网络管理协议
SNTP	[H.530] 简单网络时间协议
SOA	[X.509]机构源
SONET	[X.805] 同步光网络
S-OSF	[M.3010] 服务管理层 — 操作系统功能
SRn	[T.36] 秘密响应密钥，第 n 个。一个 12 位的十进制数
SRTP	[H.225.0] [H.235] 安全实时协议
SS	[T.36] 与 HFX40-I 完整性算法一起使用的秘密会话密钥(12 位的十进制数字)
SS7	[J.170] [X.805] 7 号信令。在电话网络中实施呼叫信令的一套协议和体系结构
SSK	[T.36] 扰码秘密密钥。一个 12 位的十进制数
SSL	[H.235] [X.805] 安全套接字协议层
SSn	[T.36] 秘密会话密钥，第 n 个，与 HFX40 密码和/或散列一起使用。一个 12 位的十进制数
SSx	[T.36] 由 X 生成的秘密会话密钥，与 HFX40 密码算法一起使用（12 位的十进制数字）
TCAP	[J.170] 事务处理应用协议。SS7 的协议栈之一，用来在信令控制节点实施远程数据库交易
TD	[J.170] 断开超时
TF	[M.3010] 变换功能
TF-MAF	[M.3010] 变换功能 — 管理应用功能
TFTP	[J.170] 简单文件传输协议
TGS	[J.170] 许可证核发服务器，是 KDC 中用来核发许可证的一个子系统。
TKx	[T.36] 传送密钥, 由 X 生成的 MPx 的加密操作。一个 16 位的十进制数
TLS	[H.235] 传输层安全性
TMN	[M.3010] [M.3210.1] [X.790] 电信管理网络
T_n	[H.530] 第 n 个时间戳
TSAP	[H.235] 传送服务访问节点
TSP	[X.790] 电信服务优先权
TTP	[X.810] 可信第三方
TTR	[X.790] 电信故障报告
UCN	[T.36] 惟一密码，例如， UCNx、UCNy。只有系统认知的一个 16 位的十进制数
UDP	[J.170] 用户数据报协议
UIN	[T.36] 唯一标识码，例如，UINx、UINy。只有系统认知的一个 48 位的十进制数
V-BE	[H.530] 被访 BE
V-GK	[H.530] 被访 GK
VLF	[H.530] 访问者位置功能
VoIP	[X.805] IP 话音业务
VPN	[X.805] 虚拟专用网
W	[H.530] 采用 Diffie-Hellman 半密钥算术组合的的复合值
WSF	[M.3010] 工作站功能
WSSF	[M.3010] 工作站支撑功能
WT	[H.530] 移动性清除标记
X	[T.36] 一个实体的名称

缩写	定义
x	[T.36]用来 表示属于 X 或由 X 生成的下标
X<<Y>>	[H.234] 由 X 生成的 Y 的证书
XOR'd	[T.36] [H.235] （被）异或
Xp	[H.234] X 实体的 RSA 公开密钥
Xp[*]	[H.234] 用 Xp 对[*]加/解密。在 RSA 中通过求幂运算实施
Xs	[H.234] X 实体的 RSA 秘密密钥
Xs[*]	[H.234] 用 Xs 对[*]加/解密。在 RSA 中通过求幂运算实施
XT	[H.530] MT 认证的隐秘标记
Y	[T.36] 第二个实体的名称
y	[T.36] 用来表示属于 Y 或由 Y 生成的下标
ZZ	[H.530]移动用户共享的秘密/口令，与相应的 AuF 共享
ZZMT	[H.530]移动终端共享的秘密，与相应的 AuF 共享
ZZ_n	[H.530] 第 n 个共享的秘密

A.2 常用安全相关术语定义

术语	定义
Access control **访问控制**	[H.235] [X.800] 防止对一个资源的非授权使用，包括防止以非授权的方式使用资源(X.800)。[J.170] 限制信息流从一个资源只流向受权个人、程序、进程或其他网络系统资源。[X.805] 访问控制安全尺度防止对于网络资源的非授权使用。访问控制确保了只有受权人员或者设备才允许访问网元、存储的信息、信息流、服务和应用。另外, 基于角色的访问控制(RBAC) 提供了不同的访问级别，以确保个人和设备只能够对于他们被授权的网元、存储的信息和信息流进行访问和实施操作。
Access control list **访问控制列表**	[X.800] 一张被授权可以访问某个资源的实体的列表，注明了实体的访问权限。
Access Node **访问节点**	[J.170] 在本文档中使用时，一个访问节点就是一个第二层终端设备，该设备终接到 CM 连接的网络端点。它取决于所用的技术。在 J.112 附件 A 中被称做 INA，在附件 B 中被称做 CMTS。
Accountability **问责制**	[X.800]确保能够认定一个实体的动作确为该实体所为的性能。
Active threat **动态威胁**	[X.800]未经授权故意改变系统状态所带来的威胁。(注 — 安全相关的动态威胁的例子可能包括：消息更改，消息重放，伪造消息插入，受权实体伪装和拒绝服务。)
Agent **代理**	[X.790] 同建议书 X.701 “系统管理概述（SMO）”中的定义，但是有如下限制。对于一个特定的电信业务（或资源）实例，在管理业务时，有可能一个系统扮演管理者角色，另一个扮演代理角色。
Alias **别名**	[X.790] 对象标识符之外的另一个名称，（通常可由客户）借此了解、引用和识别一个故障报告。

术语	定义
Application association **应用关联**	[X.790] 两个应用实体之间的合作关系，实现方式是在它们使用表示服务的过程中交换应用协议控制信息。
Application context **应用文档**	[X.790] 在一个应用关联中，为了应用实体的互通而明确定义的一套应用服务元素、相关选项以及其他必要的信息。
Application entity **应用实体**	[X.790] 与 OSI 相关的应用过程的概念。
Associated alarms **关联告警**	[X.790] 与特定故障相关的告警。
Asymmetric cryptographic algorithm **非对称密码算法**	[X.810] 在加密和相应解密的过程中对加密和解密使用不同密钥的算法。 (注 —在一些非对称密码算法中，密文解码或数字签名的生成需要使用不止一个专用密钥。)
Attack **攻击**	[H.235] 为绕过一个系统的安全机制或利用其漏洞而采取的行动。对一个系统的直接攻击利用的是安全机制基础算法、原理或性能的不足。实施间接攻击通常是绕过了安全机制或是使系统不正确地使用了安全机制。
Attribute **属性**	[X.790] 关于被管理对象的信息，用来（局部或完整）描述被管理对象。该信息由属性类型和相应的属性值（单值或多值）组成。
Attribute Authority **属性机构**	[X.509]通过发布属性证书指派特权的机构。
Attribute Authority Revocation List **属性机构撤销列表**	[X.509] AARL 是一个撤销列表，包括核发给属性机构但核发机构认为其不再有效的属性证书列表。
Attribute certificate **属性证书**	[X.509] 一种数据结构，由属性机构数字签名，通过证书拥有者的标识信息来限定某些属性值。
Attribute Certificate Revocation List **属性证书撤销列表**	[X.509] ACRL 是一个撤销列表，包含核发机构认为不再有效的属性证书列表。
Attribute type **属性类型**	[X.790] 属性组件，表明该属性给出的信息的类型。
Attribute value **属性值**	[X.790] 由属性类型表明的信息类型的一个特定实例。
Audio Server **音频服务器**	[J.170] 音频服务器用于在 IPCablecom 网络中播放参考性的通知。对于未完成的通信以及为了向用户提供增强的信息服务，媒体通知都是必需的。音频服务器服务的组件部分是媒体播放器和媒体播放控制器。
Audit 审计	[X.800] 参见安全审计。
Audit trail **审计索引**	[X.800] 参见安全审计索引。

术语	定义
Authentication **认证**	[H.235] [X.800] [X.811] 向一个实体所声明的身份提供担保，参见数据源认证和同等实体认证。（注 – 术语“认证”的使用与数据的完整性无直接关联；术语“数据完整性”可以替代使用。）。[J.170] 验证一个实体向另一个实体所声明身份的程序。[X.805] 认证安全规划用于确认通信实体之间的身份。认证确保了通信实体所声明身份的合法性（例如，个人，设备，服务或应用）并且确保了一个实体不会对以前的通信过程试图进行伪装或非授权重现。
Authentication exchange **认证交换**	[X.800] 通过信息交换来确保实体身份的机制。
Authentication function **认证功能**	[H.530] 在归属域中用于维护登记移动用户和登记移动设备安全关系的安全功能实体。
Authentication information **认证信息**	[X.800] 建立声明身份有效性的信息。I
Authentication token; (token) **认证标记; (标记)**	[X.509] 在一个坚固的认证交换过程中所传送的信息，可以用来确认它的发送者。
Authenticity **真实性**	[J.170] 确保得到的信息是未经更改或伪造且的确是由声称发布该信息的实体所生成的能力。
Authority **机构**	[X.509] 负责核发证书的机构。在本规范中规定了两种类型：认证机构用来发布公开密钥公开证书，属性机构用来发布属性证书。
Authority certificate **机构证书**	[X.509] 向一个机构（例如一个认证机构或一个属性机构）核发的证书。
Authorization **授权**	[H.235]根据身份认证授予许可权。[J.170] 使被允许访问者有权使用某个服务或设备的动作。[X.800] 权利的授予，包括根据访问权限授予访问权。
Availability **可用性**	[X.800] 能够根据受权实体的要求进行访问和使用的性能。
Availability **可用性**	[X.805]可用性安全尺度确保了在事件影响网络的情况下，不拒绝经过授权的对 网元，、存储信息，、信息流，、服务和应用的访问。灾害恢复解决方案在此讨论范畴。
Base CRL **基本 CRL**	[X.509]用于用做生成 dCRL 的基础的 CRL
Business management layer **商业管理层**	[M.3010]为整个企业负责的管理层，与标准化无关。
CA-certificate **CA 证书**	[X.509] 由一个 CA 为另一个 CA 核发的证书。
Cancelled **取消**	[X.790]管理者可以要求代理“取消”一个故障报告。管理者想终止该故障报告（因为误输入或是故障条件不再存在）。在特定的情况下（例如：故障并未经过处理或测试），代理将 “取消”故障报告而把状态更新为“由客户请求关闭”。“取消”故障报告也可能会引起商业分歧，但这已不属于的讨论范畴（例如，客户是否必须为这种故障报告付费）。

术语	定义
Capability **能力**	[X.800]用做某个资源标识符的一种标记，拥有该标记表明拥有该资源的访问权力。
Certificate **证书**	[H.235] 由安全机构或可信的第三方核发的一套与安全相关的数据，与安全信息一同被用来提供数据完整性和数据源认证服务(X.810)。在本本建议书中该术语是指“公开密钥”证书，即表示一个所有者公开密钥（及其他可选信息）是经过可信的机构以不可伪造的格式所验证并签署的数值。
Certificate policy **证书政策**	[X.509] 一套指定的规则，用来表明一个证书对于具有通用安全需求的某个特定团体和/或应用类型的适用性。例如，在给定的价格范围内，特定的证书政策可以表明在给定价格范围的货物贸易中某种类型的证书对电子数据交换交易认证的适用性。
Certificate Revocation List **证书撤销列表**	[X.509] 表明一套证书不再被证书核发者认为有效的签名列表。除了通用术语 CRL 之外，也规定了一些涵盖特定领域的 CRL 的特殊 CRL 类型。
Certificate serial number **证书序列号**	[X.509] 在核发机构中唯一的整数数值，与 CA 发布的证书明确关联。
Certificate user **证书用户**	[X.509] 需要确定地知道另一个实体公开密钥的实体。
Certificate validation **证书确认**	[X.509] 在给定的时间内确保证书的有效性，可能包括认证路径的结构和处理，并在给定的时间内确保在路径中所有证书的有效性（例如没有过期或被废除）的程序。
Certificate-using system **证书使用系统**	[X.509] 被一个证书用户使用的在该号码簿规范中所定义的功能的实施。
Certification Authority **认证机构**	[X.509] 得到一个或多个用户信任的机构，创建并分配公开密钥证书。作为一种选择，认证机构也可以创建用户密钥。 [X.810] 可信的实体（在安全政策的范畴内中），创建包含一个或多个安全相关数据类型的安全证书。
Certification Authority Revocation List **认证机构撤销列表**	[X.509]CARL 是一个撤销列表，包含向认证机构核发但核发者认为其不再有效的公开密钥证书列表。
Certificate path **证书路径**	[X.509] 号码簿信息树中对象证书的一个有序序列，该序列与路径中初始对象的公开密钥一起经过处理可产生路径中最终对象的公开密钥 。.
Channel **信道**	[X.800]信息传递路
Cipher **密码**	[H.235] 密码算法，一种数学变换。 [J.170] 在明文和密文间进行数据转换的算法。
Ciphersuite **密码套系**	[J.170] 必须同时包含加密算法和消息认证算法（例如 MAC 或 HMAC）的一个集合。通常，它也可以包括密钥管理算法，这在 IPCablecom 的内容中并不适用。
Ciphertext **密文**	[X.800] 经加密生成的数据。使最终数据的语义内容不可知晓。(注 — 密文本身也可用做加密操作的输入参数，这样就可以生成超级加密的输出结果)

术语	定义
Clearing trouble reports **清理故障报告**	[X.790] 某个代理所做的声明，表明故障报告中所确定的行动或是修复行为对象实例中所确定的行动已经圆满完成，解决了故障，或表明这样的行动已不再需要，因而故障报告将被终止。
Cleartext 明文	[X.800] 可理解的数据，其语义内容可以知晓。
Client 客户	[X.790]系统提供的或网络提供的服务的使用者。
Close-out **取消**	[X.790] 代理确定报告的故障已经被清理或是不再存在时，该故障报告就可认为被“取消”了，并且，代理会更新故障报告状态以表明故障报告“取消”。只有代理才可以改变故障报告状态到“closeOut”。管理者提出取消故障报告的要求时，故障报告的状态可以变成“closedOutByCustReq”。
Closing trouble reports **结束故障报告**	[X.790] 某个代理所做的声明，表明故障已经解决，因此被清理的故障报告只能用来生成故障历史记录和/或被删除。
Communication **通信**	[X.805] 通信安全尺度确保了信息只能在经过授权的端点之间传送（信息在这些端点之间传送时，没有转向或被窃听）。
Conditionally trusted entity **条件可信实体**	[X.810] 在安全政策的范畴内得到信任的实体，这种实体不可能违反安全政策而又不被发现。
Confidentiality **机密性**	[H.235] 防止信息泄漏给未经授权的个人、实体或程序的性能。 [J.170] 除了确定的目标，确保信息不泄漏给任何其他目标的方法。信息经过加密来保证其机密性。也叫做保密。[X.800] 防止信息泄漏给未经授权的个人、实体或程序或为其所用的性能。
Conformant management entity **一致性管理实体**	[X.790] 一个真正的开放系统，支持本本建议书中定义的互操作接口。
Contact 联系人	[X.790] 代表管理者或代理提供关于故障补充信息的个人。
Credential **证明书**	[H.530]在本本建议书中，证明书（如 HMACZZ(GKID)或 HMACZZ(W)）可以看做是一些数据，AuF（认证功能）利用密码算法把其与移动用户共用的秘密 ZZ 作用于这些数据。 在授权检查中，传送证明书来证明授权和时限
Credentials **证明书**	[X.800]传送的数据，用来确定实体所声明的身份。
CRL distribution point **CRL 发布节点**	[X.509] 获取 CRL（证书撤销列表）的一个号码簿条目或是其他发布源； 通过 CRL 发布节点所发布的 CRL 可能只包含某个 CA（证书机构）所发布的一套证书的子集的撤销条目，或是包含多个 CA 的撤销条目。
Cryptanalysis **密码分析**	[J.170] 在无权使用密钥的情况下恢复消息明文或加密密钥的程序。[X.800] 为了得到秘密变量和/或包括明文在内的敏感数据，对一个密码系统和/或它的输入和输出的分析。
Cryptographic algorithm **密码算法**	[H.235] 从一个或多个输入值计算结果的数学函数。

术语	定义
Cryptographic chaining 密码链	[X.810] 一种密码算法的使用方式，在这种方式下，由加密算法实施的转换取决于于以前的输入值或输出值。
Cryptographic checkvalue 密码校验值	[X.800] 对数据单元实施密码转换所生成的信息。（注 — 校验值的生成可能通过一步或多，它是密钥和数据单元的一个数学函数结果。通常被用来检验数据单元的完整性。）
Cryptographic system, cryptosystem 密码系统	[X.509] 密码系统是明文和密文进行相互转换的集合，将要使用的特定变换是由密钥选择的。通常用一种数学算法来规定变换。
Cryptography 密码学	[X.800]为隐藏信息内容，防止它受到未被发现的更改和/或非法使用而综合了转换数据的原理、手段和方法的学科。（注 — 密码学决定了加/解密的使用方法。密码分析学是对密码学原理、手段和方法的攻击。）
Customer 客户	[X.790]服务提供商所提供电信服务的使用者。具体地说，在本建议书的范畴内，客户是指为了达到对所使用电信服务（或资源）的控制而选择使用操作系统之间的 OSI 接口来进行跨网管理的用户。客户（或客户代表）扮演了管理者角色。不要求该接口只用于这种情况，即双方之间存在传统的电信服务客户与提供商的关系。两个电信服务提供商（运营商）为了向最终用户提供服务，可能在它们网络互通的情况下使用该接口交换故障报告。这时，客户的角色可能随情况变化，但是，在任何情况下，一个运营商将会成为客户，扮演管理者的角色，而另一个运营商将会成为供应者，扮演代理的角色。
Data communication network 数据通信网	[M.3010] 在一个 TMN（电信管理网）内或是 TMN 之间支持数据通信功能（DCF）的通信网络。
Data confidentiality 数据机密性	[X.509] 该服务用来保护数据不被非法泄漏。认证框架支持数据机密性服务。该服务可以用来防止数据被窃听。[X.805] 数据机密性安全尺度防止数据非法泄漏。数据机密性确保数据内容无法被未受权实体所理解。加密、访问控制清单和文件许可证是提供数据机密性的常用方法。
Data integrity 数据完整性	[X.800] 数据没有遭到以未授权的方式改变或破坏的性能。 [X.805] 数据完整性安全尺度确保数据准确无误。保护数据未经授权不被更改、删除、创建和复制，并且提供了这些未经授权活动的标记。
Data origin authentication 数据源认证	[X.800] 确认所接收数据的数据源与所声称的相同。
Decipherment 解密过程	[X.800] 相应的可逆加密的逆过程。
Decryption 解密	[X.800] 参见“解密过程”。

术语	定义
Defer 延期	[X.790] 推迟处理或暂不考虑一个故障报告，直到符合相应条件可以进一步处理为止。
Delegation 授权	[X.509] 把特权从一个拥有特权的实体转让给另一个实体。
Delegation path 授权途径	[X.509] 证书有序序列，与特权声明者的标记认证一起验证特权声明者的特权真实性。
Delta-CRL 部分撤销列表	[X.509] 部分撤销列表只包括从供参考的基本 CRL 发布以来证书撤销状态有所改变的项。
Denial of service 拒绝服务	[X.800]阻止经授权的资源访问或是延误紧急操作。
Digital fingerprint 数字指纹	[X.810] 数据项目特性，例如一个密码校验值或是对数据执行单向散列函数运算的结果，对于数据项目来说，它是非常独特的并且不可能找出其他能够生成同样特性的数据项目。
Digital signature 数字签名	[X.800] 数据单元的附加数据或数据单元的一种密码转换（参见“密码学”），使得数据接收方可以证明数据源和数据完整性，并防止伪造， 例如：接收方伪造。
Distinguishing identifier 独特标识符	[X.810] 唯一地标明一个实体的数据。
Downstream 下游	[J.170] 从头端到用户位置的方向。
Element management layer 元素管理层	[M.3010]负责集中或各别管理网络元素的管理层。
Encipherment 加密	[H.235] 加密是通过实施某种密码算法（加密算法）使数据对于未经授权的实体不可读的过程。解密是加密的逆操作，使密文转化为明文。[X.800] 对数据进行密码转换（参见密码学）生成密文。（注 —加密可能是不可逆的，在这种情况下，无法进行解密操作。）
Encryption 加密	[J.170] 把明文信息转换为密文的一种方法。[X.800] 参见“加密”。
End entity 端实体	[X.509] 不以签署证书为目的而使用其秘密密钥的证书主体，或是一个依赖方实体。
End-entity Attribute Certificate Revocation List 端实体属性证书撤销列表	[X.509] 发布给并非属性机构的持有者的属性证书撤销列表，证书发布者认为这些证书不再有效。
End-entity Public-key Certificate Revocation List 端实体公开密钥证书撤销列表	[X.509] 发布给并非证书机构的主体的公开密钥证书撤销列表，证书发布者认为这些证书不再有效。
Endpoint 端点	[J.170] 终端、网关或 MCU。
End-to-end encipherment 端到端加密	[X.800] 数据在起始端系统加密，相应的解密只发生在目的端系统。（参见“逐条链路加密”。）

术语	定义
Environmental variables **环境变量**	[X.509] 做出认证决定所需的政策的某些方面，不包含在静态结构当中，但特权验证者可通过某些当地方式加以使用（例如，一天内的具体时间或是经常项目差额）。
Escalating a trouble report **故障报告升级**	[X.790] 为了解决故障而表明故障报告将得到紧急有效地关注。
Event **事件**	[X.790] 改变某个对象全局状态的即时发生的事件。状态的改变可能是永久的或临时的，允许实施监控和测量等功能。事件可能生成报告，也可能不生成报告，它们可能是自发的或是在计划之中的，它们可能触发其他的事件或是由一个或多个其他事件所触发。
Event Message **事件消息**	[J.170] 捕获连接中某一部分的消息。
F interface **F 接口**	[M.3010] 在 F 参考点使用的接口。
F reference points **F 参考点**	[M.3010]F 参考点位于工作站功能模块(WSF)和操作系统功能模块(OSF)之间。
Fault management **故障管理**	[X.790] 故障管理包含了一套检测、隔离和解决电信网络及其环境中异常操作的功能。
Full CRL **完全 CRL**	[X.509] 对于给定的范畴，包含全部已撤销证书的完整撤销列表。
Function block **功能模块**	[M.3010] 需标准化的最小（可配置）TMN 管理功能单元。
G reference points **G 参考点**	[M.3010] G 参考点位于 TMN 之外，在用户和工作站功能模块之间(WSF)。尽管它传送 TMN 信息，但是并不是 TMN 的一部分。
Gateway **网关**	[J.170] 桥接 IPCablecom 语音通信世界和 PSTN 的设备。例如，媒体网关为 PSTN 提供了电路承载接口并对媒体流进行编码，信令网关在 IPCablecom 网络的边界发送并接收电路交换网络信令。
Hash function **散列函数**	[X.509] 一个将数值从较大域（可能非常大）映射到一个较小范围的（数学）函数。一个“好”的散列函数可以使得一个域中的运算结果均匀地分布（很明显是随意的）在整个域中。[X.810] 一个将数值从较大（可能非常大）的数值集合映射到一个较小的数值集合的（数学）函数。
Header **头信息**	[J.170] 在协议数据单元起始部分的协议控制信息。
Holder **持有者**	[X.509] 具有某些委派特权的实体，这些特权可能是由机构源直接委派或是由另一个属性机构间接委派。
Home border element **归属边界元素**	[H.530] 归属域中的边界元素(BE)。
Identity-based security policy **基于身份的安全政策**	[X.800] 一种以用户、用户群或代表用户行事的实体以及被访问资源/对象的身份和/或属性为基础的安全政策。
Indirect CRL **间接 CRL**	[X.509] 至少包含关于发布该间接 CRL 之外的机构所发布证书的撤销信息的撤销列表。

术语	定义
Integrity **完整性**	[H.235] 数据没有以未经授权的方式加以改变的特性。[J.170] 确保信息只能由受权者所更改的方式。 [X.800] 参见数据真实性。
Interface **接口**	[M.3010] 在参考点物理模块之间提供互连的体系结构概念。
Jurisdiction **管辖权**	[X.790] 指的是电信网络的功能分离。一个权限是下列四种类型之一：a) 本地交换承载网络；b) 互交换承载网络；c) 最终用户网络和 d) 以上几项的结合。
Kerberos	[J.170] 一个秘密密钥网络认证协议，选择使用密码算法进行加密和中央密码数据库进行认证。
Key 密钥	[J.170] 作为被选密码算法输入值的数学数值。 [X.800] 控制加/ 解密操作的符号序列。
Key agreement **密钥协议**	[X.509] 无需传送密钥而在线协商密钥值的方法，甚至是以加密的方式，例如：迪菲—赫尔曼技术（要想了解关于密钥协议机制的更多信息，参见 ISO/IEC 11770-1。 ）
Key Exchange **密钥交换**	[J.170]用于实体之间加密通信的实体之间公开密钥的交换。
Key management **密钥管理**	[H.235] [X.800] 依照某种安全政策，对密钥的生成、存储、分发、删除、存档和应用。
Key-Management **密钥管理**	[J.170] 为了运行一个安全协议，分发共享对称密钥的程序。
Link-by-link encipherment **逐条链路加密**	[X.800] 在通信系统中每一条链路上单独的数据加密应用。也见“端到端加密”。（注 — 链路加密意味着数据在转发实体中以明文方式存在。）
Logical layered architecture **逻辑分层体系结构**	[M.3010] 按照管理层分组的方式组织管理功能，并对层与层之间的关系给出描述的体系结构概念。
M reference points **M 参考点**	[M.3010] 位于 TMN 之外，在 Q 适配器功能模块（QAF）和不符合 TMN 建议书的被管实体之间的参考点。
Managed resource **被管资源**	[M.3010] 电信资源（逻辑上或物理上）中电信管理那部分的抽象概念。
Management application function **管理应用功能**	[M.3010] 表示一个或多个管理服务功能（的一部分）。
Management domain 管理域	[M.3010] 需遵循通用管理政策的被管资源的一个集合。
Management function **管理功能**	[M.3010] 被服务的用户所能察觉到的最小管理服务部分。
Management function set **管理功能集**	[M.3010] TMN 管理功能集是属于同样应用环境的一组 TMN 管理功能，也就是它们与某一特定的管理能力有关（如告警报告功能，服务管理控制）。TMN 管理功能集是功能规范的最小可重复使用项目。TMN 管理功能集必须被认为是一个整体。它的需求部分与 OSI SMF （系统管理功能）相似。

术语	定义
Management service 管理服务	[M.3010] 为实现特定电信管理需求而提供的服务。
Management layer 管理层	[M.3010] 反映了特定管理性能并包含支持该性能的一组管理信息的体系结构概念。
Manager 管理者	[X.790] 同建议书 X.701“系统管理概述（SMO）”中的定义，，但有如下限制。对于一个特定的电信服务（或资源）实例，通过一个系统扮演管理者角色，另一个系统扮演代理角色来管理服务是可能的。
Manipulation detection 处理检测	[X.800] 用于检测数据单元是否被更改（偶然地或故意地）的机制。
Masquerade 伪装	[X.800] 一个实体伪装成为另外一个实体。
Media stream 媒体流	[H.235] 媒体流可以是音频、视频、数据，或是它们的组合。媒体流传送用户或应用数据（有效载荷），但不传送控制数据。
Mobility routing proxy 移动路由代理	[H.530] 起媒介功能实体作用的可选功能实体，终结逐段转接链路的安全关联。
Network element 网元	[M.3010] 代表电信设备（或电信设备组/部分）并支持被认为属于电信环境的的设备、装置或装置组的体系结构概念，而该电信环境实施了网元功能（NEF）。
Network element function 网元功能	[M.3010]代表电信功能并且为了受到监视/控制而与 TMN OSF 功能模块通信的功能模块。
Network management layer 网络管理层	[M.3010] 从网络的观点看，负责行为管理，包括协调的管理层。
Non-repudiation 不可否认	[H.235]防止参与通信的若干实体中的一个否认参与了全部或部分通信过程。；[J.170]防止发送者事后否认其曾发送过信息或采取了某一行动的能力。[X.805]不可否认安全尺度提供了一种手段，该手段可以通过给出有关网络行为的证据来防止个人或实体否认对有关数据所实施的特殊行为 (比如职责、目的或者承诺证据；数据源证据，归属权证据，资源使用证据)，从而确保可以向第三方提供的用于证明某种行为已经发生过的证据的可用性。
Notarization 公证	[X.800] 向可信的第三方注册数据，允许以后确保其准确性，例如：内容、来源、时间和发送描述。
Object method 对象方法	[X.509] 资源调用的行为 (例如，一个文件系统可能有读、写和执行对象方法)。
One-way function 单向函数	[X.509] 一个容易计算的（数学）函数 f，但对取值范围内一般的 y 值，在定义域内很难通过计算找到符合 f(x)＝y 的 x 值。也有可能对于很少的几个给定的 y 值，计算相应的 x 值并不是很难。[X.810] 一个容易计算的（数学）函数，但是在已知其结果时，无法通过计算找到获得该结果的数值。

术语	定义
One-way hash function 单向散列函数	[X.810] 既是单向函数，又是散列函数的一种（数学函数）。
Operations system 操作系统	[M.3010]实施操作系统功能的物理模块 (OSF)。
Operations systems function 操作系统功能	[M.3010] 为了监测/协调和/或控制电信功能，包括管理功能（例如 TMN 本身），处理与电信管理相关信息的功能模块。
Outage 中断	[X.790] 服务或资源无效。
Passive threat 被动威胁	[X.800] 系统状态未发生变化的情况下，出现的未经授权泄漏信息的威胁。
Password 口令	[H.530] [X.800] 机密认证信息，通常由字符串组成。
Peer-entity authentication 对等实体认证	[X.800] 确定关联中的一个对等实体与声明的相符。
Perceived severity 察觉到的严重性	[X.790] 报告故障的个人所看到的问题的严重性。
Physical block 物理模块	[M.3010] 表现一个或多个功能模块的实现的体系结构概念。
Physical security 物理安全	[X.800] 防止资源受到故意或偶然威胁所使用的物理保护方法。
Policy 政策	[X.800]参见“安全政策”。
Policy mapping 政策匹配	[X.509] 一个域中的 CA（证书机构）要证明另一个域中的 CA 时，业界公认：第一个域的授权机构会认为第二个域中的某种特殊证书政策等同于第一个域中的某种特殊证书政策（但不必各方面均相同）。
Priority 优先权	[X.790] 管理者需要解决问题的紧急程度。
Privacy 保密	[H.235] 只有明确激活的各方才能解译的通信方式，通常通过加密和共享密钥来达到。[J.170] 确保信息不透漏给任何非意向各方的方法。信息通常被加密以提供机密性。也被称为机密。[X.800] 个人控制或影响能够收集的和存储的与其相关的信息的权力，并且该个人可能泄漏该信息或该信息可能泄漏给该个人。（注 — 因为该术语与个人权力相关，所以它不可能非常精确并且除非有需要安全的动机，它应当避免使用。）[X.805] 秘密安全尺度提供了对从观察网络行为获得的的信息的保护。这类信息包括用户访问过的网站，用户的地理位置，IP 地址和服务提供商网络中设备的 DNS 名称。
Private channel 专用信道	[H.235] 在本本建议书中，专用信道是根据在一个安全信道上事先谈判的结果确定的信道。在本建议书中，使用它处理媒体流。
Private Key 秘密密钥	[J.170] 在公开密钥密码学中使用的密钥，该密钥属于一个单独实体并必须保密。 [X.810] 在非对称密码算法中使用的密钥，其所有权受限（通常只属于一个实体）。

术语	定义
Private key **秘密密钥；** **Secret key** **密钥（建议不用）**	[X.509] (在公开密钥密码系统中) 某个用户的密钥对中只有该用户才知道的那个密钥。
Privilege 特权	[X.509] 由机构指派给实体的属性或特性。
Privilege asserter **特权声明者**	[X.509]使用其属性证书或公开密钥证书来声明特权的特权持有者。
Privilege Management Infrastructure **特权管理基础设施 (PMI)**	[X.509] 能够支持特权管理的基础设施，支持全面授权服务，与公开密钥基础设施相关。
Privilege policy **特权政策**	[X.509] 确定特权验证者向/为有资格的特权声明者提供/执行敏感服务的条件的政策。特权政策与服务属性和权限声明者属性相关。
Privilege verifier **特权验证者**	[X.509] 依据某特权政策验证证书的实体。
Proxy 代理服务器	[J.170]间接提供服务或扮演发布信息代表的工具，可以因此消除为支持某服务所需要的主机。
Public Key **公开密钥**	[J.170] 公开密钥密码算法中使用的密钥，属于一个单独实体，并公开发布。其他实体使用该密钥加密向密钥拥有者所发送的数据。 [X.810] 非对称密码算法中所使用并可公开获取得密钥。
Public Key Certificate **公开密钥证书**	[J.170] 实体的公开密钥与一项或多项与其有关标识有关的属性的捆绑，也叫做数字证书。
Public key cryptography **公开密钥密码学**	[H.235] 利用非对称密钥（加密/解密）的加密系统，在该系统中，密钥之间有数学关联，但不可进行计算。 [J.170]使用密钥对的程序，使用公开密钥和秘密密钥进行加密和解密，也叫做非对称算法。某用户的公开密钥可由其他用户公开获取，以便发送信息给公开密钥拥有者。一个用户的秘密密钥是保密的，并且只有用该秘密密钥才可以解密经公开密钥加密发送给该用户的信息。
Public Key Infrastructure **公开密钥基础设施（PK）**	[X.509] 能够支持公开密钥管理的基础设施，支持认证、加密、数据真实性或不可否认否认服务。
Public Telecommunication Operator **公众电信运营商 (PTO)**	[M.3010]电信主管部门、经认可的运营机构、民间（客户或第三方）管理机构和/或其他运营或使用电信管理网络（TMN）的组织的简称。
Public-key **公开密钥**	[X.509] (在公开密钥密码系统中)某用户的密钥对中可公开的密钥。
Public-key certificate **公开密钥证书**	[X.509] 用户的公开密钥和其他信息， 由认证机构分配给该用户的秘密密钥通过加密算法产生的不可伪造的信息。
Q adapter **Q 适配器**	[M.3010] 一种以包含 Q 适配器功能模块为特点的物理模块，将采用非 TMN 兼容接口（在 m 参考点）的 NE 类或 OS 类物理实体与 Q 接口相联接。
Q interface **Q 接口**	[M.3010] 在 Q 参考点使用的接口。

术语	定义
Q reference points Q 参考点	[M.3010] 位于 NEF 和 OSF 之间、QAF 和 OSF 之间以及 OSF 和 OSF 之间的参考点。
Reference point 参考点	[M.3010] 一种体系结构概念，用于描述管理功能模块并定义两个管理功能模块之间服务边界。
Relying party 依赖方	[X.509] 在做决定时依赖证书数据的用户或代理。
Repudiation 否认	[X.800]参与通信的一个实体否认曾参与了全部分或部分通信。
Revocation certificate 撤销证书	[X.810] 由安全机构发布的安全证书，表明某特定的安全证书已宣布无效。
Revocation list certificate 撤销列表证书	[X.810] 表明已宣布无效的安全证书列表的安全证书。
Role assignment certificate 角色指配证书	[X.509] 包含角色属性的证书，对证书主题/持有者指配一种或多种角色。
Role specification certificate 角色规范证书	[X.509] 包含角色特权指配的证书。
Root Private Key 根秘密密钥	[J.170] 最高级证书机构的秘密签署密钥。通常使用它为低级别的证书机构或其他实体签署公开密钥证书。
Routing control 路由控制	[X.800] 选择或避免特定网络、链路或中继线的路由处理过程中适用的规则。
Rule-based security policy 基于规则的安全政策	[X.800] 以对所有用户施加的全局规则为基础的安全政策。这些规则通常依赖于对被访问资源的敏感性以及对用户、用户群、或代表用户行事的实体的相应属性的拥有情况的比较。
Seal 封印	[X.810] 支持数据完整性的密码校验值，但并不保护数据不被接收方伪造（即它不提供不可否认）。当封印与数据元相关时，该数据元称作被加封数据。(注 — 尽管封印本身不提供不可否认，但一些不可否认机制却使用了封印所提供的数据完整性服务，例如，保护与可信第三方的通信。)
Secret key 秘密密钥	[X.810] 对称密码算法所使用的密钥。所有权有限（通常限于两个实体）。
Secure interaction rules 安全交互规则	[X.810] 管制安全域之间交互作用的安全政策规则。
Security administrator 安全管理员	[X.810] 负责定义或执行安全政策中一部分或多个部分的人。
Security audit 安全审计	[X.800] 对系统记录和行为的独立回顾和检查，目的是测试系统控制的适度性，确保符合已有的政策和操作程序，检测安全缺口，并对这些控制、政策和程序提出改造建议。
Security audit trail 安全审计索引	[X.800] 为帮助安全审计所收集并可能使用的数据。
Security authority 安全机构	[X.810] 负责定义、实施或强制执行安全政策的实体。

术语	定义
Security certificate **安全证书**	[X.810] 由安全机构或可信第三方发布的一套与安全相关的数据，与其他安全信息一起被用来提供数据的完整性和数据源认证服务。（注 — 所有的证书都被认为是安全证书（参见 ISO 7498-2 中的相关定义）。术语“安全证书”的采用是为了避免和 ITU-T 建议书 X.509 | ISO/IEC 9594-8 产生术语冲突，即, 目录认证标准。）
Security certificate chain **安全证书链**	[X.810] 安全证书有序序列，在序列中的第一个安全证书包含安全相关的信息，每一个后续安全证书包含用于验证前一安全证书的安全信息。
Security domain **安全域**	[X.810] 一套元素，一种安全政策，一个安全机构和一组与安全相关的行为。在域中，元素由特定行为的安全政策支配，安全政策则由域中的安全机构所管理。
Security domain authority **安全域机构**	[X.810] 负责实施一个安全域的安全政策的安全机构。
Security information **安全信息**	[X.810] 实施安全服务所需的信息。
Security label **安全标志**	[X.800] 限定资源的标志 (可能是一个数据单元) 命名或指定了该资源的安全属性（注 — 这个标识或界限既可以是明显的也可以是隐含的）
Security policy **安全政策**	[X.509] 管理安全服务和设施的使用和提供的安全机构设定的一套规则。 [X.800] 提供安全服务的一套标准。（参见“基于身份的安全政策”和“基于规则的安全政策”）。(注 — 完整的安全政策有必要解决 OSI 范围以外的许多问题。)
Security policy rules **安全政策规则**	[X.810] 在真实系统中安全域的安全政策一种表示。
Security profile **安全简表**	[H.235] 在 ITU-T H.235 之外的一（子）套一致的、可互操作的程序和特性，用于保护一个特定环境下在相关实体之间的 H.323 多媒体通信。
Security recovery **安全防御/恢复**	[X.810] 在检测到或怀疑有侵犯安全的行为要发生时所采取的行动和执行的程序。
Security service **安全服务**	[X.800] 由正在通信的开放系统的某一层所提供的服务，确保系统或数据传输有足够的安全性。
Security token **安全标记**	[X.810] 被一个或多个安全服务所保护的在通信实体之间传送的一组数据，与安全信息一起用于这些安全服务的提供。
Selective field protection **选择性字段保护**	[X.800] 对于将要被传送的消息中特定字段的保护。
Sensitivity **灵敏度**	[X.509] 表明资源价值或重要性的特性。[X.800] 表明资源价值和重要性，并可能包括其脆弱性的特性。
Service **服务**	[X.790] 该术语表示了客户从服务提供商购买或租用的电信服务的能力。服务是一个面向网元或面向设备的观点的提升。同样的服务可能由不同的网元提供，不同的服务可能由同样的网元提供。

术语	定义
Service management layer 服务管理层	[M.3010] 关注并负责服务契约问题的管理层，这些契约问题可以是正在向客户提供的或是将要向潜在的新客户提供的，契约问题包括服务订单处理、投诉处理和计价。
Service provider 服务提供商	[X.790]向客户提供电信服务的系统或网络。在本文中，服务提供商特指为了使客户能够为对所提供的电信服务（或资源）进行控制而获得跨网管理的能力，而提供 OS 间 OSI 接口的电信服务提供商（参见“客户”）。服务提供商扮演了代理角色。该接口不必限制在这种情况，即双方之间具备传统的电信服务提供商和客户关系。两个电信运营商为了向某个最终用户提供服务而使其网络互通的情况下当然可能使用该接口。这时，客户和服务提供商的角色可能随情况变化，但是，在任何给定的情况下，一个运营商都将会成为客户，扮演管理者的角色，而另一个运营商将会成为供应者，扮演代理的角色。
Service relationship 服务关系	[H.530] 指两个功能实体之间已建立的安全关联，假定存在至少一个共享密钥。
Shared secret 共享秘密	[H.530] 指密码算法使用的安全密钥，可能源自口令。
Signature 签名	[X.800] 参见“数字签名”。
Simple authentication 简单认证	[X.509] 通过简单的口令安排实现的认证。
Source of Authority 机构源	[X.509] SOA（机构源）是一个属性机构，受特定资源的特权验证者委托作为最终机构来指配一组特权。
Spamming 滥发	[H.235] 向系统过度发送未经授权数据的拒绝服务攻击。一种特定案的情况是在 UDP 端口上发送 RTP 数据包时的媒体滥发。通常系统被数据包溢满；要消耗宝贵的系统资源进行处理。
Status of a trouble report 故障报告状态	[X.790]在解决故障时从故障报告的实例化/创建以来 所达到的阶段。
Strong authentication 强认证	[X.509]通过密码证书获取的认证
Symmetric (secret-key based) cryptographic algorithm 对称（基于秘密密钥）密码算法	[H.235]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 (X.810)。
Symmetric cryptographic algorithm 对称密码算法	[X.810] 在加密和解密程序中使用相同密码的解密算法。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。
Telecommunications management network 电信管理网	[M.3010] 一种管理体系结构，包括电信设备、网络和服务的规划、提供、安装、维护、运营和管理。
Threat 威胁	[H.235] 潜在的安全侵犯 (X.800)。[X.800] 潜在的安全侵犯。

术语	定义
Time-stamp **时戳**	[X.790]用于表明 一个特定行为、动作或一个事件发生的时间值。
Traffic analysis **业务量分析**	[X.800] 通过分析业务流量变化 (有, 无, 数量, 方向和频次) 而得出的推论。
Traffic flow confidentiality **业务流机密性**	[X.800] 防止分析业务流的一种机密性服务。
Traffic padding **业务量填充**	[X.800] 产生杂散的通信实例、杂散的数据单元和/或数据单元内杂散的数据。
Transformation function 转换功能	[M.3010] 可以实现在 TMN 参考点和非 TMN 参考点（或是具备专利的或是其他标准化的）之间转换的功能模块。该功能模块的非 TMN 部分已超出了 TMN 的边界。
Trouble **故障**	[X.790]导致管理者察觉一个或多个网络服务或一个或多个被管理的资源所提供的服务质量下降的原因。
Trouble administration **故障管理**	[X.790] 故障管理由一套保证故障被报告并且其状态可被追踪的功能组成。故障管理服务包括请求故障报告格式，输入故障报告，添加故障信息，取消故障报告，请求故障报告状态，回顾故障历史，属性值变化通知（例如，故障报告状态/提交时间），对象创建/删除（故障报告），验证故障修复完成情况和修改故障管理信息。
Trouble history record **故障历史记录**	[X.790] 从故障报告中选择保留的信息记录，在故障报告结束后备用。
Trouble management **故障管理**	[X.790]共同处理故障的 CME（一致性管理实体）之间的故障报告和跟踪。(外部管理接口与内部管理接口未做区分)。
Trouble reporting **故障报告**	[X.790] 检测出故障后的一种通信行为，以便于故障管理系统可以及时排除故障。
Trouble resolution **故障排除**	[X.790] 这是为解决问题而进行的诊断盒修复行动的过程，包括指配具体工作项目或清除并结束故障报告的责任。
Trouble tracking **故障跟踪**	[X.790] 跟踪故障报告从开始到结束整个发展过程的能力。
Trouble type **故障类型**	[X.790] 被检测出的故障的描述或分类。
Trust **信任**	[X.509] 通常，第一个实体假定第二个实体的行为完全符合其期望时，则可以说第一个实体信任第二个实体。这种信任只适用于某种具体操作 。在整个体系中，信任的关键作用在于恰当地描述认证实体与某个机构的关系；一个实体应完全信任该机构能给出唯一有效并可靠的证书。 [X.810] 当且仅当实体 X 相信实体 Y 采用一种特定的方式从事了一系列活动，才能说实体 X 信任实体 Y 的该系列活动。
Trusted entity **可信实体**	[X.810] 可以违反安全政策的实体，该实体他或者做一些不该做的事，或者没有做该做的事。
Trusted functionality **可信功能性**	[X.800]按照某种标准，如由安全政策建立的标准，被认为是正确的功能性。

术语	定义
Trusted third party 可信第三方	[X.810]（在某种安全政策的范畴内）就某些安全相关活动而言得到信任的某个安全机构或其代理。
Unconditionally trusted entity 无条件可信实体	[X.810] 无需被检测到就可违反安全政策的可信实体。
User 用户	[M.3010] 为完成管理操作而应用管理服务的人或过程。
Visited border element 被访边界元素	[H.530] V-BE（被访问的边界元素）是一个放置在被访问域中的边界元素。
Workstation 工作站	[M.3010] 一个完成工作站功能(WSF)的物理模块。
Workstation function 工作站功能	[M.3010] 用于向使用人员翻译 TMN 信息或将使用人员的信息翻译成 TMN 信息的一个功能模块。
X interface X 接口	[M.3010] 在 X 参考点使用的接口。
X reference points X 参考点	[M.3010] 位于不同 TMN 内的 OSF（操作系统功能）功能模块之间的参考点。 (注 — 位于 X 参考点以外的实体可以是一个实际 TMN (OSF)的一部分或非 TMN (OSF 类)环境的一部分。 这种分类在 X 参考点是看不出来的。)
X.509 certificate X.509 证书	[J.170] 作为 ITU-T X.500 标准号码簿的一部分制定的一种公开密钥证书规范。

A.3 其他 ITU-T 术语和定义资料

ITU-T 在线 SANCHO (*Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*) 数据库提供 ITU-T 出版物中有定义的的英语、法语、西班牙语的“术语和定义”或“缩写词和首字母缩略语”。 该资料免费的在线资源，网址为 www.itu.int/sancho。 CD-ROM 版本也定期出版。上文提到的所有术语和定义都可以在 SANCHO 中找到 ，使用这些术语或定义的建议书清单也一并列出。

ITU-T 第 17 研究组编写了在 ITU-T 建议书中用到的安全定义汇编，网址为：www.itu.int/ITU-T/studygroups/com17/cssecurity.html。

附件B: 国际电联网络安全相关建议书目录

B.1 本手册中涉及的安全问题

F.400 *系统和服务概述*

本建议书概述了 MHS 整体系统和服务的定义，作为对 MHS 的全面介绍。这个概述是描述消息处理系统（MHS）和服务中系统模型和服务要素的一套建议书中的一个。本建议书概述了用于服务提供商为用户提供基于存储转发信息交换的公众消息处理（MH）服务的 MHS 系统能力。这个信息处理系统是根据国际电联应用的开放系统互联参考模型（OSI 参考模型）（X.200）的原理设计的，该系统使用了表示层服务和其他更一般化的应用服务元素提供的服务。信息处理系统可以使用 OSI 范畴内的任何网络来构建。由 MTS 提供的信息传输服务是独立于应用的。标准应用的例子有 PIM 服务（F.420+X.420），EDI 发信服务（F.435+X.435）以及话音发信服务（F.440+X.440）。 终端系统可以把信息传送（MT）服务用于双方定义的具体应用。由服务提供商提供的消息处理服务属于远程信息处理服务类别。以信息处理系统为基础的公众业务以及接入或由消息处理系统获得公众业务的内容在 F.400 系列建议书中规定。有关消息处理系统技术方面的内容详见 X.400 系列介绍。信息处理系统整体系统的体系结构在 ITU-T 建议书 X.402 中做了规定。服务要素就是在应用过程中体现的服务特色。服务要素被认为是提供给用户服务的重要组成部分，它既是基础服务的要素，又是任选的用户设施，分为必备的任选用户设施和附加的任选用户设施两类。信息处理系统的**安全**能力详见 F.400 的§.15 ，包括信息处理系统的**安全威胁**、安全模式、描述安全特点的服务要素（在附件 B **中**定义）、**安全管理**、信息处理系统安全附属物以及 IPM 安全。

课题 11/17

F.440 *消息处理服务：话音发信(VM)业务*

本建议书详细说明了公众国际话语发信服务的一般问题、操作问题以及服务质量问题，话音发信（VM）服务作为一种具体的信息处理（MH）服务是主管部门提供的一项国际电信服务，可以使用户向一个乃至多个接收者发送信息，同时采用存储转发和存储恢复相结合的技术通过电信网接收信息。话音发信服务得以让订户请求在处理和交换话音编码信息的过程中完成各种服务特性。有些特性是基本 VM 服务所固有的。主管部门如果提供了其他非基本特性的话，则可由订户自己选择，或者以单条信息为基础选择，或者选择在商定的时间段内。采用人际发信（IPM）服务的内部通信作为一种任选服务也可以由 VM 服务提供。主管部门必须在国际上提供基本特性。而订户可见的非基本特性则分为必备的和附加的。主管部门必须在国际上提供必备的任选特性。有些主管部门可提供附加的任选特性供国内使用，并根据双边协议在国际上提供。非基本特性被称为任选用户设施。VM 服务可以单独提供，也可以与各种远程信息处理服务或数据通信服务相结合。VM 服务中使用的技术技术规范和协议在 X.400 系列建议书中规定。

附件 G：**安全**的话音发信服务要素

附件 H：话音发信**安全**概述 课题 11/17

F.851 通用个人通信（**UPT**）——服务描述（服务第一部分）

本建议书旨在提供通用个人通信(**UPT**)的服务描述和操作规定。本建议书从单个 UPT 订户或 UPT 用户的角度提供了总的服务描述。UPT 还允许 UPT 用户参与用户定义的一组预订服务，用户可对这些服务提出个人要求，以形成一个 UPT 服务简表。UPT 用户使用 UPT 服务所面临的侵犯个人隐私的危险极小，也不会由于其他用户的欺诈性使用行为而造成错误支出。原则上讲，任何基础电信服务都可以用于通用个人通信服务。提供给 UPT 用户的服务仅受网络和所用终端的限制。在必备的用户特性中首先就是“UPT 用户身份认证”，而任选的用户特性有 UPT 服务提供商认证。详见第 4.4 节中的安全要求。 课题 3/2

H.233 视听服务的机密系统

保密系统包括两部分，一是机密机制或数据加密程序，二是密钥管理子系统。本建议书描述了适用于窄带视听服务的保密系统的机密部分。尽管这种加密系统需要加密算法，但此处对这样的算法未做规定，该系统适用多个具体的算法。机密系统适用于两个终端间或一个终端和一个多点控制单元（MCU）之间的点到点链路；它可以被扩展到没有解密的 MCU 的多点工作方式中 课题 G/16

H.234 视听服务的加密密钥管理和认证系统

保密系统包括两部分，一是机密机制或数据加密程序，二是密钥管理子系统。本建议书描述了适用于窄带视听服务的保密系统的认证和加密密钥管理的方法。保密是通过使用秘密密钥来实现的。密码输入到保密系统的机密部分，控制着所传数据的加密和解密的方式。如果钥被第三方得到，则保密系统将不再安全。所以用户保存好密钥对于任何保密系统来说都是十分重要的。本建议书规定了三种管理密钥的实用方法。 课题 G/16

H.235 H 系列 (H.323 和其他以 H.245 为基础的)多媒体终端的安全和加密

在不安全的网络中进行安全实时通信一般都涉及认证和保密。本建议书描述了在交互式会议框架内的增强措施，纳入了端点认证和媒体保密这样的安全服务，并描述了安全基础设施和所应用的具体保密技术。推荐的方案适用于任何使用 H245 控制协议的终端的点对点会议和多点会议。本版本（11/00）突出了椭圆曲线密码技术，安全简表（简单口令和复杂的数字签名），安全对策（媒体反滥发 ），高级加密算法，后端服务，对象识别符（见 H.323 实施者指南）。 课题 G/16

H.235 附件 F 混合安全简表

本附件描述了一个有效和可调节的以 PKI 为基础的混合安全简表，该简表利用了 H.235 附件 E 的数字签名 H.235 附件 D 的基线安全简表。建议把本附件作为任选方案。H.323 安全实体（终端、网守、网关、多点控制单元等）为了提高安全性或有需求时可实施此混合安全简表。本文中的“混合”一词指的是实际上 H.235 附件 E 的签名简表的安全程序用得较少，数字签名仍需遵循 RSA 程序。但是，数字签名技术只在绝对必要的情况下才使用，否则使用 H.235 附件 D 的基线安全简表中的高效对称

安全技术。混合安全简表适用于可调节的“全球性”的 IP 电话。此安全简表如果严格执行的话，可以克服 H.235 附件 D 中简单的基线安全简表的各种局限。而且，此安全简表如果严格执行的话，体系还可克服 H.235 附件 E 的某些缺点，如处理过程中对更宽的宽带和更高的性能的需求。例如，混合安全简表对于不同域中的各接力段的相互共享的秘密不取决于（静态）管理，这样用户可更容易地选择各自的 VoIP 提供商。所以此安全简表也支持某种用户移动性。它只在必要的情况下应用带有起签名和证书的不对称密码算法，否则使用更简单更有效的对称技术。它为 H.245 信息完整性提供了 H.245 信息隧道，同时也为信息的不可否认提出了一些对策。混合安全简表必定支持网守选路模式，并以 H.245 渠道技术为基础；对非网守选路模式的支持需要进一步研究。 课题 G/16

H.323 基于信息包的多媒体通信系统（附件 J：简单端点型的安全）

本建议书描述了通过基于信息包的网络（PBN）提供实时声音、图像、数据和/或多媒体服务的终端和其他实体，这种网络可能不提供服务质量保证。对于音像的支持是强制性的，而数据和图像则是非强制性的，但是如果支持的话，使用一种共同的操作方式则是强制性的，这样所有支持这种媒体类型的终端就可以互通了。这种基于信息包的网络包括局域网、企业内部网，城域网、内联网和网络互联（包括互联网）、点对点连接、单个网络分段，或者具有复合拓扑结构的多段互联网络，因此实体可以使用点对点、多点或广播配置。这些实体可以与 B-ISDN、N-ISDN、有服务质量保证的 LAN、GSTN 和/或无线网络中的中断互通，实体也可以综合到个人计算机中或用一个独立的设备实现，如话音电话。 课题 G/16

H.530 H.323 多媒体移动环境中 H.510 的安全

本建议书的目的在于提供一个 H.323 移动性环境的安全程序，如在描述 H.323 多媒体系统和服务的移动性的 H.510 的范围内。本建议书提供了关于 H.510 安全程序的细节。 到目前为止，版本 1 和 2 中 H.235 的信令能力是拟在主要为静态的 H.323 环境下处理安全问题的。这种环境和多媒体系统可以在网守区域内达到某种有限的流动性。举例来说，在一个分布式的移动性环境中，对于跨越具有很多相关实体的不同域的移动用户和终端而言，保障其漫游大体上只能得到 H.323 有限的支持，具体说只能得到 H.235 有限支持。在关于终端移动性的 H.510 中提出的 H.323 移动性方案也形成了一种新的情况，从安全的角度展现了其灵活多变的特点。漫游的 H.323 用户和移动终端必须通过国外被访域的认证。同样，移动用户也希望获得被访域真实身份的证明。除此以外，获得关于终端身份的证据以最终完成用户认证也是很重要的。这就要求对用户和被访域进行相互认证，同时作为任选项目还要求对终端的身份进行相互认证。由于移动用户是在其归属域预订服务并获得口令，通常只有归属域认识他或她，而被访域一开始并不认识该移动用户。因此,被访域不能与移动用户和移动终端共享已建立的安全关系。为了让被访域获得对移动用户和移动终端进行认证和授权的担保，被访域可以通过中间网络和服务实体把某些安全任务转交给归属域进行，如授权检查或者密钥管理。这也要求保证被访域和归属域之间的通信和密钥管理的安全。虽然从原则上讲，H.323 移动性环境比 H.323 闭合网更加开放，但这当然也需要适当保证密钥管理的安全。同样，移动性域内和跨域的通信也值得保护以防范恶意干扰。 课题 G/16

J.93 关于有条件进入有线电视系统数字电视二次传输的要求

本建议书规定了保护在线缆前端和最终用户之间的有线电视网上传输的 MPEG 数字电视信号的数据保密和进入要求。其处理过程所需的确切的加密算法不属 J.93 的范围，而是由各区域和/或业界自定。
第 9 研究组

J.96 修正案 1 确保遵循建议书 J.89 远程国际 MPEG-2 电视传输的保密性的技术方法

本建议书包括遵循 MPEG-2 专业格式（4:2:2）的数字电视远程国际传输的有条件进入的共用标准。本建议书描述了基于使用称做会话字的固定明钥的 DVB-CSA 规范的基本互操作扰码系统（BISS）。另一个向后兼容的模式为插入加密会话字而引入了一个附加机制，然而同时保存了互操作性。
课题 6/9

J.170 IPCablecom 安全(J.sec)

本建议书规定了可为 IPCablecom 网络系统提供安全的安全体系结构协议、算法、相关的功能要求和技术要求。按照规定，对每个网元接口必须提供认证、接入控制、信息和承载内容完整性、机密性及不可否认安全服务。
课题 6/ 9

M.3010 电信管理网的原则

本建议书规定了电信管理网（TMN）体系结构（TMN 功能体系结构，TMN 信息体系结构和 TMN 物理体系结构）的概念及其基本要素。本建议书描述了这三种体系结构之间的关系，给出了如何从功能和信息体系结构获得物理体系结构的要求的框架。本建议书仅有一部分是关于安全问题的。给出了划分管理功能性的逻辑参考模型，即逻辑分层体系结构（LLA）。本建议书还规定了为了获得互操作性如何展示 TMN 的一致性和依从性。TMN 的要求涉及到确保管理信息的受权用户安全访问管理信息的能力。TMN 包括若干功能模块，为了确保通过接口交换的信息及驻留在应用程序中的信息的安全，模块的安全功能性是采用安全技术实现的，以保护 TMN 环境。安全原则和机制还与控制 TMN 用户对 TMN 相关信息的访问权有关。
课题 7/4

M.3016 电信管理网安全概述（M.3sec）

本建议书概述了识别电信管理网络所面临的安全威胁的框架，并概括了如何在建议书 M.3010 描述的 TMN 功能体系结构的范畴内应用现有的安全服务。

M.3210.1 IMT2000 类别的安全管理——要求

本建议书是电信管理网管理服务系列建议书中的一个，描述了 IMT2000 网络的管理服务、目标和网络管理的诸方面。本建议书通过规定新的功能集、功能和参数以及增加新的语义和限制，构建了 ITU-T M.3400 所确定的功能集。本建议书描述了安全管理服务的一个子集，以提供对安全管理的要求和分析，同时概述了在 IMT-2000 移动网络中的欺诈管理问题。重点放在两个服务提供商之间的 X

接口，和二者之间为了检测和预防欺诈所需的服务管理，方法是以运行欺诈信息收集系统作为监测订户的一组规定行为的手段，避免他们因长期拖欠漫游期间产生的账单而形成的财务风险。
课题 14/4

M.3320 对于 X 接口的要求

本建议书是涉及为了管理电信网络和服务而进行的信息传输的系列建议书的一部分，其中仅有部分内容是有关安全问题的。本建议书的目的是对于各主管部门之间电信管理网的信息交换的所有的功能要求、服务要求和网络层面的要求定出了基本框架。本建议书还为使用电信管理网络 X 接口进行信息交换的各主管部门、经认可的运营机构、其他网络运营商、服务提供商、客户和其他实体提供了一个框架模式。
课题 9/4

M.3400 电信管理网管理功能

本建议书是电信管理网（TMN）系列建议书中的一个，提出了 TMN 管理功能及 TMN 管理功能集的规范。制定其内容是为了支持任务信息基础 B（角色、资源和功能），它与 ITU-T M.3020 中所述的 TMN 接口规范方法论中的任务 2（描述了 TMN 管理范畴）有关。在分析 TMN 管理范畴时，宜应考虑最大限度地使用本建议中提到的 TMN 管理功能集。
课题 7/4

Q.293 调用安全措施的间隔

本建议书摘自蓝皮书，仅包括 Q.293 第 8.5 至 8.9 节（调用安全措施的间隔）。
第 4 研究组

Q.813 远程操作服务要素的安全转换应用服务要素

本建议书提出了支持安全转换的规范，如加密、散列算法、密封和签名，重点在于整个远程操作服务要素（ROSE）协议数据单元（PDU）。安全转换用于提供各种安全服务，如认证、机密性、完整性和不可否认。本建议书描述了一种安全转换方法，在应用层实施和在任何基础的 OSI 堆层中无需任何安全特定的功能性。
课题 18/4

Q.815 用于整体信息保护的安全模块规范

本建议书规定了配合建议书 Q.814“电子数据互换交互式代理规范”使用的任选安全模块，该模块为整个协议数据单元（PDU）提供安全服务。特别是该安全模块支持发端和收端得不可否认服务和整个信息的完整性。
课题 18/4

Q.817 TMN PKI—数字证书和证书撤销列表概况

本建议书解释了数字证书和证书撤销列表是如何用于 TMN 的， 并对证书和证书撤销列表的扩展使用提出了要求。本建议书旨在增强使用公开密钥基础设施（PKI）支持安全相关功能的 TMN 元素的互操作性。本建议书的目的是在一个 TMN 内为分发和管理密钥而提供可互操作和可调节的机制，跨所有接口并在 X 接口上支持不可否认服务。它应用于所有 TMN 接口和应用。 PKI 设施能被用于许多安全功能，例如认证、完整性、不可否认和密钥交换（M.3016）。然而，本建议书没有规定这些功能如何实现，用不用 PKI 实现。
课题 18/4

Q.1531 服务集 1 的 UPT 安全要求

本建议书为用户到网络和在建议书 F.851 中定义的 UPT 服务集 1 的相互通信规定了 UPT 安全要求。本建议书包括了使用 DTMF 接入和基于带外 DSS1 的用户接入的 UPT 的安全问题的各个方面。

第 15 研究组

Q.1741.1 关于使用 UTRAN 接入网的 1999 年版 GSM 演进 UMTS 核心网的 IMT-2000 参考资料

本建议书包括涉及以下 3GPP 安全规范：

TS 21.133: 安全威胁和要求
TS 22.100: UMTS 第一阶段
TS 22.101: UMTS 服务原则
TS 33.102: 安全体系结构
TS 33.103: 安全综合指导方针
TS 33.105: 加密算法要求
TS 33.106: 合法侦听要求
TS 33.107: 合法侦听体系结构和功能
TS 33.120: 安全目标和原则

SSG

Q.1741.2 关于使用 UTRAN 接入网的第 4 版 GSM 演进 UMTS 核心网的 IMT-2000 参考资料

本建议书包括涉及以下 3GPP 安全规范：

TS 21.133: 3G 安全；安全威胁和要求
TS 22.048: (U)SIM 应用工具包的安全机制；第 1 阶段
TS 22.101: 业务问题；业务原则
TS 33.102: 3G 安全；安全体系结构
TS 33.103: 3G 安全；综合指导方针
TS 33.105: 加密算法要求
TS 33.106: 合法侦听要求
TS 33.107: 3G 安全；合法侦听体系结构和功能
TS 33.120: 安全目标和原则
TS 33.200: 网络域安全 － MAP
TS 35.205, .206, .207,和 .208: 3G 安全；MILENAGE 算法集的说明：3GPP 认证的一个实例算法集和密钥生成函数 f1, f1*, f2, f3, f4, f5 和 f5*;(.205: 概要; .206:算法说明; .207: 执行器的检测数据; .208: 设计一致性测试数据)

SSG

Q.1741.3 关于使用 UTRAN 接入网的第五版 GSM 演进 UMTS 核心网的 IMT-2000 参考资料

本建议书包括涉及以下 3GPP 安全规范：

TS 22.101: 业务问题；业务原则
TS 33.102: 3G 安全；安全体系结构
TS 33.106: 合法侦听要求

TS 33.107: 3G 安全；合法侦听体系结构和功能
TS 33.108: 3G 安全；合法侦听（LI）的移交接口
TS 33.200: 网络域安全 －MAP
TS 33.203: 安全；网络域安全（NDS）；IP 网络层安全
TS 35.205, .206, .207, .208 和 .909:3G 安全；MILENAGE 算法集说明：3GPP 认证的一个实例算法集和密钥生成函数 f1, f1*, f2, f3, f4, f5 和 f5*;(.205: 概要; .206:算法说明; .207: 执行器的检测数据; .208: 设计一致性测试数据; .909:总结及设计和评估的结论) SSG

Q.1742.1 关于使用 cdma2000 接入网的 ANSI-41 演进核心网的 IMT-2000 参考资料

本建议书将标准制定组织（SDO）公布的核心网标准与 IMT-2000 家族成员“使用 cdma2000 接入网的 ANSI-41 演进为核心网”于 2001 年 7 月 17 日通过的那些 3GPP2 规范进行了结合。在未来的 ITU-T 建议书 Q.1742.2 中将包括于 2002 年 7 月通过的 3GPP2 规范和已公布的核心网标准。无线接口和无线接入网络以及 IMT-2000 家族成员的 SDO 标准都将包含在 ITU-R M.1457 中。其他 IMT-2000 家族成员的联合都在 ITU-T Q.174x 系列中定义了。本建议书将这个 IMT-2000 家族成员的核心网的区域性标准融合成一个全球的建议书。 SSG

Q.1742.2 关于使用 cdma2000 接入网的 ANSI-41 演进核心网的 IMT-2000 参考资料（于 2002 年 7 月 11 日前通过的）

本建议书将区域性标准制定组织（SDO）公布的核心网标准与 IMT-2000 家族成员“使用 cdma2000 接入网的 ANSI－41 演进核心网”到 2002 年 7 月 11 日为止通过的那些 3GPP2 规范进行了结合。到 2001 年 7 月 17 日为止通过的 3GPP2 规范与地区标准制定组织公布的核心网标准结合在 ITU-T Q.1742.1 中。到 2003 年 7 月为止通过的 3GPP2 规范将与已公布的核心网标准在未来的 ITU-T 建议书 Q.1742.3 中融合。 无线接口和无线接入网络以及 IMT-2000 家族成员的 SDO 标准都将包含在 ITU-R M.1457 中。其他 IMT-2000 家族成员的联合都在 ITU-T Q.174x 系列中定义了。本建议书将这个 IMT-2000 家族成员的核心网的区域性标准融合成一个全球的建议书。 SSG

Q.1742.3 Q.1742.3 引用的安全方面的技术规范

系统间规范：

N.S0003-0 用户识别模块（1.0 版；2001 年 4 月）
N.S0005-0 蜂窝无线通信系统系统间操作（1.0 版；没有日期）
N.S0009-0 IMSI(1.0 版；没有日期)
N.S0010-0 宽带扩频系统的增强特征（1.0 版；没有日期）
N.S0011-0 OTASP 和 OTAPA(1.0 版；没有日期)
N.S0014-0 认证增强（1.0 版；没有日期）
N.S0018 TIA/EIA-41-D 预付费（1.0.0 版；2000 年 7 月 14 日）
N.S0028 GSM MAP 和 ANSI-41 MAP B 版修订版：0（1.0.0 版；2002 年 4 月）

包数据规范：

P.S0001-A 无线 IP 网络标准（3.0.0 版；2001 年 7 月 16 日）
P.S0001-B 无线 IP 网络标准（1.0.0 版；2002 年 10 月 25 日）

业务和系统方面规范：

S.R0005-B cdma2000 扩频系统修订版：B 的网络参考模型
（1.0 版；2001 年 4 月 16 日）
S.R0006 无线特征描述版：0（1.0.0 版；1999 年 12 月 13 日）
S.R0009-0 用户识别模块（1.0 版；第一阶段）修订版：0（1999 年 12 月 13 日）
S.R0018 预付费（1.0 版；第一阶段）修订版：0（1999 年 12 月 13 日）
S.R0019 基于位置的业务系统（1.0.0 版；LBSS）第一阶段描述（2000 年 9 月 22 日）
S.R0032 增强的用户认证（1.0 版；ESA）和增强的用户保密（ESP）(2000 年 12 月 6 日)
S.R0037-0 cdma2000 扩频系统（2.0 版；2002 年 5 月 14 日）的 IP 网络体系结构模型
S.R0048 3G 移动设备标识（1.0 版；MEID）(2001 年 5 月 10 日)
S.R0053 公共加密算法（1.0 版；2002 年 1 月 21 日）
S.R0054 公共加密算法接口规范（1.0 版；2002 年 1 月 21 日）
S.S0055 增强的加密算法（1.0 版；2002 年 1 月 21 日）
S.R0058 IP 多媒体域系统要求（1.0 版；2003 年 4 月 17 日）
S.R0059 遗赠 MS 域－第一步系统要求（1.0 版；2002 年 5 月 16 日）
S.R0066-0 基于 IP 的位置服务第一阶段要求（1.0 版；2003 年 4 月 17 日）
S.R0071 遗赠系统包数据监测要求第一阶段要求（1.0 版；2002 年 4 月 18 日）
S.R0072 所有 IP 包数据监测要求第一阶段要求（1.0 版；2002 年 4 月 18 日）
S.R0073 互联网空中手持设备配置管理（1.0 版；IOTA）第一阶段
（2002 年 7 月 11 日）
S.S0078 公共安全算法（1.0 版；2002 年 12 月 12 日） SSG

T.30 普通交换电话网文件传真传输的程序

附件 G 为使用 HKM 和 HFX 系统的安全 G3 文件传真传输规定了程序。附件 H 在 RSA 算法的基础上在 G3 传真中提供了安全。 第 16 研究组

T.36 使用第三组传真终端的安全能力

本建议书定义了两个可以用于文本安全传真传输的独立技术解决方案。这两个技术解决方案是基于 HKM/HFX40 算法和 RSA 算法的。 第 16 研究组

T.123 修订版 附件 B 扩展的传输连接

T.123 修订版这个附件的特征是有提供安全能力谈判的连接谈判协议（CNP）。这个安全机制应用了包括网络和点到点传输安全的不同方式并包括了例如 TLS/SSL, IPSEC w/o IKE 或手工密钥管理，X.274/ISO TLSP 和 GSS-API 等方法。 课题 1/6

T.503 四类传真文档交换的文档应用框架

本建议书定义了一个可以用于任何远程信息处理业务的文件应用框架。它的用处是指定一种适用于只包含光栅图形的第四组传真文件交换格式。文件是以一定的格式进行交换，这种格式使接收者可以原样显示或打印传真文件。 第 16 研究组

T.563 四类传真设备的终端特性

本建议书定义了四类传真设备的所有方面以及与物理网络的接口。 第 16 研究组

T.611 三类传真、四类传真、电传、电报、电子邮件和文件传输业务的可编程通信接口（**PCI**）**APPLI/COM**

本建议书定义了一个称为“APPLI/COM”的可编程通信接口，这个接口提供了对不同通信业务，例如三类电传或其他电传业务的统一访问。本建议书描述了结构、信息内容和在两个实体间交换信息内容的方法（例如：LA，本地应用和 CA，通信应用）。任何通信都是之前有注册步骤和结束有注销步骤，这两个步骤有助于实现对多用户系统特别重要的安全方案。它们同时提供在 LA 和 CA 之间实现安全机制的方法。本建议书构建了一个高级别的 API（应用编程接口），这个 API 屏蔽了所有通信细节但给应用设计者提供了强大的控制权和对通信活动的监测权。 第 8 研究组

X.217 信息技术 – 开放系统互联 – 联合控制服务元素的服务定义

本建议书为在一个开放系统互联环境中的应用联合控制定义了联合控制服务元素（ACSE）服务。ACSE 支持面向连接和无连接模式通信。在 ACSE 中定义了三个功能单元。强制核心功能单元用于建立和释放应用联合。ACSE 包括两个可选功能单元，一个是可选认证功能单元，这个单元在联合建立期间为支持认证的交换信息提供了额外的功能而不需要增加新的业务。ACSE 认证功能可以用于支持一个认证方法的有限类。

修正案 1：支持无连接模式的认证机制 课题 11/17

X.227 信息技术 – 开放系统互联 – 联合控制服务元素的面向连接的协议：协议规范

本协议规范定义了适用于希望在一个开放系统互联的环境中用面向连接的模式进行互联的系统间的通信例子，例如：应用联合控制的应用服务元素的一个面向连接模式的协议和联合控制服务元素（ACSE）。这个协议规范包括用于建立和释放应用联合的核心功能单元。认证功能单元在联合建立期间为支持认证的交换信息提供了额外的功能而不需要增加新的业务。ACSE 认证功能可以用于支持一个认证方法的有限类。应用内容协商功能单元在联合建立期间的应用选择提供了额外的功能。这个协议规范包括一个用状态表描述协议机器的附件，称为联合控制协议机（ACPM）。这个协议规范包括一个用于不同目的的使用带有 AE 标题密码描述的简单认证机制的附件以及一个认证机制规范的例子。给这个认证机制指定了以下命名方式（ASN.1 数据类型对象识别号）：

{joint-iso-itu-t(2) association-control(2) authentication-mechanism(3) password-1(1)}。

对于这个认证机制，口令是认证值。认证值的数据类型将是“图形字符”。 课题 11/17

X.237 信息技术— 开放系统互联 — 联合控制服务元素的无连接协议：协议规范

本建议书的修正案 1 包括描述协议模块中的 ASN.1 扩展标记。为了支持在 A-UNIT-DADA APDU 中的认证参数传输，它也增加了无连接的 ACSE 协议规范。 课题 11/17

X.257 信息技术 — 开放系统互联 — 联合控制服务元素的无连接协议：协议实现一致性声明（PICS）形式

本建议书为在建议书 X.237 中指明的联合控制服务元素（ACSE）OSI 无连接协议提供了协议实现一致性声明（PICS）形式。PICS 形式以表格形式描述了无连接 ACSE 协议的强制和可选元素。

课题 11/17

X.272 帧中继网络的数据压缩和加密

本建议书定义了帧中继网络的数据压缩业务和加密业务包括数据压缩的处理和封装，安全数据压缩，帧中继认证和加密。网络中的数据压缩业务将增加网络的有效吞吐量。在公网上传输敏感数据的需求要求有确保数据加密的设施。为了达到最优压缩率，必须在加密数据前对他进行压缩。因此，为了更好地处理数据加密协议而在数据压缩业务中提供设备是值得地。由于压缩和后来加密数据的任务是加强计算的，效率是通过同步数据压缩和加密（安全数据加密）实现的。数据压缩协议基于 PPP 连接控制协议（IETF RFC 1661）和 PPP 加密控制协议（IETF RFC 1968 和 1969）。本建议书应用于用 Q.933 附件 E 压缩的未编号信息（UI）帧。它将数据压缩和加密用于永久虚拟连接（PVC）和交换虚拟连接（SVC）。 课题 10/17

X.273 信息技术 — 开放系统互联 — 网络层安全协议

本建议书说明了在适用于连接模式和无连接模式网络层协议簇的 OSI 安全模型中支持完整性、机密性、认证和访问控制服务的协议。这个协议支持通过使用例如加密密钥的加密机制、安全标签和指定的安全属性来支持这些服务。 课题 11/17

X.274 信息技术 － 电信和系统间信息交换 － 传输层安全协议

本建议书说明了在 OSI 安全模型传输层中能够支持完整性、机密性、认证和访问控制服务的协议。协议通过使用例如加密密钥的加密机制、安全标签和指定的属性来支持这些服务。

课题 11/17

X.400/F.400 消息处理系统和服务概述

本建议书定义了用户代理（UA）到 UA、消息传输代理（MTA）到 MTA、UA 到 MTA 和 UA 到消息存储（MS）机密性、完整性、认证、不可否认和访问控制应用层安全服务的消息处理系统（MHS）元素。（见 F.400） 课题 11/17

X.402 信息技术－消息处理系统（MHS）：总体结构

本建议书定义了为实现应用层定义的机密性、完整性、认证、不可否认性和访问控制服务而在 MHS 协议中使用的安全程序和对象识别符。 课题 11/17

X.411 信息技术－消息处理系统（MHS）－消息传输系统：抽象服务定义和程序

本建议书定义了支持应用层定义的机密性、完整性、认证和不可否认服务的机制和程序。这个协议通过使用建议书 X.509 定义的加密机制、安全标签和数字签名来支持这些服务。虽然本建议书定义了使用不对称加密技术，但也还支持对称加密技术。 课题 11/17

X.413 信息技术－消息处理系统（MHS）：消息存储：抽象服务定义

本建议书定义了支持应用层定义的完整性、访问控制、认证、完整性和不可否认服务的机制、协议和程序。这个协议支持代表消息存储直接用户的这些服务。 课题 11/17

X.419 信息技术－消息处理系统（MHS）：协议规范

本建议书通过提供应用层的认证和访问控制服务，以为 MHS 实体和远处的用户识别安全访问来定义了程序和应用内容。 课题 11/17

X.420 信息技术－消息处理系统－人与人之间的消息系统

本建议书为应用层定义的为人与人之间的消息用户或用户代理的直接用户间的对象交换定义了机制、协议和程序。用层定义的安全服务支持应完整性、机密性、认证和访问控制。

课题 11/17

X.435 信息技术－消息处理系统：电子数据交换消息系统

本建议书为电子数据交换（EDI）用户代理的直接用户间的对象交换定义了机制、协议和程序。应用层定义的安全服务支持完整性、机密性、认证和访问控制。 课题 11/17

X.440 信息技术－ 消息处理系统：话音消息系统

本建议书为了话音用户代理的直接用户间的对象交换定义了机制、协议和程序。应用层定义的被支持的这些安全服务有完整性、机密性、认证和访问控制。 课题 11/17

X.500 信息技术－开放系统互联－号码簿：概念、模型和服务的概述

本建议书定义了号码簿和它的安全特征。 课题 9/17

X.501 信息技术－开放系统互联－号码簿：模型

本建议书定义了号码簿使用的 X.509 公开密钥和属性证书框架。 课题 9/17

X.509 信息技术－开放系统互联－ 号码簿：

---- 认证框架（1993 版 － 第二版）
---- 认证框架（1997 版 － 第三版）
---- 公开密钥和属性证书框架
（200 版－第四版）

本建议书为公开密钥证书和属性证书定义了一个框架，并通过目录为认证管理服务定义了一个框架。它描述了两级的认证：简单认证，使用密码作为通过认证的证明；和强认证，包括加密技术实现的证书。当简单认证提供一些防止非授权访问的有限保护，只有强认证能被作为提供安全服务的基础。这些被定义的框架可以被用于为公共密钥基础设施（PKI）和特权管理基础设施（PMI）描述应用。公开密钥证书的框架包括代表证书它自己的数据对象规范和不再被信任的已发出的证书的撤回通知。虽然它定义了 PKI 的一些关键组件，它没有完整地定义一个 PKI。然而，它提供了建设完整 PKI 及其规范的基础。属性证书的框架包括用于代表证书本身的数据对象规范和不再被信任的已发证书的撤回通知。虽然他定义了 PMI 的一些关键组件和，但它没完整地定义一个 PKI。然而，它提供了建设完整 PKI 及其将要制定的规范的基础。还定义了为支持目录中的 PKI 和 PMI 对象并比较有效值和存储值的信息对象。 课题 9/17

X.519 信息技术－开放系统互联－目录：协议规范

本建议书为在目录实体绑定期间识别安全访问定义了程序和应用内容。 课题 11/17

X.733 信息技术－开放系统互联－系统管理：警报功能

本建议书定义了一个系统管理功能，为了系统管理这个系统管理功能可以在集中或分散的管理环境中被应用程序相互作用。本建议书定义了一个包括了普通定义、服务和功能单元的功能，它被的应在 OSI 参考模型的应用层。这个功能定义的报警通知提供了一个管理可能需要遵照系统固有的运行条件和服务质量的信息。 课题 17/4

X.735 信息技术－开放系统互联－系统管理：日志控制功能

本建议书定义了一个系统管理功能，为了系统系统管理功能可以在一个集中或分散的管理环境中被应用程序相互作用。本建议书定义了日志控制功能并包括了服务和两个功能单元。这个功能定义在应用层。 课题 17/4

X.736 信息技术－开放系统互联－系统管理：安全报警功能

本建议书|国际标准定义的安全报警功能。安全报警功能是一个系统管理功能，为了系统管理的目的这个系统管理功能可以在一个集中或分散的管理环境中的应用程序的交换信息，是由 CCITT 的建议书 X.700 | ISO/IEC 7498-4。本建议书 | 国际标准被安装在 CCITT 建议书 X.200 | ISO7498 的应用层和根据 ISO/IEC 9545 提供的模型。CCITT 建议书 X.701 1 ISO/IEC 10040 定义了系统管理功能的作用。这个系统管理功能定义的安全报警通知提供了与运行情况和服务质量相关的安全信息。

课题 14/4

X.740 信息技术－开放系统互联－系统管理：安全审计跟踪功能

本建议书|国际标准定义了安全审计跟踪功能。安全审计跟踪功能是一个系统管理功能，它能通过在一个集中或分散的管理环境中交换为系统管理目标而由 CCITT 建议书 X.700 1 ISO 7498-4 定义的信息和命令交换。本建议书|国际标准被放在 CCITT 建议书 X.200 1 ISO 7498 的应用层并是根据 ISO/IEC 9545 提供的模型定义的。CCITT 建议书|ISO/IEC 10040 描述了系统管理功能的作用。 课题 14/4

X.741 信息技术 － 开放系统互联 － 系统管理：访问控制的目标和特性

本建议书|国际标准说明了一个访问控安全模型并为建立和管理与 OSI 系统管理相关的访问控制的必要管理信息。任何情况下应用的安全策略都未被说明并被留下作为一个实现选择。这个规范是普通应用并适用于任何应用的安全管理。 课题 14/4

X.800 CCITT 应用的开放系统互联安全体系结构

本建议书定义了与安全相关的总体结构元素，这个元素可以被适当地应用于要求在开放系统间保护通信的环境中。为允许安全通信并由此在 OSI 中提供一个统一的安全方法，在参考模型的框架中，建立了为修订现有建议书或制定新建议书的指导方针和约束条件。为了覆盖通信协议的总体框架元素的安全问题本建议书扩展了参考模型，但没有在参考模型中论述。本建议书概述了参考模型的安全服务和相关机制，并在参考模中定义了可以应用这些服务和机制的位置。 课题 10/17

X.802 信息技术 – 低层安全模型

本建议书描述了 OSI 参考模型低层（传输、网络、数据链接、物理）安全服务修订版的跨层问题。它描述了这些层的体系结构概念、各低层间相关安全交互的基本原理和低层中安全协议的设置。
课题 10/17

X.803 信息技术 – 开放系统互联 – 高层安全模型

本建议书描述了 OSI 参考模型高层（应用、表示和会话层）安全安全服务和机制的选择、设置和应用。 课题 10/17

X.805 提供端到端通信系统的安全体系结构

本建议书定义了在适当地应用时特别是在多提供商环境中能确保网络被很好地保护而不受恶意和疏忽攻击的与安全相关的总体结构元素，和高实用性、适当的反应时间、完整性、可升级性和精确计费功能等性能参数的理的操作。 课题 10/17

X.810 信息技术 – 开放系统互联 – 开发系统的安全框架：概述

本建议书定义了开放系统安全服务被指定的框架。这部分安全框架描述了安全框架的组织结构，定义了安全框架许多部分都适用的安全概念，并描述了框架其他部分定义服务和机制的相互管理。这个框架描述了应用于开放系统认证的所有方面、认证和访问控制等其他安全功能间的关系和认证的管理要求。 课题 10/17

X.811 信息技术 – 开放系统互联 – 开放系统安全框架：认证框架

本建议书为认证管理定义了一个总体框架。认证的主要目的是为了遏制伪装和重复的攻击。
课题 10/17

X.812 信息技术 – 开放系统互联 – 开放系统的安全框架：访问控制框架

本建议书为访问控制管理定义了一个总体框架。访问控制的主要目的是为了遏制计算机和通信系统的非授权操作威胁；这些威胁经常细分为非授权使用、泄密、篡改、破坏和拒绝服务。 课题 10/17

X.813 信息技术 – 开放系统互联 – 开发系统的安全框架：不可否认框架

本建议书为不可否认服务管理定义了一个总体框架。不可否认服务的目标就是收集、维护、获取和确认数据传输中的关于发送者和接收者识别确认证明。 课题 10/17

X.814 信息技术 – 开放系统互联 – 开放系统的安全框架：机密性框架

本建议书为机密性服务管理定义了一个总体框架。机密性是对非授权个人、实体和程序不可访问或不公开信息的属性。 课题 10/17

X.815 信息技术 – 开发系统互联 – 开放系统安全框架：完整性框架

本建议书为完整性服务管理定义一个总体框架。数据没有以非授权的方式被更改或破坏的属性被成为完整性。 课题 10/17

X.816 信息技术 – 开放系统互联 – 开放系统的安全框架：安全审计和警报框架

本建议书为处理安全警报和为开放系统实施安全审计描述了一个基本模型。安全审计是一个独立的系统记录和活动的调查和检查过程。安全审计服务提供了一个能说明、挑选和管理在安全审计过程中要记录的事件的审计权威。 课题 10/17

X.830 信息技术 – 开放系统互联 – 一般高层安全：概述、模型和注释

本建议书属于为支持安全服务管理的 OSI 高层协议的辅助建设提供一套设备的一系列建议书。本建议书定义了如下内容：a)安全交换协议功能和安全传输的通用模型；b)一套支持在抽象体系规范中的可选区域保护要求规范的符号工具；c)一套向关于这个系列的建议书覆盖的一般上层安全设施应用提供情报的指导原则。 课题 10/17

X.831 信息技术 – 开放系统互联 – 一般高层安全：安全交换服务元素（SESE）服务定义

本建议书属于为支持安全服务管理的 OSI 高层协议的辅助建设提供一套设备的一系列建议书。本建议书定义了由安全交换服务元素（SESE）提供的服务。SESE 是便于在 OSI 应用层中支持安全服务管理的安全信息通信的一个应用服务元素（ASE）。 课题 10/17

X.832 信息技术 – 开放系统互联 – 一般高层安全：安全交换服务元素（SESE）协议规范

本建议书属于为支持安全服务管理的 OSI 高层协议的辅助建设提供一套设备的一系列建议书。本建议书说明了由安全交换服务元素（SESE）指定的协议。SESE 是便于在 OSI 应用层中支持安全服务管理的安全信息通信的一个应用服务元素（ASE）。 课题 10/17

X.833 信息技术 – 开放系统互联 – 一般高层安全：保护传输句法规范

本建议书属于为支持安全服务管理的 OSI 高层协议的辅助建设提供一套设备的一系列建议书。本建议书| 国际标准定义了与支持应用层安全服务的表示层关连的保护传输句法。 课题 10/17

X.834 信息技术 – 开放系统互联 –一般高层安全：安全交换服务元素（SESE）协议实现一致性陈述（PICS）的形式

本建议书 | 属于关于一般高层安全（GULS）的一系列协议。它是 ITU-T 建议书 X.832 定义的安全交换服务元素协议和 ITU-T 建议书 X.830 定义的安全交换的协议实现一致性陈述（PICS）的形式。附件 C.本建议书以支持一个具体实现的一致性评估的形式描述了标准化能力和选项。 课题 10/17

X.835 信息技术 – 开放系统互联 – 一般高层安全：保护传输句法协议实现一致性陈述（PICS）的形式

本建议书 | 属于关于一般高层安全（GULS）的一系列协议。他是 ITU-T 建议书 X.833 定义的保护传输语句协议的协议实现一致性陈述（PICS）的形式。本建议书以支持一个具体实现的一致性评估的形式描述了标准化能力和选项。 课题 10/17

X.841 信息技术 – 安全技术 – 访问控制的安全信息对象

这个关于安全信息对象（SIOs）的建议书为访问控制提供了对象定义，为了避免同一个功能出现多个和不同的定义安全标准中都需要这个标准定义。用抽象语句符号 1（ASN.1）对这些对象进行了精确定义。这个建议仅涵盖了安全信息对象（SIOs）的静态方面。 课题 10/17

X.842 信息技术 – 安全技术 – 一般高层安全：使用和管理可信第三方服务的原则

本建议书为使用和管理可信的的三方（TTP）服务提供了指导原则、基本职责和提供服务的清晰定义、它们的种类和它们的目的、TTP 的作用和责任以及使用其服务的机构。本建议书定义了 TTP 服务主要不同的种类包括时戳、不可否认、密钥管理、证书管理和电子公证。 课题 10/17

X.843 信息技术 – 安全技术 – 支持数字签名应用的 TTP 服务规范

本建议书定义了为生成不可否认的文件而需要支持数字签名应用的服务。这也就是文件完整性和真实性的生成器，被描述的服务也可被用于实现完整性和真实性服务。 课题 10/17

X.901 信息技术 – 开放分布式处理 – 参考模型：概述

快速增长的分布式处理已经导致了对开放分布式处理（ODP）标准化的调整框架。这个参考模型提供了一个框架。它生成了一个支持分布式、相互作用和可移植性的体系结构。本建议书包含 ODP 范围、密钥概念的合理说明和 ODP 体系结构的框架。它包括关于这个参考模型是如何说明和应用于它的用户的说明材料，它的用户可能包括标准制订者和 ODP 体系结构的构造者。它还包括一个分类目录，这个目录要求根据建议书 X.903 定义的一致性参考点表示的标准化范围。ODP 系统必须确保安全，例如必须以确保系统设施和数据不被非授权访问、非法使用和任何威胁或攻击破坏的方式被建设和维护。对间接作用及移动的部分系统和系统用户很难达到安全要求。ODP 系统的安全规则可以定义：探测安全威胁的规则；清除安全威胁的保护规则；任何安全破坏所超成损失的限制原则。
课题 26/17

X.902 信息技术 – 开放分布式处理 – 参考模型：基础

本建议书包含了分布式处理系统正常描述的（任意的）概念和分解框架的定义。它介绍了 ODP 标准的一致性原则和使用方法。这些细节足以支持建议书 X.903 并建立对新规范技术的要求。
课题 26/17

X.903 信息技术 – 开放分布式处理 – 参考模型：体系结构

本建议书包含把分布式处理开放必要特征的规范。这是 ODP 标准必须遵守的约束条件。它是用建议书 X.902 定义的描述技术。
课题 26/17

X.904 信息技术 – 开放分布式处理 – 参考模型：体系结构的语义学

本建议书包含在建议书 X.902 的第 8 和第 9 款中定义的 ODP 模型概念标准化。标准化是通过用不同标准的正式描述技术的概念来解释每一概念。
课题 26/17

B.2 本手册中未涉及的安全问题（可靠性和外部设施物理保护）

防止腐蚀、外界碰撞、火灾、人为破坏和其他形式的对公共通信所有类型线缆及相关设施的破坏的外部设施的保护，是从网络可靠性和可用性角度提高信息传输安全级别的一个要素。设备和线缆建设、安全和监控对保证线路性能是非常重要的。越多的信息被传输，通信设施的物理保护越重要。L 系列建议书包括可以提高通信设施和信息传输安全级别的技术。

L.3 线缆护套

由于线缆是直接埋入地下的，护套通过确保线缆不受由石头和挖掘设备或工具的破坏、动物和昆虫的啃咬、化学或电解的腐蚀、大气放电和靠近电力线而引起的机械破坏，而用于保护线缆的安全安装和可靠使用。
课题 8/6

L.4 铝制线缆外壳

铝普遍用于包裹线缆，因为它比使用铅包裹线缆的成本要低而且铝包裹线缆能很大程度上满足技术要求。使用铝包线缆特别适用于干线线缆。 课题 8/6

L.5 使用非铅和铝的其他金属制成的线缆外壳

其他类型的外壳例如波纹铝、铜带等，可以用于特殊应用。 课题 8/6

L.7 接地保护应用

一些通过接地保护的地下金属结构被用于这些由普通保备保护的结构的防腐蚀。一些地下金属结构的接地保护系统是由金属结构和有阴极保护的普通保护设备间电耦合和导电设备组成。接地保护技术提高了地下结构的可靠性，改善了阴极保护设备的有效性并减少了投资总额和保护系统的维护成本 课题 7/6

L.16 用作保护覆盖金属线缆外壳的传导塑料材料（CPM）

CPM 线缆最大的好处就是可以综合防护腐蚀、闪电、电力和牵引线的影响，降低接地维护成本，简化保护方案。 课题 8/6

L.20 为通信设施生成一个火警代码

对于现有建筑物及设计和建设新的建筑物，根据每一建筑物设计的用途，包括火灾安全和防火的最小指导原则，在布设通信安全管理设施时必须生成一个内部火警安全代码。 课题 2/6

L.21 火灾探测和报警系统，探头和报警发声设备

为了保护财产和生命，安装防火探测和报警系统有许多用处，例如探测和定位火灾，为协助抑制和/或扑灭火灾准备，紧急疏散处置，呼叫火警。 课题 2/6

L.22 防火

考虑到发生火灾会造成严重的损失及安全、服务提供和经济部门通信系统防火的重要性，必须考虑到如下几个方面，例如降低火灾几率、将建筑物分成不同的区域（用火区）以减少和延缓火灾的扩散，火灾统计。 课题 2/6

L.23 灭火 — 建筑物里灭火装置和设备的分类及分布

根据通信机房建筑物的用途、位置及使用情况，所采用的灭火方法是不同的。这些就是决定一开始为防火安装的辅助设施数量的主要因素。 课题 2/6

L.25 光导纤缆网络维护

维护系统和程序都能独立于传输设备来监控光缆网络的传输质量。 课题 5/6

L.28 海陆缆的外附加保护

由于环境现象（例如，海浪、水下地震和塌方）和人为活动影响海床（例如，捕鱼、铺设和维护其他业务和缆线），因此浅水缆故障的可能性要比深水缆高。
除了光缆设施所采用的不同外壳－例如岩石外壳（RA）、单层或双层铁丝外壳外，如果需要应该采用附加的外保护。这些保护都能应用于靠近海岸的浅水中和水边与海滩连接处，或沿着线缆路由线路因为外部因素或海床特点可能会破坏线缆的地方。 课题 10/6

L.32 穿过防火区

考虑到在通信建筑物的用火区边缘有大量的直线缆穿过，它降低了灭火系统的有效性，有效措施可能是采取被动吸烟和火灾控制措施，例如用阻燃材料封闭直线缆穿过的地方或用线缆管理（保护）系统。 课题 2/6

L.45 从通信网络的外部设施减小对环境的影响

详细说明了为减小由于在外界使用外部设备而造成的影响（例如，能量和二氧化碳）。这是基于生命周期分析也就是产品的使用周期。 课题 1/6

L.46 保护通信线缆和设施免受生物攻击

描述了生物攻击和保护通信线缆免受攻击的措施。它涉及生物攻击的种类、线缆的缺陷、破坏的特点和认为保护包括依赖线缆位置设施的方法。 课题 1/6

以下建议书介绍了 SDH 和 OTN 网络的可用性规定：

G.841 SDH 网络保护体系结构的类型和特性

这各建议书描述了同步数字系统（SDH）网络的各种保护机制及他们的目标和应用。保护方案被分为 SDH 线路保护（在区域或线路层）和子网连接保护（用内部监控、非打扰监控和子层监控）。
课题 15,16,17,18/15

G.842 SDH 网络保护体系结构的互相配合

本建议书描述了网络保护体系结构之间的互相配合机制。互相配合是为环网间交换流量的单节点和双节点互联。每个环网可以为微软共享保护或为 SNCP 保护而被配置。 课题 15,16,17,18/15

G.808.1 普通保护交叉－线性轨迹和子网保护

本建议书提出了线性保护交换的概观。它包括了基于光传输网络（OTN）、同步数字系统（SDH）网络和异步传输模式（ATM）网络的保护方案。环网保护概述和双节点子网（例如，环网）互联方案将在其他建议书中说明。 课题 Q.15,16,17,18/15

G.873.1 光传输网络（OTN）－线性保护

本建议书定义了 APS 协议和光通道数据单元（ODUk）级光传输网络线性保护方案的保护交换操作。本建议书中考虑到的保护方案是 ODUk 轨迹保护；用内部监测的 ODUk 子网连接保护；用非插入监测的 ODUk 子网连接保护；和用子层监测的 ODUk 子网连接保护。

课题 Q.15,16,17,18/15

G.781 同步层功能

SDH 和 PDH 时钟源的可靠性。本建议书定义了一个基本同步发布组件库，称为“自动功能”和一套规则，通过这些规则那些组件结合起来实现了数字传输设备同步功能。

课题 Q.15,16,17,18/15

G.911 光纤光系统可靠性和可用性的参数和计算方法

光线光系统的可靠性和可用性：本建议书为描述光纤光系统的可靠性和可用性的最小的一套必要参数。系统的可靠性和维护、激活光设备可靠性、被动光设备可靠性及光线和光缆可靠性各有不同的参数。本建议书也为计算设备、网元和系统的预期可靠性提供了指导原则和方法。包括例子。

课题 Q.15,16,17,18/15

G.784 SDH 管理

SDH 管理。G.784 介绍了 SDH 网络元素的故障、配置、计费、性能和安全管理（FCAPS）功能。这些记录中的安全管理问题现在都是‘为了进一步研究’。 课题 Q.14/15

G.874 光传输网络元素的管理问题

OTN 管理。G.874 介绍了 OTN 网络元素的故障、配置、计费、性能和安全管理（FCAPS）功能。在这些记录中的安全管理问题现在都是‘为了进一步研究’。 课题 Q.14/15

G.7712/Y.1703 数据通信网络的体系结构和规范

本建议书包括管理通信网（MCN）和信令通信网（SCN）的安全问题。本建议书中提供的数据通信功能支持无连接网络服务。附加功能将会被加到这个新版建议书中以支持连接的网络业务。

课题 Q.14/15

注：G.650,660-690,950-970 系列中的建议书可能包含一些可靠性相关网络元素。

附件C：研究组和有关安全课题清单

ITU-T 的标准化工作是通过技术研究组（SG）完成的，技术研究组中的 ITU-T 成员代表为各个领域中的国际通信制定建议书（标准）。SG 主要以研究课题的形式开展工作。每个工作组在通信标准的一个特定领域中进行技术研究。每个工作组由国际电信标准化全会（WTSA）任命一名主席和若干副主席。以下是 2001-2004 年研究期中 ITU-T 研究组的名称和任务清单，与安全工作有关的研究课题清单列在其后。

SG 2	服务提供、网络和性能的运行方面问题 服务定义、编号方式、路由和全球移动性领导研究组
要求：负责研究服务提供、定义和服务竞争运营要求等相关原则；编号方式、命名、寻址要求和资源分配包括保留和分配的标准和程序；人力资源；网络运营方面的问题和相应的性能要求包括网络流量管理、服务质量（流量工程、运营性能和服务测量方法）；传统通信网和新兴网络间互联互通运营方面的问题；运营商、制造商和用户对网络运营不同方面反馈的评估。	
主要与安全相关的课题： －课题 5/2 －网络服务质量	

SG 3	资费和会计原则包括与通信经济和政策相关的问题
要求：负责研究国际通信业务的资费和会计的相关原则和与通信经济和政策相关的问题。为了这个目标，研究组 3 将特别鼓励它的成员达成共识以为有效的服务制定一个尽可能低的资费并考虑在可靠的基础上保持独立的通信财务管理。	
主要与安全相关的课题 无	

SG 4	通信管理，包括 TMN TMN 领导研究组
作为管理活动的领导研究组，SG4 从事于以下几个方面的安全问题： a) 体系结构上对管理接口的考虑因素和要求 b) 保护管理网络（即管理平台）的具体要求，特别是网络趋于融合， c) 保护管理信息和安全参数管理的协议和模型	

通信网络的管理根据不同层次上的抽象被定义为，从管理网络元素的信息到用户服务管理。管理系统及管理系统和网络元素间信息交换的安全要求依赖于管理网络是在一个管理域中还是在两个管理域中。基于体系结构原理，明确的要求、机制和协议支持已在现存建议书中定义，而且另外的建议书也在制定中。

主要与安全相关的课题：

－课题 16/4 － 对 IMT-2000 和智能网的 TMN 管理支持

SG 5	电磁环境影响的保护

SG 5 负责研究保护通信网络和设备免受干扰和意外，而且研究电磁兼容（EMC）的相关问题。在完成他们的使命时，SG 5 已研究了一些问题并制定了许多关于网络安全中抵抗电磁威胁的建议书和手册。电磁威胁包括恶意人为高能瞬变现象，例如高位电磁脉冲（HEMP）和高能微波（HPM）。同样，电磁安全可能包括由于设备意外无线电辐射造成的信息泄漏。恶意威胁和相应的克制技术的特性类似于应用于自然或无意电磁干扰的技术特性。因此，研究控制电磁干扰（EMI）和保护免受意外的研究组 5 的传统活动是保证网络安全免受恶意人为威胁。虽然恶意人为电磁威胁和无意或自然电磁环境有许多相似点，但它们还是有一定显著差别的。在完成他们的使命时，在完成他们的使命时，SG 5 已研究了一些课题并制定了许多关于网络安全中抵抗电磁威胁的建议书和手册。

电磁安全的两个原则领域是

- 通信网络和设备的抵抗性和免疫性克制人为高能瞬变现象。这些威胁包括
  - － 高海拔核爆炸产生的电磁范围－高位电磁脉冲（HEMP）。
  - － 高能电磁（HPE）发生器包括高能微波（HPM）和超宽带（UWB）信号源。
- 由于设备意外无线电辐射造成的通信网络信息泄漏的可能性。

通过大量出现在论文、新闻报道和电视节目等媒体中的相关介绍，对这些现象的安全威胁的认识已经加强了。

恶意威胁和相应的克制技术的特性类似于应用于自然或无意电磁干扰的技术特性。例如，HEMP 类似于闪电产生的电磁脉冲。减少设备中多余无线电能量的防护和过滤技术也能减少无意能量泄漏的可能性。因此，研究控制电磁干扰(EMI)和保护免受闪电意外的研究组 5 的传统活动是保证网络安全免受恶意人为威胁。以下表格是 2001-2004 年研究期中分配给研究组 5 的关于网络安全的问题。
主要与安全相关的课题： -课题 2/5 – 宽带接入系统的 EMC（为减少信息泄漏的可能性而对宽带接入系统多余辐射的控制） -课题 4/5 – 新型通信设备和接入网络的抵抗性（为减少信息泄漏的可能性而对宽带接入系统的多余辐射进行的控制） -课题 5/5 – 固定、移动和无线系统的防雷（用于防雷的技术同样提供一定程度的防辐射设备以防 HEMP 和 HPE）。 -课题 6/5 –屏蔽结构和将所有的通信系统接地（合适的屏蔽和接地措施可以帮助设备防辐射以防 HEMP 和 HPE） -课题 12/5 –现有 EMC 建议书的维护和改进（通信设备的 EMC 提高了设备的抗导电能力和象有辐射的 HEMP 环境和 HPE 环境的防辐射能力。同样，通信息设备的 EMC 减少了信息泄漏的可能性）。 -课题 13/5 –现有抵抗性建议书的维护和改进（防雷设备提高了设备的 HEMP 感应振荡抵抗性）

SG 6	室外设施
要求：负责研究室外设施相关问题，例如建筑、安装、连接、终端，防腐蚀和环境破坏引起的其他形式的破坏，除电磁处理之外的所有类型的公共通信线缆和相关设施。	
主要与安全相关的课题： -课题 1/6 – 通信设施的环境课题 -课题 5/6 – 光缆网络的维护	

SG 9	综合宽带有线网络和电视与声音传输 综合宽带有线和电视网络的领导研究组
ITU 关于“综合宽带有线网络和电视与声音传输”研究组（SG9）是关于综合宽带有线网络和电视网络的领导研究组。SG9 制定和维护如下建议书： • 使用有线电缆和光纤铜轴混合的网络主要是为家庭提供电视和声音节目而设计的，例如综合宽带网络同样承载语音或其他实时性业务，视频点播，交互业务等。 • 用通信系统组成，主要分发和次要分发电视、声音节目和相似的数据业务。 在这个角色，SG9 评估宽带网络和业务的威胁和弱点，证明安全目标，评估对策和定义安全体系结构。被介绍的主要安全领域是安全宽带服务，安全 VoIP 业务，安全家庭网络业务和互动电视业务的安全应用环境。	

安全相关的活动已集中于以下一些领域：

- *安全宽带服务*：为宽带接入网提供安全服务。即，有线调制解调器的认证，加密密钥管理，加密和完整的传输数据和安全下载有线调制解调器软件。
- *安全 VoIP 业务*：IP 有线电视通信系统是一个在使用 IP 协议的有线电视网络上承载实时服务的特殊工程，特别是 IP 语音和视频。IP 有线电视通信系统提供的安全服务包括多媒体终端（MTA）认证，服务提供商对 MTA 的认证，安全设备管理和配置，安全设备管理，安全信令和安全媒体。
- *安全家庭网络业务*：增强的电缆调制解调器能够提供家庭网络业务例如防火墙和网络地址转换。提供给增强电缆调制解调器的安全服务包括服务提供商对多媒体终端适配器（MTA）的认证，MAT 对服务提供商的认证，安全设备管理和配置，安全设备管理，包过滤/防火墙功能性，安全防火墙管理和安全下载增强电缆调制解调器软件。
- *互动电视业务的安全应用环境*：互动电视业务基于在 Java 和多媒体家庭平台(MHP)规范中定义的安全服务。

主要与安全相关的课题：

-课题 6/9 – 数字有线电视分发到户的条件访问和复制保护方法和准则

-课题 13/9 – 有线电视网络上的 IP 语音和视频应用

SG 11	信令要求和协议 *智能网的牵头研究组*

要求：负责研究信令要求和互联网协议(IP)簇的相关功能，一些移动性相关功能，多媒体功能和对现有建议书中关于 ATM，N-ISDN 和 PSTN 的访问和互联信令协议簇的修订。

主要与安全相关的课题：

-课题 1/11 – 对新的、增值的、基于 IP 和基于智能网业务信令支持的信令要求

-课题 6/11 – 对拨号互联网访问和语音的业务互联与在基于 IP 网络上的数据和多媒体通信的业务互联信令支持的信令要求。

-课题 12/11 – 增强窄带和宽带业务的访问和网络信令

SG 12	网络和终端的端到端传输性能 *服务质量和性能的领导研究组*

要求：负责指导网络的端到端传输性能，终端和它们的互联，与质量感觉及用户对文本、语音和图象应用接受的相关问题。这个工作包括所有网络（例如那些基于 PDH,SDH,ATM 和 IP 的网络）的相关传输问题和所有通信终端（例如，手持设备，免提设备，头戴设备，移动设备，音视频设备和互动语音响应设备）。

主要与安全相关的课题：

课题 12/12 – 使用互联网协议(IP)网络承载语音业务的传输性能的考虑要素

课题 13/12 – 多媒体服务质量/性能要求

SG 13	多协议和 IP 网络及它们间的互联 IP 相关主题，B-ISDN，全球信息基础设施和卫星主题的领导研究组

根据研究组 13 的职责特点和如下研究领域

- 含有多个域的不同网络间的互联互通，
- 为传送高质量和可靠的网络业务的多协议和创新技术。
- 体系结构、互联互通和匹配、端到端考虑因素、路由和传输要求等特定主题。

就像 IP 相关主题、B-ISDN、全球信息基础设施、卫星相关主题和新的下一代网络计划的领导研究组一样，广义上有许多安全问题将被影响。

传统上，ITU-T 研究组 13 在处理体系结构和网络结构问题时已经包含了安全问题，因为知道完全有必要处理这些问题（从体系结构到观点的实现）是为了确保有一个实用并可靠的网络。

在或多或少新而开放的数字包交换技术和自由主义的环境中安全方面的难题增加了，例如在 GII 概念里。在 GII（或 GII 的子集 NGN）的“增值链”概念中，当包含第三方时以上都是非常真实的。在这个环境中，安全的所有方面将成为一个非常重要的问题并必须以一种含蓄的方式介绍。

因此，研究组 13 决定将每个最新和最终修订的建议书中的章节涉及到的安全问题合并为建议书中一个专门介绍安全的章节。即使建议书中不涉及安全问题，也必须在这个特殊的安全章节中注明。这个决议已经在 SG17 中达成共识并被提交给了 ITU-T 的所有研究组。

SG13 更决定，建议书中有关安全的说明都必须报告给 ITU-T 的 17 研究组，以及时更新“被许可的安全建议书目录”和“ITU-T 许可的安全定义纲要”。

而且新的 NGN 计划用 6.6 节中的特别注意事项介绍了一些章节中的安全问题。

主要与安全相关的课题

课题 1/13 – 一整个异构网络环境的原则、要求、框架和体系机构

课题 3/13 – OAM 和 IP 网络及其他网络的网管

课题 4/13 – 宽带和 IP 相关资源管理

课题 6/13 – IP 网络的性能和正在融合的全球信息基础设施

课题 7/13 – B-ISDN/ATM 网元调度和可用性性能

课题 8/13 – 传输错误和可用性性能

课题 10/13 – 核心网结构和互联互通原则

课题 11/13 – 允许在公众网上承载 IP 业务的机制

SG 15	光学和其他传输网络 接入网传输和光学技术领导研究组

SG15 中的课题 14（课题 14/15）负责说明管理和控制要求以及支持传输设备的信息模型。Q14/15 已经遵循了 ITU 为这些设备和模型的定义而建立的 TMN 概念和框架。安全管理是 TMN 五个管理功能目录中的一个。安全管理已在课题 14/15 的研究范围中。

- 传输设备管理的要求：G.7710/Y.1701, G.784, 和 G.874 分别介绍了在一个对多数技术都很普通的传输网络元素中的设备管理功能（EMF），特别是 SDH NE 和 OTN NE。为日期和时间、故障管理、配置管理、计费管理、性能管理和安全管理定义的应用。这些应用来源于 EMF 功能和它们要求的说明。在这些建议书中的安全管理要求都在被研究。
- 数据通信网络体系机构和要求：G.7712/Y.1703 为可以支持与通信管理网络（TMN）相关的分布式管理通信、与自动交换传输网络（ASTN）相关的分布式信令通信和其他分布式通信（例如，语音通信，软件下载）的数据通信网络（DCN）定义了体系结构要求。不同应用（例如，TMN,ASTN 等）要求基于数据包的通信网络在不同的网络元素间传输信息。例如，TMN 要求象管理通信网络（MCN）中定义的通信网络在两个 TMN 网络元素（例如，NEF 和 OSF 网络元素）间传输管理信息。ASTN 要求象信令通信网络（SCN）中定义的通信网络在两个 ASTN 网络元素（例如，CC 网络元素）间传输信令信息。G.7712/Y.1703 为了 MCN 安全要求参照的是 M.3016。SCN 安全要求在 G.77.12/Y.1703 中被定义。
- 分布式呼叫和连接管理：G.7713/Y.1704 为用户网络接口（UNI）和网络节点接口（NNI）都提供了分布式呼叫和连接管理的要求。本建议书中的要求为实现自动呼叫操作和连接操作指定了接口间的通信。安全属性和其他属性被指定认证呼叫和连接操作（例如，这可能包括允许呼叫请求和可能的呼叫请求的完整性检测认证的信息）。
- 自动交换光网络中的路由体系结构和要求：G.7715/Y.1706 说明了为自动交换光网络（ASON）框架中建立交换连接（SC）和软永久连接（SPC）路由功能的要求和体系结构。本建议书涵盖的主要领域包括 ASON 路由体系结构和包括路径选择、路由属性、抽象信息和状态图在内的功能组件。本建议书参考了安全考虑因素的 ITU-T Rec. M.3016 和 X.800。特别地，依靠使用路由协议的上下文它说明了在机密性、数据完整性、可说明性和实用性的 ITU-T Rec.M.3016 中定义的整体安全目标可具有不同的重要级别。被提出的路由协议的安全分析应该介绍以下基于 ITU-T Rec. X.800 的条款（包括伪装、窃听、未授权的访问、衰减或错误信息（包括重放攻击），否认、伪造和拒绝服务）。

- ASON 管理的框架：G.fame 介绍了 ASON 控制层和管理层与 ASON 控制层之间的互通的管理问题。将包括：故障管理、配置管理、计费管理、性能管理和控制层网络元素安全管理要求。

与安全有关的主要课题：

-课题 14/15 – 传输系统和设备的网络管理

SG 16	多媒体业务、系统和终端 关于多媒体业务、系统和终端、电子商务的领导研究组

16 研究组是关于多媒体业务、系统和终端的领导研究组并领导着电子商务研究。课题 G(WP2/16)包括“多媒体系统和业务的安全”并介绍了以下一些安全问题。

增强多媒体（MM）应用象基于包交换网络的电话，IP 语音，电视电话会议、MM 消息、音频/视频流及其他都在异构网络环境中面临着不同程度严峻的安全威胁。滥用、恶意篡改、窃听、和拒绝服务攻击只是一小部分潜在的威胁；特别是在 IP 网络上。

大家一致认为，那些应用都能通过普通的安全措施来达到有普通的安全要求；例如，通过网络安全。然而，MM 应用典型地采取了能够被安全措施很好地在应用层被执行的应用说明安全需求。课题 G 关注于 MM 应用的应用安全问题和并认为采取补充的网络安全措施是合适的。

主要与安全相关的课题

-课题 G/16 – 多媒体系统和业务的安全

SG 17	数据网络和通信软件 关于帧中继、通信系统安全、语言和描述技术的领导研究组

要求：负责研究数据通信网、包含网络、目录和安全的开放系统通信的应用、技术语言及其应用方法和通信系统软件的其他方面。

与安全相关的课题：

课题 9/17 – 目录业务和系统

课题 10/17 – 安全要求、通信系统和业务的模型及指导方针（注：17 研究组同意将课题 10/17 分成 6 个独立的课题：G/17- 安全计划；H/17 – 安全体系结构和框架；I/17 – 网络安全；J/17 – 安全管理；K/17 – 远距离生物测定；和 L/17 – 安全通信业务）

SSG	特别研究组“IMT-2000 和超 IMT-2000” 关于 IMT2000 和超 IMT 2000 的移动性领导研究组
关于“IMT-2000 和超 IMT-2000”的 ITU-T 特别研究组已经将安全作为在 IMT-2000 的 Q.1741.X(3GPP)和 Q.1742.x(3GPP2)系列建议书中定义的 IMT-2000(3G)家族成员参考建议书的重要方面。这包括对潜在威胁的评估、介绍潜在威胁的安全要求列表、安全目标和原则、确定的安全体系结构（例如，安全特征和机制），加密算法要求，合法监听体系结构和功能。这些研究都安排在 SSG 的课题 3，6 和 7 中。合法监听研究的主要目标是认证需要由服务提供商提供给国家司法机关的有用的监听和监测信息。监听的相关信息和通信内容可能与技术无关或是依赖于 3G 及演进的 3G 移动网络。	
与安全相关的主要课题： - 3/SSG －现有和演进 IMT-2000 系统的认证 - 6/SSG － 演进的 IMT-2000 系统的融合 - 7/SSG －已通过的和现有的 IMT- 2000 系统的统一	

与安全有关的 ITU-T 建议书一览表

安全体系结构框架

X.800 – 安全体系结构
X.802 – 低层安全模型
X.803 – 高层安全模型
X.805 – 提供端到端通信的安全体系结构
X.810 – 开放系统安全框架：概述
X.811 – 开放系统安全框架：认证框架
X.812 – 开放系统安全框架：接入控制框架
X.813 – 开放系统安全框架：不可否认框架
X.814 – 开放系统安全框架：机密性框架
X.815 – 开放系统安全框架：完整性框架
X.816 – 开放系统安全框架：安全审计和告警框架

协议

X.273 – 网络层安全协议
X.274 – 运输层安全协议

帧中继的安全

X.272 – 经由帧中继网的数据压缩和保密

安全技术

X.841 – 访问控制的阿安全信息目标
X.842 – 可信第三方服务的使用和管理指南
X.843 – 支持数字签名应用的 TTP 服务的规范

号码簿服务和认证

X.500 – 概念、模型和服务概述
X.501 – 模型
X.509 – 空凯密钥和属性证书框架
X.519 – 协议规范

网络管理安全

M.3010 – 电信管理网的原理
M.3016 – TMN 安全概述
M.3210.1 – IMT-2000 安全管理的 TMN 管理服务
M.3320 – TMN X 接口的管理要求框架 **M.3400** – TMN 管理功能

系统管理

X.733 – 告警报告功能
X.735 – 登录控制功能
X.736 – S 安全告警报告功能
X.740 – 安全审计跟踪功能
X.741 – 访问控制的目标和属性

传真

T.30 附件 G – 采用 HKM 和 HFX 系统的安全三类文件传真传输的程序
T.30 附件 H – 基于 RSA 算法的三类传真的安全
T.36 – 使用第三组传真终端的安全能力
T.503 – 四类文件传真互换的文件应用概况
T.563 – 四类传真设备的终端特性

电视和有线电视系统

J.91 – 确保远程电视传输秘密的技术方法
J.93 – 关于有条件进入有线电视系统数字电视二次传输的要求
J.170 – IPCablecom 安全规范

多媒体通信

H.233 – 视听服务的机密系统
H.234 – 视听服务的加密密钥管理和认证系统
H.235 – H 系列 (H.323 和其他以 H.245 为基础的)多媒体终端的安全和加密
H.323 附件 J – 基于信息包的多媒体通信系统 — H.323 附件 F 的安全（简单端点型的安全）
H.350.2 – H.235 的号码簿认证服务体系结构
H.530 – H.323 多媒体移动环境中 H.510 的安全

ITU-T 建议书可从 ITU 网站 http://www.itu.int/publications/bookshop/how-to-buy.html 获取(该网站还包括关于有限制地获取 ITU-T 建议书的信息)

目前在 ITU-T 开展的与安全有关的重要工作包括

远程生物识别，安全管理，移动性安全，应急电信

有关 ITU-T 及其研究组的详情见: http://www.itu.int/ITU-T