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

ITU-T 电信标准化部门

2006 年

国际电信联盟

ITU-T – 电信标准化局 (TSB)
Place des Nations – CH-1211 Geneva 20 – Switzerland
电子邮件: tsbmail@itu.int 网址: www.itu.int/ITU-T

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

ITU-T 国际电信联盟
电信标准化部门

2006

国际电信联盟

致谢

本手册的编写得到了众多作者的帮助，他们或者参与制定了相关ITU-T建议书，或者参加了ITU-T的研究组会议、讨论会和研讨会。对下列供稿人：Herb Bertine, David Chadwick, Martin Euchner, Mike Harrop, Sándor Mazgon, Stephen Mettler, Chris Radelet, Lakshmi Raman, Eric Rosenfeld, Neal Seitz, Rao Vasireddy, Tim Walker, Heung-Youl Youm, Joe Zebarth, 以及国际电联电信标准化局各位顾问，谨致特别的谢意。

目录

前言

直到不久前，电信和信息技术安全问题还主要存在于银行、航空和军事应用等专业领域。不过随着数据通信，特别是互联网应用的迅速、广泛的增长，安全几乎成了每个人的事。

信息通信技术安全问题日渐受到重视的现象可能受到流传甚广的病毒、蠕虫、黑客和对个人隐私的威胁等事件的影响。但是，随着计算技术和联网成为日常生活的重要组成部分，毫无疑问，需要采取有效的安全措施来保护政府、业界、商务、关键基础设施和消费者的计算机和电信系统。此外，越来越多的国家已经形成数据保护立法，这些立法也要求与数据机密性和完整性的示范标准相一致。

人们应该把安全作为一个深思熟虑的过程，应用于从系统的设想和设计到系统的安装和部署的全过程。在制定标准时，对安全的考虑必须始终从一开始就成为工作的一部分，而不应作为事后的补救措施。在标准和系统开发的设计阶段对安全问题考虑不周，很容易导致产生易受攻击的弱点。通过对安全事项保持清醒的认识，通过确保对安全问题的考虑成为规范的一个基本组成部分，以及通过提供指导意见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，标准化委员会在保护电信和信息技术系统方面所起的作用是至关重要的。

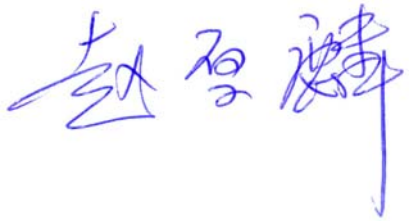
多年来，国际电信联盟的电信标准化部门 ITU-T 一直积极参与电信和信息技术的安全工作。但是，鉴于各种信息繁多，人们并不总是很容易弄清楚哪些已得到研究，以及到哪里去找相关资料。本手册尝试将关于 ITU-T 相关工作的所有已知信息综合在一起，以方便人们的检索。

本手册旨在为技术人员、中层管理人员以及负责制定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。

本手册的第一版是 2003 版，于 2003 年 12 月出版，时值信息社会高峰会议（WSIS）第一阶段会议召开前夕。本手册的出版引起了世界各地信息通信技术界的热烈反响。受此鼓舞，并考虑到读者的宝贵建议和反馈意见，我们又编写了第二版。该版本于 2004 年 10 月出版，采用了新的结构，补充了新的资料，并对有些部分做了进一步阐述。2004 年 10 月 5-14 日在弗洛里亚诺波利斯举行了世界电信标准化全会（WTSA-04），第三版，也就是现在的 2006 版，考虑了因这届全会而出现的研究组与研究课题的新结构。

我向国际电联电信标准化局的工程师们表示赞赏，他们在来自国际电联成员的有关专家们的支持下完成了本手册第一版的大部分章节，任务艰巨，成绩显著。我还要向给我们提出宝贵建议的人们以及为本手册新版做出贡献的人们表示赞赏。对 ITU-T 安全事项牵头研究组第 17 研究组主席 Herbert Bertine 先生以及来自第 17 研究组和其他 ITU-T 研究组的合作者队伍，我表示特别的谢意。

我相信，本手册将成为关注处理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。



国际电联电信标准化局主任

赵厚麟

2006 年 6 月，日内瓦

概要

通信业通过开发能够缩小社会差距的通信基础设施，极大地促进了几乎所有产业部门和世界每个角落的全球生产率和效率的提高。之所以出现这一情况，在很大程度上归因于采用了像 ITU-T 这类标准化组织制定的标准。这些标准保证了网络运作的互操作性和效率，而且为下一代网络（NGN）打下了基础。但是，尽管标准不断地满足了最终用户和通信业的需要，随着开放界面与协议的使用越来越多、新的市场参与者的多元化、应用与平台的充分多样性以及未必经过充分测试的实际应用，导致恶意使用网络的机会不断增加。近年来，全球网络上都观察到安全侵犯（如病毒、破坏存储数据机密性的攻击）激增，经常造成巨大的损失。由此引出的问题是，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。在很大程度上，答案在于制定非常牢靠的规范，应对对通信基础设施任何部分的安全威胁。以此为目标，标准组织的工作包括开发标准化的安全结构与框架、制定安全管理标准、开发安全专用协议和开发保证通信协议安全的技术，还包括制定措施，从总体上把通信标准的潜在弱点降至最小程度。

本安全手册的目是对 ITU-T（有时与其他标准开发组织协作）为保障通信基础设施及相关服务和应用的安全而制定的众多建议书做一个综述。

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 节介绍了在 ITU-T 建议书中定义的基本安全体系结构和要素，还介绍了已经规定的讨论网络应用端对端安全问题的八个安全尺度 – 保密、数据机密性、认证、数据完整性、不可抵赖、访问控制、通信安全和可用性。这些一般化的原则也作为一个基础，用于许多其他安全服务与机制的标准。

第 3 节介绍了威胁、弱点和风险三个基本安全概念，解释了这些概念之间的关系及其与标准机构的相关性。

第 4 节以前几节的资料为基础，提出了电信网的安全要求。该节特别讨论了电信网安全的目标和可以用于达到这些目标的服务。

第 5 节介绍了公开密钥与特权管理基础设施的重要概念。这些基础设施，包括其基础机制，对支持认证与授权服务尤其重要。

ITU-T 已在其建议书中为若干系统与服务制定了安全规定，且从第 6 节可以看出，本手册的一个着重点在于应用。这些应用包括 IP 话音与 IP 多媒体应用 (H.323 和 IPCablecom)、医疗保健和传真。在布署体系以及如何制定协议以满足安全需求方面对这些应用进行了描述。除提供应用信息的安全外，还需要保障网络基础设施和网络服务管理的安全。第 6 节还包括一些标准实例，这些标准制定了处理网络管理问题的安全规定。

第 7 节讨论安全的可用性尺度与基础设施层。这属于 ITU-T 核心职能范围中的两个，尽管并不总是被认为有助于安全。给出了可用性计算的资料和提高传送网可用性的方式的资料。该节最后给出了保障外部设备安全的指导意见。

第 8 节概括了 ITU-T 最近批准的关于事故管理机构和安全事故处理的指导原则。鉴于电信与信息系统基础设施中的安全威胁不断发展，这一问题被普遍认为具有根本的重要性。

此外，本手册还含有与安全问题有关的现行版本的 ITU-T 建议书目录 — 附件 A 中的清单进一步全面展示了 ITU-T 关于安全工作的迹象。本手册还给出了关于安全及本手册论及的其他议题的缩写与定义清单，摘自相关 ITU-T 建议书及其他资料来源（如 ITU-T SANCHO 数据库和 ITU-T 第 17 研究组制定的《ITU-T 批准的安全定义汇编》）。这部分资料在附件 B 中给出。附件 C 归纳了每一 ITU-T 研究组所做的安全相关工作。附件中的这些资料将不断更新，在www.itu.int/ITU-T可以查到。

总之，ITU-T 不仅在 IP 相关技术研究方面，而且在满足不同产业部门千差万别的安全需求方面，一直是积极主动的。本手册从以下两个方面揭示了 ITU-T 建议书是怎样提供解决办法的：一般性的框架与体系结构和特定的系统与应用 — 后者已由网络与服务提供商在全球实施。

1 手册范围

本手册概述了电信和信息技术中的安全问题，描述了实际问题并指明了 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。手册还涵盖了安全的其他方面，尤其是与可用性有关的部分 — ITU-T 有许多这方面资料可提供，以及与环境性损害有关的部分 — ITU-T 在这方面也很活跃。本手册还包括第二版发布以来安全相关标准化工作取得的成果。另外，所讨论的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，本手册的后续版本会处理这部分问题。

本手册的目标读者包括工程师、产品经理、学生、专业人员，以及希望深入了解实际应用中安全问题的负责制定和执行电信规则的相关人员。

2 基本安全体系结构和服务

在二十世纪八十年代前期的通信标准化工作中，人们已经认识到需要对安全体系结构的要素加以讨论。开放系统安全体系结构（ITU-T X.800 建议书）即由此形成。不过，人们也认识到另一点，就是对支持安全服务与机制而言，这不过是开发一套标准的第一阶段。这一工作大多是与 ISO 协作完成的，在此基础上形成了更多的建议书，包括规定了如何将特定类型的保护施用于特定环境的安全模型与框架。此外，还确认了对其他安全体系的需求，如用于开放分布式处理的安全体系结构和用于提供端对端通信的系统的安全体系结构。最近公布的 ITU-T X.805 建议书涉及这一需求，并通过给出旨在提供端对端网络安全的安全解决方案而补充了 X.800 系列建议书。

2.1 开放系统安全体系结构（X.800）

第一个要标准化的通信安全体系结构是 ITU-T X.800 建议书的开放系统安全体系结构。该建议书规定了可以按照所需保护的环境施用的一般性安全相关体系结构要素。尤其是 X.800 建议书概括描述了安全服务和用于提供这种服务的相关安全机制。它还按照七层开放系统互连（OSI）基本参考模型规定了实施安全服务最适宜的位置。

ITU-T X.800 建议书关注的只是某条通信路径直观的性能，这些性能允许终端系统间进行安全的信息传送。该建议书并未打算提供任何种类的实现规范，也未给出任何方法来评估某种实现与该标准或任何其他安全标准的一致性。该建议书也根本没有表明终端系统为支持 OSI 安全特性可能需要的附加安全措施。

尽管 X.800 是作为 OSI 安全体系结构专门制定的，但 X.800 的基础概念已经显示出具备更广的实用性和包容性。该标准特别重要，因为其中的基础安全服务（*身份认证、访问控制、数据机密性、数据完整性和不可抵赖*）以及如*可信功能性、事件检测和安全审查与恢复*等其他更一般化（普遍）服务的定义，代表了这方面第一个国际一致意见。在 X.800 之前，关于所需的基础安全服务都有哪些、每种服务到底起什么作用，存在各种意见。X.800 反映了国际上关于这些服务的完全一致的意见。（第 2.3 节将详细讨论基础安全服务。）

X.800 代表了关于描述安全特性所用术语的含义、关于保护数据通信所需的那组安全服务以及关于这些安全服务的性质的一种重要的一致意见，其价值和普遍适用性就来自这个事实。

在 X.800 的形成过程中，还确认了对相关的附加通信安全标准的需求。因此，在 X.800 制定之后，开展了关于若干辅助性标准和补充性体系结构建议书的工作。下文将讨论其中的一些建议书。

2.2 低层与高层安全模型（X.802和X.803）

低层与高层安全模型（分别为 ITU-T X.802 和 X.803 建议书）用于显示安全框架中形成的安全概念是如何应用于开放系统体系结构的特定范围的。

“高层安全模型”（X.803）的用途是向标准开发人员提供体系结构模型，用于开发七层 OSI 模型的高层中与应用无关的安全服务和协议。该建议书为会话层、表示层和应用层的安全服务之间的定位和相互关系提供了指导意见。该建议书特别说明了在应用层和表示层如何处理安全传送功能（如加密）。另外，引入了*安全交换*的概念。还对*安全政策*和*安全状态*做了说明。

“低层安全模型”（X.802）为开发 OSI 模型的低层适用的安全相关协议和协议要素提供了指导意见。该模型说明了低层之间安全交互的基本内容，还说明了安全协议的定位。

2.3 安全框架（X.810-X.816）

制定“安全框架”是为了对 X.800 规定的安全服务提供一个全面、统一的描述。这些框架旨在从各方面讨论安全服务如何适用于特定的安全体系结构，包括未来可能出现的安全体系结构。框架重点关注的是为系统、系统内的对象和系统间的交互提供保护。框架不涉及系统或机制的构建方法。

框架既涉及数据要素，也涉及用于获得特定安全服务的操作序列（不包括协议要素）。这些服务可适用于系统内相互通信的实体，也可适用于系统间交换并由系统管理的数据。

2.3.1 安全框架概况（X.810）

“安全框架概况”介绍了其他框架，说明了所有框架中共同的概念，包括安全域、安全授权和安全政策。该建议书还说明了可用于安全地传送认证与访问控制两种信息的一种通用数据格式。

2.3.2 认证框架（X.811）

*认证*是对一个实体自称的身份提供保证。实体不仅包括人类用户，还包括设备、服务和应用。认证还对一个实体未试图冒名顶替或未经授权地重播一个先前的通信提供保证。X.800 确认了两种形式的认证：*数据来源认证*（即证实所收数据的来源是声称的那个）和*对端实体*认证（即证实某个关联中的对端实体是声称的那个）。

认证框架占据了一系列认证标准顶部的一个位置，这些标准给出了概念、命名法和认证方法的分类。这一框架规定了认证的基本概念；确认了认证机制的可能类别；规定了这些机制类别的服务；确认了支持这些机制类别的协议的功能要求；确认了认证的一般管理要求。

认证通常在识别之后。识别、认证和授权所用的信息应加以保护。

2.3.3 访问控制框架（X.812）

*访问控制*是为了防止未经授权而使用资源，包括防止以未经授权的方式使用资源。访问控制确保只有得到授权的人员或设备才被允许访问网络单元、存储的信息、信息流、服务和应用。

访问控制框架对一个模型做了说明，包括开放系统中访问控制的各个方面、与其他安全功能（如认证和审查）的关系以及访问控制的管理要求。

2.3.4 不可抵赖框架（X.813）

*不可抵赖*是防止实体事后否认其实施了某一行为的能力。不可抵赖涉及确认可在事后用于戳穿虚假主张的证据。X.800 说明了两种形式的不可抵赖服务，即*有交付证据的不可抵赖*，用于戳穿接收者否认曾收到数据的谎言，以及*有来源证据的不可抵赖*，用于戳穿发送者否认曾发出数据的谎言。不过更一般地讲，不可抵赖的概念可以扩展到许多不同的范围，包括数据的生成、提交、存储、传输与接收的内容的不可抵赖。

不可抵赖框架扩展了 X.800 所述的不可抵赖安全服务的概念，并给出了开发这些服务的框架。不可抵赖框架还确认了支持这些服务的可能机制和不可抵赖的一般管理要求。

2.3.5 机密性框架（X.814）

*机密性*是不向未经授权的个人、实体或过程提供信息或泄露信息的属性。

机密性服务的用途是防止未经授权泄露信息。机密性框架通过规定机密性的基本概念、规定机密性的可能类别和每一类别机密性机制可能需要的设施、确认所需的管理与支持服务，以及通过探讨同其他安全服务与机制的交互作用，处理信息检索、发送与管理中的机密性问题。

2.3.6 完整性框架（X.815）

*数据完整性*是指数据没有以未经授权的方式被改变的属性。总的来说，完整性服务涉及需要确保数据没有受损，或如果受损，让用户了解这一事实。尽管完整性涉及不同的方面（如数据完整性和系统完整性），但 X.800 几乎仅关注数据完整性。

完整性框架涉及信息检索、传送与管理中数据的完整性。它规定了完整性的基本概念；确认了完整性的可能类别和各类别机制所用的设施；确认了支持各类别机制所需的管理，并探讨了完整性机制与支持服务同其他安全服务与机制的交互作用。

2.3.7 审查与告警框架（X.816）

安全审查是对系统记录与活动的独立复审与考察，以便测试系统控制的适当性，确保与既定政策和运营程序的一致性，检测破坏安全的行为，并提出控制、政策与程序方面的指征变化。安全告警是在检测到符合安全政策规定的告警条件的安全相关事件时生成的消息。

审查与告警框架规定了基本概念，给出了安全审查与告警的一般模型，确定了审查与告警机制的类别，规定了用于这些机制类别的服务，确认了支持这些机制的功能要求，并确认了安全审查告警的一般管理要求。

2.4 提供端对端通信的系统的安全体系结构（X.805）

近来网络的安全体系结构又得到了重新审视。由此形成了 ITU-T X.805 建议书，该建议书为提供端对端网络安全而规定了一种安全体系结构。该体系结构可适用于其端对端安全问题与网络的基础技术无关的任何种类的网络。这些一般性原则与定义适用于所有应用，尽管诸如威胁与弱点的细节以及应对或防止的对策根据应用需求的不同而有所不同。

该安全体系结构是根据层和平面两个主要概念规定的。各安全层为第一个轴线，涉及对构成端对端网络的网络单元与系统的要求。为保证端对端的安全在每一层实现，在区分跨不同层的要求时使用了分层次的方法。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提供端对端安全时不同应用允许重复使用。每一层的弱点不同，因此针对性措施也根据每层需求来规定。基础设施层包括网络传输设施和单独的网络单元。属于基础设施层的组成部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。服务层涉及为用户提供的网络服务的安全。这些服务的范围从租用线服务这样的基础连接性服务延伸到即时消息这样的增值服务。应用层涉及对客户所用的网络应用的要求。这些应用可能像电子邮件那么简单，也可能像协同视觉化那么复杂，在石油勘探或汽车设计等场合要使用非常高端的视频转换。

第二个轴线涉及网络中实施的活动的安全。该安全框架定义了三个安全平面，表示一个网络中发生的三种受保护的活动。这些安全平面是：（1）管理平面，（2）控制平面和（3）最终用户平面。这些安全平面分别涉及与网络管理活动、网络控制或信令活动和最终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平面关注的是运营、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。控制平面与通过网络建立（和修改）端对端通信的信令有关，与网络中所用的媒介和技术无关。最终用户平面涉及客户访问与使用网络的安全。该平面还负责处理最终用户数据流的保护。

该框架还利用安全层和安全平面两条轴线（三个安全平面和三个安全层）定义了旨在讨论网络安全的八个尺度。这些尺度在下文定义。从体系结构的角度看，这些安全尺度是作用于由层和平面构成的 3 乘 3 矩阵中的每一个方格的，由此可决定合适的应对措施。图 2-1 表示安全体系结构中的安全平面、层和尺度。关于管理平面的第 6.4 节表明了其他 ITU-T 建议书如何处理 3 乘 3 矩阵中管理平面的三个方格。

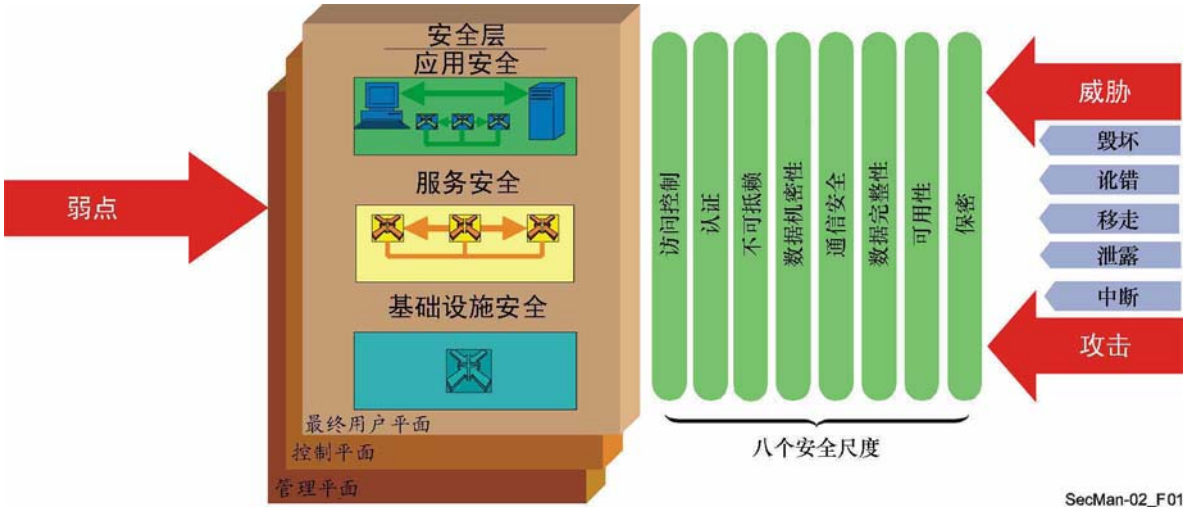


图 2-1－ITU-T X.805建议书中的安全体系结构的要素

X.805 是以 X.800 的概念和上文讨论的安全框架（X.810-X.816）为基础形成的。尤其是 X.800 基础安全服务的功能性（访问控制、认证、数据机密性、数据完整性和不可抵赖）与 X.805 相应安全尺度的功能性是匹配的（如图 2-1 所示）。另外，X.805 的通信安全、可用性和保密三个安全尺度提供了新型的网络保护。下面回顾一下八个安全尺度。

— 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得到授权的个人或设备访问网络单元、存储的信息、信息流、服务和应用。

— 认证安全尺度用于证实通信实体的身份。认证确保了参与通信的实体（如个人、设备、服务或应用）具有自称的身份，还对一个实体未试图冒名顶替或未经授权地重播一个先前的通信提供保证。

— 不可抵赖安全尺度通过给出各种网络相关活动的可用证据（如义务、意图或承诺的证据；数据来源证据，所有权证据，资源使用证据），为防止个人或实体否认实施了涉及数据的某种行为提供了方法。它确保了提供给第三方用于证实已发生某种事件或行为的证据是可用的。

— 数据机密性安全尺度防止数据遭未经授权的泄露。数据机密性确保未经授权的实体无法理解数据内容。加密、访问控制清单和文档权限是提供数据机密性的常用方法。

— 通信安全安全尺度确保信息只在得到授权的端点间流动（信息在这些端点间流动时无法改向或被中途拦截）。

— 数据完整性安全尺度确保数据的正确性或准确性。防止数据遭未经授权的修改、删除、生成和复制，并给出这些未经授权活动的迹象。

— 可用性安全尺度确保对网络单元、存储的数据、信息流、服务和应用的得到授权的访问不因影响网络的事件而被拒绝。灾害恢复解决方案就属于这个类别。

— 保密安全尺度对从观察网络活动可能得出的信息提供保护。这种信息的例子包括用户访问过的网站、用户的地理位置以及服务提供商网络中设备的 IP 地址与 DNS 名称。

在定义和规划阶段，通过在每一安全层和平面顾及每一安全尺度，X.805 安全体系结构可以指导制定全面的安全政策定义、事故应对与恢复计划以及技术体系结构。X.805 安全体系结构还可以用做安全评估的基础，在政策和程序已经展开、技术已经部署的情况下检查安全计划的实施是如何处理安全尺度、层与平面的。一旦实施了安全计划，就必须予以维护，以适应不断变化的安全环境。X.805 安全体系结构可以通过确保对安全计划的修改在每一安全层与平面顾及每一安全尺度，来协助管理安全政策与程序、事故应对与恢复计划以及技术体系结构。

3 保护的基础：威胁、弱点和风险

在形成任何安全框架的过程中，对要保护的资产、保护这些资产必须应对的威胁、与这些资产有关的弱点以及这些威胁和弱点对资产产生的整体风险有一个清醒认识是十分重要的。

总的来说，在 ICT 安全范围内要保护的资产如下：

— 通信和计算服务；

— 信息和数据，包括与安全服务有关的软件和数据；以及

— 设备和网络设施。

根据 X.800，安全威胁是一种潜在的破坏安全的行为。威胁的例子包括：

— 未经授权泄露信息；

— 未经授权毁坏或修改数据、设备或其他资源；

— 信息或其他资源的盗窃、移动或损失；

— 中断或拒绝服务；以及

— 假冒或顶替得到授权的实体。

威胁可能是*偶发的*或*故意的*，也可以是*主动的*或*被动的*。偶发威胁是没有预谋的威胁，如系统或软件功能失常或实际设备失效。故意威胁是实施蓄意行为的某人实现的威胁（故意威胁如果得以实现，则称为*攻击*）。主动威胁是导致状态有所改变的威胁，如改变数据或毁坏实际设备。被动威胁不引起状态的改变。窃听就是被动威胁的一个例子。

*安全弱点*是可被用来破坏系统或系统所含信息的瑕疵或不足（X.800）。弱点会让威胁成为现实。

弱点有四种类型：*威胁型*弱点来源于很难预测未来可能的威胁；*设计和规范型*弱点来源于协议设计中的错误或疏忽使其本质上具有弱点；*实现型*弱点是协议实现中的错误产生的弱点；*运行和配置型*弱点来源于实现中选项的错误使用或软弱的部署政策（例如在 WiFi 网络中没有强制使用加密）。

*安全风险*是在安全弱点被利用，即在威胁得以实现的情况下衡量其所致消极影响的尺度。尽管风险是无法消除的，但一个安全目标是把风险降到可接受的水平。为了做到这一点，有必要理解威胁和弱点并采取适当的应对措施（即安全服务与机制）。

尽管威胁或威胁的促发因素会改变，但安全弱点在系统或协议的寿命期内是一直存在的，除非采取处理弱点的具体措施。采用标准化的协议，基于协议的安全风险就会非常高并且是全局范围的。因此了解和辨识协议中的弱点并在确认弱点后采取措施处理是十分重要的。

标准化机构既有责任，也有独特的能力解决规范中体系结构、框架和协议等方面固有的安全弱点。即便充分了解了与信息处理和通信网络有关的风险、弱点和威胁，如果不按照相关的政策系统地实施安全措施，也无法达到足够的安全，而这一政策也需要定期复审和更新。另外，还需要对安全管理和事故处理做出完备的规定。这包括识别出预防或应对安全事故的责任和规定的措施（条文、控制手段、应对措施、要采取的保护性措施或要开展的行动）。ITU-T 正在制定新的建议书，涉及安全管理的这些方面。

4 电信网的安全要求

本节给出了从使用者，包括电信网的运营人员的角度看在安全性质的需求方面和安全性质的特征方面要考虑的基本问题。这些要考虑的问题是从电信市场各方的需求得出的。本节主要指出了 ITU-T E.408 建议书《*电信网安全要求*》批准后取得的成绩。该建议书给出了安全要求的概况，提出了确认总体电信网（既包括固定也包括移动；既有话音也有数据）安全威胁的框架，并对可降低由威胁产生的风险的应对措施的规划提供了指导意见。

该建议书具有通用的性质，没有确认或处理具体网络的要求。

没有考虑新的安全服务，而是寻求利用其他 ITU-T 建议书和其他机构的相关标准中的现有安全服务。

实施既定的要求将会促进下列电信网安全领域的国际合作：

- 信息共享和信息传播；
- 事故协调和危机应对；
- 安全人员的招聘与培训；
- 法律实施的协调；
- 保护关键基础设施和关键服务；以及
- 制定适用的法规。

为了成功地实现这种合作，对网络的国家级组成部分的要求必须在国家层面实施。

4.1 理由

对国际电信通用网络安全框架的要求来自不同的源头：

- 客户/订户需要树立对网络和所提供的服务的信心，包括大灾（含民间暴力活动）发生时服务的可用性（尤其是应急服务）。
- 公共团体/政府机构的指令和立法中要求安全，以保证服务可用性、公平竞争和隐私保护。
- 网络运营商/服务提供商自身需要安全，以在国家和国际层面保护其运营和商业利益，承担他们对客户和公众的义务。

对电信网的安全要求宜应基于国际公认的安全标准，因为这样做有益于重复利用，避免另起炉灶。与被保护的交易的价值相比，提供和使用安全服务与机制可能相当昂贵。因此，根据被保护的服务提供客户定制的安全能力非常重要。所用的安全服务与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服务的安全简表。

标准化有利于解决方案和产品的重复利用，意味着安全可以更快、更便宜地实现。

在安全方面，标准化的解决方案对系统的供应商和用户的重要益处是一样的，即产品开发的规模效益和电信网中各部件的互操作性。

有必要为电信网提供安全服务与机制，使其免遭恶意攻击，如拒绝服务、窃听、欺骗、篡改消息（修改、延迟、删除、插入、重播、重选路由、错选路由、改变消息顺序）、抵赖或伪造。保护包括防止攻击、发现攻击和从攻击中恢复，以及管理安全相关信息。保护还必须包括预防服务因自然事件（天气等）或恶意攻击（暴力行为）而中断的措施。必须制定有关规定，允许得到正式授权的合法机构进行窃侦听和监测。

4.2 电信网的一般安全目标

本节说明电信网中采取的安全措施的终极目标，重点放在要达到怎样的要求而不是如何完成这些要求。

电信网的安全目标如下：

a） 只有得到授权的用户才能访问和使用电信网。

b） 得到授权的用户应能够访问他们获准访问的资产并对其进行操作。

c） 电信网应能根据网络的安全政策设定的水平提供保密功能。

d） 所有用户均应对自己在电信网中的行为负责，也只对自己的行为负责。

e） 为了确保可用性，应保护电信网免受未经请求的访问或操作。

f） 应有可能检索来自电信网的安全相关信息（但只有得到授权的用户才能检索此类信息）。

g） 在检测到破坏安全的行为时，应按照预定计划以受控的方式对其进行处理，尽量减小潜在危害。

h） 在检测到违反安全的行为之后，应能够恢复正常的安全级别。

i） 电信网的安全体系结构应能提供一定的灵活性，以便支持不同的安全政策，如不同强度的安全机制。

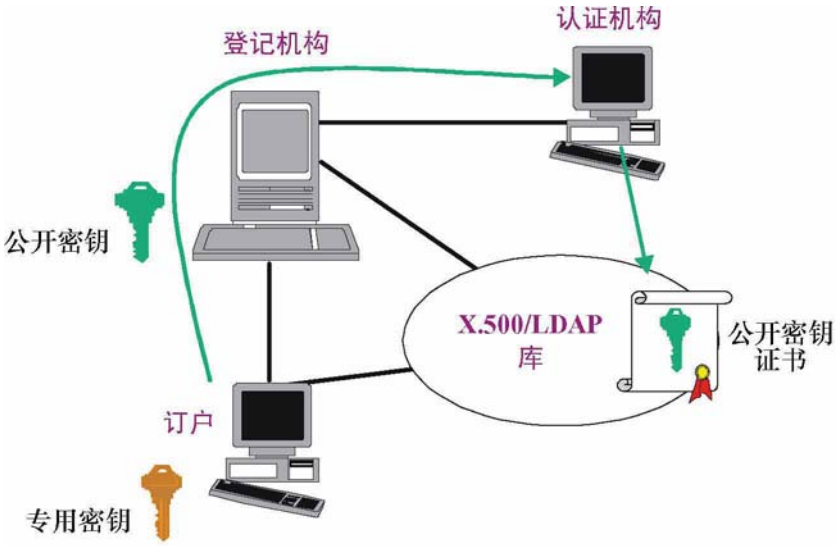
“访问资产”一词应理解为不但有可能完成操作，还有可能读取信息。

可以看出，实施下列安全措施，就可完成上述电信网安全目标的前五个：

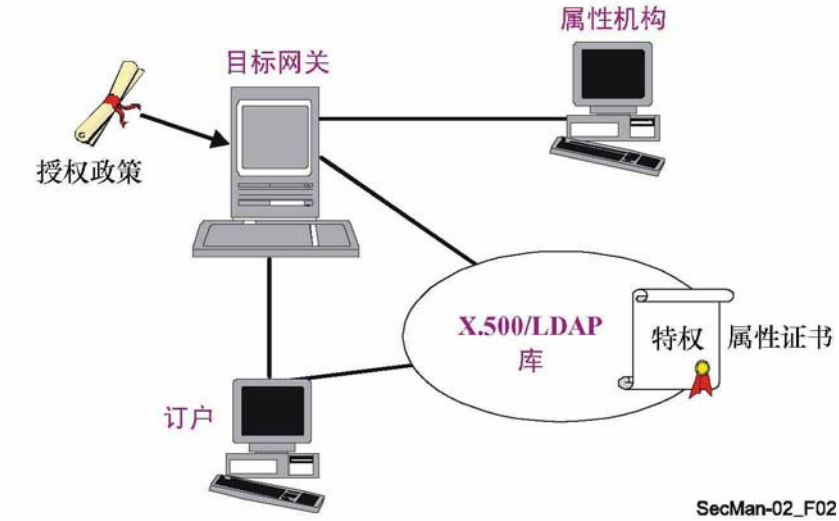
- 机密性；
- 数据完整性；（当然也需要系统程序的完整性）
- 责任制，包括认证、不可抵赖和访问控制；以及
- 可用性。

5 公开密钥和特权管理基础设施

ITU-T X.509 建议书《号码簿：公开密钥和属性证书框架》提供了基于公开密钥证书和认证机构的强认证公开密钥基础设施(PKI)标准。PKI 支持公开密钥管理，由此支持认证、加密、完整性和不可抵赖。PKI 的基础技术是公开密钥加密，下文对它做了说明。除规定 PKI 的认证框架之外，X.509 还以属性证书和属性机构为基础规定了特权管理基础设施（PMI），用于在强授权环境中确保用户的权利与特权。PKI 与 PMI 的构成如图 5-1 所示。



(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

图 5-1－PKI与PMI的构成

5.1 秘密密钥和公开密钥加密

对称（或秘密密钥）密码术是指加密和解密使用同一密钥的密码系统，如图 5-2（a）所示。对称密码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给各方。

非对称（或公开密钥）密码术系统如图 5-2（b）所示使用一对密钥 — 一个公开密钥和一个专用密钥。公开密钥可以广而告之，而专用密钥则必须总是秘而不宣。专用密钥通常存在一个智能卡或令牌上。公开密钥从专用密钥产生，且虽然这两种密钥在数学上相关，但没有可行的办法反过来从公开密钥算出专用密钥。要采用公开密钥加密安全地发送保密数据给某人，发送者需用接收者的公开密钥对数据加密。接收者用其相应的专用密钥对数据解密。公开密钥也可用于对数据施加数字签字，以证实某份文件或报文确实是自称发送者（或发报者）的人发送的。数字签字实际上是一份数据摘要，用签字者的专用密钥产生并附在文件或报文上。接收者用发送者的公开密钥证实数字签字的有效性。（注：某些公开密钥系统采用两对公开密钥/专用密钥，一对用于加密/解密，另一对用于数字签字/验证。）

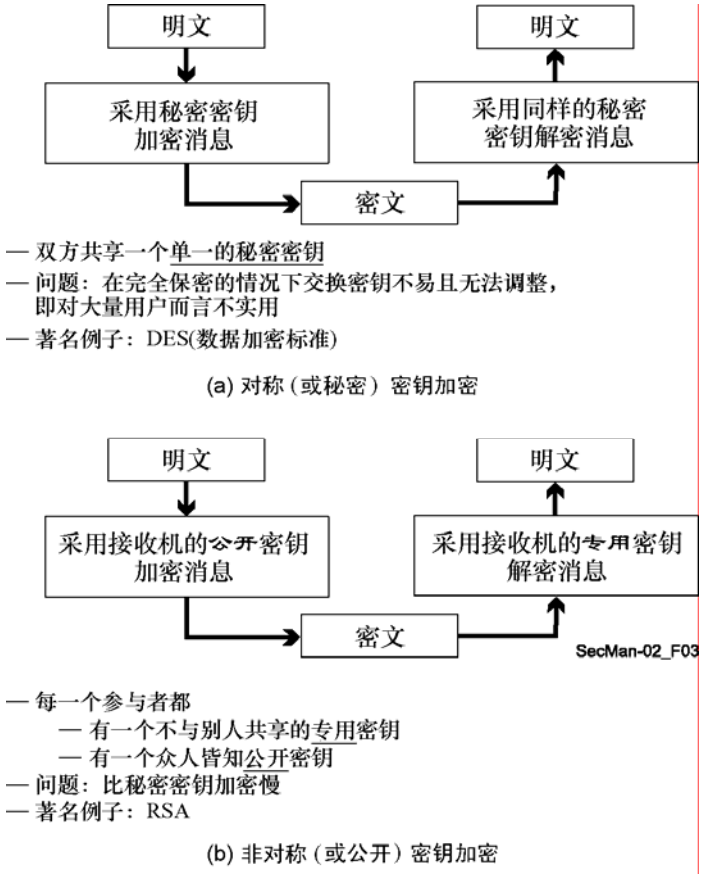


图 5-2－对称（或秘密）与非对称（或公开）密钥加密过程和主要性能图示

采用对称加密，每对用户必须有一对不同的密钥，且必须安全地分发和持有这些密钥。另一方面，采用非对称加密，可以在一个号码簿中公布公开加密密钥，每个人都可以用同一个（公开）加密密钥向一个特定用户发送数据。这就让非对称加密比对称加密更容易产生变化。不过从计算时间看，非对称加密成本较高，采用非对称加密对整个报文加密效率较低。因此，实际上非对称加密通常用于交换对称密钥，然后采用一种计算效率更高的对称算法用该对称密钥对报文的正文加密。如果报文需要数字签字，则先用一个安全的单向散列函数（如 SHA1 或 MD5）对报文进行散列运算，形成的 160 或 128 比特散列值采用发送者的专用密钥进行非对称加密并附在报文上。

应注意的是，如果整个报文是加密的，无论采用对称还是非对称加密，都不可能将报文发送给接收者，因为经转节点无法确定接收者的地址。因此报文头通常必须是未加密的。

公开密钥系统的安全运转在很大程度上取决于公开密钥的有效性。公开密钥通常以数字证书的形式公布，而数字证书保存在某个 X.500 号码簿中。证书不仅含有公开加密密钥及视情况含有个人使用的签字验证密钥，而且还含有包括证书有效性在内的附加信息。因任何原因撤销的证书通常都列在号码簿的证书撤销列表（CRL）中。在使用公开密钥之前，通常要按照 CRL 检查有效性。

5.2 公开密钥证书

公开密钥证书（有时被称做“数字证书”）是验证非对称密钥对所有者的一种方式。公开密钥证书将一个公开密钥与其所有者的名称紧紧联系在一起，并经证明这一关联的可信机构数字签发。这一可信机构被称做认证机构 (CA)。国际认可的公开密钥证书格式在 ITU-T X.509 建议书中定义。简而言之，一个 X.509 公开密钥证书包含一个公开密钥、使用该密钥的非对称算法的标识、密钥对所有者的名称、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 证书政策信息的扩展字段。整个证书然后用该 CA 的专用密钥数字签发。X.509 证书可以广泛公开，比如说在万维网站上、在 LDAP 号码簿中或附在电子邮件的电子名片（Vcard）上。CA 的签字保证其内容不会在不知晓的情况下被改动。

为能够验证一个用户的公开密钥证书的有效性，需要获得签发该证书的 CA 的有效公开密钥以验证该证书上 CA 的签字。一个 CA 可以让另一个（高级）CA 证明它的公开密钥，所以验证公开密钥可能涉及一个证书链。最终这个链必须在某处结束，通常我们就是在此处遇到作为 “可信根”CA 的证书。根 CA 公开密钥作为自我签发的证书发布（该根 CA 由此证明这是它自己的公开密钥）。签字让我们得以验证密钥和 CA 名称自该证书生成以来未被篡改。但是，我们无法对一个自我签发的证书中嵌入的 CA 名称信以为真，因为这个名称是 CA 自己加进去的。因此，公开密钥基础设施中的关键部分是，应以让我们相信该公开密钥确实属于自我签发的证书中提到的根 CA 的方式，安全地分发根 CA 公开密钥（作为自我签发的证书）。否则，我们无法相信是否有人冒充根 CA。

5.3 公开密钥基础设施

PKI 的主要目的是发布和管理公开密钥证书，包括根 CA 自我签发的证书。密钥管理包括密钥对的生成、公开密钥证书的生成、公开密钥证书的撤销（例如用户的专用密钥有了变动）、密钥与证书的保存和记录及其到期后的销毁。每个 CA 根据一套政策运行，ITU-T X.509 建议书提供了在该 CA 发放的证书的扩展字段中发布某些这种政策信息的机制。CA 采用的政策规则和程序通常在该 CA 公开发布的证书政策 （CP）和认证惯例声明（CPS）文件中规定。这些文件有助于确保我们对 CA 发放的公开密钥证书的信任的评估有一个共同的基础，不论是国际上的还是跨行业的。这些文件还提供了建立机构间信任的（部分）法律框架，也规范了对发布的证书使用上的限制。

应该注意，为了利用公开密钥证书进行认证，要求端点使用相关的专用密钥值提供数字签字。仅仅交换公开密钥证书并不能避免中间人攻击。

5.4 特权管理基础设施

ITU-T X.509 建议书的早期版本《号码簿：认证框架》（1988、1993 和 1997）规定了公开密钥基础设施的基本元素，包括公开密钥证书的定义。2000 年批准的 ITU-T X.509 建议书修订版包括对属性证书的重要增补并纳入了特权管理基础设施（PMI）框架。（与 PKI 相比，PMI 管理的是支持综合授权服务的特权。）这些规定的机制考虑了在多供应商和多应用的环境下设置用户访问特权。

PMI 和 PKI 的概念相似，但 PMI 涉及授权，而 PKI 集中在认证。图 5-1 和表 5-1 说明了这两种基础设施的相似之处。

表 5-1－特权管理和公开密钥基础设施特性比较

特权管理基础设施	公开密钥基础设施
源机构（SoA）	根认证机构（信任锚）
属性机构（AA）	认证机构
属性证书	公开密钥证书
属性证书撤销列表	证书撤销列表
PMI 机构撤销列表	PKI 机构撤销列表

为用户指配特权的目的是保证他们遵循源机构规定的安全政策。属性证书中政策相关信息与用户名称绑定在一起，并包括几个组成部分，如图 5-3 所示。

版本
持有者
发布者
签字 (算法标识)
证书序号
有效期
属性
发布者独特标识
扩展字段

图 5-3－X.509属性证书结构

ITU-T X.509 建议书中描述了 PMI 控制的五个组成部分：特权主张者、特权验证者、对象方法[1]、特权政策和环境变量（见图 5-4）。该技术使特权验证者能控制特权主张者按特权政策获得对象方法。

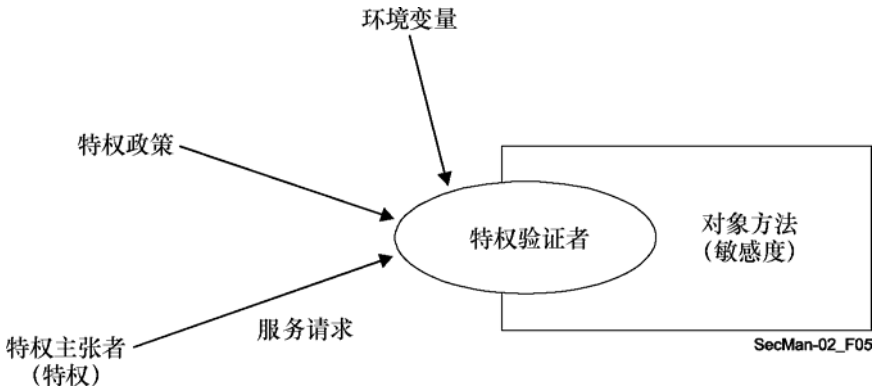


图 5-4－ITU-T X.509 PMI控制模式

在有必要为某种实现指派特权时，ITU-T X.509 建议书中考虑的 PMI 指派模式包括四个部分：特权验证者、源机构、其他属性机构和特权主张者（见图 5-5）。

1 对象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具有读取、写入或执行等对象方法）。

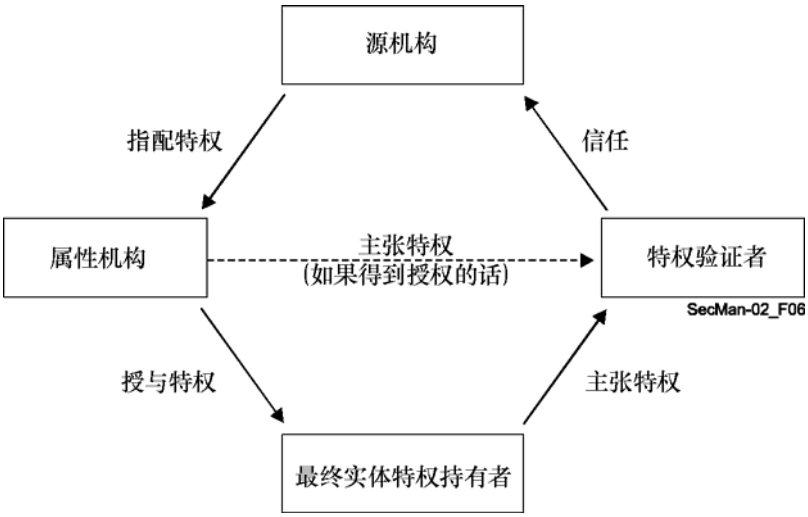


图 5-5－ITU-T X.509 PMI 特权指派模式

近来有些授权方案是按照基于角色的访问控制（RBAC）模式实现的，认为用户也是一个角色 。授权政策将一组许可与某个角色联系起来。在访问某种资源时，按政策检查用户的角色以便开展后续行动。第 6.5.2 节说明的电子处方应用解释了 RBAC 系统的使用。

6 应用

本节介绍的应用属于两个完全不同的类别。第一类关注的是最终用户应用。其中一个例子就是 IP 话音（VoIP），例中对用于提供这种最终用户应用的网络体系结构和组成做了说明。讨论了对支持多媒体应用的三个平面而言要考虑的安全问题和解决方法，其中以 VoIP 作为多媒体应用的一个特例。本节考虑的其他最终用户应用是在有线电视网上提供基于 IP 的实时服务的 IPCablecom 系统，以及传真传输。本节论及的不限于电信行业的应用包括电子医疗保健，特别是电子处方系统。第二类关注的是网络管理应用。提供商提供的服务要满足质量和完整性要求，安全问题是需要考虑的重要因素。因此，对网络管理活动给予适当的特权和授权是非常有必要的。

6.1 采用H.323系统的VoIP

IP 话音（VoIP），也称为 IP 电话，是通过采用网际协议（IP）的网络提供过去一直由公众交换电话网（PSTN）（电路交换）提供的服务，而互联网就是以 IP 协议为基础的。这些服务包括使用最多的话音服务，但也包括其他形式的媒体，包括电视与数据，如应用程序共享和电子白板功能性。VoIP 还包括一些相关的补充服务，如电话会议（网络桥接）、呼叫前转、呼叫等待、多线连选、呼叫改发、呼叫寄存、咨询和呼叫随我转移（跟随）等，以及许多其他智能网服务，其中一些也包括话音频带数据。互联网话音服务是 VoIP 的一种特殊运用，它的话音流由公众互联网骨干网承载。

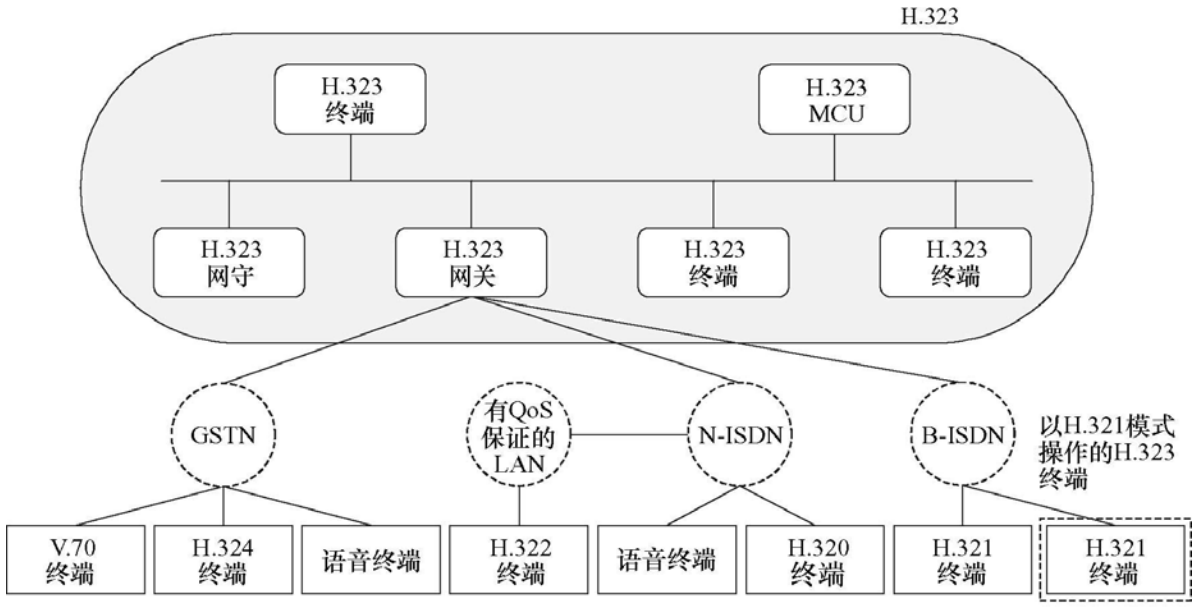
H.323 是一个总括性的 ITU-T 建议书，它为通过包括互联网、局域网（LAN）和广域网（WAN）在内不提供服务质量（QoS）保证的的分组交换网进行声音、电视和数据通信奠定了基础。这些网络主要是目前的企业办公网络，还包括以太网上的分组交换 TCP/IP 和 IPX、高速以太网和令牌环网技术。遵守了 H.323，多厂商的多媒体产品和应用就可以互操作，使得用户在通信时不必担心产品的兼容性。H.323 是第一个规定的 VoIP 协议，被认为是 VoIP 类产品的基础，用于消费者、企业、服务提供商、娱乐业和专业应用。作为 H.323 系统一部分的核心建议书如下。

- H.323 — “总括性”文件，描述 H.225.0、H.245 以及其他一些有关文件在提供基于包的多媒体会议服务时的用法。
- 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（H.310、H.323 和 H.324 共有的）。
- H.235.x — 基于 H.323 的系统的安全。
- H.246 — 与 PSTN 的互通。
- H.450.x — 补充服务。
- H.460.x — H.323 协议的各种扩展。
- H.501 — 移动性管理和域间/域内通信协议。
- H.510 — 用户、终端和服务的移动性。
- H.530 — H.510 的安全规范。

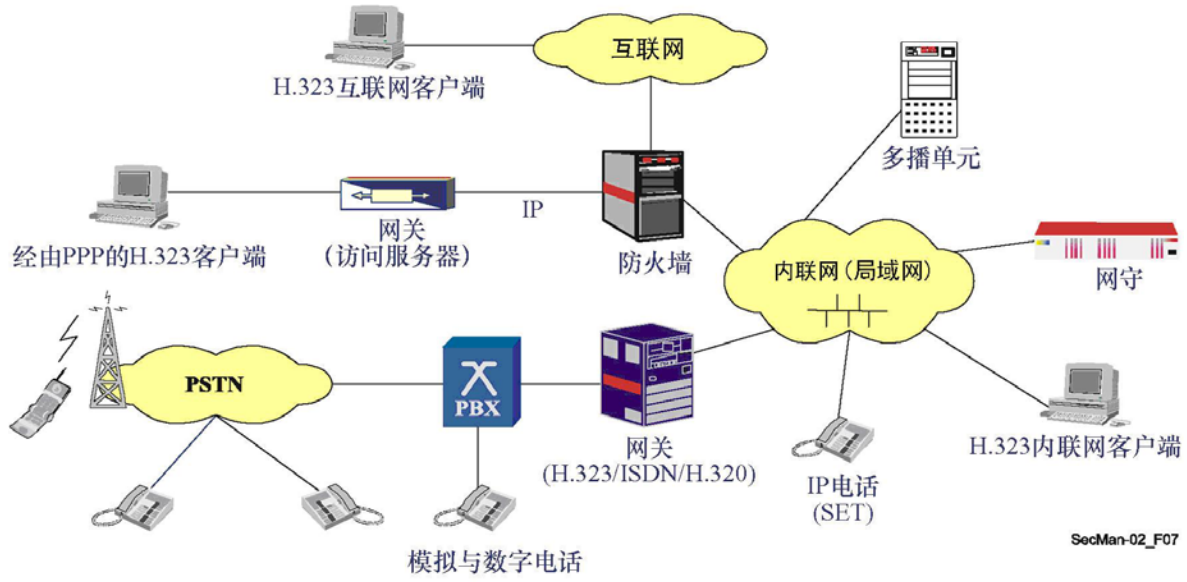
ITU-T 于 1996 年批准了第一版 H.323 建议书，1998 年 1 月批准了第二版，现在的第六版是 2006 年获得批准的。这个标准涵盖的范围宽泛，既涉及独立的设备，也涉及嵌入式个人计算机技术，还涉及点对点和点对多点会议。ITU-T H.323 建议书论及呼叫控制、多媒体管理和带宽管理，以及不同网络间的接口。

H.323 是一个比较大的通信标准系列的一部分，这些标准使电视会议得以跨网络进行。这个系列建议书称做 H.32x，包括 H.320 和 H.324，分别论及 ISDN 和 PSTN 通信。本入门读物对 H.323 标准的益处、体系结构和应用做一个概述。

H.323 定义了以网络为基础的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，可能还有边界元素或对等元素。以上网络单元见图 6-1。



(a) H.323系统及其组成部分[Packetizer]



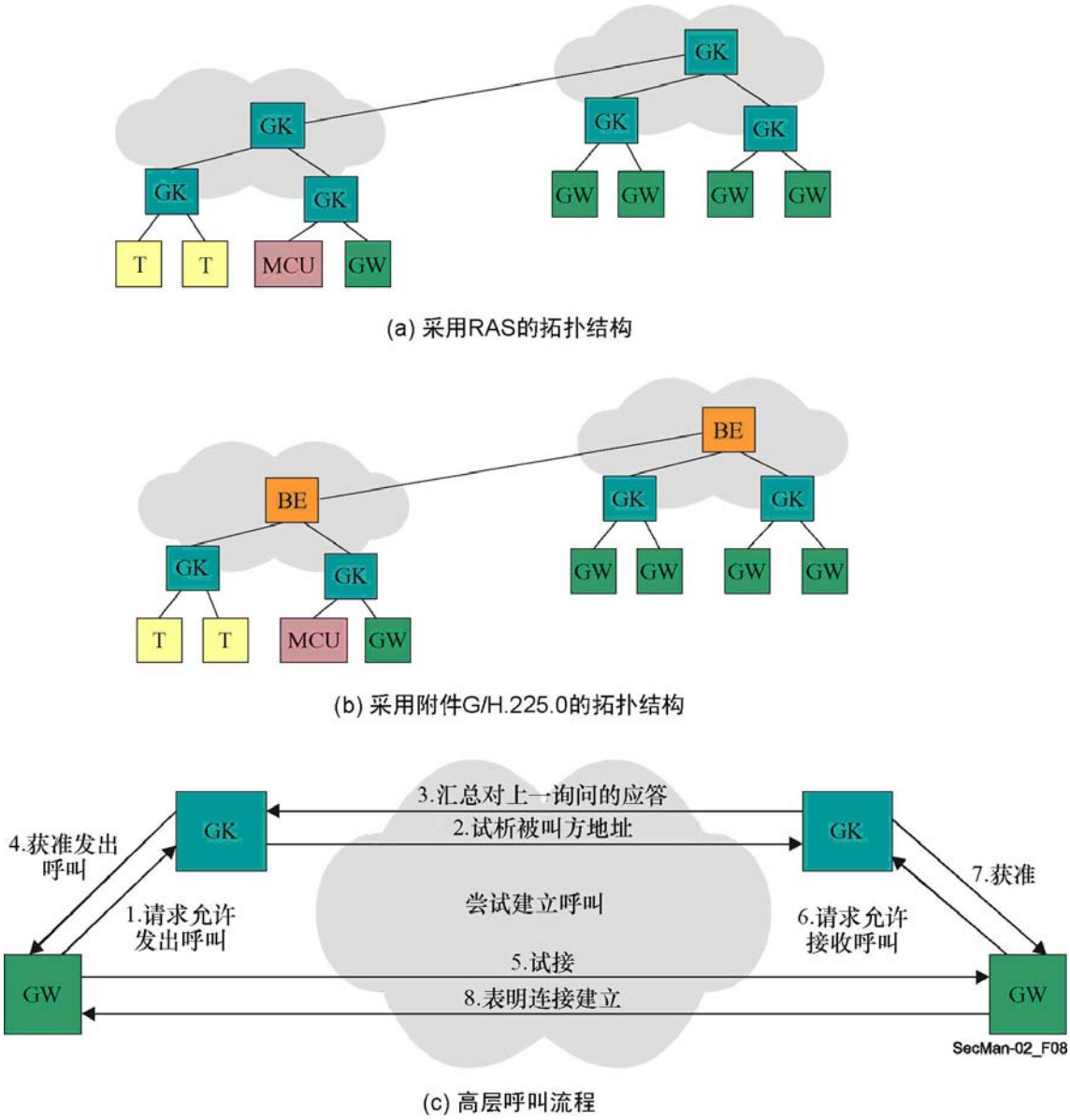
(b) H.323部署方案[Euchner]

图 6-1－H.323 系统: 组成部分和配置方案

终端（*T*）是位于提供双向通信的 IP 骨干网上的客户端点。H.323 终端必须支持话音通信，并且可以支持电视编解码器、T.120 数据会议协议以及多点控制单元（MCU）能力。例如：IP 电话、可视电话、交互式话音应答（IVR）设备、话音邮件系统、“软件电话”（如 NetMeeting™）等。

网关（*GW*）可以提供许多服务，最常见的就是在 H.323 端点与其他终端类型间的转换功能。这个功能包括传输格式间的转换（如 H.225.0 到 H.221 的转换）和通信程序间的转换（如 H.245 到 H.242 的转换）。此外，网关可以在各种声音与电视编解码器之间进行转换，并在分组交换侧和电路交换网侧执行呼叫建立与清除。

网守（*GK*）是 H.323 衍生网络中的一个最重要的组成部分，在其辖区内对所有的呼叫处理起着核心作用，并为在册端点提供呼叫控制服务。许多情况下，H.323 网守的作用相当于一个虚拟交换机，因为它可以实现准入控制、地址解析，并且可以直接在端点间建立呼叫，或可以通过网守自身发送呼叫信令，实现例如跟随/定位、忙时呼叫转移等功能。与网守关联的设备有边界（或对等）元素（*BE*），用来在管理域内交换寻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 6-2 所示。



图例：BE：边界元素；GK：网守；GW：网关；MCU：多点控制单元；
T：终端；RAS：注册、准入和状态协议

图 6-2－管理域之间的通信

多点控制单元（*MCU*）支持三个或多个端点间的会议。H.323 协议规定，MCU 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任何媒体流。由多点处理器来处理媒体流，它能够混合、交换和处理声音、电视和/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专用组件中或是作为其他 H.323 组件的一部分。

已投入生产的 H.323 网络当今每月承载着数十亿分钟的话音和视频业务量；当今大部分的 VoIP 业务量都是通过 H.323 协议传输的。据估计，目前 VoIP 业务量已占国际长途电话分钟数的百分之十以上，而且 H.323 视频业务量也在稳步上升。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 被证实是一个极具扩展性的解决方案，H.323 产品从组件和芯片到无线电话和电视会议硬件，可同时满足服务提供商和企业的需求。

下面是 H.323 系统提供的功能性列表：

- 话音、电视和数据会议性能；
- 不同终端类型间的通信，包括个人计算机（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、IP 文本和 IP 调制解调；
- 大量补充服务（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、终端和服务终端的移动性；
- 支持应急服务信令。

应用 H.323 协议的例子包括运营商从事的批发转接服务，特别是 VoIP 骨干网（与话音服务四类交换机相当）和电话卡服务的转接。在集团通信中 H.323 协议被用于 IP-PBX 交换机、IP 交换中心（IP-Centrex）、话音虚拟专网、话音和数据集成系统、WiFi 电话、呼叫中心的实施以及移动业务。在专业通信中，H.323 协议广泛应用于话音（或音频）和电视会议，用于话音/数据/电视集成和远程教育。在家庭环境中，用途包括宽带视听接入、个人计算机到电话、电话到个人计算机以及个人计算机到个人计算机呼叫； 还可用于定制新闻和信息的分发。

6.1.1 多媒体和VoIP中的安全问题

由于 H.323 系统中的所有单元从地理位置讲是分布式的，且由于 IP 网络天然的开放性所致，出现了一些安全威胁，如图 6-3 所示。

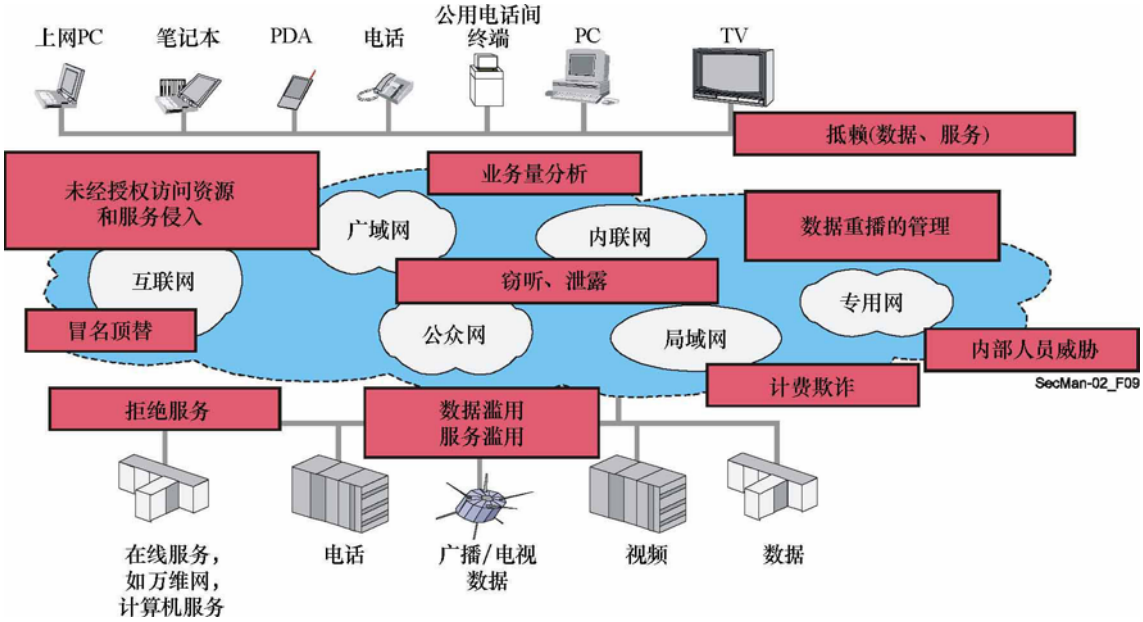


图 6-3－多媒体通信中的安全威胁

下面进一步说明总体而言多媒体通信和 IP 电话系统中的主要安全问题 [Euchner]。

- 用户和终端认证：VoIP 服务提供商为了准确搞清服务使用量，也可能为了按服务使用量计费，需要知道谁正在使用其服务。作为认证的一个先决条件，用户和/或终端必须用某种身份来标识。然后，用户/终端必须证实其声称的身份是真实的。这种情形通常通过强密码认证程序（例如受保护的口令或 X.509 数字签字）进行。同样，用户可能也想知道他们正在与谁通话。

- 服务器认证：VoIP 用户之间通常是通过某些带有相关服务器（网守、多播单元、网关）的 VoIP 基础设施实现相互通信，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，例如冒名顶替、中间人攻击、IP 地址欺骗和连接劫持。

- 呼叫授权是一个判断过程，以确定用户/终端是否真的被允许使用像服务特性（例如呼叫 PSTN）那样的服务资源或网络资源（QoS、带宽、编解码器等）。特别常见的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冒名顶替、滥用与欺诈、操控与拒绝服务等攻击。

- 信令安全保护解决的是保护信令协议免于操控、滥用以及机密性和保密问题。信令协议的保护一般通过密码加密方式以及完整性和重播保护来完成。应特别注意，为达到实时通信的临界性能要求，可以通过尽量少的握手过程和尽量短的往返时间以避免过长的呼叫建立时间或由于安全处理造成的数据包延迟或抖动而引起的语音质量的降低。

- 话音机密性是通过加密话音数据包，也就是加密 RTP（实时传送协议）有效载荷实现的，以防止对被调查话音数据的窃听。通常，对多媒体应用的媒体数据包（例如视频）也要加密。进一步的媒体数据包的保护还包括有效载荷的认证/完整性保护。

- 密钥管理不仅包括在与用户和与服务器有联系的各方间安全分发密钥资料的所有任务，还包括更新过期的密钥和遗失的密钥等任务。密钥管理可以是独立于 VoIP 应用的一个任务（口令提供），在动态协商表明安全能力的安全简表及分发基于会话的密钥时，也可以与信令综合在一起。

- 跨域安全涉及的问题是，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实施了不同的安全特性。因而有必要能够动态地协商安全简表和安全能力，如密码算法及其参数。在跨越域的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越过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。不过实际上，人们可能要面对超过 H.323 考虑范围之外的其他安全问题（例如安全政策、网管安全、安全服务提供、实施安全、操作安全或安全事故处理）。

6.1.2 H.235.x分支系列建议书概述

在 H.323 多媒体系统中，ITU-T H.235.0 建议书规定的安全框架包括 H.323 的安全机制和安全协议规范。1998 年第二版 H.323 系统中第一次引入了 H.235。此后，随着时间的推移，H.235 有了进一步的发展，巩固了已有的安全机制，增加了更多成熟的安全算法（例如高安全性、高速的 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。第四版 H.235.0-H.235.9 是目前系列的基于 H.323 的系统的 ITU-T 安全建议书，可以为小型企业集团和大型运营商提供可调整的安全性。

原先的第三版 ITU-T H.235 建议书的结构有了显著变化，建议书的所有各部分和附件组成了一整套独立的 H.235.x 分支系列建议书，其中的 ITU-T H.235.0 建议书包含“H 系列（H.323 和其他基于 H.245 的）多媒体系统安全框架”。该建议书概述了 H.235.x 分支系列，并包含采用基线文本的共用程序。

简而言之，ITU-T H.235.x 系列建议书提出了控制协议的密码保护（H.225.0 RAS 与呼叫信令和 H.245）以及音频/视频媒体流数据的密码保护。在 H.323 信令的所有不同进程中，H.235 规定了协商想要的和必需的密码服务、密码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”点对点通信，还支持多个多媒体终端在集团内通信时带有多播单元（即 MCU）的多点配置。

H.235 利用了专门优化的安全技术来达到严格的性能要求，如椭圆曲线密码算法和最新的 AES 加密。通过加密 RTP 有效载荷在应用层实现话音加密。这样就有益于通过采用与数字信号处理器（DSP）和话音压缩编解码器的紧密相互作用实现体积小巧的端点，而无需特殊的操作系统平台。像已有的互联网安全包和标准（IPsec，SSL/TLS）这样的现有安全工具如果可用并适用，就可以在 H.235 中被（重新）使用。

图 6-4 给出了 H.235 的应用范围，包括用于建立呼叫（H.225.0 和 H.245 模块）和双向通信（对含有压缩的音频和/或视频的 RTP 有效载荷加密）的相关规定。这些功能性包括认证、完整性、保密和不可抵赖的机制。网守通过对端点的准入控制来实现认证，并提供不可抵赖机制。基于 IP 的传送层和低层安全超越了 H.323 和 H.235 的范围，但通常可以用 IETF 的 IP 安全（IPsec）和传送层安全（TLS）协议来实现。总的来说，IPsec 或 TLS 能够用来提供 IP 层的认证和非强制性地提供机密性（即加密）功能，而无论上面运行的是什么样的（应用）协议。同时也不必为此升级应用协议，只需在每一端升级安全政策。

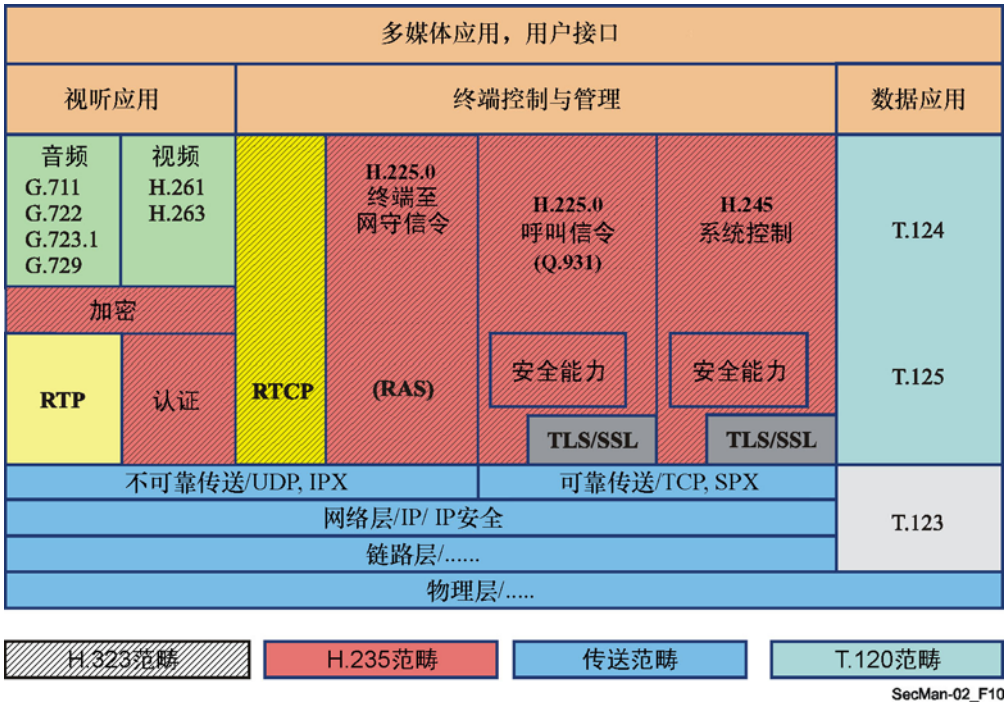


图 6-4－H.235 提供的H.323 安全[Euchner]

ITU-T H.235.x 系列建议书含有各式各样的安全措施，可以适用于不同的目标环境，如企业内/企业间和运营商内/运营商间。依据不同的假设，如可用的安全基础设施和终端能力，以及不同的平台，如简单端点或智能端点，H.235.x 提出了一系列个性化可互操作的专用安全简表。这些可用的安全简表提供的安全技术，范围从包括口令保护（关于 H.225.0 信令的认证和消息完整性的 H.235.1）在内的简单秘密共享简表到使用数字签字和 X.509 PKI 证书（H.235.2）的更复杂的简表。这样就既可以用较简单但难于升级的技术实施逐跳保护，也可以用可升级的 PKI 技术实现端对端保护。H.235.3 被称为混合安全简表，因为该建议书综合了 H.235.1 中的对称安全程序和 H.235.2 对 PKI 证书与签字的使用，从而达到了优化的性能和较短的呼叫建立时间。H.235.3 进一步提出了一种可能性，在一个以代理为基础的功能性安全处理器实体中非强制性地进行大量计算操作。

H.235.4 放松了对网守选路、以服务器为中心的体系结构的依赖，提出了“直接选路和选择性选路呼叫的安全”，并给出了保证同层安全模式的安全措施。该建议书规定了集团环境和跨域环境下的密钥管理程序。H.235.4 还特别涉及前面提到过的方案，即网守以直接选路的方式操作，或者网守也可能有选择性地只完成一部分 H.225.0 呼叫信令的选路。

尽管不少 H.235 安全简表假定了 H.323 网守选路模式，但 H.235.4 更偏向于安全的同层通信，目的是从 H.323 信令选路任务中释放有关的网守，形成总的来说更强的调节能力和性能。在支持直接选路呼叫的 H.235.4 中，网守大多在其域内进行本地操作以便完成用户/终端认证，并完成注册、准入、地址解析和带宽控制。另一方面，各终端以端对端的方式直接在端点之间完成 H.323 呼叫的建立；见图 6-5 所示的方案。

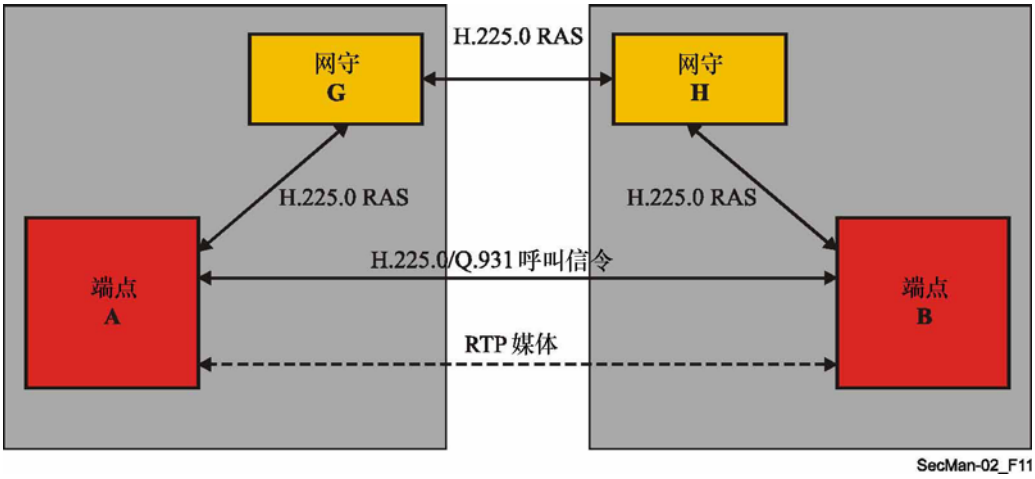


图 6-5－H.235.4直接选路方案

一旦端点（EP）A 请求网守（GK）G 受理对 EP B 的呼叫，一个网守（不是集团环境中的 GK G 就是跨域环境中的 GK H）为 A 和 B 两个端点生成端对端呼叫信令密钥。端点 A 以一种非常类似于 Kerberos 的方式（见 ITU-T J.191 建议书中的某种应用），在一个安全令牌中安全地获得已生成的密钥，同时还获得端点 B 的带有同一密钥的另一个安全令牌。在发起呼叫时，EP A 一方面直接向 EP B 申请保护呼叫信令的密钥，另一方面还把带有同一密钥的另一个安全令牌转发给 EP B。H.235.4 能够使用 H.235.1 或 H.235.3 的 H.235 安全简表。

H.235.4 对跨域方案提出了进一步的程序上的支持，可以对端点或网守不支持 Diffie-Hellman 密钥协议的情况加以区分；而最终得到的结果是，端点 A 和端点 B 得到了一个共享的会话秘密，用于从认证、完整性和机密性方面对 H.323 信令实施端对端保护。

为了给采用个人身份号（PIN）或口令对用户进行认证的系统提供更强的安全，H.235.5 提出了另一种用公开密钥法为 PIN/口令的使用提供安全保障的“使用弱共享秘密在 RAS 中的安全认证框架”。目前规定了一个特定的安全简表，利用加密密钥交换法对强共享秘密进行协商，以避免被动或主动（中间人）攻击。该框架允许用其他以公开密钥为基础的协商方法规定新的安全简表。

ITU-T H.235.6 建议书《具有本地 H.235/H.245 密钥管理的话音加密简表》归纳了对 RTP 媒体流加密所需的所有程序，包括在 H.245 信令字段内完整表示的环境密钥管理。

为了更好地与会话发起协议（SIP）和安全实时传送协议（SRTP）融合在一起，ITU-T H.235.7 建议书 《在 H.235 中将 MIKEY 密钥管理协议用于安全实时传送协议（SRTP）》在 H.235 中采用了安全实时传送协议（SRTP，RFC 3711）。该建议书规定了在 H.235.7 中如何使用 IETF MIKEY 密钥管理进行端对端 SRTP 媒体密钥分发。

另外，ITU-T H.235.8 建议书《使用安全信令信道的 SRTP 的密钥交换》含有一种补充方法，其目的是在采用某种安全传送方法的专用端对端信道中发送 SRTP 密钥设置参数；这类似于 IETF 的会话描述协议（SDP）的说明中采用的方式。无论采用 IPsec（互联网安全协议）、TLS（传送层安全协议）还是 CMS（密码消息句法），都可以实现这种安全的信令传送信道。

让 H.323 信令穿越 NAT（网络地址解析）和防火墙（FW）实际上曾一直是一个主要的实施障碍。ITU-T H.235.9 建议书《H.323 的安全网关支持》纳入了可以让 H.323 端点/终端发现 H.323 网关的安全程序，可以认为这种实体含有 H.323 NAT/FW 应用层网关（ALG）的功能性。由被认为是可信的 H.323 信令网关检测正在进行的信令事务并参与 H.225.0 信令的密钥管理。

H.235.0 虽然主要涉及“静态”H.323 环境，较少涉及移动性规定，但还是认为有必要在分布式 H.323 环境中提供安全的用户和终端移动性。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 H.530 建议书通过探讨以下安全问题涵盖了上述安全需求：

- 被访外部域的移动终端/用户认证和授权；
- 被访域的认证；
- 安全的密钥管理；
- 移动终端和被访域之间的信令数据保护。

图 6-6 示出了 H.530 讨论的基本方案，其中 H.323 移动终端（MT）既可通过归属网守（H-GK）直接连至其归属域，也可连至一个被访域中的外部网守（V-GK）。由于被访域不能识别移动终端和用户，被访网守首先必须询问对 MT 进行注册和识别的归属域中的认证功能（AuF）。因此，被访域把认证的任务交给归属域中的 AuF 处理，并让 AuF 完成认证和决定是否授权。另外，AuF 采用 H.530 中的嵌入式密码安全协议让 V-GK 确信 MT 与 V-GK 动态密钥之间存在密码学上的捆绑关系。AuF 以安全的方式将其决定作为响应返回给在终端注册阶段出现的被访网守。

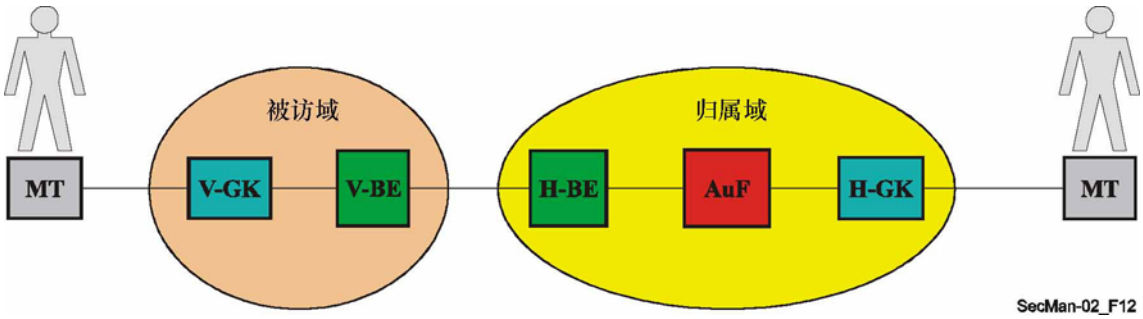


图 6-6－H.530方案

被访域与归属域之间的通信采用了基于 H.323 的移动性管理和域内/跨域通信所用的通用 H.501 协议。一收到 AuF 的认证与授权决定，被访网守与 MT 即商定在其安全关联存在期间二者共享的新动态链路密钥。该链路密钥用于保护 MT 与 V-GK 之间的任何进一步 H.323 信令通信；多媒体信令通信只在被访域本地发生，不需要与归属域的交互作用。

H.530 考虑了非常简化的安全体系结构，其中 MT 只与其归属域的 AuF 共享一个预置的共享秘密（如注册口令），而不需要与任何被访域共享一个既定的安全关联。各域之内以及域间实体的安全保护只需要对称的共享秘密；举例来说，这种对称共享秘密可以通过跨域服务层管理来建立。H.530 重复使用现有的 H.235 安全简表，如 H.235.1，以保证 H.501/H.530 信令消息的跨域安全。

除 H.235.0 外，H.350 和 H.350.2 也采用轻型号码簿访问协议（LDAP 和）和安全套接字层（SSL/TLS）规定了可升级的密钥管理。ITU-T H.350.x 建议书提出了一些重要的能力，使企业和运营商能安全地管理使用 IP 话音和 IP 电视服务的大量用户。H.350 提出了一种将 H.323、SIP、H.320 和通用消息服务与号码簿服务联系起来的方法，令现代的身份管理措施得以应用于多媒体通信。此外，这个体系结构还为存放这些协议的安全证明提供了标准化位置。

H.350 没有改变任何特定协议的安全体系结构。不过，H.350 确实提供了一个视情况存放认证证明的标准化位置。应该注意的是，H.323 和 SIP 都支持共享秘密认证（分别见 H.235.1 和 HTTP 文摘）。而这些方法要求呼叫服务器拥有使用口令的权限。因此，如果呼叫服务器或 H.350 号码簿受到损害，口令也可能受到损害。这些不足与其说是 H.350 本身的不足，不如说是系统（H.350 号码簿或呼叫服务器）及其操作方面的不足所致。

极力提倡呼叫服务器和 H.350 号码簿在共享信息前进行相互认证。此外，还极力提倡 H.350 号码簿与呼叫服务器之间或与端点之间的通信应该建立在 SSL 和 TLS 等安全通信通道上。

应该注意，LDAP 服务器上的访问控制列表属于安全政策问题，而不是该标准的一部分。建议系统管理员在设置对 H.350 属性的访问控制时要符合常识。例如，地址属性可能是公开使用的，但口令属性只应由得到认证的用户使用。

6.1.3 H.323和NAT/FW设备

构思互联网时原本考虑了“端对端”原则。也就是说，网络上的任何设备都可以直接与网络上的任何其他设备通信。不过由于担心安全和 IPv4 网络地址短缺，在网络的边界处常常会使用防火墙和网络地址解析（NAT）设备。这些边界包括住宅域、服务提供商域、企业域，有时还包括国家域。在某个域内，有时要使用不止一个防火墙或 NAT 设备。

防火墙旨在对信息如何跨越网络边界实施严格控制，通常防火墙要设置为阻断大部分 IP 通信。除非防火墙明确设置为允许外部设备的 H.323 业务量通过边界到达内部的 H.323 设备，否则简直无法通信。这对 H.323 设备的任何用户来说都是个问题。

NAT 设备将内部域中所用的地址转换成外部域中所用的地址，或者反过来。住宅域或企业域中所用的地址并不总是从 RFC 1597 规定的专用网络地址空间得到分配，但通常如此。这些地址空间是：

类别	地址范围	IP 地址数量
A	10.0.0.0 – 10.255.255.255	16 777 215
B	172.16.0.0 – 172.31.255.255	1 048 575
C	192.168.0.0 – 192.168.255.255	65 535

NAT 设备对大多数 IP 协议产生的问题更让人烦心，尤其是在协议中承载 IP 地址的那些协议。H.323、SIP 和在分组交换网上运行的其他实时通信协议必须提供 IP 地址和端口信息，以便让参与通信的其他各方了解向何处发送媒体流（如音频和视频流）。

ITU-T 对跨越 NAT/FW 的问题做了研究，形成了关于 H.323 系统的一系列三个建议书，使这些系统得以无缝跨越一个或多个 NAT/FW 设备。这几个建议书是 H.460.17 （《采用 H.225.0 呼叫信令连接传送 H.323 RAS 消息》）、H.460.18（《H.323 信令跨越网络地址解析器和防火墙》） 和 H.460.19（《H.323 媒体跨越网络地址解析器和防火墙》）。

所有这些建议书都利用了第四版 H.323 中引入的“通用扩展性框架”，这说明任何第四版或更高版本的 H.323 设备都可以经过改造而支持这些 NAT/FW 跨越程序。另外，H.460.18 还做出了一些规定，可以让不符合这些建议书的旧设备借助于一个“代理”设备正确地跨越 NAT/FW 边界。

图 6-7 说明了一个特殊的“代理”设备是如何帮助“不了解”NAT/FW 的设备正确地跨越 NAT/FW 边界的：

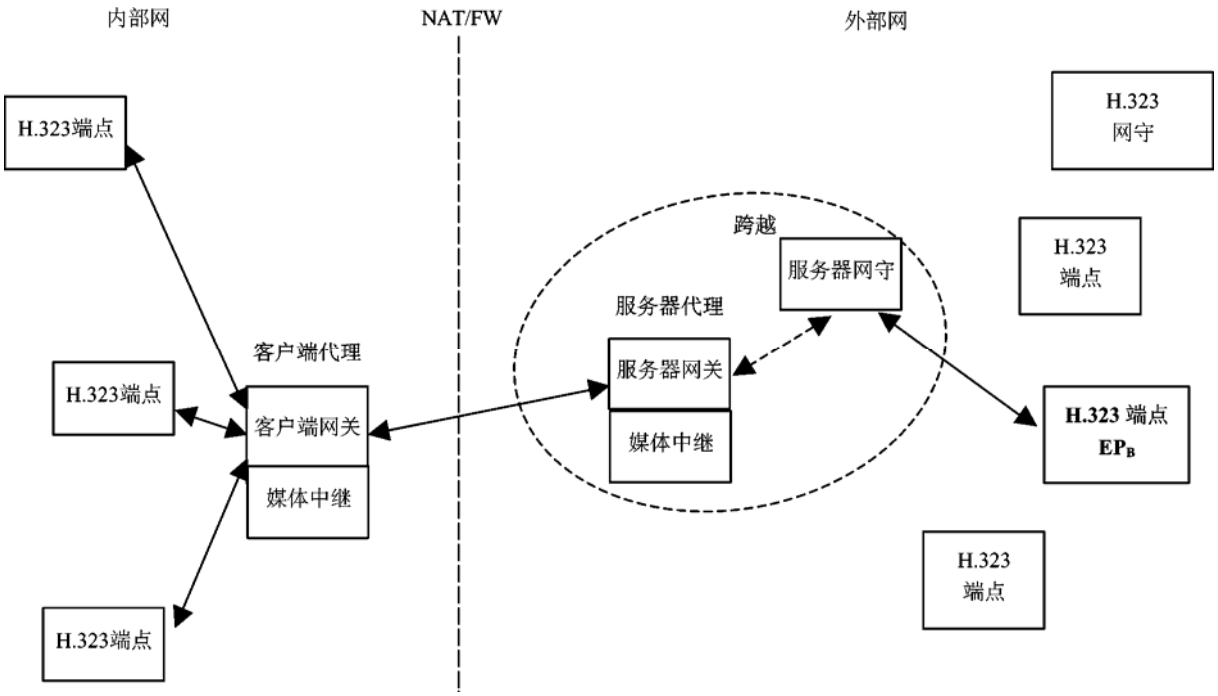


图 6-7－H.460.18体系结构，完全分解的实施方案

上述拓扑结构可能也适合其他情况，比如某个企业希望控制 H.323 呼叫信令和媒体穿越网络所经过的路由。但是 H.460.17 和 H.460.18（二者涵盖了穿越 NAT/FW 的信令问题）确实也考虑了端点无需任何特殊内部“代理”设备的帮助而跨越 NAT/FW 边界的问题。图 6-8 对一种这样的拓扑结构做了说明：

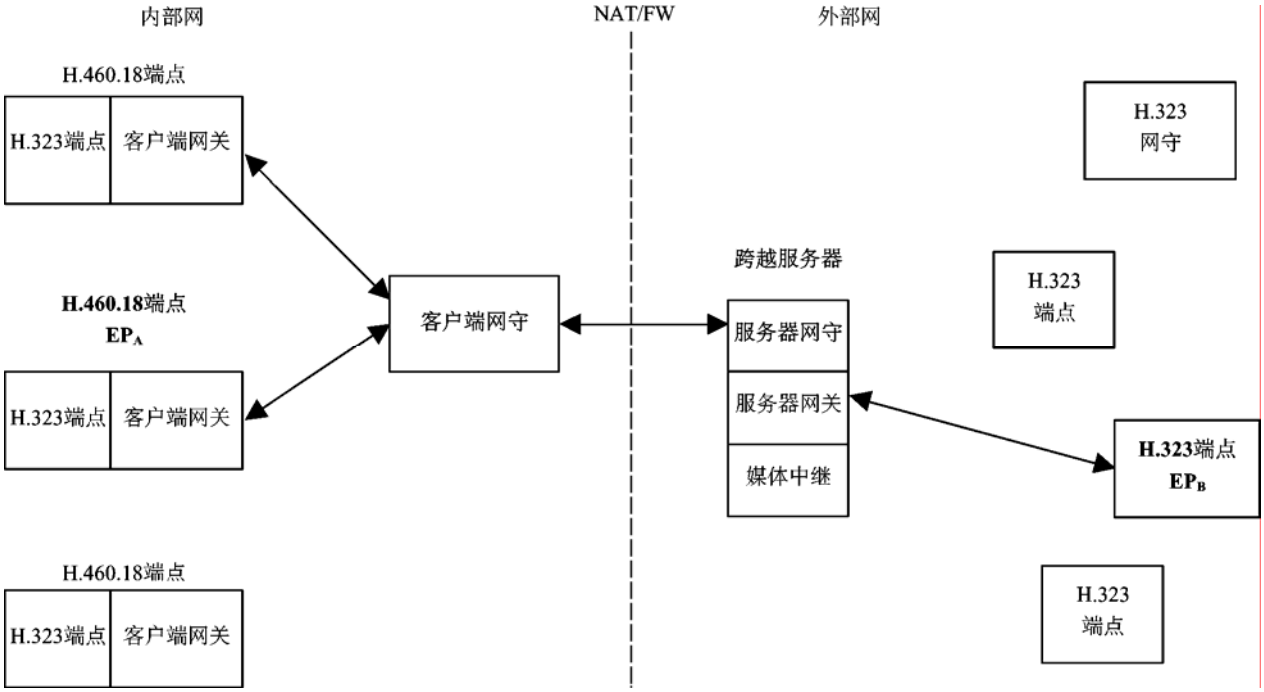


图 6-8－网守通信体系结构

在上述以 H.460.18 为基础的拓扑结构中，内部网上的端点为了解析外部实体的地址（如把电话号码或 H.323 URL 转换成 IP 地址）而与驻留在内部网中的网守通信。内部网中的网守则与外部网中的网守通信，以便交换该寻址信息并将该信息返给主叫端点。内部网中的设备在向外部网中的设备发出呼叫时，会采用 H.460.18 规定的程序在 NAT/FW 设备上撕开必要的“小洞”，让内部网的信令到达外部网。另外，该内部网中的设备还会采用 H.460.19 规定的程序撕开必要的“小洞”，让媒体流正确地跨越内部网到达外部网，或者反过来。

如果主叫和被叫设备分别位于由 NAT/FW 设备和公众互联网隔开的不同专用网内，则必须具备至少一个“服务器网关”或一个“媒体中继”设备（在 H.460.18 中规定），以便在两个专用网之间正确地为信令和媒体选路。设备的这种组合通常也称为“会话边界控制器”。原因很简单，因为按照设计，没有公众网中某个实体帮助“代传”，一个专用网中的 IP 数据包就无法进入另一个专用网。

当然，在同一专用网内始发和终接的呼叫会像现在一样没有问题，不需要任何特殊呼叫处理程序；H.460.17、H.460.18 和 H.460.19 并未削弱同一内部网中 H.323 设备的正常操作。

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（例如话音通信）。ITU-T J.160 建议书规定了 IPCablecom 系统的体系结构。IPCablecom 体系结构在很高的层面考虑了三个种网络：“J.112 HFC 接入网”、“被管 IP 网络”和 PSTN。接入节点（AN）提供“J.112 HFC 接入网”与“被管 IP 网络”之间的连接。信令网关（SG）和媒体网关（MG）二者提供“被管 IP 网络”与 PSTN 之间的连接。IPCablecom 的参考体系结构如图 6-9 所示。

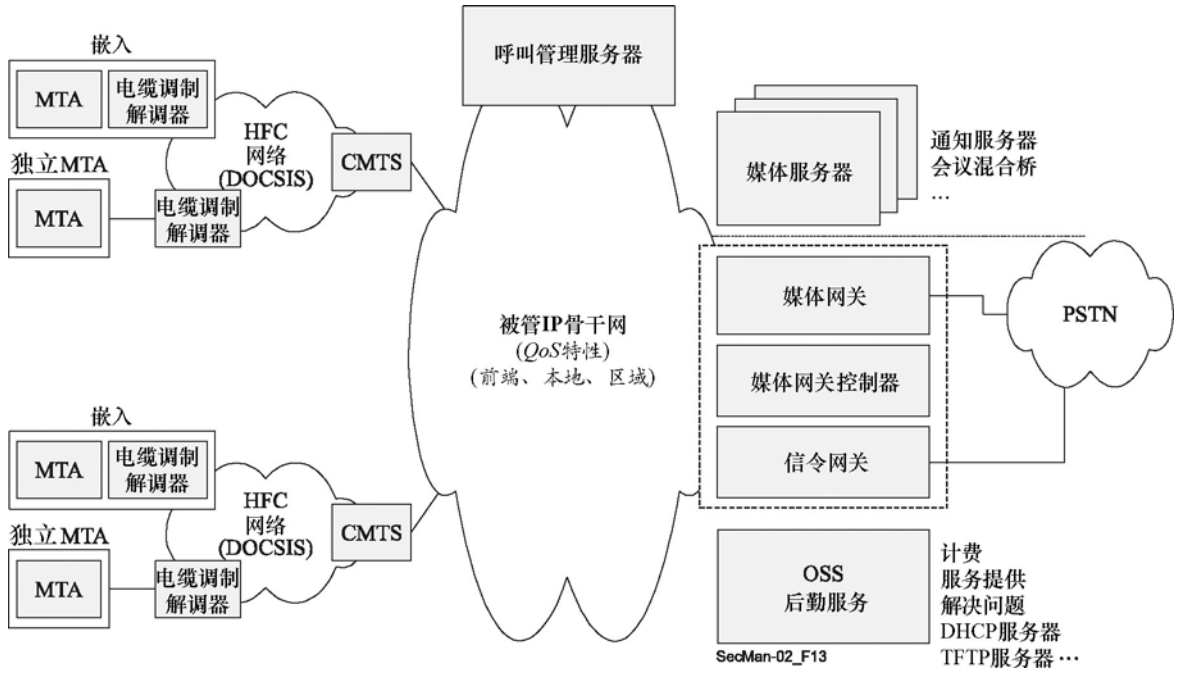


图 6-9－IPCablecom参考体系结构[J.165]

J.112 光纤同轴混合（HFC）缆接入网提供客户住所与线缆前端之间高速、可靠和安全的传送。这个接入网可以提供 J.112 的所有能力，包括服务质量和到物理层的接口，该接口是通过电缆调制解调器终端系统（CMTS）实现的。

被管 IP 网络具有多种功能。首先，它负责 IPCablecom 系统基本功能组件之间的互联，这些组件负责信令、媒体、服务提供和服务质量的确立。此外，被管 IP 网络在其他被管 IP 与 J.112 HFC 网络间提供远程 IP 连接。被管 IP 网络包括以下功能组件：呼叫管理服务器、通知服务器、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）后勤服务器。

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服务。CMS 是位于 IPCablecom 网络中被管 IP 部分的一个可信网络单元。通知服务器（ANS）是逻辑网络组件，它根据网络中发生的事件管理和播放信息音与消息。信令网关功能在 IPCablecom 网络边缘发送和接收电路交换网的信令。对于 IPCablecom 系统，信令网关功能只支持七号信令系统形式的非设施关联信令（多频音形式的设施关联信令直接由媒体网关功能来支持）。媒体网关控制器（MGC）接收并经转 IPCablecom 网络与 PSTN 网络之间的呼叫信令信息。它负责维护并控制需要与 PSTN 网络互联的呼叫的整体呼叫状态。媒体网关（MG）提供 PSTN 与 IPCablecom 的 IP 网络之间的承载连接。每一个承载连接用一个端点来代表，由 MGC 指示 MG 建立并控制与 IPCablecom 网络上其他端点的媒体连接。MGC 还指示 MG 检测并生成与 MGC 所知的呼叫状态相关的事件与信号。运营支撑系统后勤服务器包括支撑核心经营流程中的经营、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、会计管理和配置管理。IPCablecom 规定了一组有限的运营支撑系统功能组件与接口，用于支撑媒体终端适配器（MTA）设备的提供和载有计费信息的事件消息。

6.2.1 IPCablecom的安全问题

每个 IPCablecom 的协议接口都面临对订户和服务提供商二者构成安全风险的威胁。例如，媒体流通路可能穿越大量潜在未知的互联网服务和骨干网服务提供商的线路。结果，媒体流可能会很容易受到恶意窃听从而泄露通信秘密。

6.2.2 IPCablecom的安全机制

IPCablecom 的安全是在低层堆栈元素上实现的，因此大多使用 IETF 规定的机制。IPCablecom 体系结构通过对每个已有的协议接口具体规定向协议接口提供所需服务的基础安全机制（如 IPsec），对这些威胁做了处理。在 X.805 体系结构的范畴内，IPCablecom 安全服务的概述部分论及了如图 2-1 所示的三个平面和三层的所有九个方格。例如，IPsec 支持控制平面的信令协议服务。通过使用第三版简单网络管理协议（SNMPv3）实现了管理基础设施的安全。

通过 IPCablecom 的核心服务层实现的安全服务是认证、访问控制、完整性、机密性和不可抵赖。IPCablecom 协议接口可以不使用、使用一种或多种这些服务来解决其特定的安全要求。

IPCablecom 安全通过以下措施解决每个有关协议接口的安全要求：

- 确定每个有关协议接口特有的威胁模型；
- 确定解决已知的威胁所要求的安全服务（认证、授权、机密性、完整性和不可抵赖）；
- 具体规定提供所需安全服务的特定安全机制。

这些安全机制既包括安全协议（如 IPsec、RTP 层安全和 SNMPv3 安全），也包括支撑的密钥管理协议（如 IKE、PKINIT/Kerberos）。同样，IPCablecom 的核心安全服务包括一种为 RTP 媒体流提供端对端加密的机制，以此充分减少对通信秘密的威胁。图 6-10 归纳了所有 IPCablecom 安全接口。如果没有示出密钥管理协议，就意味着此时它对于那个接口不是必需的。IPCablecom 系统中没有安全要求的接口在图 6-10 中没有示出。

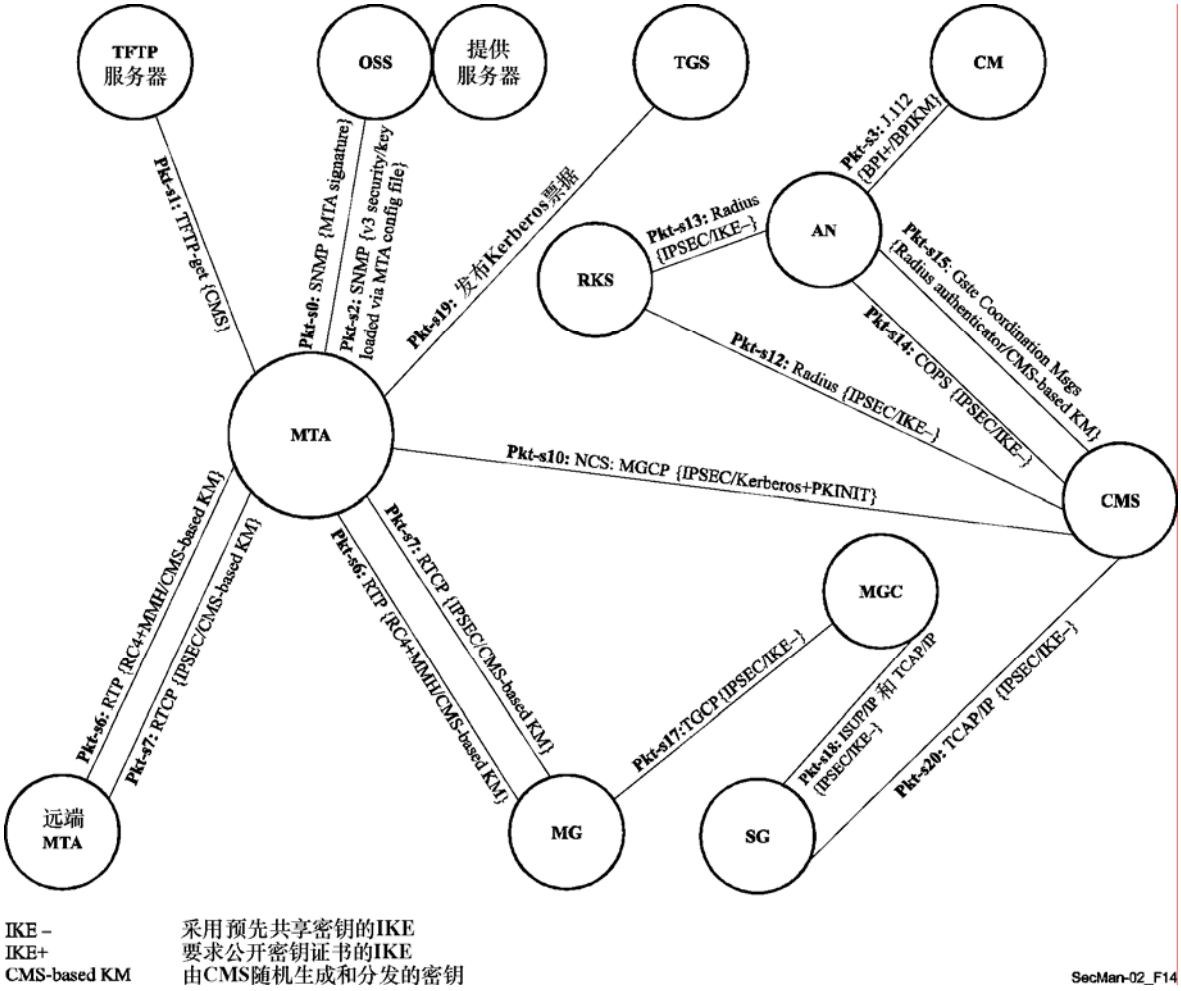


图 6-10－IPCablecom安全接口（表示为 <标签>: <协议> { <安全协议> / <密钥管理协议> }）

IPCablecom 安全体系结构把设备的提供分成三个不同的动作：订户注册、设备提供和设备授权。*订户注册*过程建立一个永久的订户计费账户，用于通过 MTA 的序列号或 MAC 地址向 CMS 独一无二地确认 MTA 的身份。该计费账户也用于识别订户为 MTA 预订的服务。订户注册可以发生在带内或带外。订户注册过程的实际规范超出了 IPCablecom 的范围，且对每一个服务提供商都可能不一样。对于**设备提供**，MTA 设备验证在（使用 Kerberos 认证和密钥管理）首次建立自身与提

供服务器间的 SNMPv3 安全性时下载的配置文档的真实性。然后由提供服务器向 MTA 提供配置文档的位置和配置文档的一个散列值。MTA 检索配置文档、对配置文档执行散列运算，并将结果与提供服务器给出的散列值比较。如果散列值匹配，配置文档则通过了认证。为保证通信秘密，配置文档可以非强制性地加密（为了安全地将配置文件加密密钥传送到 MTA，还必须启用 SNMPv3 通信秘密）。设备授权指的是已提供的 MTA 设备向呼叫管理服务器确认自己的身份，并在满负荷工作前与该服务器建立安全关联。设备授权使随后的呼叫信令在已建立安全关联的情况下得到保护。

信令流量和媒体流都是受到保护的。所有的信令流量，包括 QoS 信令、呼叫信令以及 PSTN 网关接口信令，都将受到 IPsec 协议的保护。IPsec 安全关联的管理可以通过采用 Kerberos/PKINIT 和 IKE 两个密钥管理协议来实施。Kerberos/PKINIT 用于在 MTA 客户端及其 CMS 服务器之间交换密钥；而 IKE 则用于管理所有其他信令的 IPsec 安全关联。至于媒体流，每个媒体的 RTP 包都要为通信保密而单独加密，并经过认证来验证包的完整性与发出者。尽管唯一要求的加密算法是 AES，但 MTA 是能够协商特定的加密算法的。每一个 RTP 包都含有非强制性的信息认证代码（MAC）。MAC 的算法也可以协商，尽管目前只规定了 MMH 一种。MAC 的计算涉及包的未加密的字头和加密的有效载荷。

加密和 MAC 计算所用的密钥是从端对端秘密和随机数算出的，端对端秘密和随机数在发送 MTA 与接收 MTA 之间作为呼叫信令的一部分进行交换。因此，为媒体流安全而进行的密钥交换，其自身的安全是通过呼叫信令的安全来保障的。

运营支撑系统（OSS）和计费系统也规定了安全要求。由 IPCablecom 设备中的 SNMP 代理运行 SNMPv3。SNMPv3 用户安全模型[RFC 2274]提供了 SNMP 流量的认证和保密服务。SNMPv3 基于浏览的访问控制[RFC 2275]可以用来对管理信息库（MIB）对象实施访问控制。

IKE 密钥管理协议的作用是在记录保存服务器（RKS）和每个生成事件消息的 IPCablecom 网元之间，确定加密与认证密钥。在建立网络 IPsec 安全关联时，这些密钥必须在每个 RKS（主用、备用等）与所有 CMS 和 AN 间生成。可能存在 MGC 和 RKS 间的密钥交换，并且留给了 IPCablecom 第一阶段的供应商去解决。事件消息是通过 RADIUS 传送协议从 CMS 和 AN 发送到 RKS 的，该协议本身由 IPsec 实施保护。

6.3 安全的传真传输

传真是一种非常普遍的应用。最初规定是在 PSTN 上传输（ITU-T T.4 建议书），然后是在 ISDN 上传输（ITU-T T.6 建议书），再近一些，传真扩展到了通过 IP 网络（含互联网）传送，即利用 ITU-T T.37 建议书进行非实时传输（电子邮件转发）和利用 ITU-T T.38 建议书（用 RTP）进行实时传输。无论是 PSTN、ISDN 还是 IP 网络，传真传输面临的两个典型安全问题都是连接认证（有时候是不可抵赖）和传输数据的机密性。但由于 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 建议书规定了两个独立的技术解决方案，可以用于在安全传真传输范畴内实现对被交换文件的加密。这两个技术解决方案以 HKM/HFX40 算法（附件 A/T.36）和 RSA 算法（附件 B/T.36）为基础。虽然上述两种算法都限定会话密钥不能超过 40 比特（源于 1997 年批准该建议书

时国家法规中的规定），但也为需要较长密钥的算法规定了一个（在 40 比特会话密钥的基础上）产生冗余会话密钥的方法。附件 C/T.36 描述了 HKM 系统的用途，该系统通过实体 X 和 Y 间的单向注册方法或通过实体 X 和 Y 之间秘密密钥的安全传输为传真终端提供安全的密钥管理能力。附件 D/T.36 讨论了利用 HFX40 传输密码系统为传真终端提供消息机密性的程序。最后，附件 E/T.36 描述了 HFX40-I 散列算法，包括其用途、必要的计算和为实现传真消息的完整性而在传真终端间交换的信息，作为消息加密的一种选定的或预先设定的替代方案。

此外，T.36 规定了以下安全服务：

- 相互认证（强制性的）。
- 安全服务（非强制性的），包括相互认证、消息完整性和消息接收确认。
- 安全服务（非强制性的），包括相互认证、消息机密性（加密）和会话密钥建立。
- 安全服务（非强制性的），包括相互认证、消息完整性、消息接收确认、消息机密性（加密）和会话密钥建立。

根据上面规定的这些安全服务确定了四个安全简表，如下面的表 6-1 所示。

表 6-1－附件H/T.30安全简表

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

6.3.1 采用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（终端或终端制造商）间的安全文件通信提供如下能力：

- 实体相互认证（强制性的）；
- 秘密会话密钥建立；
- 文件机密性；
- 接收确认；
- 文件完整性确认或否认。

密钥管理是通过附件 B/T.36 中规定的 HKM 系统提供的。规定的程序有两个：第一个是注册，第二个是秘密密钥的安全传输。通过注册建立共同的秘密，让所有后续传输得以安全地提供。在后续传输中，HKM 系统提供相互认证、用于保证文件机密性和完整性的一个秘密会话密钥、接收确认以及文件完整性的确认或否认。

文件机密性通过附件 D/T.36 中定义的密码获得。该密码使用 12 位十进制数字的密钥，这个密钥与 40 比特的会话密钥大致相同。

文件的完整性利用附件 E/T.36 中规定的系统获得，而 ITU-T T.36 建议书规定了散列算法，包括有关的计算和信息交换。

在注册模式中，两个终端交换能让各实体唯一识别对方的信息。这是以一次性秘密密钥的用户间达成的协议为基础的。每个实体都存储着与其唯一相关的一个 16 位数，实体利用这个数字完成注册。

在需要安全传输一个文件时，发送终端向接收实体传送一个与接收实体相关的 16 位秘密数、一个随机数以及一个加密的会话密钥作为给接收实体的口令。作为回应，接收终端向发送实体传送一个与发送实体相关的 16 位数字密钥、一个随机数以及发送实体发出的口令的再加密版本。同时它向发送实体传送一个随机数和一个加密的会话密钥作为给发送实体的口令。发送终端回应一个随机数和从接收实体返回口令的再加密版本。通过这个程序，两个实体间实现了相互认证。同时，发送终端传送一个随机数和用于加密与散列运算的加密会话密钥。

文件传输后，发送终端向接收实体传送一个随机数和一个加密会话密钥作为给接收实体的口令。同时，它还传送一个随机数和加密的散列值，使得接收实体能确保接收文件的完整性。接收终端向发送实体传送一个随机数和发送实体发出的口令的再加密版本。同时，它还传送一个随机数和加密的“完整性文件”信息，用于确认或否认已收到文件的完整性。用于保证文件完整性的散列算法要对整个文件执行。

还有一种不涉及两个终端间任何安全信号交换的超越模式。用户商定一个用于人工输入的一次性秘密会话密钥。发送终端利用该密钥完成对文件的加密，而接收终端利用该密钥完成解密。

6.3.2 使用RSA的传真安全

附件 H/T.30 规定了以 RSA 密码机制为基础提供安全特性的机制。*Rivest, Shamir & Adleman* (RSA)算法详见[*ApplCryp*，466-474 页]。具有安全特性的传输文件的编码方案可以是 ITU-T T.4 和 T.30 建议书中规定的任一种（改进的 Huffman、MR、MMR、附件 D/T.4 规定的字符模式、BFT、附件 C/T.4 中规定的其他文件传送模式）。

数字签字（认证和完整性类型的服务）所用的基本算法是采用一对“公开密钥”/“秘密密钥”的 RSA 算法。

如果是提供非强制性机密性服务的话，用于文件加密的含有会话密钥“Ks”的令牌也用 RSA 算法加密。在这种用途中，被称为（“加密公开密钥”/“加密秘密密钥”）的密钥对不同于认证和完整性类型的服务所用的密钥对。这是为了分清两种用途。

ISO/IEC 9796（《具备消息恢复功能的数字签字方案》）中描述了附件 H/T.30 中所用的 RSA 的实施。

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/IEC 9796 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**数字签字算法**（DSA）机制[*ApplCryp*, 483-502 页]。

在附件 H/T.30 的方案中，默认的方式是不使用*认证机构*，然而它们可以非强制性地用于确认传真消息发送者公开密钥的有效性。在这种情况下，公开密钥可以按照 ITU-T X.509 建议书来确认。附件 H/T.30 中描述了发送者公开密钥证书的传输方法，但证书的确切格式还有待进一步研究，且证书的实际传输是在协议中进行协商。

作为一个必备特性，提供了一种*注册模式*。它允许发送者和接收者在双方间的任何安全传真通信之前以保密方式注册和存储对方的公开密钥。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（公开密钥特别长，达 64 字节或更长）。

因为注册模式允许交换公开密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。

正如该附件所述，有时对“散列函数”的结果也要实施签字。

可以使用的散列函数或者是（SHA-1，*安全散列算法*），一种来自美国国家标准和技术学会（NIST）的算法，或者是 MD-5（RFC 1321）。对于 SHA-1，散列运算结果的长度为 160 比特，而对于 MD-5，散列运算结果的长度为 128 比特。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。使用这个算法还是使用另一个算法将在协议中进行协商（见后面内容）。

为提供机密性服务对数据进行加密是非强制性的。附件 H/T.30 中记录了五个可选的加密方案：FEAL-32、SAFER K-64、RC5、IDEA 和（ITU-T T.36 建议书描述的）HFX40。在一些国家，使用这些方案须遵守国家法规。

还有其他一些非强制性算法可以使用。这些算法的选择要符合 ISO/IEC 18033 系列。

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协商。利用会话密钥进行加密。会话密钥的基本长度是 40 比特。对于使用 40 比特会话密钥的算法（如 HFX40），会话密钥“Ks”是加密算法中实际使用的密钥，而对于要求密钥长度超过 40 比特的加密算法（如 FEAL-32、IDEA、SAFER K-64 分别要求：64 比特、128 比特和 64 比特），可以利用冗余机制获得必要的长度。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

根据第 2.4 节讨论的安全体系结构，保障控制平面上的流量的安全至关重要。该流量用于监视和控制通信网。管理流量通常按照完成故障、配置、会计、审查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的建立，也涉及与安全体系结构三个平面和三个层有关的信息安全的管理。本节描述的是后者。

在传统的电信网中，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 ITU-T M.3010 建议书所述的电信管理网（TMN）。TMN 是单独的，与公众网基础设施隔开，因此任何由公众网最终用户平面的安全威胁引起的破坏都不会扩散到 TMN。由于这种分离，保护管理网流量的安全就比较容易，因为访问该平面只限于得到授权的网

络管理员，流量也仅限于有效的管理活动。随着下一代网络的引入，用于最终用户应用的流量有时可能又会和管理流量混和在一起。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，但它也带来了许多新的安全难题。最终用户平面的威胁现在成为了管理和控制平面的威胁。管理平面现在已经发展成多数最终用户都能访问，多种类型的恶意活动也成为可能。

为了提供一个完整的端对端解决方案，对于网络基础设施、网络服务和网络应用的每一类型网络活动（如管理平面活动、控制平面活动和最终用户平面活动）都要采取各种安全措施（如访问控制、认证）。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络单元（NE）和管理系统（MS）。

如下所述，尽管有不少标准可用于确保维护电信基础设施所需管理信息的安全，但管理问题的另一个范畴还与环境有关，在这种环境内中，为了跨越地理边界向客户提供像租用线这样的端对端服务，或者为了监管机构或政府部门完成灾害恢复，不同的服务提供商需要相互合作。

6.4.1 网络管理体系结构

ITU-T M.3010 建议书规定了用于确定电信网的网络管理的体系结构，其实际体系结构如图 6-11 所示。管理网规定了各种接口，用于确定在不同层面完成 OAM&P 功能所需的交换。

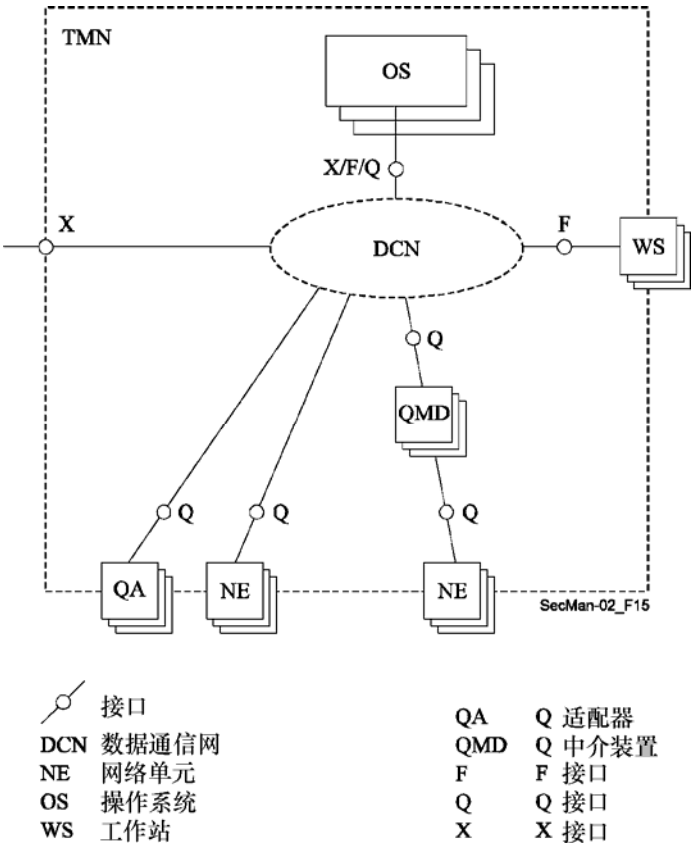


图 6-11－M.3010中实际体系结构的例子

从安全的观点看，对不同的接口有不同的需求。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之间。虽然 Q 接口和 X 接口都需要安全服务，但 X 接口要求的应对措施是更为牢靠和必要的。ITU-T M.3016.0 建议书概述了这些接口的安全威胁，并给出了确定这些威胁的框架。在 M.3016 系列建议书中，M.3016.1 规定了详细的要求，M.3016.2 概括了安全服务，M.3016.3 则规定了在 ITU-T M.3010 建议书说明的 TMN 功能体系结构内能够应对威胁的机制。由于各标准开发组织没必要对所有要求都提供支持，M.3016.4 给出了一种根据安全要求、安全服务和安全机制拟定安全简表的书写格式，可以用该书写格式遵守某个组织的独特安全政策。ITU-T M.3320 建议书则详细描述了 X 接口的具体问题。不同通信层的协议问题在 ITU-T Q.811 和 Q.812 建议书中做了具体规定。

在管理范畴内讨论安全问题时涉及两方面。其一涉及端对端活动（如 VoIP 服务）的管理平面。掌管用户的管理活动必须用安全的方式来实现。这指的是为部署端对端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。不论何种应用，例如无论是 VoIP 或还是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得到管理。这就是常说的*安全信息的管理*。前面的第 5 节规定的 PKI 就是这方面的一个例子。ITU-T M.3400 建议书规定了若干与这两方面都有关的功能。

已经根据 X.805 的框架制定了若干建议书，涉及管理平面（见图 2-1）三个方格的管理功能。下面几小节对这些建议书中的一部分做了说明，并介绍这些建议书是如何讨论安全需求的。除了管理平面三个层的建议书外，还有其他建议书规定一般的或普通的服务，例如存在实际发生的破坏安全的行为时的告警报告、审查功能和为不同目标（如管理实体）规定保护等级的信息模型。

6.4.2 管理平面和基础设施层的交叉

该方格处理如何保护网络基础设施单元的管理活动，也就是传输和交换单元及连接这两种单元的链路，还有终端系统，如服务器。像提供网络单元这样的活动必须由得到授权的用户完成，就是一个例子。端对端的连接可以按接入网和核心网来考虑。这些网络可能使用不同的技术。已经制定了建议书，对接入网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）。这种接入网的用户特权的管理是用 ITU-T Q.834.3 建议书中的统一建模方法学规定的，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 。在这些建议书中描述的接口就是图 6-11 中所示的 Q 接口。它适用于单元管理系统和网络管理系统之间。单元管理系统用来管理单独的网络单元并由此了解由一个或多个供应商提供的单元的软硬件体系结构的内部细节，而网络管理系统是在端对端网络层面上开展活动并涉及多供应商管理系统。图 6-12 示出了单元管理系统的用户用于创建、删除、分配和使用访问控制信息的各种对象。用户许可清单包含每个得到授权的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口令并授权使用许可清单中允许的功能性。

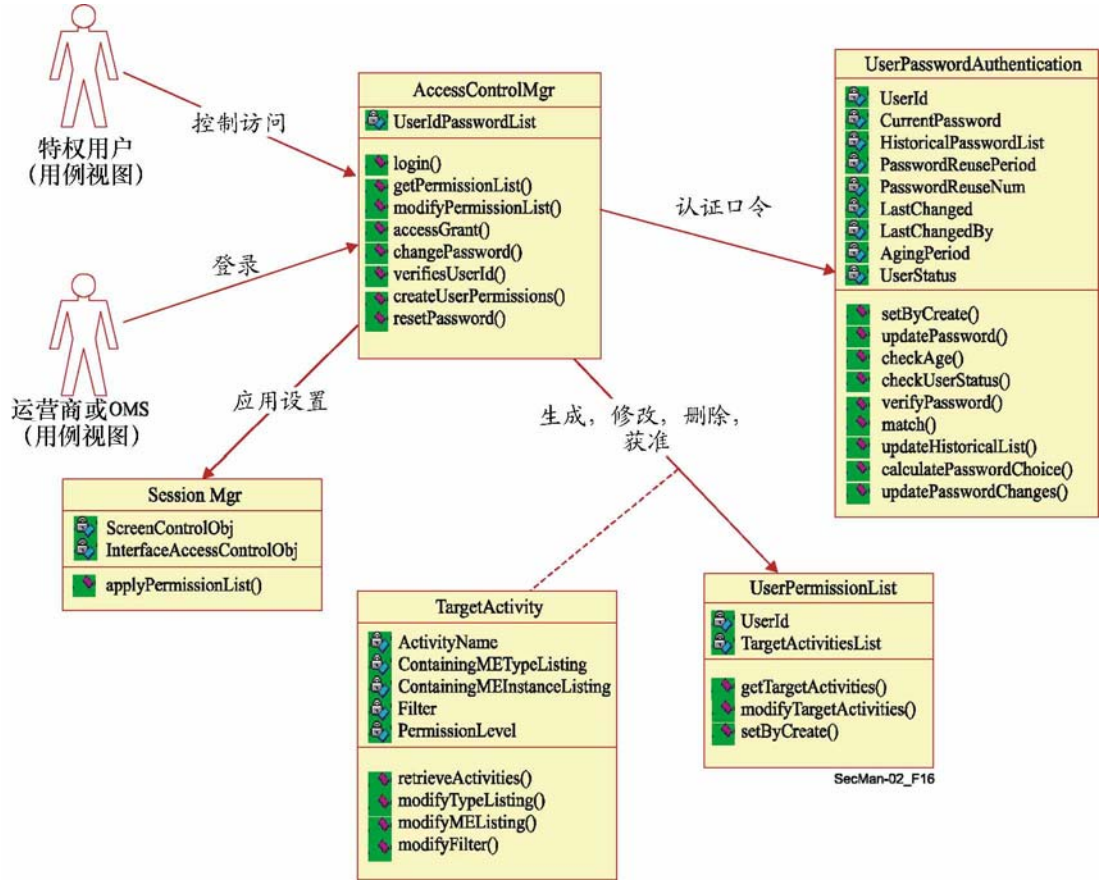


图 6-12－Q.834.3中的用户特权管理

6.4.3 管理平面和服务层的交叉

管理平面和服务层的交叉适合保护涉及监视和控制网络资源的活动，这些资源是为了保证提供商的服务而准备的。ITU-T 建议书探讨了这一交叉的两个方面。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。第二方面就是规定哪些行政管理交换是合法的。这样的规定有助于检测破坏安全的行为。在出现破坏安全的行为时，经常采用特定的管理系统对其进行管理。

建议书中探讨第一方面服务管理活动的例子，是关于连接管理的 ITU-T M.3208.2 建议书。拥有可按需提供的链路的服务客户使用这种服务来形成一个端对端的租用电路连接。这种连接管理服务允许订户在可按需提供的资源范围内建立/激活、修改和删除专用电路 。由于是用户提供端对端连接，有必要确保只有得到授权的用户允许执行这些操作。为与该服务相关的管理活动规定的安全尺度是第 2.4 节中讨论的八个尺度的一个子集，包括对等实体认证、数据完整性控制（防止在传输中未经授权修改数据）和访问控制（确保一个订户不能恶意地或无意地获取另一订户的数据）。

ITU-T M.3210.1 建议书是规定与无线服务管理平面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方面。

在一个无线网络中，当用户从归属网漫游到被访网时，他们可能跨越不同的管理域。在 ITU-T M.3210.1 建议书中规定的服务描述了归属地的欺诈管理域如何从一个订户在被访网注册开始收集关于该订户的适当信息。图 6-13 中的 a）和 b）方案示出了或者由归属网或者由被访网发起的监视管理活动。在某个订户向被访网注册至从该网络注销离开该网络期间，归属网中的欺诈检测系统会要求关于订户此期间活动的信息。然后根据具体服务级别的或某个订户的呼叫详情记录与跟踪（分析）形成一个与使用情况有关的说明文件。欺诈检测系统可随后根据欺诈行为分析和生成适当的告警。

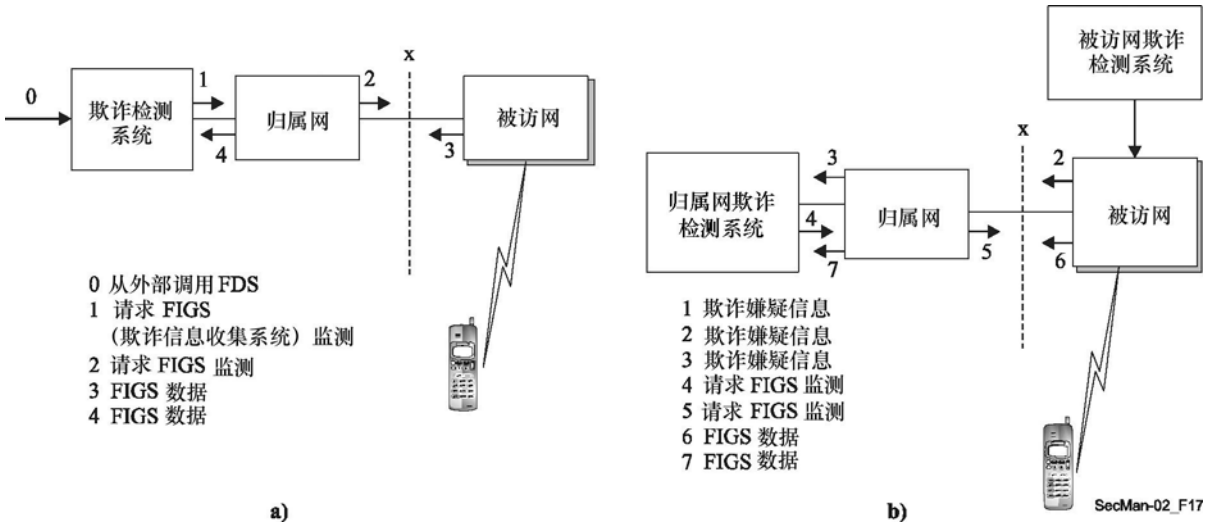


图 6-13－ITU-T M.3210.1建议书中的无线服务欺诈管理

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个方格，对应于保护基于网络的最终用户应用。报文发送和号码簿应用等已在 X.400 系列和 X.500 系列建议书中做了规定。

需要保证管理活动安全的另一类应用是管理应用本身。这种表述好像有些兜圈子，最好还是用例子来解释。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。考虑一下服务提供商为了提供端对端连接服务而使用其他服务提供商的连接服务的情况。根据规章制度或市场环境，一些服务提供商可能提供接入服务，而其他运营商，称为*局间运营商*，可能提供长途连接。局间运营商租用本地服务提供商的接入服务来提供跨地区的端对端连接。在出现服务损失时，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服务故障

而要求授权。得到授权的系统和用户应采取必要措施检索所报故障的状况。图 6-14 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中的邮箱管理，要对访问特权加以管理，防止未经授权获取故障报告。一个服务提供商只允许报告自己租用服务的故障，而非其他提供商租用服务的故障。

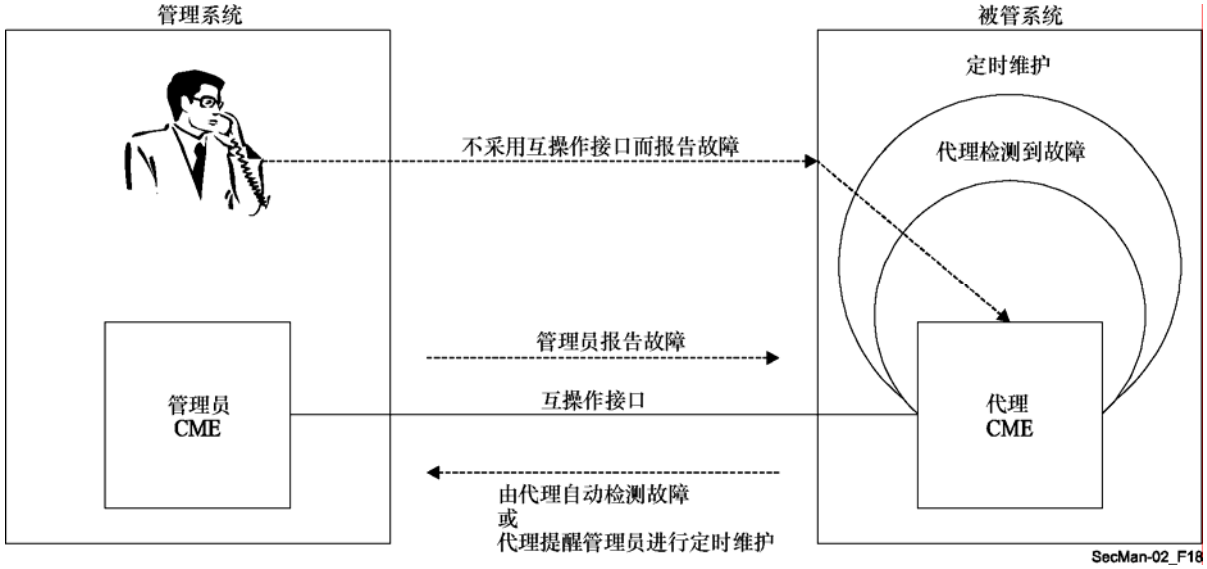


图 6-14－ITU-T X.790建议书规定的故障管理报告的产生

ITU-T X.790 建议书对这种管理应用做了规定，并采用访问控制列表和双向认证等机制保护这些活动。这种应用和认证安全机制已经用这些建议书实施和部署了。

6.4.5 通用安全管理服务

ITU-T X.736、X.740 和 X.741 建议书规定了在接口使用公共管理信息协议（CMIP）时适用于管理平面所有三个方格的公共服务。下面简要介绍这些建议书中包含的服务。注意，所有这些功能都相应地被认为是管理平面的活动。

6.4.5.1 安全告警报告功能：告警报告总的来说在管理接口中是一个关键功能。如果检测到一项失效，不管是由于操作原因（电路组件的失效）还是因为违反了安全政策，都向管理系统发出告警报告。告警报告含有若干参数，以便管理系统确定失效的原因并采取纠正措施。任何事件的参数都含有一个强制性字段，称为事件类型，还含有一组其他字段，叫做事件信息。后一组信息包括告警的严重程度、告警的可能原因、破坏安全行为的检测装置等内容。告警原因与事件类型有关，如表 6-2 所示。

表6-2－安全告警原因

事 件 类 型	安全告警原因
完整性破坏	复制信息 信息遗失 检测到信息改动 信息失序 意外信息
业务破坏	拒绝服务 服务中断 程序错误 未加规定的原因
实物破坏	线缆改动 检测到侵入 未加规定的原因
安全服务或机制破坏	认证失效 泄露机密 不可抵赖失效 未经授权的访问尝试 未加规定的原因
时域破坏	迟到的信息 密钥过期 营业时间之外的活动

这些告警原因在 X.736 中有进一步的解释。其中若干原因与前面几段讨论的威胁有关。

6.4.5.2 安全审查索引功能：为了让某个安全管理用户能够记录破坏安全的行为并得到破坏安全行为的审查索引，ITU-T X.740 建议书确定了若干需要审查索引的事件。这些事件是连接、断开、安全机制利用、管理操作和使用量结算。模型采用 ITU-T X.735 建议书规定的日志机制，这是被管系统生成的记录任何事件的一般日志。由审查索引功能确定了两种与破坏安全的行为有关的事件。这两种事件是服务报告和使用情况报告。服务报告与一项服务的提供、拒绝和恢复有关。使用情况报告用于表明已经生成了一份含有涉及安全的统计数据的记录。与任何事件一样，对于服务报告也规定了若干原因值。举例来说，这些值是请求服务、拒绝服务、服务失效、服务恢复等。可视情况规定新的事件类型，因为 ITU-T X.740 建议书中规定的两种事件将来不一定够用。

6.4.5.3 ITU-T X.741 建议书非常详细地规定了与为各种被管实体分配访问控制权有关的模型。满足该建议书中访问控制规定的要求包括防止未经授权生成、删除、更改管理信息，对事件进行获准的操作符合操作发起者的访问权限，防止向未经授权的接收者发送管理信息。规定了各种级别的访问控制权以满足上述要求。对于管理操作来说，建议书中的规定有利于多种层次的访问限制：整个被管实体、实体的属性、属性值、访问关联及对实体采取的行动。已经确定了若干方案，如以能力为基础、以标签为基础和以关联为基础的访问控制清单，一项访问控制政策可以实施这些方案中的一种或多种。在该模型中，根据政策或访问控制信息（ACI）确定允许还是不允许请求的操作。举例来说，ACI 包括规则、发起者身份、请求访问的目标的身份、关于发起者的认证信息等。该模型特性十分丰富，无论何种应用都不一定需要所有能力。

6.4.5.4 以 CORBA 为基础的安全服务：X.700 系列建议书假定采用 CMIP 作为管理接口协议，但业界也出现了将基于公共对象请求代理的协议、服务和目标模型用于管理接口的其他趋势。ITU-T Q.816 建议书规定了在管理接口的范畴内采用这些服务的框架。为了支持这些接口的安全要求，该建议书引用了用于安全的公共服务的 OMG 规范。

6.5 电子处方

医疗保健的提供需要并产生了大量各种数据和信息。这些数据和信息需要安全地收集、处理、分发、获取和使用，并遵守严格的道德和法律规则。这一点对临床信息与管理信息尤其重要，但对其他类型的信息，如流行病学、文献与知识数据库信息，也很重要。

这些类型的数据、信息的源头处在医疗保健基础设施内外，位于与各自用户远近不同的地方。实际上，用户需要和产生的是这些类型信息的组合，各类信息所起的作用也处在不同阶段，例如一位医生可能在检查患者时参考知识数据库，并在病历记录上相应登记，该记录可用于计费。

医疗保健就诊和处置是多面的。例如，它们发生在医患之间；在医生之间；在医生与专业咨询者之间；在患者与测试实验室、制药机构和康复中心等卫生机构之间。这种就诊可能发生在所在社区、在国家的另一地区或国外。所有这些就诊都在就诊实际开始前就需要数据和信息，同时在就诊期间或其后同样产生数据和信息。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，完整的病历记录、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，因此口头和书面语言是交流和保存病程记录的主要形式，而交通则主要是使用公路、铁路和空运等公共和私人服务。在现代化的医疗保健远程信息处理工具出现和成长之前，电话业务网络逐步发展，一度成为国内外卫生专家和机构的通信网络。

技术在医疗保健机构的临床/医学部分的应用稳步增长，包括仪器和设备，特别是传感和测量设备、实验室服务、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医疗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，这种以技术为基础的服务与主流医疗保健服务之间的交流成为这类服务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。正像话音通信是医生的诊所和医疗保健机构里安装电话的主要动力，电子邮件是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，对其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呈几何级数增长，在一国之内和各国之间，甚至在最贫穷的国家，情况都是如此。例如，电子处置取代了并非确实需要当

面就诊的那些功能，如书写、发送处方和报告，安排预约和服务日程，分诊，以及在电信服务性能许可时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医疗，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意见的系统。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。

上面提到的所有发展还对卫生部门需要并使用的相关的管理信息系统（MIS）有重要影响，如医院的 MIS。这种系统不再是医院治疗病人的从入院到出院/转院的行政管理系统，而是包括了许多智能化的便于医务人员使用的接口，比如说，可以通过这些接口连到临床决策支持系统、远程医疗链路、门户网站等。

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或他们认为必要的任何时候，获得其所需的医学资料，如电子病历记录，或获得一件工具或仪器。而解放双手这个特性意味着必须找到不用医务人员人工干预（如开门或敲击计算机键盘）的识别和授权解决方案。

因此，医疗保健部门是一个信息高度密集型的部门，医疗保健和与医疗保健有关的数据和信息的收集、流动、处理、显示和分发，对一国之内和各国之间医疗保健服务的运转和发展的效能、效率和经济性十分关键。

一个至关重要的要求是所有这类流动必须安全和保密地进行，同时必须严格地遵守道德和法律规则与规定。

6.5.1 电子医疗保健应用中要考虑的PKI和PMI问题

通过把各认证机构连在一起，PKI 再造了现实世界的分级结构，无论是地缘政治层面（区域—国家—省（市）—行政区），还是专业层面（医疗保健—药品—外科—专科手术—供应商等）。此外，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，这个现实使得用于医疗保健的标准化 PKI/PMI 规定变得不可或缺了。

医疗保健系统的技术互操作性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采用了像 ITU-T X.509 建议书这样的标准。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 不应影响用户与卫生部门用其他 PKI/PMI 认证的人进行互操作的能力（这自然涉及到关于访问控制和卫生部门其他相关政策的起码的最低标准化）。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共同的根。技术标准的采用、不同基础设施的技术互操作性和一些政策的标准化将保证全球卫生事务有一个十分有效率和综合的环境。

6.5.2 索尔福德电子处方系统

[*Policy*]中描述的电子处方系统是电子医疗保健中应用 PKI 和 PMI 的很好的例子。考虑到英国参与电子传输处方（ETP）计划的专业人员众多（34 500 名全科医师； 10 000 名有处方权的护士，未来几年将增长至 120 000 名； 44 000 名注册药剂师和 22 000 名牙医），而真正需要授权的极少（即各种级别的开处方、配药许可权，免费处方准许权），基于角色的访问控制（RBAC）似乎是使用 ETP 的理想授权机制。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其集中是特别重要的，否则这个系统就无法管理了。

每一位专业人士都有一个授予他们在本专业领域从业的主管部门。在英国，由英国医学总会（GMC）负责医生资格注册和由于渎职而取消其行医资格。英国牙医总会（GDC）对牙医、英国护士和助产士协会（NMC）对护士、皇家药剂学院对药剂师都有同样的管理权。由于这些部门的这项管理职责都执行得很好，因此上述 ETP 系统中的角色分配分别被赋予这些部门。

2001 年 6 月成立的劳动和退休保障部（DWP）接管了上届政府中的社会安全部、教育和就业部的职能。它负责支付失业补助和养老金并与处方药价格管理局（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、17 或 18 岁受全日制教育的青年人，领取收入补助或求职津贴的人或其配偶，现行国家卫生系统（NHS）低收入计划完全救助证明（HC2）持有人，孕妇和过去 12 个月内生产过的妇女，以及战争致残养恤金领取者。因此该准许权的管理被分配给 DWP 和 PPA 的不同部门。

每一位专业人士由其专业管理部门授予角色属性证书，这个证书被存储在属于该专业管理部门的 LDAP 号码簿中。ETP 系统如果有权访问 LDAP 号码簿，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 号码簿（或号码簿簇）中，则 ETP 系统将能通过访问这个 LDAP 号码簿来决定免费领取处方药的权利，药剂师不必再询问患者是否有权。后者只是在患者刚变为有权时才需要，例如一个孕妇刚被全科医师诊断为怀孕，而 DWP 又不能及时颁发官方属性证书的情况。

这些角色随后由授权决策引擎（例如 PERMIS，见网站 www.permis.org）用于根据 ETP 政策来决定医生能否开处方、药剂师能否配药和患者能否享受免费处方药。在初始化时，每种 ETP 应用（处方系统、配药系统、PPA 系统）读入 ETP 政策，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 号码簿中提取人员的角色，并根据该政策做出决定。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参与的情况下自动进行，他们无需担心系统如何或在哪存储和使用证书。

图 6-15 是英国实施电子处方系统的一个例子，它示出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（如一个使用公开密钥证书的 PKI 系统）也提供强授权（如一个 PMI 系统）的安全基础设施，在此核准医务人员所具有的具体权利，因为他们的角色都储存在属性证书中。传统模型使用包含在每一个特定应用（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（如用户名/口令、信用卡等）。在采用 PKI 和 PMI 的新模型中，用户只需要一个令牌 — 用户的公开密钥证书 — 以便从地理上和/或拓扑结构上分散的不同服务和不同资源中受益。用户属性证书由系统储存而不是由用户持有，而且证书是按照要求在组件间传输，以便允许访问。由于属性证书是由签发者数字签发的，它们不可能在上述传输中被篡改。

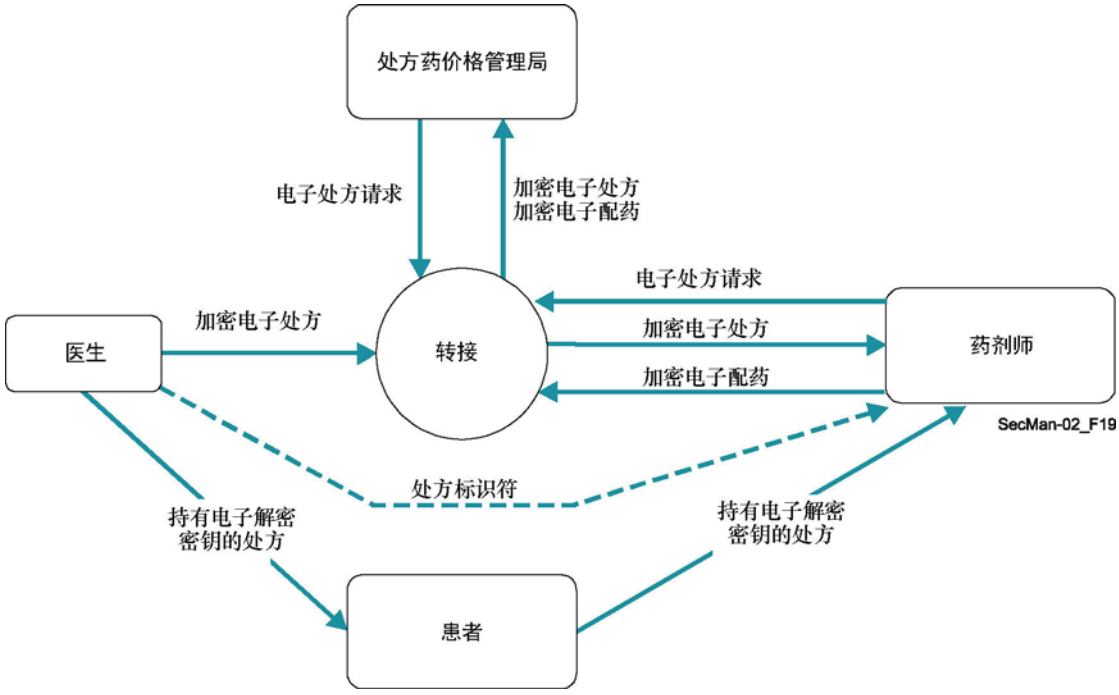


图 6-15－索尔福德电子处方系统

在图 6-15 所示的例子中，电子处方由医生开出，进行数字签字（用于认证），使用一个随机会话密钥对称加密（为了机密性），然后将电子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，然后检索处方并解密。与目前的纸质处方系统一样，最终是患者控制谁有权给他按方抓药。但这还不够。对谁有权开方和配置何种药物及谁有权享受免费处方药进行控制也是必要的。

虽然上面的描述说明了一个紧凑的综合系统，但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政策等的系统，该系统依靠可信第三方对不同的参与者进行认证和授权。即使有可用的 PKI 和 PMI 专门解决方案，使用像 ITU-T X.509 建议书这样的标准化解决方案目前仍能促进更普遍地在全球使用电子处方。

6.6 安全的移动端对端数据通信

具备数据通信能力的移动终端（像 IMT-2000 移动电话、便携式计算机或带有无线卡的 PDA）销售广泛，为连至移动网的移动终端提供的各种应用服务正在出现（如移动电子商务）。在电子商务环境下，安全是必要的，甚至是绝对必要的。

从移动运营商的角度看，要考察的安全领域很多（如 IMT-2000 移动电话网的安全体系结构）。不过从移动用户的角度和应用服务提供商（ASP）的角度加以考察也很重要。

从移动用户的角度和 ASP 的角度考察移动通信的安全问题时，移动终端和应用服务器之间的移动端对端数据通信的安全问题就成为最重要的问题之一了。

另外，对于将一个移动网连至开放网的移动系统而言，有必要对 OSI 参考模型高层（应用层、表示层和会话层）进行安全考察，因为移动网（如 IMT-2000 移动电话网、无线局域网、蓝牙）的实施或开放网的实施是多种多样的。

6.6.1 移动端对端数据通信系统的安全技术框架

ITU-T X.1121 建议书对高层移动终端与应用服务器之间安全的移动端对端数据通信的模型做了说明。对移动用户和 ASP 之间的移动端对端数据通信的安全框架规定了两种安全模型：“通用模型”和“网关模型”。移动用户采用移动终端访问 ASP 提供的各种移动业务。ASP 通过应用服务器向移动用户提供移动业务。移动安全网关将数据包从移动终端转向应用服务器，把以网络为基础的移动通信协议转换成以开放网为基础的协议，反之亦然。

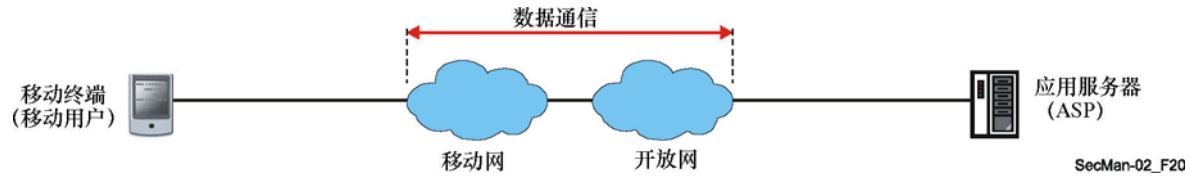


图 6-16－移动用户与ASP之间移动端对端数据通信的通用模型

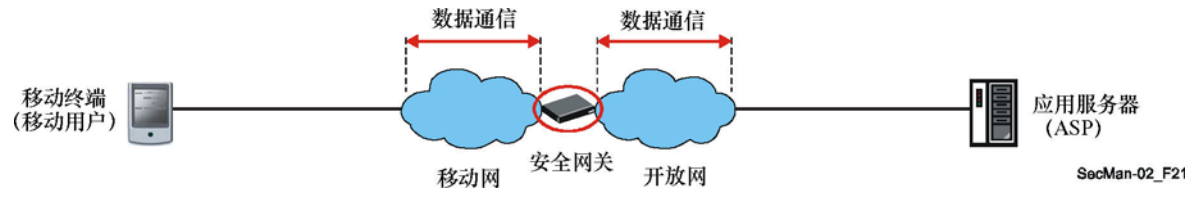


图 6-17－移动用户与ASP之间移动端对端数据通信的网关模型

ITU-T X.1121 建议书还从移动用户的角度和 ASP 的角度说明了两种模型的移动端对端数据通信的安全威胁和安全要求。威胁有两种类型：一种是存在于任何开放网中的一般型，另一种是专门面向移动的移动性型安全威胁。图 6-18 描绘了移动端对端数据通信网中的威胁。

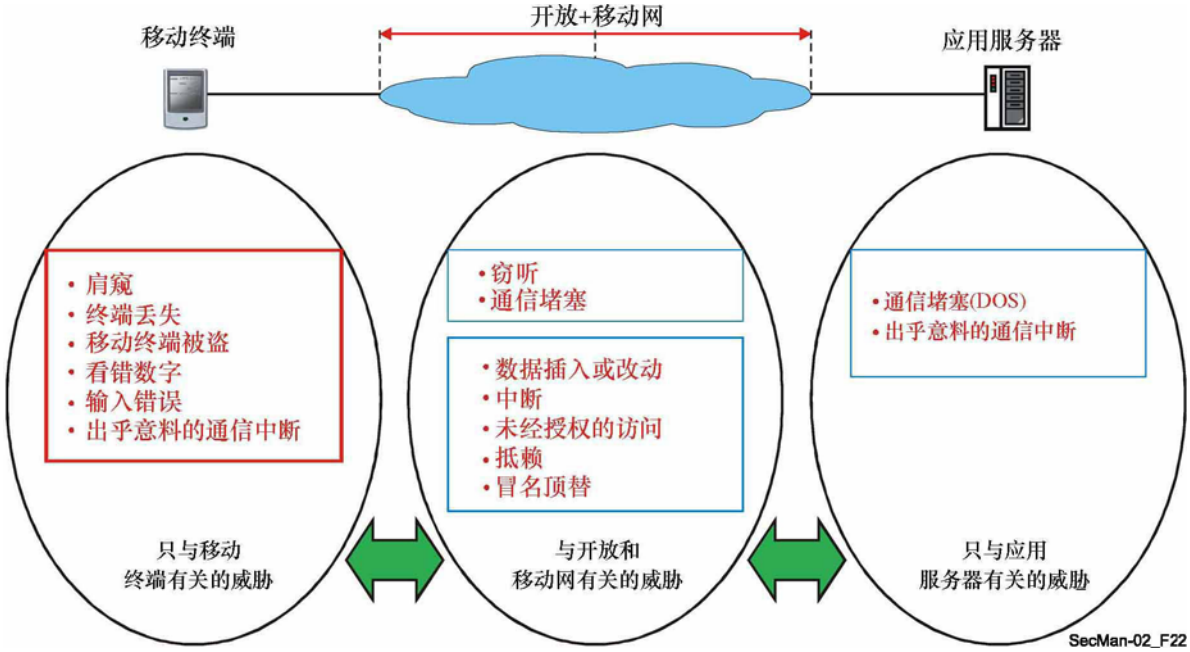


图 6-18－移动端对端通信中的威胁

另外，ITU-T X.1121 建议书确定了移动端对端数据通信中各实体在需要时实施安全技术的位置和实体间的相互关系（见图 6-19）。

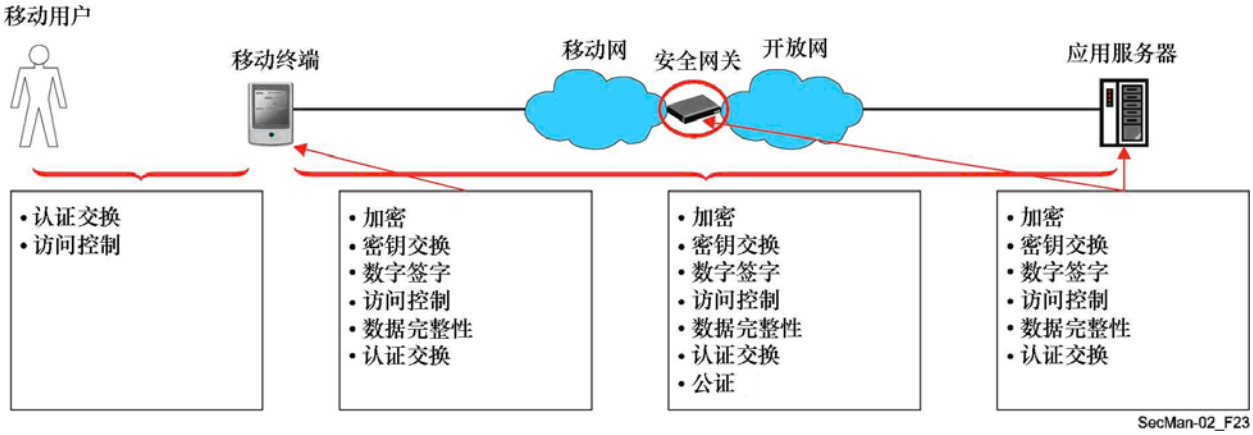


图 6-19－各实体所需的安全功能及实体间的关系

6.6.2 安全的移动端对端数据通信中要考虑的PKI问题

本节与 ITU-T X.1122 建议书有关。尽管 PKI 技术对于保护移动端对端数据通信非常有用，但在构建安全的移动系统时移动数据通信特有的某些性质可能会要求对 PKI 技术加以改进。规定了两种类型的 PKI 模型以提供移动端对端数据通信的安全服务。一种属于通用 PKI 模型，在移动端对端数据通信中不存在安全网关功能；另一种属于网关 PKI 模型，通过安全网关与移动网和开放网连接。图 6-20 描绘了移动端对端数据通信的通用 PKI 模型。该模型涉及四个实体。移动用户的证书机构（CA）向移动用户发布移动用户证书，并对存储着由用户 CA 发布的证书撤销列表（CRL）的库进行管理。移动用户的验证机构（VA）向移动用户提供在线证书验证服务。ASP 的 CA 向应用服务提供商发布 ASP 证书，并对存储着由 ASP 的 CA 发布的证书撤销列表（CRL）的库进行管理。ASP 的验证机构提供 ASP 证书的在线证书验证服务。

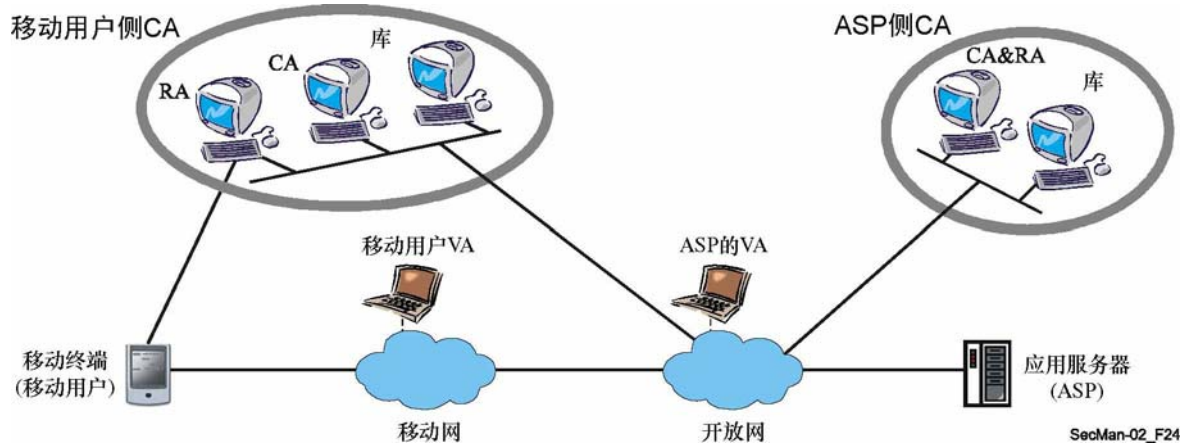


图 6-20－移动端对端数据通信的通用PKI模型

根据公开密钥/专用密钥产生位置的不同，存在两种证书发布方法。一种方法是在移动终端的生产厂家产生和编制加密密钥对。另一种方法是在移动终端上产生加密密钥对，或像插在移动终端上的智能卡那样产生无法改动的令牌。图 6-21 描绘了移动终端利用证书管理程序获取证书的程序，其中加密密钥对在移动终端上产生。

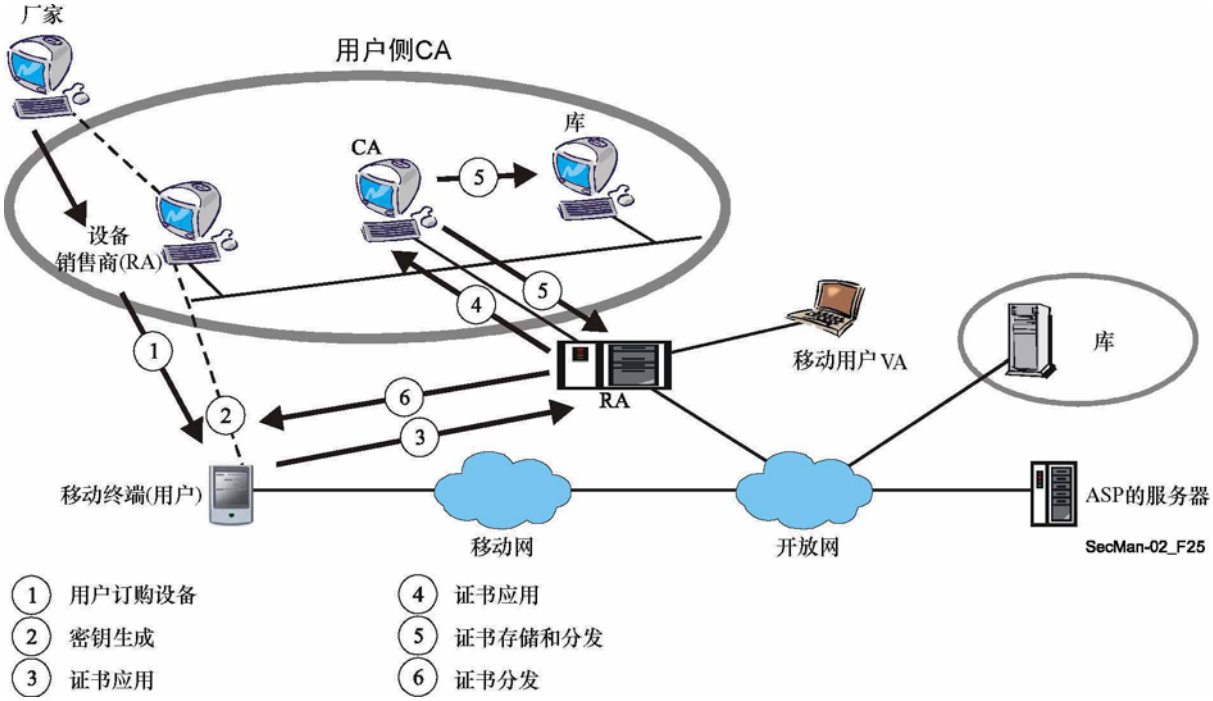


图 6-21－移动终端的证书发布程序

移动终端的计算能力和存储容量都有限。因此，在线证书验证方案优于根据 CRL 进行的离线证书验证方案。移动终端如果收到了采用证书链的消息—签字对并打算验证该签字的有效性，则应在采用证书验证方案对证书进行验证之后再使用证书。图 6-22 描绘了移动终端的在线证书验证程序。

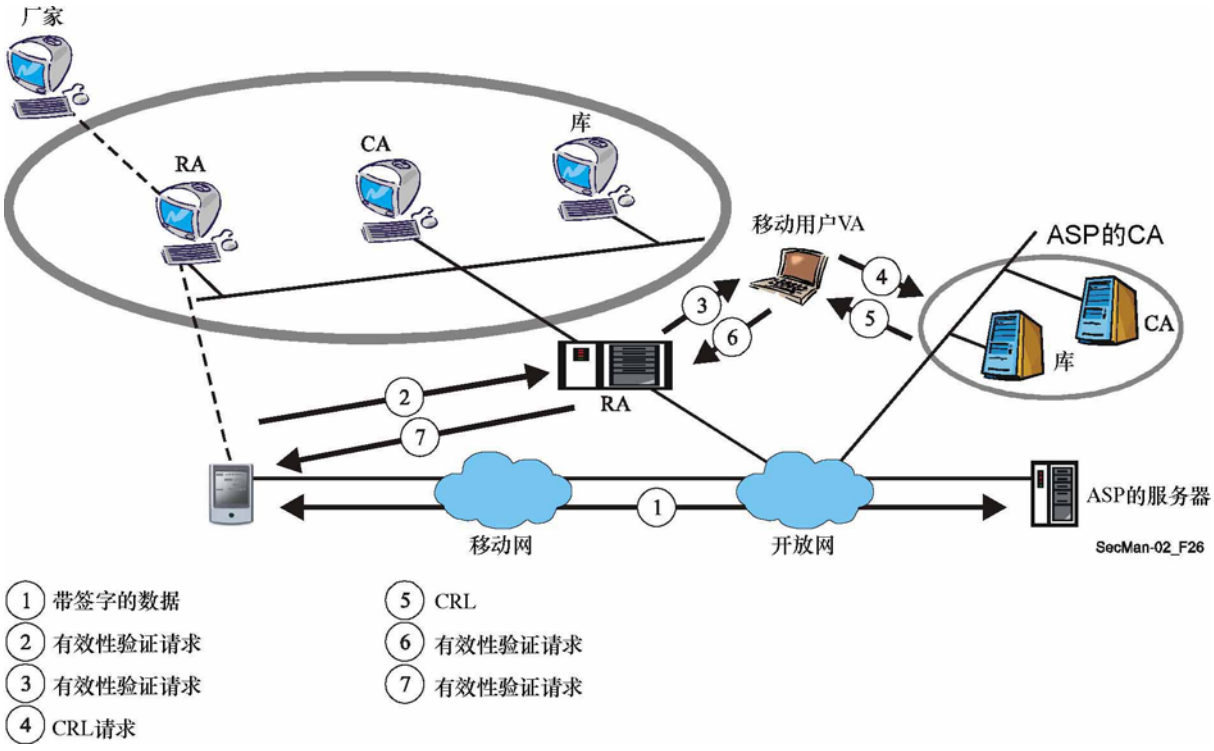


图 6-22－移动端对端数据通信的证书验证程序

移动端对端数据通信的 PKI 系统可用于两种用途模型：一种可用于会话层，另一种可用于应用层。会话层用途模型提供诸如客户端认证、服务器认证和机密性与完整性服务等安全服务。应用层用途模型提供移动端对端数据通信的不可抵赖服务和机密性服务。

最后，ITU-T X.1122 建议书从以下几个角度说明了以 PKI 为基础构建安全的移动系统需要考虑的问题：与开放系统中现有的基于 PKI 的系统的互操作性，PKI 在移动环境中的用途（包括密钥产生问题、证书应用与发布问题、证书使用问题和 CA 问题），以及 PKI 的一般问题（包括证书的生命周期管理问题）。在以 PKI 技术为基础构建安全的移动系统时该建议书可用做指导文件。

7 可用性尺度和基础设施层

第 2 节介绍的 ITU-T X.805 建议书提到：

- 安全尺度，是用于处理网络安全一个特定方面的一组安全度量值；
- 安全层。安全尺度是适于一系列网络设备和网络设施群，这些系列称为安全层。

可用性安全尺度确保不会因影响网络的事件而拒绝对网络单元、已存信息、信息流、服务和应用的得到授权的访问。灾害恢复解决方案即包括在这一类中。

基础设施安全层由网络传输设施及受安全尺度保护的单独的网络单元组成。基础设施层代表了网络、网络服务与应用的基本构件。基础设施层组成部分的例子包括单独的路由器、交换机和服务器以及单独路由器、交换机和服务器之间的通信链路。

作为上述各概念的一部分，ITU-T 规定了数量众多、五花八门的功能、实施和运行要求。这些要求可能涉及差错性能、拥塞控制、失效报告和纠正措施，以及许多其他问题。本节其余部分从不同的角度看待与通信网有关的要求，目的是限制传输资源不可用性的风险与后果。

为了便于电信网运营商在考虑可用性目标时挑选适当的网络拓扑结构，建议参考 ITU-T G.827 建议书附件 A《通路拓扑结构与端对端通路可用性计算示例》。

7.1 通路拓扑结构与端对端通路可用性计算

图 7-1 和图 7-2 示出了可用预定通路元素构建的基本通路拓扑结构。

图 7-1 示出了没有保护的简单基本通路；图 7-2 示出了添加端对端保护的通路，为强化保护该通路应采用一个单独路由。

这种形式的保护称为 1+1。每一通路都是双向连接，从同时固定连接到两条通路的每一端发出信号，每一接收机都有一个切换装置，以挑选最佳信号。

一种更经济的安排是采用一个保护通路来保护其他通路。这种做法称为 1:n 安排，发送机和接收机二者都需要用于挑选信号的切换机。

就端对端可用性计算而言，采用不可用性比率更为方便。ITU-T G.827 建议书在其附件 A 中给出了一些基本原则，用于评估简单基本通路（图 7-1）、1+1 端对端保护（图 7-2）或 1:n 保护率拓扑结构的可用性。

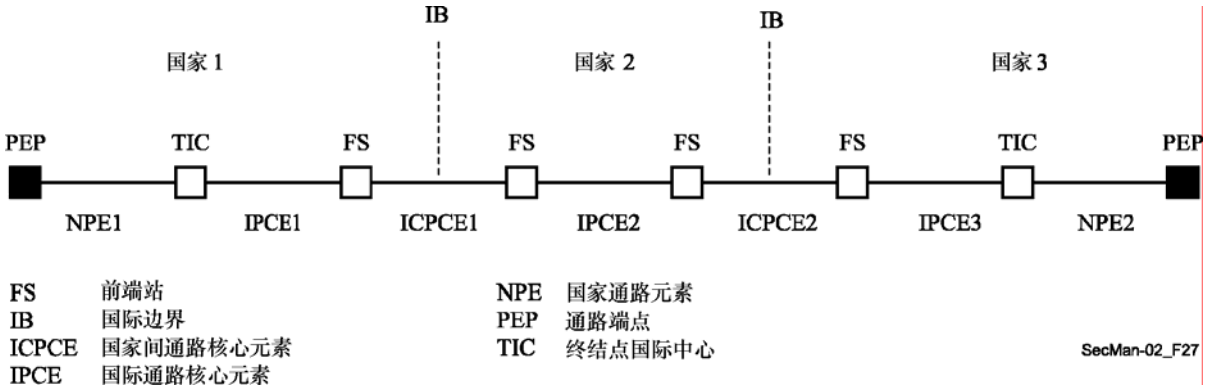


图 7-1－没有保护的简单基本通路示例

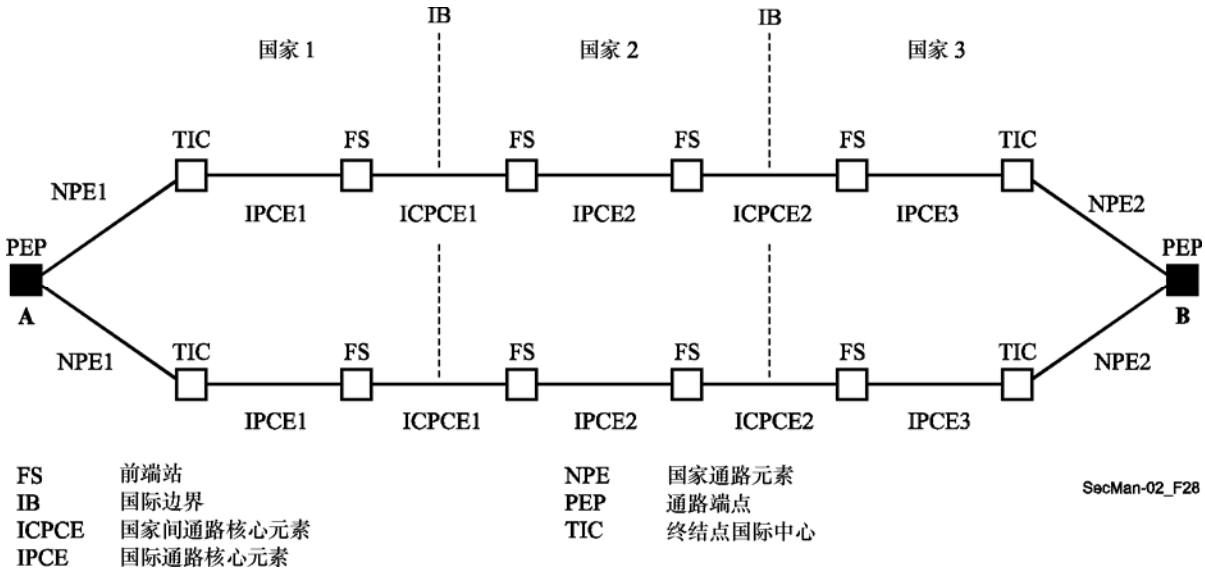


图 7-2－有端对端保护的通路示例

第 7.3 节给出了更复杂的拓扑结构，如同步数字系列（SDH）环状拓扑，表明业务量可以在一个失效链路附近重新选路，而保护路由取决于环上各节点的交换能力且不一定是两个节点之间的最短距离。对于更复杂的拓扑结构，评估可用性的问题就更困难了。附录一/G.827 中给出的几篇文章谈到了这个问题。

7.2 增强传送网的可用性 — 概貌

第 7.2 至第 7.4 节对更常见的用于增强传送网可用性的方式所具有的体系结构特点做了说明。通过用其他专用或共享的资源实体替换失效的或降质的传送实体来完成这种增强。替换通常在检测到缺陷、性能下降或外部（如网络管理）请求时发生。

保护 — 保护利用了节点间预先分配的能力。最简单的体系结构是每一工作实体有一个专用保护实体（1+1）。最复杂的体系结构是由 n 个工作实体共享 m 个保护实体（m:n）。保护切换既可以是单向的，也可以是双向的。单向保护切换只在单向失效的情况下对受影响的业务量方向采取切换动作。

恢复 — 恢复利用了节点间任何可用的能力。总的来说，恢复所用的算法会涉及重选路由。如果使用了恢复，则要保留一定百分比的传送网能力用于工作业务量的重选路由。

ITU-T G.805 建议书给出了这方面的关键资料。

7.3 保护

只有采用具备很高的可靠性和很强的生存能力的网络基础设施，才能达到很高的服务可用性。因此，如果具有很高可靠性的设备出现故障，则必须有能力切换到一个备用的信号源（保护信道）。

保护分为两类。一类是设备保护，备有富余的电路组件。因此如果电路组件出现硬失效，则另一个会自动接入。还有一类是网络保护。网络保护通过提供信号通行的备用通路防止光纤切断。这些备用通路既可以是专用的，也可以是共享的。图 7-3 示出了这种机制。

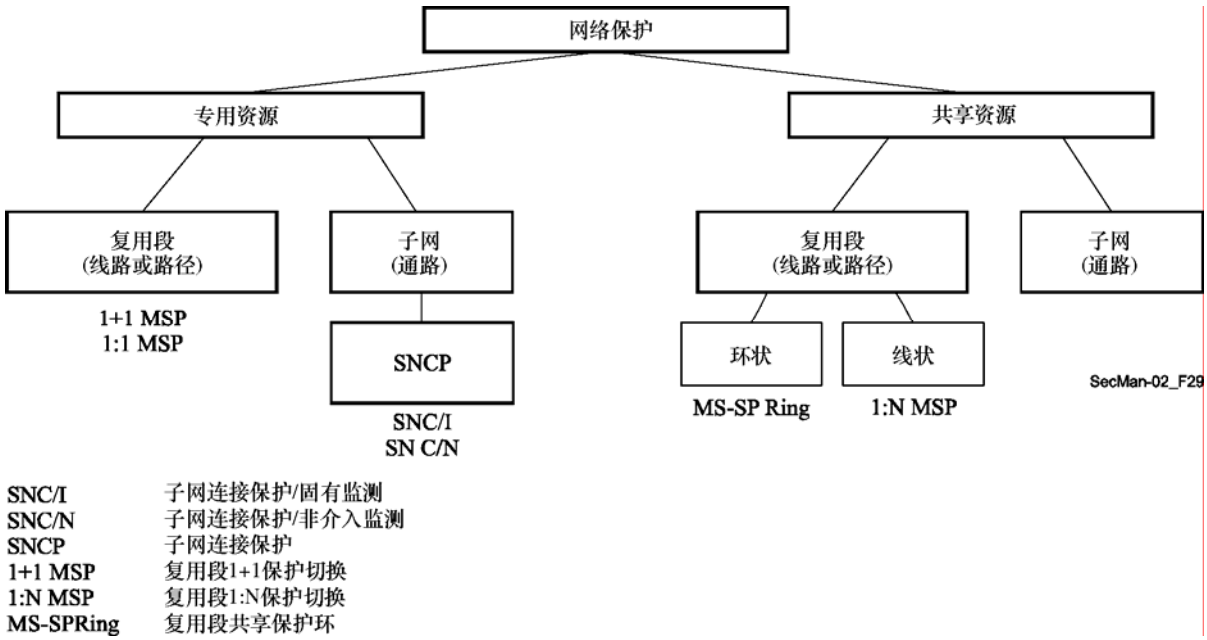


图 7-3－不同的保护交换

保护机制可以是单向的或双向的。还可以或是回送式的，或是非回送式的。这几个名词在 ITU-T G.780/Y.1351 建议书中有定义。

单向保护规定为“对于单向故障（即只影响一个传输方向的故障），只切换受影响的（路径、子网连接（SNC）等）方向。”这表明在进行保护切换时，只在接收机侧（本地节点）做出本地决定，不考虑远端节点的状态。这属于在单向失效（即只影响一个传输方向的失效）的情况下，只有受影响的方向切换到保护。

双向保护规定为“对于双向故障，包括受影响和不受影响在内的（路径、子网连接等）两个方向都切换。”这表明在进行保护切换时， 本地和远端的状态都要考虑。这属于在单向失效（即只影响一个传输方向的失效）的情况下，包括受影响和不受影响在内的两个方向都切换到保护。

回送（保护）操作规定为“在回送操作中，如果切换请求终止，业务量信号（业务）总是返还到（或维持在）工作 SNC/工作路径；即此时工作 SNC/工作路径已从缺陷中恢复或外部请求已被清除。”这表明在回送操作模式中，如果工作信道已从故障中恢复，保护信道上的信号会切换回工作信道。

非回送（保护）操作规定为“在非回送操作中，如果切换请求终止，业务量信号（业务）并不返还到工作 SNC/工作路径。” 这表明在非回送操作模式中（只对 1+1 体系结构适用），如果失效的工作信道又回到无故障状态，会继续在保护信道上挑选正常的或受保护的业务量信号。

最常见的操作形式如下：

- 1:1 MSP（复用段 1:1 保护切换，见第 7.3.1 节）
- 1+1 MSP（复用段 1+1 保护切换，见第 7.3.2 节）
- MS-SPRing（复用段共享保护环，见第 7.3.3 节）
- SNCP（子网连接保护，见第 7.3.4 节）

这些保护机制将会得到进一步讨论。不过，有一组共同的参考建议书是适用的：G.841（特性）、G.842（互通）、G.783（功能模型）、G.806（缺陷）和 G.808.1（通用保护切换）。

7.3.1 复用段1:1保护切换

图 7-4 示出了网络示意图。

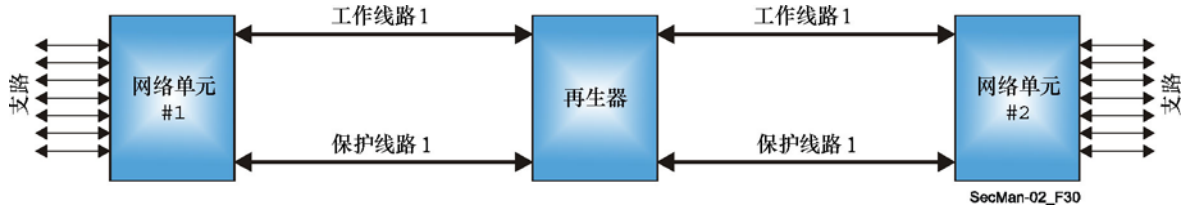


图7-4－1:1保护切换网络示意图

在 1:1 保护切换中，每一工作信道都有一条保护信道。保护信道也可以载送其他可以预占的业务量。

图 7-5 示出了网络单元内部的示意图。

图 7-5－复用段1:1线路保护

在正常条件下，“额外业务量”可以在保护信道上载送。不过如果收到了正确的 K1/K2 字节（启动了保护功能），则“正常业务量”在“头端”被桥接到保护信道，而在“尾端”进行切换。通过 K1 和 K2 字节对保护信道进行控制。

这相当于同步传送模块第 N 级（STM-N 级，N≥1）的线路保护。

能够触发切换的条件是强制切换和若干缺陷或失效条件（如信号失效、信号缺失、过多差错、信号降质）。详情见 ITU-T G.806 建议书。

7.3.2 复用段1+1保护切换

图 7-6 示出了网络示意图。

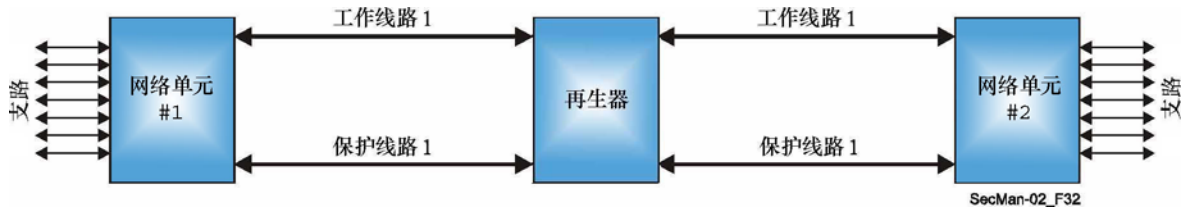


图 7-6－1+1保护切换网络示意图

在 1+1 保护切换中，每一工作信道都有一条保护信道。保护信道载送工作信道信号的副本。

图 7-7 示出了网络单元内部的示意图。

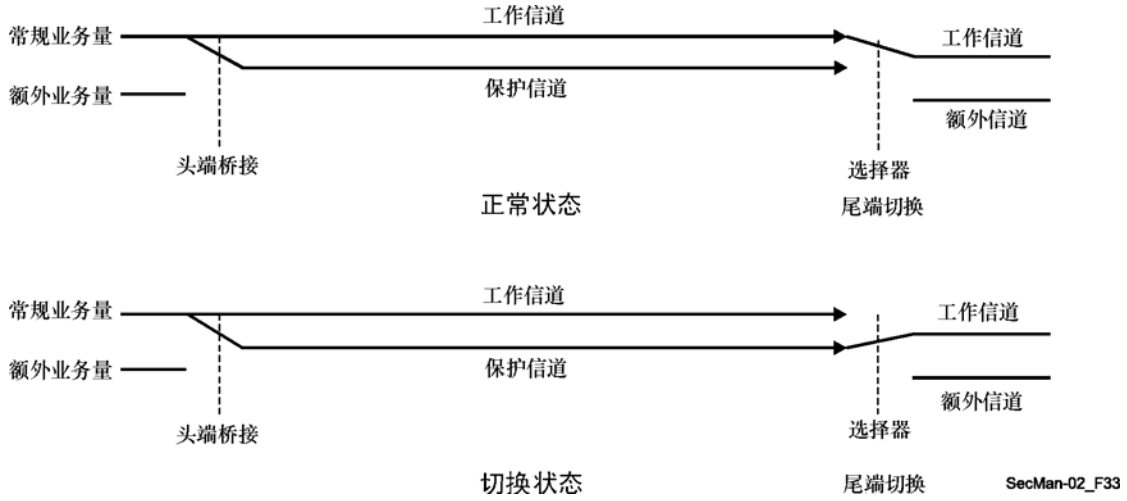


图 7-7－复用段1+1线路保护

发送的信号固定桥接到保护线路。接收机挑选好一些的信号。

在 1+1 保护方案中，不存在“额外业务量”能力。这是由线路保护功能完成的。因此这只对 STM-N 起作用，而不管线路速率如何。该方案可看做 1:1 保护切换的子集。该方案不要求控制机制（复用段开销（MSOH）的自动保护切换字节 K1 和 K2）即可工作。它根据与第 7.3.1 节相同的故障条件进行切换。

这种保护机制有一种版本称做双向 1+1，两端的选择器都切换。这种版本要求通过发送 K1/K2 字节进行控制。

7.3.3 MS-SPRing保护切换

图 7-8 示出了网络示意图。

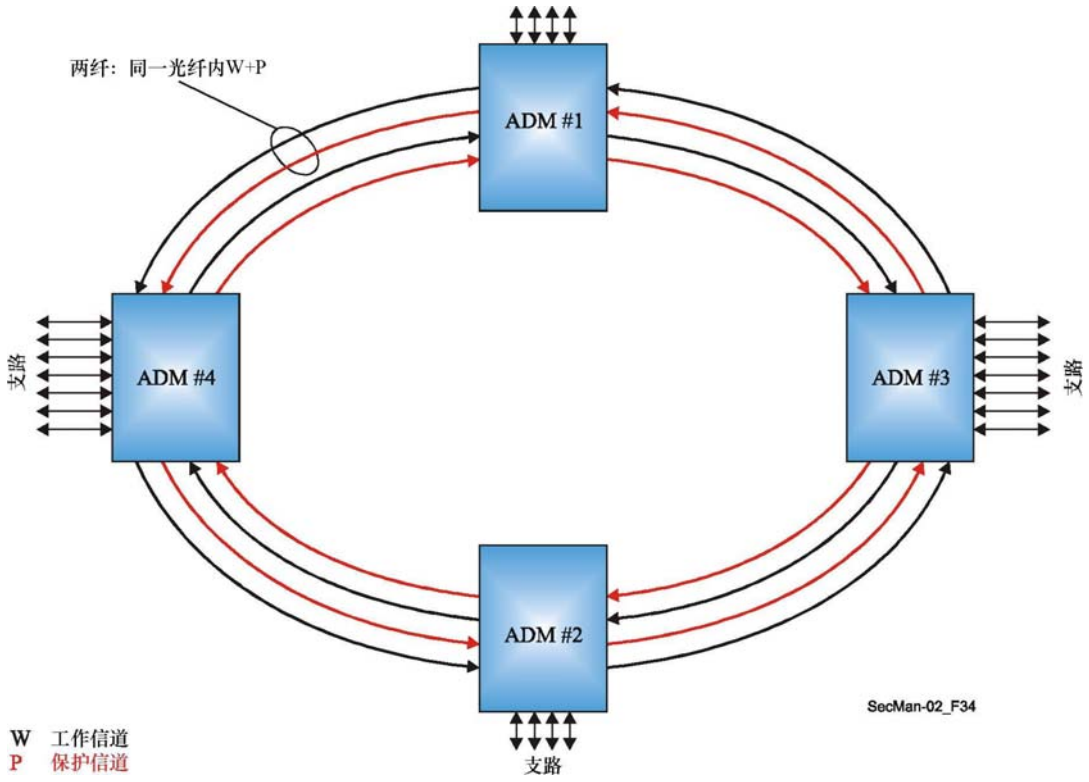


图 7-8－MS-SPRing保护切换网络示意图

两纤 MS-SPRing 结构在 SDH 网中占主导地位。环的每一跳都有两根光纤，每根载送工作信道和保护信道的一半带宽（如在采用管理单元（AU）的 STM-64 线路中，1 至 32 的 AU-4 用于工作，而 33 至 64 的 AU-4 用于保护）。一根光纤上工作信道的正常业务量受相反方向的保护信道的保护。

图 7-9 示出了两纤 MS-SPRing 的功能。

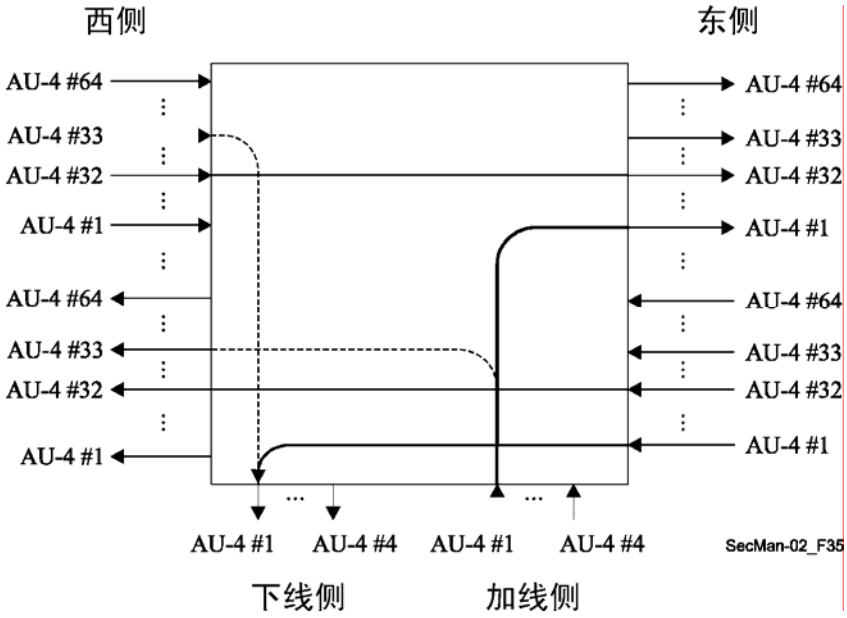


图 7-9－采用STM-4加线—下线的STM-64环

在图 7-9 中，成分信号“加线 AU-4 #4”转达到“东侧 AU-4 #1 发送”。该信号从“东侧 AU-4 #1 接收”下线到“下线 AU-4 #1”。图 7-9 也示出了 AU-4 #32 上的直通连接。

如果东侧光纤发生断裂，则“加线 AU-4 #1”必须从西侧保护（“西侧 AU-4 #32 发送”）发送出去，而接收信号则从西侧保护（“西侧 AU-4 #33 接收”）下线到“下线 AU-4 #1”。西侧的 AU-4 #32 必须环回到 AU-4 #64。西侧的 AU-4 #32 应该已经环回到断裂另一侧的保护信道（AU-4 #64），所以在该节点，保护（“西侧 AU-4 #64 接收”）必须环回到工作信道（AU-4 #32）。

以 AU-4 或 AU-3 的颗粒度对光纤上的所有信号完成保护切换。利用复用段开销（MSOH）的自动保护切换字节 K1 和 K2 发送要求和确认信息。K1 和 K2 在载送保护信道的线路上发送。这些字节在两个方向（东和西）上发送，一个方向是长通路，另一个方向是短通路。

在节点隔离或节点业务量加线/下线（同一时隙不同跨段的业务）失效的情况下为了防止把业务量送到错误的客户端，需要进行静噪。关于静噪的说明，请查阅附录二/G.841。

信号失效和信号降质故障的情况与线路保护切换相同（见第 7.3.1 节）。

要考虑的切换配置有四种：

- 正常（无故障）
- 东侧故障（必须在西侧环回且只能从西侧加线/下线）
- 西侧故障（必须在东侧环回且只能从东侧加线/下线）
- 四纤 MS-SPRing 跨段切换（切换至保护，无环回）

7.3.4 SNCP保护切换

图 7-10 示出了网络示意图。

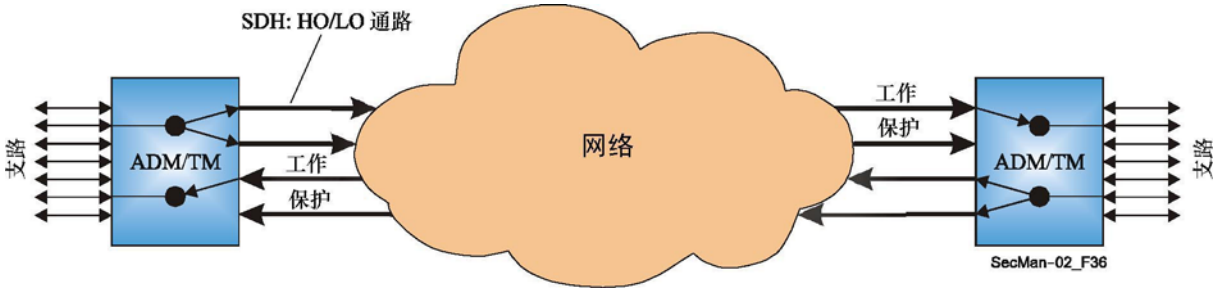


图 7-10－SNCP保护切换

SNCP 以通路为基础。因此一次只能切换一个信号（AU-3、AU-4 等）。也可以把它看做单独通路的单向 1+1。保护切换是在通路层次进行的：

- SDH：高阶虚拟容器 HO — VC-4/3，
  低阶分支单元 LO — TU-3/2/11/12

未采用协议（强制切换除外）。工作备份与保护备份之间的切换决定取决于本地条件，这两个备份都要监测。

- 保护切换时间要求是不到 50 ms。因此对于一条具有特宽带宽，如 10 Gbit/s 或 40 Gbit/s 的光纤，在光纤切断且所有通路都受到 SNCP 保护的情况下，如果完成保护切换的软件在状态机中的处理和控制台与中心控制器之间的信息传输有缺陷的话，该目标时间一般无法满足。

7.4 恢复

ITU-T G.805 建议书对传送网可用性增强技术做了说明。用术语“保护”（用预先分配的备用资源替代失效的资源）和“恢复”（利用备用容量通过重选路由替代失效的资源）对这些技术进行分类。总的来说，保护动作在几十毫秒的范围内完成，而恢复动作通常在几百毫秒至几秒的时间范围内完成。

ASON（自动切换光网络）控制平面为网络运营商提供了一种能力，向用户提供可选择服务类别（CoS）（如可用性、中断时长、差错秒等）的呼叫。保护和恢复是（网络所用的）支持用户所要求的 CoS 的机制。对于支持某一呼叫的特定连接而言，生存能力机制（保护、恢复或没有任何措施）的挑选取决于：网络运营商的政策、网络的拓扑结构和所用设备的能力。在为完成一个呼叫而串接的各连接上，可采用不同的生存能力机制。如果一个呼叫经过的网络具有一个以上运营商，则每一网络都应为经转连接的生存能力负责。UNI 或 E-NNI 处的连接请求将只含有请求的 CoS，且不属显式保护或恢复类型。

一个连接的保护或恢复可由管理平面的一个命令来调用或临时停用。这些命令可用于完成预定的维护活动。命令也可在某些异常失效条件下用于取代自动操作。

见 ITU-T G.8080/Y.1304 建议书。

7.5 外部设备

电信系统的安全问题涉及许多方面。与外部设备的物理安全有关的问题也在 ITU-T 的考虑之内。让硬件能从火灾、自然灾害和人员故意或偶然的侵入威胁中复原的问题也在讨论之列。涉及的两个最重要的安全问题包括让系统、线缆、外壳、机箱等各部件具备实际抵御损害的能力，还包括对系统实施监测，以在可能的情况下防止任何损害，或以最快的方式对出现的问题做出反应并恢复系统的功能性。

总的来说，这些安全问题要考虑的最重要的因素如下：

- 数据损害/损失的原因：
  - — 网络维护；
  - — 事故或灾难（无意的）；
  - — 恣意破坏（故意的；随机的）；
  - — 不合格人员的访问（如市民、其他运营商的技术人员）；
  - — 犯罪行为（如损害终端或搭线盗用；盗窃线缆；非法搭线窃听）；
  - — 故意行为；集中的武力或暴力。
- 设备的环境状况：
  - — 室内地点（中心局，客户住所）；
  - — 户外架空（遭受人为/自然行为的损害）；
  - — 户外街道上（有可能因施工而受到损害）；
  - — 户外地下（地下导管或导向装置）。

总的来说，关于物理层，推荐采取下列预防措施。这些措施中的大多数由运营商各自根据当地做法和规则加以管理：

- 避免采用街面上的节点（机箱、托架、暗线箱）：由于容易受到事故、恣意破坏、暴力行为、火灾和公众的好奇心的影响，采用地下节点与线缆更为安全；
- 钢制机箱（或其他类似于钢的箱体）应具备“防改动”结构；
- 所有机壳都应具有加锁或密封措施，避免外人接触；
- 设备线缆用管道铺设比直埋更为安全：如挖掘作业产生的意外损害；
- 终端点或分界点在网络与客户侧之间应具备（可锁定的）分割装置；或在不同运营商的电路之间具备此类装置；
- 室内客户终端比户外（墙面固定）客户终端更为安全（如出现盗窃情况时）；
- 可以建议在网络的固定地点存放线缆的备用部分，以易于修复意外损害（架空与地下两种情况）；

- 对于光纤设备，建议采取一定程度的电路分离和动态光稳定度，以避免在网络维护期间损失数据/扰动服务；
- 对于关键线路，建议采用实际分离的线缆和网络完成备份（备用线路）（如用于银行、医院的环形结构）。

可采取的其他措施包括：

- 制定户外设施的安全保障程序；
- 建立火灾探测系统，监视和控制户外装置；
- 在有不止一个运营商提供多种服务的网络相同部分，如 POTS、ISDN、xDSL 等，确定在不产生有害相互影响的情况下安全共存的评估准则；
- 采用可简便实现分类计价的技术方案，与此同时在全世界普遍采用的网络拓扑结构内维持完整性、可靠性和互操作性；
- 沿地下线缆安装信令装置；
- 为外部设备提供监测、维护支持和测试系统；
- 探讨对传输媒质 — 光纤 — 的物理完整性起主要保护作用的线缆的设计；
- 探讨各方面问题：线缆结构，光纤分割，集线器与机壳，分路装置，调研与路由规划，海缆船的特性，装载与铺设活动，修理方法，登陆海缆的保护与测试方法。

8 用于电信组织的事故管理机构和安全事故处理（指导原则）

对安全的管理和认识包括若干过程。规定处理和散播与安全有关的事故信息的结构和程序也在其中。这也是 ITU-T 专家应对一项紧急需求并制定 ITU-T E.409 建议书所涵盖的一个范畴。ITU-T E.409 建议书《事故管理机构和安全事故处理：用于电信组织的指导原则》的目的，是分析、安排和推荐在与提供国际电信业务有关的电信组织内部建立事故管理机构的方法，重点是事故的流程和结构。流程和处理在确定某件事是否划分为事件、事故、安全事故或危机时十分有用。流程还涉及需要首先做出的关键决定。

该建议书给出了一个概貌和框架，对规划事故管理机构和安全事故处理提供了指导。

该建议书是通用性质的，未确定或讨论对具体网络的要求。

该建议书旨在促进关于电信网安全的国际发展，但如果这些要求也可用于国内信息通信网（ICN），则这种发展也可得到促进。

随着国际电信中计算机的使用越来越多，计算机犯罪也开始出现了。过去几年，计算机犯罪确实暴增，几次国际和国内调查都证实了这一点。在大多数国家，还没有关于计算机非法侵入或安全事故的准确数字，特别是与国际电信有关的数字。

电信组织或公司大多没有处理信息通信网（ICN）安全问题的专门机构（虽然可能有处理各类危机的一般性危机处理队伍）。发生 ICN 安全事故时采取专门处理的方式，也就是谁检测到 ICM 安全事故谁就负责尽力处理。某些组织可能会试图忽视或掩盖 ICN 安全事故，因为这些事故可能会影响到其生产、可用性和营业收入。

在检测到 ICN 安全事故时，检测到事故的人员往往不知道向谁报告。这就可能导致系统或网络管理人员为摆脱问题而采取一种规避措施或临时解决办法。他们没有获得授权、没有时间或专门知识去纠正系统，避免 ICN 安全事故再次出现。这也是最好由受过培训的部门或小组以及时正确的方式处理安全事故的主要理由。另外，许多问题可能涉及很多领域，如媒体关系、法定权利、法律实施、市场份额或财务。

在报告或处理一个事故时，采用不同的分类方法会引起误解。这也可能反过来导致 ICN 安全事故既未得到应有重视，也无法为制止、限制和防止事故再次发生而采取及时措施。由此对受影响的组织（受害者）可造成严重后果。

为了能够完成事故处理和事故报告，人们必须了解事故是如何检测、处理和解决的。通过确定事故的一般性结构，就有可能获得一个事故（如物理事故、行政或组织方面的事故以及逻辑事故）的结构与流程的全景图。一套统一的术语是对言辞达成共同理解的基础。

8.1 定义

“安全事故”一词可以规定为“有可能对组织的资产构成安全影响的违反安全的行为、安全威胁、安全弱点和安全失灵”。在 ITU-T E.409 建议书中，假定“事故”比“安全事故”严重程度低，而“信息安全事故”是“安全事故”的一个特定类型。

图 8-1 示出了事件金字塔。在底部我们可以找到“事件”，接下来是“事故”、“安全事故”，顶部是“危机”和“灾难”。一个事件越靠近顶部，程度就越严重。为了利用 ICN 领域内涉及安全事故的稳定的常见术语，建议采用下列定义：

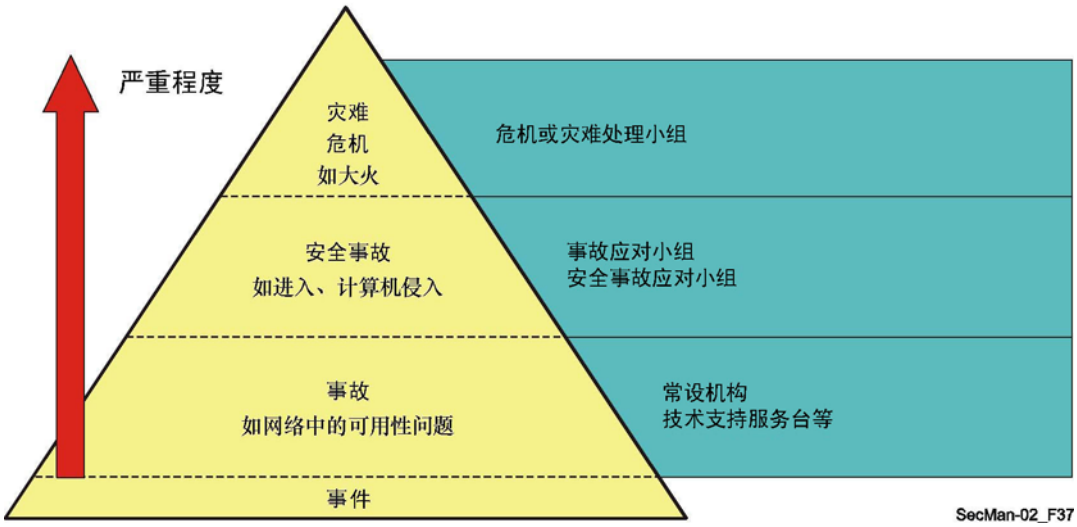


图 8-1－ITU-T E.409建议书中的事件金字塔

8.1.1 事件（Event）：一个事件是一次可观察到的现象，无法（完全）预知或控制。

8.1.2 事故（Incident）：一个事故是可能导致不太严重的一次现象或一种情况的事件。

8.1.3 安全事故（Security Incident）：一个安全事故是让安全的某一方面受到威胁的任何有害事件。

8.1.4 信息通信网（ICN）安全事故：涉及 ICN 安全的任何实际或疑似有害事件。这种事故包括：

- 通过网络侵入 ICN 计算机系统；
- 计算机病毒现象；
- 刺探能通过网络进入一定范围计算机系统的弱点；
- PABX 呼叫泄露；
- 由外部或内部未得到授权的行为引起的任何其他不希望出现的事件，包括拒绝服务攻击、灾害和其他紧急情况等。

8.1.5 危机（Crisis）：危机是由可引起严重消极后果的事件 — 或得知即将出现可引起严重消极后果的事件 — 引起的状态。在危机出现期间，最理想的情况下，人们可能有机会采取措施避免危机成为灾难。在出现灾难的情况下，人们通常会启用“工作延续计划”（BCP），由危机管理组处理事宜。

8.2 理由

兹建议，设立了（计算机安全）事故应对小组（CSIRT）的电信组织首先应采取的措施是宣布其所用的分类法，以避免误解。采用同样的“语言”，协作就会更容易。

兹建议，各组织采用术语“事故”和“ICN 安全事故”；根据后者的严重程度确定各自的进一步细分。本质上讲，ICN 安全事故指任何不希望出现的未得到授权的事件。这表明，根据一个组织的动机、经历和可用的专业资源，ICN 安全事故包括计算机侵入、拒绝服务攻击或病毒。在设立了有效的抗病毒小组的组织内，病毒可能不会被看做是 ICN 安全事故，而只是个事故。

这种进一步细分的例子或样板可以是：

— 事故
  - 违反了上网礼节（发垃圾邮件、滥用内容等）
  - 违反了安全政策
  - 个别病毒

— ICN 安全事故
  - 扫描和刺探
  - 计算机侵入
  - 计算机损毁或损害（可用性攻击，如轰炸、DoS 攻击）
  - 恶意软件（病毒、木马、蠕虫等）
  - 信息窃贼和间谍
  - 假冒

在术语方面采用同样的颗粒度和准确度，就有可能在以下几方面获得经验：

- 严重程度和范围方面的指导意见；
- 表明对敏捷程度的需求（如恢复所需的安全级别）；
- 提出可能的应对措施；
- 涉及的可能开销。

9 结论

长久以来，ITU-T 已制定了一系列关于安全的基础建议书：X.800 是关于开放系统互连安全体系结构的参考文件；X.810-X.816 系列规定了开放系统的安全框架，分别涉及概貌、认证、访问控制、不可抵赖、机密性、完整性和安全告警及审查告警。再近一些，制定了 ITU-T X.805 建议书，说明了提供端对端通信的系统的安全体系结构。X.805 体现的体系结构上的改动顾及了因多网络和多服务提供商环境的出现而导致的越来越多的威胁和弱点。关于公开密钥和属性证书框架的 ITU-T X.509 建议书无疑是安全应用方面被其他标准或直接或暗含引用最多的 ITU-T 文件，这些其他标准都是以 X.509 的原则为基础的。

除这些框架建议书外，ITU-T 还在其建议书规定的若干系统与服务方面制定了安全规定。在本手册中，第 6 节对其中一些做了说明：采用 H.323 的 IP 话音或 IPCablecom、安全的传真传输和网络管理。还给出了公开密钥与特权管理基础设施应用在电子医疗保健中运用的一个例子。使用者要注意，ITU-T 建议书中涉及的电信与信息技术的安全需求还包括许多其他方面。这些方面以及若干 ITU-T 研究组正在研究的欺诈预防和灾害恢复等问题，将在本手册未来的版本中进一步讨论。通过组织或参与关于安全的国际研讨会或讨论会，开发安全项目，指定 ITU-T 安全工作牵头研究组并与其他标准开发组织（如 ISO/IEC JTC 1/SC 27）协作，ITU-T 关于安全问题的工作得到了加强。

参考资料

除本手册中提到的 ITU-T 建议书（可在 http://www.itu.int/ITU-T/publications/recs.htm 见到）外，还采用了下列资料。

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

[Chadwick] CHADWICK (D.W.), "*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] EUCHNER (M.), PROBST (P.-A.), "*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] CHADWICK (D.W.), MUNDY (D.), "*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 Telecommunication Security" www.itu.int/ITU-T/studygroups/com17/tel-security.html (Catalogue of Approved Recommendations related to Telecommunication Security; Approved ITU-T Security Definitions)

[Shannon] SHANNON (G.), "*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] MANDIL (S.), DARBELLAY (J.), "*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

ISO/IEC 18033-1:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: General*

ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*

ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/IEC 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*

附 件 A

涉及安全的ITU-T建议书目录

由 ITU-T 第 17 研究组汇编，该研究组是有关电信安全的牵头研究组。

编　　号	名　　称	主要目的与安全问题	研　究　组
E.408	电信网的安全要求	概述了安全要求，提供了一个用于确定一般电信网络（固定的和移动的；话音的和数据的）安全威胁的框架，给出了对策规划指南，可用于减少因威胁而引起的风险。	SG2
E.409	事故处理机构和安全事件处理：用于电信组织的指导原则	分析、构造和提出了一种在（涉及提供国际电信业务的）电信组织内建立一个事故管理机构的方法，关注的主要是事故流程和结构。在确定某事件是该划入事件、事故、安全事故还是危机类别时，流程和处理是有用的。流程还包括需要首先做出的关键性决定。为了能够完成事故处理和事故报告，人们必须了解事故是如何检测、处理和解决的。通过确定事故的一般性结构，就有可能获得一个事故（如物理事故、行政或组织方面的事故以及逻辑事故）的结构与流程的全景图。一套统一的术语是对言辞达成共同理解的基础。	SG17
F.400	消息处理系统 和业务概述	概述了 MHS 总体系统和业务的定义，作为对 MHS 的全面介绍。这个概述是一套建议书中的一个，这套建议书用于描述消息处理系统（MHS）和业务的系统模型和业务要素。本建议书概述了 MHS 的能力，服务提供商用它来为用户提供公众消息处理（MH）业务，使用户能够按存储转发方式来交换信息。消息处理系统是根据 ITU-T 应用（X.200）的开放系统互连参考模型（OSI 参考模型）原理设计的，使用了表示层业务和其他更一般化的应用业务要素提供的服务。消息处理系统（MHS）可以使用 OSI 范畴内的任何网络来构建。由 MTS 提供的消息传输业务是独立于应用的。标准应用的例子有 IPM 业务（F.420＋X.420）、EDI 发信业务（F.435＋X.435）以及话音发信服务（F.440＋X.440）。终端系统可以将消息传送（MT）业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业务属于远程信息处理业务类别。建立在消息处理系统（MHS）基础之上的公共业务以及接入或由消息处理系统（MHS）获得公众业务的有关内容在 F.400 系列建议书中定义。有关消息处理系统（MHS）技术方面的内容在 X.400 系列建议书中定义。消息处理系统（MHS）总体系统体系结构在 ITU-T X.402 建议书中定义。业务要素是在应用过程中体现的服务特色。业务要素被认为是提供给用户的服务的重要组成部分，它是基本服务的要素，或是可选的用户设施，分为基本的可选用户设施或附加的可选用户设施两类。消息处理系统（MHS）的安全能力在 F.400 的第 15 节中描述，包括消息处理系统（MHS）的安全威胁、安全模式、描述安全特点的业务要素（在附件 B 中定义）、安全管理、消息处理系统（MHS）的安全附属物以及 IPM 的安全。	SG17

F.440	消息处理业务： 话音发信（VM）业务	规定了公众国际话音发信（VM-）业务的一般性问题、操作问题以及服务质量问题，话音发信（VM-）业务是一种特殊的消息处理（MH）业务，是主管部门提供的一项国际电信服务，使订户能够向一个或多个接收方发送消息，并采用存储转发和存储恢复相结合的技术，通过电信网络接收消息。VM 业务使订户能够在处理和交换话音编码消息过程中请求完成各种服务特性。有些特性是基本 VM 业务中所固有的。如果主管部门提供了其他非基本特性的话，那么可以由订户自己来选择，或者按逐条消息的方式进行选择，或者在商定的时间段内进行选择。采用人际发信（IPM）业务的双向通信作为一种可选业务也可以由 VM 业务提供。主管部门必须使基本特性在国际上可用。而订户可见的非基本特性则分为基本的特性和附加的特性。主管部门必须使基本的可选特性在国际上可用。附加的可选特性可以由某些主管部门提供，供国内使用，并根据双边协议在国际上可用。非基本特性称为可选的用户设施。VM 业务可以通过任何通信网络提供。VM 业务可以单独提供，也可以与各种远程信息处理业务或数据通信业务一起提供。VM 业务中使用的技术规范和协议在 X.400 系列建议书中定义。 附件 G：安全话音发信业务要素；附件 H：话音发信安全概述。	SG17
F.851	通用个人电信（UPT）－ 业务描述（业务集 1）	旨在提供通用个人通信（UPT）的业务描述和操作规定。本建议书从单个 UPT 订户或 UPT 用户的角度提供了总的业务描述。UPT 还允许 UPT 用户参与用户定义的一组预订业务，用户可以对之提出个人要求，以形成一个 UPT 业务概况。UPT 用户使用 UPT 业务所面临的、侵犯私密性的风险极小，也不会因其他用户的欺诈性使用行为而造成错误支出。原则上，通过通用个人通信（UPT）业务，可以利用任何基础电信业务。提供给 UPT 用户的业务仅受网络和所用终端的限制。在基本的用户特性中，首先是“UPT 用户身份认证”，而可选的用户特性有 UPT 服务提供商认证。详见第 4.4 节中的安全要求。	SG2
G.808.1	通用保护切换 － 线性路径和子网保护	概述了线性保护切换。它包括基于光传送网络（OTN）、同步数字系列（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予以说明。	SG15
G.827	端对端国际恒定比特率数字通路的可用性性能参数和目标	规定了有关通路要素和国际恒定比特率数字通路可用性的性能参数和目标。这些参数独立于物理网络的类型，它们支持端对端通路，如光纤、无线电接力或卫星。在用于提高可用性和计算网络单元相结合之端对端可用性的方法中包括了指南。	SG12
G.841	SDH 网络保护体系结构的类型和特性	描述了同步数字系列（SDH）网络的各种保护机制及其目标和应用。 保护方案分为 SDH 路径保护（在区域或通路层）和 SDH 子网连接保护（通过内部监控、非侵入式监控和子层监控）。	SG15

G.842	SDH 网络保护体系结构的相互作用	描述了网络保护体系结构之间的相互作用。相互作用为的是环网间交换业务流量的单节点和双节点之间的互联。每个环网可配置用于 MS 共享保护或 SNCP 保护。	SG15
G.873.1	光传送网络（OTN） — 线性保护	规定了 APS 协议和光信道数据单元（ODUk）级上光传送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 路径保护；以内部监测方式进行的 ODUk 子网连接保护；以非侵入监控方式进行的 ODUk 子网连接保护；以及以子层监测方式进行的 ODUk 子网连接保护。	SG15
G.911	光纤系统可靠性和可用性的参数和计算方法	确定了描述光纤系统的可靠性和可用性所需的最小参数集。为系统的可靠性和维护、有源光设备的可靠性、无源光设备的可靠性以及光纤和光缆的可靠性提供了不同的参数。本建议书还为计算设备、单元和系统的预期可靠性提供了指南和方法，包括例子。	SG15
H.233	视听业务的机密性系统	保密系统包括两部分，一是机密性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业务的保密系统的机密性部分。尽管这种加密系统需要一种加密算法，但此处对这样的算法未做规定：该系统适用于多个具体的算法。机密性系统适用于两个终端之间或一个终端与一个多点控制单元（MCU）之间的点对点链路；它可以扩展为多点工作方式，在这种方式下，MCU 上没有解密。	SG16
H.234	视听业务的加密密钥管理和认证系统	保密系统包括两部分，一是机密性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密钥管理方法。通过秘密密钥的使用来实现保密。密钥装载到保密系统的机密性部分，控制着所传数据的加密和解密方式。如果第三方得到了正在使用的密钥，那么保密系统将不再安全。因此，用户保管好密钥对任何保密系统而言都是十分重要的。本建议书规定了三种备选的密钥管理实用方法。	SG16
H.235	H 系列（H.323 和其他基于 H.245 的）多媒体终端的安全和加密	描述了在 H.3xx 系列建议书框架内所做的改进，纳入了安全业务，如认证和保密（数据加密）。建议的方案适用于任何使用 ITU-T H.245 控制协议的、简单的点对点和多点会议。例如，H.323 系统通过分组网络进行操作，不提供服务质量担保。出于同样的技术原因，基础网络不提供服务质量担保，不提供安全业务。通过非安全网络进行的安全实时通信通常涉及两个主要方面的问题 — 认证和保密。 本建议书描述了 H.3xx 系列多媒体终端将使用的安全基础设施和特殊的保密技术。本建议书将涵盖交互式会议方面的问题。这些领域包括在会议中交换的所有实时媒体流的认证和保密，但不限于此。它提供了 H.323 实体之间所需的协议和算法。 本建议书利用了 ITU-T H.245 所支持的通用设施，因此，与本控制协议一起使用的任何标准都可使用本安全框架。预计可能的话，其他 H 系列终端也可互操作和直接使用本建议书中所描述的各种方法。本建议书一开始将不在所有领域中彻底实施，而是专门突出端点认证和媒体保密。	SG16

		本建议书包括以一般方式协商业务和功能性的能力，使用的是选择性考虑的加密技术。所用的具体方式与系统能力、应用需求和特定的安全政策制约有关。它支持不同的加密算法，具有适用于不同目的的不同选项，如密钥长度。可以为特殊的安全业务分配某些密码算法（如为快速媒体流加密分配一种特定的密码算法，为信令加密分配另一种特定的密码算法）。 还应注意到，某些可用的密码算法或机制可能是为出口或其他国家问题（如有限的密钥长度）保留的。除了标出非标准或专用的密码算法，本建议书还支持标出熟知的算法。没有特别要求的算法；不过，强烈建议端点支持尽可能多的适用算法，以便实现互操作性。这类似于支持 ITU-T H.245 建议书的概念，它不确保两个实体的编解码器之间的互操作性。 第 2 版本的 ITU-T H.235 替代了第 1 版本的 H.235，做了若干改进，如椭圆曲线密码、安全简表（基于简单口令的和复杂的数字签字）、新的安全对策（媒体反滥发）、支持高级加密算法（AES）、支持后端服务、定义的对象标识符，以及依据 H.323 实施者指南进行的改变。 第 3 版本的 H.235 替代了第 2 版本的 H.235，增加了一个用于加密 DTMF 信号的程序、用于媒体有效载荷加密的 AES 加密算法对象标识符、用于媒体流加密的增强型 OFB（EOFB）流密码加密模式、用于平滑 NAT/防火墙穿越的附件 D 只有认证选项、有关 RAS 信道的密钥分发程序、更加安全的会话密钥传送以及更加牢靠的会话密钥分发与更新程序、确保负载流安全的程序、新的附件 I 对直接选路呼叫的更安全的支持、提供更加灵活的错误报告的信令方式、澄清和有效改善伴随更长的 Diffie-Hellman 参数的快速启动安全和 Diffie-Hellman 信令，以及依据 H.323 实施者指南进行的改变。 附件 F/H.235：《混合安全简表》。本附件描述了一个有效和可调节的、基于 *PKI* 的混合安全简表，它利用了附件 E/H.235 的数字签字和附件 D/H.235 的基线安全简表。建议把本附件作为一个可选方案。H.323 安全实体（终端、网守、网关、MCU 等）为了提高安全性或一旦需要时，可实施此混合安全简表。本文中“混合”一词指的是：来自附件 E/H.235 签字简表中的安全程序实际上用得较少；数字签字仍需遵循 RSA 程序。不过，数字签字技术只在绝对必要的情况下才使用，否则使用 H.235 附件 D 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”IP 电话。如果严格执行此安全简表的话，可以克服附件 D/H.235 简单、基线安全简表的各种局限。而且，如果严格执行此安全简表的话，还可以克服附件 E/H.235 的某些缺点，如处理过程中对更大宽带和更高性能的需求。例如，混合安全简表不依赖于对在不同域中各接力段相互共享秘密的（静态）管理。这样，用户可更容易地选择其各自的 VoIP 供应商。因此，本安全简表也支持某种用户移动性。它只在必要时应用带有签字和证书的非对称密码算法，否则使用更简单、更有效的对称技术。它为 H.245 消息完整性提供了 H.245 消息隧道，并且为消息的不可抵赖做出了一些规定。混合安全简表要求 GK 路由模型，并以 H.245 隧道技术为基础；对非 GK 路由模型的支持有待进一步研究。	

		附件 G/H.235：《在 H.235 中将 MIKEY 密钥管理协议用于安全实时传送协议（SRTP）》。可利用本附件部署 IETF 的安全实时传送协议（SRTP）的媒体安全，其中 MIKEY 密钥管理在有关的端点之间端对端地提供了必要的密钥和安全参数。可以在 H.235 附件 G 衍生的 H.323 系统之间的 H.323 域内部署附件 G。附件 G 为 H.225.0 RAS 和呼叫信令以及 H.245 并连同相应的规程定义了在安全上的协议扩展。。另外，附件 G 还给出了支持与 IETF SIP 实体互通的能力，这些实体是已经实施了 MIKEY 密钥管理和 SRTP 的实体。应注意的是，附件 G 是作为一个 H.235 安全简表起草的，可当做一种选择方案，补充其他的 H.235 媒体安全特性（见 H.235 的附件 B 和 D.7）。 注 — H.235 已经重新做了如下编排： • H.235.0，H.323 安全：H 系列（H.323 和其他基于 H.245 的）多媒体系统的安全框架 • H.235.1，H.323 安全：基线安全简表 • H.235.2，H.323 安全：签字安全简表 • H.235.3，H.323 安全：混合安全简表 • H.235.4，H.323 安全：直接选路和选择性选路呼叫的安全 • H.235.5，H.323 安全：使用弱共享秘密在 RAS 中的安全认证框架 • H.235.6，H.323 安全：具有本地 H.235/H.245 密钥管理的话音加密简表 • H.235.7，H.323 安全：在 H.235 中将 MIKEY 密钥管理协议用于安全实时传送协议（SRTP） • H.235.8，H.323 安全：使用安全信令信道的 SRTP 的密钥交换 • H.235.9，H.323 安全：H.323 的安全网关支持	
H.323	基于分组的多媒体通信系统	描述了通过分组网络（PBN）提供实时语音、视频、数据与/或多媒体通信服务的终端和其他实体，它可能不提供服务质量担保。对语音的支持是强制性的，而对数据和视频的支持是可选的，但如果支持的话，使用一种共同的操作模式则是强制性的，这样，所有支持这种媒体类型的终端就可以互通了。分组网络可以包括局域网、企业内部网、城域网、内部网络和相互联接的网络（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的网络，因此，各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 与/或无线网络中的终端实现互通，实体也可以综合到个人计算机中，或用一个独立的设备来实现，如可视电话。 附件 J：简单端点类型的安全	SG16
H.350.2	H.235 的号码簿业务体系结构	描述了代表 H.235 各要素的 LDAP 方案。它是与 H.350 相关的一个辅助类别，它的许多功能源自该体系结构。在执行本建议书之前，实施者应对 H.350 进行详细评估。其属性包括 H.235 身份、口令和证书要素。这些要素可以下载至端点上，用于自动配置，或通过网守进行访问，用于呼叫信令和认证。 本建议书的范围不包括有关 LDAP 号码簿自身或其所含数据使用的标准方法。本方案的目的不是在 H.235 协议中对所有可能的数据元素进行描述，而是描述为完成 H.350 中所列举之设计目标所需的最小集。	SG16

H.530	H.510 中 H.323 移动性的对称安全程序	提供了 H.323 移动性环境中的安全程序，如在用于描述 H.323 多媒体系统和业务移动性的 H.510 范围内。本建议书提供了有关 H.510 安全程序的细节。到目前为止，第 1 版本和第 2 版本中的 H.235 信令能力是为处理大多数静态 H.323 环境下的安全问题而设计的。这些环境和多媒体系统可以在网守区域内达到某种有限的移动性。举例来说，在一个移动的分布式环境中，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，对保证其漫游安全，一般而言，H.323 只能提供非常少的支持，具体地说，H.235 只能提供非常少的支持。在关于终端移动性的 H.510 中所述的 H.323 移动性情况构成了一种新的情况，也从安全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，移动用户希望获得有关被访域真实身份的证据。除此以外，获得有关终端身份的证据以最终完成用户认证也是非常有用的。因此，这就要求用户和被访域进行相互认证，同时作为可选项还要求终端的身份和被访域进行相互认证。由于移动用户是在其归属域预订服务并获得口令，因此通常只有归属域知晓他或她，而被访域一开始并不知晓该移动用户。因此，被访域不能与移动用户和移动终端共享任何已建立的安全关系。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，如授权检查或者密钥管理。这也要求确保被访域与归属域之间的通信和密钥管理安全。虽然原则上移动的 H.323 环境比封闭的 H.323 网络更加开放，但这当然也需要适当保证密钥管理的安全。同样，移动性域内的和跨移动性域的通信也需要保护，以防范恶意干扰。	SG16
J.93	关于有条件进入有线电视系统数字电视二次分配的要求	规定了保护在线缆前端与最终订户之间的有线电视网上所传输 MPEG 数字电视信号的数据保密和访问要求。其处理过程所需的确切的密码算法不在 J.93 范围之内，而是由各区域与/或业界自行确定。	SG9
J.96	确保遵循 ITU-T J.89 建议书之远程国际 MPEG-2 电视传输私密性的技术方法	包含一个遵循 MPEG-2 专业格式（4:2:2）的、有关数字电视远程国际传输有条件接入系统的公用标准。本建议书描述了基于使用称为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引入了一个附加的机制，并同时保留了互操作性。	SG9
J.112	交互式有线电视业务的传输系统	已在许多国家建立了数字电视业务，并已广泛认识到，应将数字电视带来的益处扩展至能够提供交互式业务。有线电视分配系统尤其适于实现双向数据业务，本建议书补充和扩展了 J.83 “用于有线分配电视、声音和数据业务的数字多节目系统”的范围，用于通过同轴电缆和光纤同轴混合缆提供交互式的双向数据业务。考虑到现有的不同媒体环境，本建议书还包含了若干附件。为引入快速国际互联网接入和/或交互式有线电视业务，建议使用这些系统，以便获得规模经济效益，并推动互操作性。提出了安全要求，建议使用经由电缆安全系统（DOCSS）的数据规范（SP-DOCSS）、 可移动安全模块规范（SP-RSM）和基线经由电缆的数据安全规范（SP-BDS）。	SG9

J.160	利用电缆调制解调器通过有线电视网络传输时间临界业务的体系结构框架	提出了体系结构框架，使有线电视运营商能够通过其网络提供时间临界业务，网络性能已得到增强，能够支持电缆调制解调器。通过 IPCablecom 核心业务层提供的安全服务有认证、访问控制、完整性、机密性和不可抵赖。IPCablecom 协议接口可以利用零个、一个或多个这些服务来满足其特殊的安全需求。通过以下方式，IPCablecom 安全服务解决每个组成协议接口的安全需求： • 确定每个组成协议接口特定的威胁模型； • 确定解决所确定威胁所需的安全服务（认证、授权、机密性、完整性和不可抵赖）； • 规定用于提供要求之安全服务的特殊安全机制。 安全机制包括安全协议（如 IPsec、RTP 层安全、SNMPv3 安全）和支撑性的密钥管理协议（如 IKE、PKINIT/Kerberos）二者。	SG9
J.170	IPCablecom 安全规范	规定了可为 IPCablecom 网络提供系统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。按照文中的规定，必须为每个网络单元接口提供认证、访问控制、消息和承载内容完整性、机密性和不可抵赖安全服务。	SG9
J.191	用于增强电缆调制解调器的 IP 特征包	提出了一系列基于 IP 的特性，它们可以加入到电缆调制解调器中，将使有线电视运营商能够为其客户提供额外的增强业务集，包括支持 IPCablecom 服务质量（QoS）、增强的安全、额外的管理和供应特性、改进的寻址和分组处理。这些基于 IP 的特性驻留在逻辑元素入口业务（PS 或只是入口）中。包含这些增强特性的电缆调制解调器是一个 IP 增强型电缆调制解调器（IPCM），是 J.190 HA 设备类别的一种实现方式。如 ITU-T J.190 建议书中所述，HA 设备类别包括电缆调制解调器功能性以及入口业务功能性。第 11 章 安全性：规定了在安全环境中向 PS 可靠传送基于电缆的 IP 业务所需的安全接口、协议和功能需求。任何安全技术的目的都是保护价值，不论是收益流，还是某种类型的可购买信息资产。当网络用户认识到收益流的价值，付出努力和金钱，发明一种技术来收回付出的费用时，就存在对该收益流的威胁。附件 C：安全威胁和防止措施。	SG9
M.3010	电信管理网的原则	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，描述了这三种体系结构之间的关系，给出了如何从 TMN 功能和信息体系结构获得 TMN 物理体系结构规范要求的框架。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）。为了获得互操作性，本建议书还定义了如何验证 TMN 的一致性和依从性。TMN 的要求涉及确保安全访问管理信息用户授权之管理信息的能力。TMN 包括若干功能模块，模块的安全功能性采用安全技术实现，用以保护 TMN 环境，目的是确保通过接口交换的信息以及驻留在管理应用程序中的信息的安全。安全原则和机制还与控制 TMN 用户对 TMN 应用程序相关信息的访问权有关。	SG4

M.3016	管理平面的安全	概述了识别电信管理网（TMN）所面临安全威胁的框架，并概括了如何在 ITU-T M.3010 建议书所描述的 TMN 功能体系结构范畴内应用现有的安全服务。本建议书是一个一般性建议书，并不确定或解决某个特定 TMN 接口的需求。 注 — ITU-T M.3016 建议书已经重新做了如下编排： • M.3016.0 — 管理平面的安全：概述 • M.3016.1 — 管理平面的安全：安全需求 • M.3016.2 — 管理平面的安全：安全服务 • M.3016.3 — 管理平面的安全：安全机制 • M.3016.4 — 管理平面的安全：简表书写格式	SG4
M.3210.1	IMT2000 安全管理的 TMN 管理业务	是电信管理网（TMN）管理业务系列建议书中的一个，描述了 IMT2000 网络管理业务、目标和管理方面的内容。本建议书描述了安全管理业务的一个子集，以提供对安全管理的需求和分析，并概述了在 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 接口上，以及二者之间为了检测和预防欺诈所需的管理业务，方法是运行欺诈信息收集系统（FIGS），监控一组规定的订户行为集，限制其因长期拖欠漫游期间产生的账单而形成的财务风险。通过定义新的功能集、功能和参数以及增加额外的语义和限制，在 ITU-T M.3400 建议书所确定的功能集基础上，形成本建议书。	SG4
M.3320	TMN X 接口的管理要求框架	是一系列建议书中的一部分，这些建议书涉及电信网络和业务管理中的信息传输，其中仅有部分内容是有关安全方面问题的。本建议书的目的是为各主管部门之间的电信管理网（TMN）信息交换的所有功能、业务和网络层面需求定义一个需求框架。本建议书还为利用电信管理网（TMN）X 接口在主管部门、经认可的运营机构、其他网络运营商、服务提供商、客户和其他实体之间进行信息交换提供了一个通用框架。本建议书含有 TMN X 接口的安全需求规范。	SG4
M.3400	TMN 管理功能	是电信管理网（TMN）系列建议书中的一个，提出了 TMN 管理功能和 TMN 管理功能集的规范。制定其内容是为了支持任务信息库 B（角色、资源和功能），它与 ITU-T M.3020 建议书中所述的 TMN 接口规范方法中的任务 2（描述了 TMN 管理范畴）有关。在分析 TMN 管理范畴时，应考虑最大限度地使用本建议中提到的 TMN 管理功能集。它包括对 TMN 所支持之安全管理功能的描述。	SG4
Q.293	请求引用安全措施的时间间隔	本建议书摘自蓝皮书，仅包括 Q.293 第 8.5 节（请求引用安全措施的时间间隔）至第 8.9 节（负荷分担法）。	SG4
Q.813	远程操作业务要素的安全转换应用业务要素 （STASE-ROSE）	提出了支持安全转换的规范，如加密、散列算法、封印和签字，重点在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、完整性和不可抵赖。本建议书描述了一种提供安全转换的方法，它在应用层实施，在任何基础的 OSI 堆层中无需任何安全特定的功能性。通过支持 ROSE PDU 的安全转换和相关安全信息的交换，本建议书增强了 TMN 的安全性。	SG4

Q.815	用于整体消息保护的安全模块规范	规定了一个配合 ITU-T Q.814 建议书《电子数据互换交互式代理规范》使用的可选安全模块，它为整个协议数据单元（PDU ）提供了安全服务。尤其是该安全模块支持发送方和接收方的不可抵赖服务，以及总的消息完整性。	SG4
Q.817	TMN PKI 一 数字证书和证书撤销列表概况	解释了如何将数字证书和证书撤销列表用于 TMN 中，并对证书和证书撤销列表扩展的使用提出了要求。本建议书旨在增强各 TMN 元素之间的互操作性，它们使用公开密钥基础设施（PKI）来支持安全相关的功能。本建议书的目的是在一个 TMN 内为分发和管理密钥提供可互操作、可调节的机制，跨越所有接口，并在 X 接口上支持不可抵赖服务。它适用于所有的 TMN 接口和应用。它独立于所用的通信协议栈或网络管理协议。PKI 设施可用于许多安全功能，例如认证、完整性、不可抵赖和密钥交换（M.3016）。不过，本建议书没有规定如何实现这些功能，用还是不用 PKI。	SG4
Q.1531	业务集 1 的 UPT 安全要求	为适用于 UPT 业务集 1 的用户到网络通信和网际通信规定了 UPT 安全要求，如 ITU-T F.851 建议书所定义的那样。本建议书涉及了所有有关使用 DTMF 接入和基于带外 DSS1 的用户接入之安全方面问题。	SG11
Q.1741.1	由 GSM 演进的采用 UTRAN 接入网的 UMTS 核心网 1999 年版的 IMT-2000 参考资料	包括以下涉及 3GPP 安全规范的内容：*TS 21.133*：安全威胁和要求；*TS 33.102*：安全体系结构；*TS 33.103*：安全综合指南；*TS 33.105*：加密算法要求；*TS 33.106*：法律许可的侦听要求；*TS 33.107*：法律许可的侦听体系结构和功能；*TS 33.120*：安全目标和原则。	SG19
Q.1741.2	由 GSM 演进的采用 UTRAN 接入网的 UMTS 核心网第 4 版的 IMT-2000 参考资料	包括以下涉及 3GPP 安全规范的内容：*TS 21.133*：安全威胁和要求；*TS 22.048*：（U）*SIM* 应用工具包的安全机制；*TS 22.101*：业务方面问题；业务原则 *TS 33.102*：安全体系结构；*TS 33.103*：安全综合指南；*TS 33.105*：加密算法要求；*TS 33.106*：法律许可的侦听要求；*TS 33.107*：法律许可的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 一 *MAP*；*TS 35.205. .206. .207* 和*.208*：对 *MILENAGE* 算法集的说明。	SG19
Q.1741.3	由 GSM 演进的 UMTS 核心网第 5 版的 IMT-2000 参考资料	包括以下涉及 3GPP 安全规范的内容：*TS 22.101*：业务方面问题；业务原则 *TS 33.102*：安全体系结构；*TS 33.106*：法律许可的侦听要求；*TS 33.107*：法律许可的侦听体系结构和功能；*TS 33.108*：法律许可的侦听（*LI*）的移交接口；*TS 33.200*：网络域安全 一 *MAP*；*TS 33.203*：基于 *IP* 业务的接入安全；*TS 33.210*：安全；网络域安全（*NDS*）；IP 网络层安全；*TS 35.205. .206. .207*、*.208* 和*.909*：对 *MILENAGE* 算法集的说明。	SG19
Q.1742.1	由 ANSI-41 演进的采用 cdma2000 接入网的核心网的 IMT-2000 参考资料	本建议书说明了标准开发组织（SDO）已公布的核心网标准与截至 2001 年 7 月 17 日批准的 3GPP2 规范之间的关系，适用于“由 ANSI-41 演进的采用 cdma2000 接入网的核心网”的 IMT-2000 系列成员。在 ITU-T Q.1742.1 建议书中将说明截至 2002 年 7 月批准的 3GPP2 规范与已公布的核心网标准之间的关系。ITU-R M.1457 建议书说明无线电接口和无线电接入网与 SDO 的适用于该 IMT-2000 系列成员的标准之间的关系。ITU-T Q.174x 系列建议书确定与其他 IMT-2000 系列成员的关系。本建议书综合了若干标准开发组织关于该 IMT-2000 系列成员的核心网的相关标准，成为一个全球性的建议书。	SG19

Q.1742.2	由 ANSI-41 演进的采用 cdma2000 接入网的核心网的（截至 2002 年 7 月 11 日批准的）IMT-2000 参考资料	本建议书说明了区域性标准开发组织（SDO）已公布的核心网标准与截至 2002 年 7 月 11 日批准的 3GPP2 规范之间的关系，适用于“由 ANSI-41 演进的采用 cdma2000 接入网的核心网”的 IMT-2000 系列成员。在 ITU-T Q.1742.1 建议书中说明了截至 2001 年 7 月 17 日批准的 3GPP2 规范与已由区域性标准开发组织公布的核心网标准之间的关系。在 ITU-T Q.1742.3 建议书中将说明截至 2003 年 7 月批准的 3GPP2 规范与已公布的核心网标准之间的关系。ITU-R M.1457 建议书说明无线电接口和无线电接入网与 SDO 的适用于该 IMT-2000 系列成员的标准之间的关系。ITU-T Q.174x 系列建议书确定与其他 IMT-2000 系列成员的关系。本建议书综合了若干标准开发组织关于该 IMT-2000 系列成员的核心网的区域性标准，成为一个全球性的建议书。	SG19
Q.1742.3	由 ANSI-41 演进的采用 cdma2000 接入网的核心网的（截至 2003 年 6 月 30 日批准的）IMT-2000 参考资料	Q.1742.3 引用的有关安全的技术规范。 *系统间规范*: N.S0003-0 用户身份模块（1.0 版；2001 年 4 月） N.S0005-0 蜂窝无线电通信系统间操作（1.0 版；无日期） N.S0009-0 IMSI（1.0 版；无日期） N.S0010-0 宽带扩展频谱系统的先进特性（1.0 版；无日期） N.S0011-0 OTASP 与 OTAPA（1.0 版；无日期） N.S0014-0 认证增强（1.0 版；无日期） N.S0018 TIA/EIA-41-D 预付费用（1.0.0 版；2000 年 7 月 14 日） N.S0028 GSM MAP 与 ANSI-41 MAP Rev. B 的网络互通 修订：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） *业务与系统方面的规范*: S.R0005-B cmda2000 扩展频谱系统参考模型 修订：B（1.0 版；2001 年 4 月 16 日） S.R0006 无线特性描述 修订：0（1.0.0 版；1999 年 12 月 13 日） S.R0009-0 用户身份模块（1.0 版；第 1 阶段）修订：0（1999 年 12 月 13 日） S.R0018 预付费用（（1.0.0 版；第 1 阶段）修订：0（1999 年 12 月 13 日） S.R0019 基于位置的服务系统（1.0.0 版；LBSS）第 1 阶段描述（2000 年 9 月 22 日） S.R0032 增强订户认证（1.0 版；ESA）和增强订户保密（ESP）（2000 年 12 月 6 日） S.R0037-0 cmda2000 扩展频谱系统的 IP 网络体系结构模型（2.0 版；2002 年 5 月 14 日） S.R0048 3G 移动设备标识符（1.0 版；MEID）（2001 年 5 月 10 日） S.S0053 公用加密算法（1.0 版；2002 年 1 月 21 日）	SG19

		S.S0054 公用加密算法的接口规范（1.0 版；2002 年 1 月 21 日） S.S0055 增强加密算法（1.0 版；2002 年 1 月 21 日） S.R0058 IP 多媒体域的系统需求（1.0 版；2003 年 4 月 17 日） S.R0059 遗留 MS 域 — 第一步系统需求（（1.0 版；2002 年 5 月 16 日） S.R0066-0 基于 IP 的位置服务第 1 阶段需求（1.0 版：2003 年 4 月 17 日） S.R0071 遗留系统包数据监视需求第 1 阶段需求（1.0 版；2002 年 4 月 18 日） S.R0072 全 IP 包数据监视需求第 1 阶段需求（1.0 版；2002 年 4 月 18 日） S.R0073 互联网空中手柄配置管理（1.0 版；IOTA）第 1 阶段（2002 年 7 月 11 日） S.S0078-0 公用安全算法（1.0 版；2002 年 12 月 12 日）	
T.30	普通交换电话网中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*基础之上规定了 G3 传真中的安全。	SG16
T.36	使用 3 类传真终端的安全能力	规定了两个独立的技术解决方案，它们可用于安全传真传输领域。这两个技术解决方案基于 HKM/HFX40 算法和 *RSA 算法*。	SG16
T.123 **附件 B**	扩展的传输连接	T.123 修订版的这个附件主要论述*连接协商协议（CNP）*，它提供了安全能力协商。所用的安全机制包括按点对点方式来保证网络和传输安全的各种不同方法，包括如 TLS/SSL、IPSEC w/o IKE 或人工*密钥管理*、X.274/ISO TLSP 和 GSS-API 等方法。	SG16
T.503	4 类传真文件交换的文件应用概况	规定了一个可用于任何远程信息处理业务的文件应用框架。其目的是规定一种适用于交换只包含光栅图形的 4 类传真文件的交换格式。文件以一种经格式化的格式进行交换，它使接收方能够按发送方的意图显示或打印传真文件。	SG16
T.563	4 类传真设备的终端特性	规定了 4 类传真设备的一般性问题以及与物理网络的接口。	SG16
T.611	3 类传真、4 类传真、电传、电报、电子邮件和文件传输业务的编程通信接口（PCI）APPLI/COM	规定了一个称为“APPLI/COM”的编程通信接口，它提供了对不同通信业务的统一接入，如 3 类用户传真或其他远程信息处理业务。本建议书描述了结构、消息内容以及本地应用（LA）与通信应用（CA）之间的交换方式。任何通信开始之前都有一个注册过程，并都用注销过程予以结束，这两个过程有助于实现对多用户系统尤其重要的安全方案，并提供在 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），它为应用设计者提供了强大的、对通信活动的控制和监控功能。	SG16

X.217	信息技术 — 开放系统互连 — 联合控制业务元素的业务定义	为开放系统互连环境中的应用联合控制规定了联合控制业务元素（ACSE）业务。ACSE 支持通信的面向连接模式和无连接模式。在 ACSE 中定义了三个功能单元。强制性的核心功能单元用于建立和释放应用关联。ACSE 包括两个可选功能单元，一个是可选的认证功能单元，它在联合建立期间为交换信息提供了额外的功能，以支持认证，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 给出了支持无连接模式的认证机制。	SG17
X.227	信息技术 — 开放系统互连 — 联合控制业务元素的面向连接的协议：协议规范	本协议规范规定了适用于系统间通信例子的程序，它希望在开放系统互连环境中以面向连接的模式实现互联，即针对应用联合控制、联合控制服务元素（ACSE）中应用业务元素的一个面向连接模式的协议。本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交换信息提供了额外的功能，以支持认证，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为应用内容的选择提供了额外的功能。本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）。本协议规范包括一个描述简单认证机制的附件，它使用一个带 AE 标题的口令，用于一般目的，还包括一个认证机制规范的例子。给这个认证机制指定了以下（ASN.1 数据类型对象标识符）名称： {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。认证值的数据类型应为“图形字符串（GraphicString）”。	SG17
X.237	信息技术 — 开放系统互连 — 联合控制业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-DATA APDU 中的认证参数传输，它还增加了无连接的 ACSE 协议规范。	SG17
X.257	信息技术 — 开放系统互连 — 联合控制业务元素的无连接协议：协议实现一致性声明（PICS）形式	为在 ITU-T X.237 建议书中规定的联合控制业务元素（ACSE）的 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 协议的强制性元素和可选元素。PICS 形式用于指明某个特定的无连接 ACSE 协议实现方案的特性和选择。	SG17

X.272	帧中继网络上的数据压缩和加密	规定了帧中继网络的数据压缩业务和加密业务，包括数据压缩的协商和封装、安全数据压缩、经由帧中继的认证和加密。网络中的数据压缩业务将增加网络的有效吞吐量。在公众网络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，必须在数据加密前对之进行压缩。因此，为了更好地协商数据加密协议，需要在数据压缩业务中提供设施。由于压缩和之后的数据加密任务计算量巨大，因此需要通过同步数据压缩和加密（安全数据加密）来获得效率。数据压缩协议基于 PPP 链路控制协议（IETF RFC 1661）和 PPP 加密控制协议（IETF RFC 1968 和 1969）。本建议书适用于利用 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）。	SG17
X.273	信息技术 — 开放系统互连 — 网络层安全协议	规定了支持完整性、机密性、认证和访问控制业务的协议，它们在 OSI 安全模型中确定，适用于连接模式和无连接模式的各网络层协议。通过使用诸如加密密钥等加密机制、安全标签和指定的安全属性，该协议为这些业务提供支持。	SG17
X.274	信息技术 — 系统间电信与信息交换 — 传输层安全协议	规定了在 OSI 安全模型传送层中能够支持完整性、机密性、认证和访问控制服务的协议。通过使用诸如加密密钥等加密机制、安全标签和指定的安全属性，该协议为这些业务提供支持。	SG17
X.400/ F.400	消息处理系统和业务概述	规定了消息处理系统（MHS）业务元素，用于有关机密性、完整性、认证、不可抵赖和访问控制的用户代理（UA）到 UA、消息传输代理（MTA ）到 MTA 、UA 到 MTA 、UA 到消息存储（MS）安全业务，与应用层相关。（见 F.400）	SG17
X.402	信息技术 — 消息处理系统（MHS）：总体结构	本建议书规定了在 MHS 协议中所用的安全程序和对象标识符，用于有关机密性、完整性、认证、不可抵赖和访问控制的各业务，与应用层相关。	SG17
X.411	信息技术 — 消息处理系统（MHS） — 消息传输系统：抽象业务定义和程序	规定了支持机密性、完整性、认证和不可抵赖业务的机制和程序，它们与应用层相关。通过使用 ITU-T X.509 建议书所确定的加密机制、安全标签和数字签字，该协议为这些业务提供支持。虽然本建议书规定了使用非对称加密技术的协议，但也支持对称加密技术。	SG17

X.413	信息技术 — 消息处理系统（MHS）：消息存储：抽象业务定义	规定了支持完整性、访问控制、认证和不可抵赖业务的机制、协议和程序，它们与应用层相关。该协议支持代表消息存储直接用户的这些业务。	SG17
X.419	信息技术 — 消息处理系统（MHS）：协议规范	通过提供与应用层相关的认证和访问控制业务，本建议书为 MHS 实体和远程用户确定安全访问规定了程序和应用内容。	SG17
X.420	信息技术 — 消息处理系统（MHS） — 人与人之间的发信系统	为个人间的消息用户或代表其直接用户的用户代理间的对象交换规定了机制、协议和程序，它们与应用层相关。支持的安全业务有完整性、机密性、认证和访问控制，与应用层相关。	SG17
X.435	信息技术 — 消息处理系统：电子数据交换发信系统	为代表其直接用户的电子数据交换（EDI）用户代理间的对象交换规定了机制、协议和程序。支持的安全业务有完整性、机密性、认证和访问控制，与应用层相关。	SG17
X.440	信息技术 — 消息处理系统：话音发信系统	为代表其直接用户的话音用户代理间的对象交换规定了机制、协议和程序。支持的安全业务有完整性、机密性、认证和访问控制，与应用层相关。	SG17
X.500	信息技术 — 开放系统互连 — 号码簿：概念、模型和业务概述	与其他建议书一起，用于推动信息处理系统之间的互联，以提供号码簿服务。一系列此类系统及其所持有的号码簿信息，可以看作是一个有机的整体，称为号码簿。号码簿持有的信息总的称为号码簿信息库（DIB），通常，它可用于推动对象之间的通信，如应用实体、人员、终端和分发列表。号码簿在开放系统互连中起着重要的作用，其目标是以各互联标准之外的最低技术协议实现信息处理系统之间的互联。本建议书引入了号码簿和 DIB 的概念，并构建了模型，概述了其所提供的业务和能力。其他各建议书利用这些模型来定义号码簿所提供的抽象业务，并规定通过本业务所能获得或传播的协议。本建议书规定了号码簿及其安全特性。	SG17
X.501	信息技术 — 开放系统互连 — 号码簿：模型	为号码簿提供了众多不同模型，作为 X.500 系列建议书中其他 ITU-T 建议书的框架。各模型是总体（功能）模型、管理权威机构模型、一般性号码簿信息模型，提供了号码簿用户和管理用户有关号码簿信息、一般性号码簿系统代理（DSA）、DSA 信息模型、运营框架和安全模型的观点。它规定了号码簿如何使用其 X.509 公开密钥和属性证书框架。	SG17

X.509	信息技术 — 开放系统互连 — 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（2000 版 — 第四版） 公开密钥和属性证书框架（2005 版 — 第五版）	为公开密钥证书和属性证书规定了一个框架，并为号码簿用向其用户提供认证服务规定规定了一个框架。它描述了两个级别的认证：简单认证，使用密码来验证身份是否满足要求；强认证，涉及利用加密技术生成的证书。简单认证提供一些防止非授权访问的有限保护，只有强认证才能被用作为提供安全服务的基础。定义的各框架可以用于为公开密钥基础设施（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数据对象规范，用于描述证书自身，以及对已发放的、但不再信任的证书的撤销通知。它定义了 PKI 的一些关键部件，但它并没有完整地定义一个 PKI。不过，它提供了建造完整的 PKI 及其规范的基础。属性证书的框架包括包括数据对象规范，用于描述证书自身，以及对已发放的、但不再信任的证书的撤销通知。它定义了 PMI 的一些关键部件，但它并没有完整地定义一个 PMI。不过，它提供了建造完整的 PMI 及其规范的基础。本建议书还定义了信息对象，用于持有号码簿中的 PKI 和 PMI 对象，并用于有效值和存储值的比较。	SG17
X.519	信息技术 — 开放系统互连 — 号码簿：协议规范	规定了程序和应用内容，以便在号码簿实体绑定期间确定安全访问。	SG17
X.680	信息技术 — 开放系统互连联网和系统方面问题 — 抽象句法记法一（ASN.1）：基本记法规范	提供了一种称为抽象句法记法一（ASN.1）的标准记法，用于定义信息数据的句法。它定义了众多简单数据类型，并规定了引用这些类型的记法以及规定这些类型值的记法。一旦需要定义信息的抽象句法，就可应用 ASN.1 记法，而无需以任何方式限制信息如何编码以便传输。ASN.1 用于定义数据类型、值以及数据类型的约束条件，即定义了众多简单类型及其标签，规定了引用这些类型的记法以及规定这些类型值的记法；定义了自更多基本类型构造新类型的机制，规定了定义这些类型并指定其标签以及规定这些类型值的记法；定义了 ASN.1 中所用的字符集（通过参考其他建议书）。数据类型（或简短的类型）指的是信息的一个类别（例如，数值型的、文本型的、静态图像或视频信息）。数据值（或简短的值）指的是数据类型的一个实例。本建议书定义了若干基本类型及其相应的值，以及将它们结合为更复杂类型和值的规则。在一些协议体系结构中，每个消息都说明为一个八位字节的二进制值。不过，标准编写者需要定义非常复杂的数据类型，以便承载其消息，而无需关注其二进制表示形式。为了说明这些数据类型，它们需要一种记法，它不必确定每个值的表示形式。ASN.1 就是这样一种记法。该记法通过规定一个或多个称为编码规则的算法进行补充，编码规则用于确定八位字节的值，八位字节用于承载应用语义（称为传送句法）。注：ASN.1 系列建议书（尤其是 ASN.1 独特的、规范的编码规则）已在许多安全相关的标准和建议书中得到广泛应用。尤其是 H.323 以及 X.400 和 X.500 系列，很大程度上依赖于 ASN.1。这些建议书已经成为并将继续成为安全相关工作的重要构件。	SG17

X.681	信息技术 — 开放系统互连联网和系统方面问题 — 抽象句法记法一（ASN.1）：信息对象规范	提供了 ANS.1 记法，它允许定义信息对象类别以及单个信息对象和信息对象集，并赋予参考名称，即提供了用于规定信息对象类别、信息对象、信息对象集的记法。一个信息对象类别定义了一个概念性表格（一个信息对象集）的形式，在信息对象类别中，每个列表示一个字段，每个完整的行定义一个信息对象。应用设计者经常需要设计一个协议，它将与信息对象某种类型众多实例中的某一个一起工作，其中的类别实例可以通过多个其他实体进行定义，并可随时间加入。此类信息对象类别的例子指的是远程操作业务（ROS）的“操作”和 OSI 号码簿的“属性”。本建议书提供了允许定义信息对象类别以及单个信息对象和信息对象集的记法，并赋予参考名称。见上面的“注”（X.680）。	SG17
X.682	信息技术 — 开放系统互连联网和系统方面问题 — 抽象句法记法一（ASN.1）：约束规范	是抽象句法记法一（ASN.1）的一部分，提供了用于规定用户定义的约束条件、表格约束条件和内容约束条件的记法。本建议书提供了有关一般性约束条件和异常说明的 ASN.1 记法，利用它可以对结构化数据类型的数据值做出限制。当约束条件出现冲突时，记法还提供了信令。应用设计者需要一种记法来定义结构化数据类型，以便承载其语义，还要求记法对可能出现的值做出进一步限制。此类约束条件的例子指的是限制某些部件的范围，或使用一个特定的信息对象集来限制一个“ObjectClassFieldType”部件，或使用“AtNotation”来规定部件之间的关系。见上面的“注”（X.680）。	SG17
X.683	信息技术 — 开放系统互连联网和系统方面问题 — 抽象句法记法一（ASN.1）：ASN.1 规范的参数化	是抽象句法记法一（ASN.1）的一部分，定义了用于参数化 ASN.1 说明的记法，即定义了用于参数化数据类型参考名称和参数化数据类型赋值的方法，在编写规范时，这对设计者是非常有用的，其中有些方面的问题在开发的某些阶段并没有定义，留待之后阶段填充，以便产生一个抽象句法的完整定义。应用设计者需要编写规范，其中的某些方面问题没有定义。这些方面将在之后由一个或多个其他研究组（每个研究组以其自己的方式）做出定义，以便产生一个完全定义的规范，用于定义一个抽象句法（每个研究组一个）。在某些情况下，甚至在抽象句法定义阶段，规范的某些方面问题（例如绑定）也可能没有做出定义，有待通过来自其他机构的国际标准化简表或功能简表说明来完成。见上面的“注”（X.680）。	SG17
X.690	信息技术 — ASN.1 编码规则：基本编码规则（BER）、规范编码规则（CER）和特异编码规则（DER）	规定了一组基本编码规则（BER），它可用于利用 ASN.1 记法定义的类型值，即用于获得类型值的传送句法说明，类型值利用 ITU-T X.680 系列建议书（指的是抽象句法记法一或 ASN.1）中所规定的记法进行定义。应用这些编码规则来产生一个有关此类值的传送句法。在这些编码规则的说明中暗示了它们还可用于解码，即这些基本的编码规则也可用于此类传送句法的解码，以便确定正在传送的数据值。本建议书还规定了一组规范和特异编码规则，限定了值只能编码为基本编码规则所提供的可选值中的一个，即它还定义了一组特异编码规则（DER）和一组规范编码规则（CER），两组编码规则都提供了对基本编码规则（BER）的约束条件。它们之间的主要区别在于：DER 使用确定长度的编码形式，而 CER 使用不确定长度的编码形式。DER 更适于小编码值，而 CER 更适于大编码值。在这些编码规则的说明中暗示了它们还可用于解码。见上面的“注”（X.680）。	SG17

X.691	信息技术 — ASN.1 编码规则：压缩编码规则（PER）	X.680 系列建议书描述了抽象句法记法一（ASN.1），这是一种用于定义在对等应用间所交换消息的记法。本建议书描述了一组编码规则，它可用于所有 ASN.1 类型的值，以便获得比基本编码规则及其衍生物（在 X.690 中描述）所能获得的、更加紧凑的表示形式，即它规定了一组分组编码规则，可用于获得一种有关 ITU-T X.680 建议书中所定义之类型值的传送句法。分组编码规则还可用于此种传送句法的解码，以便确定正在传送的数据值。有多组编码规则可用于 ASN.1 类型值。该编码规则之所以称为分组编码规则（PER），是因为它们获得了一种比基本编码规则及其衍生物（在 ITU-T X.690 建议书中描述）所能获得的、更加紧凑的表示形式。见上面的“注”（X.680）。	SG17
X.692	信息技术 — ASN.1 编码规则：编码控制记法（ECN）＋附件 E：对 Huffman 编码的支持	定义了编码控制记法（ECN），用于规定 ASN.1 类型或部分类型的编码，它们不同于标准编码规则所提供的那些编码，如基本编码规则（BER）和分组编码规则（PER）。它提供了若干有关此类规范的机制。它还提供了将编码规范连接至其所适用之类型定义的方法。ECN 可用于 ASN.1 规范所有类型的编码，但也能与标准编码规范一起使用，如 BER 或 PER，只用于规范具有特殊需求的类型的编码。一个 ASN.1 类型规定一组抽象值。编码规则将这些抽象值的表示形式规定为一系列比特。见上面的“注”（X.680）。	SG17
X.693	信息技术 — ASN.1 编码规则：XML 编码规则	抽象句法记法一（ASN.1）的颁布使之成为了普遍使用的记法，用于定义对等应用间所交换的消息。本建议书规定了可用于 ASN.1 类型值编码（利用扩展标记语言（XML））的编码规则，即规定了一组基本的 XML 编码规则（XER），可用于获得一种有关 X.680 系列建议书中所定义之类型值的传送句法。本建议书还规定了一组规范的 XML 编码规则，它提供了对基本 XML 编码规则的约束条件，产生有关任何给定 ASN.1 值的唯一编码。在这些编码规则的说明中暗示了它们还可用于解码。利用这些编码规则产生这些值的传送句法。在这些编码规则的说明中暗示了它们还可用于解码。有多组编码规则可用于 ASN.1 类型值。本建议书定义了两组编码规则，它们使用扩展标记语言（XML）。这些称为 ASN.1 的 XML 编码规则（XER），两组编码规则都能产生一个 W3C XML 1.0 兼容的 XML 文档。第一组称为基本的 XML 编码规则，第二组称为规范的 XML 编码规则，原因是只能用一种编码规则来对 ASN.1 值进行编码。（规范编码规则通常用于使用安全相关特性的应用，如数字签字。）	SG17
X.733	信息技术 — 开放系统互连 — 系统管理：警报功能	出于系统管理目的，规定了一个系统管理功能，它可以在集中或分散的管理环境中被应用程序使用，用于交互。本建议书定义了一个包括一般性定义、业务和功能单元的功能，它置于应用层中。该功能定义的告警通知提供了有关一个管理者可能需要遵照系统运行条件和服务质量进行行动的信息。	SG4
X.735	信息技术 — 开放系统互连 — 系统管理：日志控制功能	出于系统管理目的，规定了一个系统管理功能，它可以在集中或分散的管理环境中被应用程序使用，用于交互。本建议书定义了日志控制功能，并包括各业务和两个功能单元。该功能置于应用层中。	SG4

X.736	信息技术 — 开放系统互连 — 系统管理：安全警报功能	出于系统管理目的，规定了安全报警功能，它是一个系统管理功能，可以在集中或分散的管理环境中被应用程序使用，用于信息交换。本建议书置于应用层中。该系统管理功能定义的安全报警通知提供了与运行条件和服务质量相关的安全信息。	SG4
X.740	信息技术 — 开放系统互连 — 系统管理：安全审查索引功能	出于系统管理目的，规定了安全审查索引功能，它是一个系统管理功能，可以在集中或分散的管理环境中被应用程序使用，用于信息交换和指挥控制。该功能置于应用层中。	SG4
X.741	信息技术 — 开放系统互连 — 系统管理：访问控制的对象和属性	规定内阁了适用于为应用（使用 OSI 管理业务和协议）提供访问控制的规范。本建议书确定的访问控制信息可用于支持基于访问控制列表、能力、安全标签和内容限制条件的访问控制方案。	SG4
X.790	ITU-T 应用的故障管理功能	注意从服务供应商和业务用户角度出发，做好系统和通信网络的异常管理。异常，即“故障”，指的是一个问题，是网络用户感知的服务质量方面的负面影响。当检测到故障时，可能是报警的结果，故障报告可以由用户输入，或由系统自动生成。故障报告的管理是需要的，以确保它引起注意，并清除故障，使服务恢复至其原先性能水平。定义的报告格式应使用户能够报告故障，而后使供应商能够处理故障。在服务供应商处理故障期间，业务用户可以通过提交信息请求来确定处理工作的当前状况。当故障排除后，供应商可以告知用户。包括特殊的故障类型；不过，由一个特殊的应用来使用本建议书可能要求该应用特定的故障类型 — 以便满足处理要求。当出现故障时，网络可能正与另一个网络共同作用来提供一项服务，并且问题或异常可能源自另一个网络。因此，有必要通过接口在管理系统之间交换故障管理信息，接口可以是客户与服务供应商之间的接口，或服务供应商与服务供应商之间的接口，并可以代表辖区间和辖区内边界。除了交换已检测到的故障信息之外，也需要交换有关业务不可用的高级信息。因此，服务供应商可能需要告知客户有关今后业务不可用的信息（例如因计划中的维护）。范围包括所有上述管理信息交换过程。	SG4
X.800	CCITT 应用的开放系统互连安全体系结构	规定了与安全相关的总体体系结构元素，它们可适当地应用在要求在开放系统之间保护通信的环境中。为实现安全通信，并由此在 OSI 中提供一个统一的安全方法，在参考模型的框架内，建立了指导方针和约束条件，用于改进现有的建议书或制定新的建议书。为了覆盖作为通信协议总体体系结构元素的安全方面问题，本建议书扩展了参考模型，但并没有在参考模型中进行论述。本建议书概述了参考模型所提供的安全业务和相关机制，并在参考模中规定了可以应用这些业务和机制的位置。	SG17

X.802	信息技术 — 开放系统互连 — 低层安全模型	描述了 OSI 参考模型低层（传送层、网络层、数据链接层、物理层）安全服务修订版的跨层问题。它描述了这些层共有的体系结构概念、各层间安全有关的交互基础以及低层中安全协议的设置。	SG17
X.803	信息技术 — 开放系统互连 — 高层安全模型	描述了 OSI 参考模型高层（应用层、表示层和会话层）安全安全服务和机制的选择、设置和使用。	SG17
X.805	提供端对端通信之系统的安全体系结构	规定了安全相关的、总的体系结构元素，在适当应用时、尤其在多供应商环境中，可确保网络得到妥善的保护而免受恶意与疏忽攻击，并按规定的性能参数运行，如高可用性、适当的响应时间、完整性、可升级性、精确计费功能等。	SG17
X.810	信息技术 — 开放系统互连 — 开放系统的安全框架： 概述	规定了一个框架，其中规定了开放系统的安全业务。这部分安全框架描述了安全框架的组织结构，定义了安全框架多个部分要求的安全概念，描述了在框架其他部分中所确定的业务与机制之间的相互关系。该框架描述了适用于开放系统的有关认证的所有方面问题、认证与访问控制等其他安全功能之间的关系、认证的管理要求。	SG17
X.811	信息技术 — 开放系统互连 — 开放系统的安全框架：认证框架	为认证的提供规定了一个总体框架。认证的主要目的是抵御伪装和重播威胁。	SG17
X.812	信息技术 — 开放系统互连 — 开放系统的安全框架：访问控制框架	为访问控制的提供规定了一个总体框架。访问控制的主要目的是抵御计算机和通信系统的非授权操作威胁；这些威胁常被细分为以下类别：非授权使用、泄密、篡改、破坏和拒绝服务。	SG17
X.813	信息技术 — 开放系统互连 — 开放系统的安全框架：不可抵赖框架	为不可抵赖服务的提供规定了一个总体框架。不可抵赖服务的目标是收集、维护、提供，以及有关数据传输中发送方和接收方身份鉴别的不可抵赖证据的验证。	SG17

X.814	信息技术 — 开放系统互连 — 开放系统的安全框架：机密性框架	为机密性服务的提供规定了一个总体框架。机密性指的是不对未经授权个人、实体或程序提供或透露信息的属性。	SG17
X.815	信息技术 — 开放系统互连 — 开放系统的安全框架：完整性框架	为完整性服务的提供规定一个总体框架。完整性指的是数据没有以未经授权方式进行更改或破坏的属性。	SG17
X.816	信息技术 — 开放系统互连 — 开放系统的安全框架：安全审查和警报框架	为处理安全警报和为开放系统实施安全审查描述了一个基本模型。安全审查是一个独立的、对系统记录和活动进行评估和检查的过程。安全审查业务提供了一个审查权威机构，它能够规定、选择和管理在安全审查索引过程中需要记录的事件。	SG17
X.830	信息技术 — 开放系统互连 — 一般高层安全：概述、模型和记法	属于一个系列的建议书，它们提供了一套设施，辅助 OSI 高层协议的构建，支持安全服务的提供。本建议书定义了以下内容：a）安全交换协议功能和安全转换的通用模型；b）一套符号工具，为在抽象语法规范中规范可选的区域保护要求提供支持；c）一套资料性指南，它有关本系列建议书所覆盖的一般性高层安全设施的应用。	SG17
X.831	信息技术 — 开放系统互连 — 一般高层安全：安全交换业务元素（SESE）业务定义	属于一个系列的建议书，它们提供了一套设施，辅助 OSI 高层协议的构建，支持安全服务的提供。本建议书规定了由安全交换服务元素（SESE）提供的服务。SESE 是一个应用业务元素（ASE），它促进了安全信息的通信，支持 OSI 应用层中安全业务的提供。	SG17
X.832	信息技术 — 开放系统互连 — 一般高层安全：安全交换业务元素（SESE）协议规范	属于一个系列的建议书，它们提供了一套设施，辅助 OSI 高层协议的构建，支持安全服务的提供。本建议书规定了由安全交换业务元素（SESE）所规定的协议。SESE 是一个应用业务元素（ASE），它促进了安全信息的通信，支持 OSI 应用层中安全业务的提供。	SG17

X.833	信息技术 — 开放系统互连 — 一般高层安全：保护传输句法规范	属于一个系列的建议书，它们提供了一套设施，辅助 OSI 高层协议的构建，支持安全服务的提供。本建议书规定了保护传输句法，它与支持应用层中安全业务的表示层相关。	SG17
X.834	信息技术 — 开放系统互连 — 一般高层安全：安全交换业务元素（SESE）协议实现一致性声明（PICS）的形式	属于有关一般性高层安全（GULS）的一系列协议。它是 ITU-T X.832 建议书中所规定的安全交换业务元素协议和 ITU-T X.830 建议书中所描述的安全交换的协议实现一致性声明（PICS）形式。 附件 C 以一种支持对某个特定实现做出一致性评估的形式描述了标准化能力和选项。	SG17
X.835	信息技术 — 开放系统互连 — 一般高层安全：保护传输句法协议实现一致性声明（PICS）的形式	属于关于一般性高层安全（GULS）的一系列协议。它是 ITU-T X.833 建议书中所规定的保护传输句法协议的协议实现一致性声明（PICS）形式。本建议书以一种支持对某个特定实现做出一致性评估的形式描述了标准化能力和选项。	SG17
X.841	信息技术 — 安全技术 — 访问控制的安全信息对象	提供了安全标准中共同需要的对象定义，从而避免同一功能出现多个、不同的定义。用抽象句法记法一（ASN.1）对这些定义进行了精确描述。本建议书仅涵盖了安全信息对象（SIO）的静态方面问题。	SG17
X.842	信息技术 — 安全技术 — 使用和管理可信第三方业务的原则	为使用和管理可信的第三方（TTP）业务提供了指南，清晰规定了基本的职责和提供的服务及其描述和目的，规定了 TTP 的作用和责任以及使用其服务的实体。本建议书确定了 TTP 业务的主要不同种类，包括时戳、不可抵赖、密钥管理、证书管理和电子公证。	SG17
X.843	信息技术 — 安全技术 — 支持数字签字应用的 TTP 业务规范	规定了为生成不可抵赖的文件而需要支持数字签字应用的业务。由于这意味着文件的完整性和创建者的真实性，被描述的业务也可用于实现完整性和真实性业务。	SG17

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导致对开放分布式处理（ODP）标准化协调框架的需求。本参考模型提供了一个框架，它创建了一个支持分布、相互作用和有机移植的体系结构。本建议书概述了 ODP 范围、密钥概念的调整和解释、ODP 体系结构的框架。它包含有关其用户、标准编写者和 ODP 系统构建者如何解释和应用该参考模型的解释性材料。它还包含一个有关所需标准化领域的分类目录，依据 X.903 建议书中所确定的一致性参考点进行说明。ODP 系统必须确保安全，即必须以确保系统设施和数据免受未经授权访问、非法使用和任何其他威胁或攻击破坏的方式进行建设和维护。通过远程交互、系统和系统用户的移动性，很难满足安全要求。ODP 系统的安全规则可以定义：检测安全威胁、避免安全威胁、限制因任何安全漏洞而引起的任何破坏。	SG17
X.902	信息技术 — 开放分布式处理 — 参考模型：基础	包含了（任意的）分布式处理系统规范描述的概念和分析框架定义。它介绍了 ODP 标准的一致性原则和使用方法。这些细节仅足以建立新规范技术的要求。	SG17
X.903	信息技术 — 开放分布式处理 — 参考模型：体系结构	包含了对要求之特性所做的规范，其特点是开放的分布式处理。这些是 ODP 标准必须遵守的约束条件。它使用来自 ITU-T X.902 建议书的描述技术。	SG17
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	规范化了 ITU-T X.902 建议书第 8 节和第 9 节中所定义的 ODP 建模概念。从构建不同的标准化形式描述技术角度出发，通过对每个概念的解释，实现了规范化。	SG17
X.1051	信息安全管理系统 — 电信需求（ISMS-T）	对电信组织而言，信息与支撑过程、电信设施、网络与线路都是重要的经营资产。电信组织要恰当地管理其经营资产并正确、成功地延续其经营活动，信息安全管理绝对必要的。本建议书提出了对电信组织的信息安全管理需求。本建议书在电信的整体经营风险范畴内为在册信息安全管理系统（ISMS）的确定、实施、运作、监视、复审、维护和改进规定了要求。本建议书规定了实施专用于单独电信业务或一部分电信业务的安全控制的要求。	SG17

X.1081	远程生物统计多模式模型 — 一个用于规范远程生物统计安全保障方面问题的框架	规定了一个远程生物统计多模式模型，它为规范四个相互关联的安全问题提供了一个公共的框架：私密、认证、安全和保密。该远程生物统计多模式模型涵盖了安全保密多模式人机交互中的所有可能性，部分源自 ISO 31 和 IEC 60027-1 标准。在电信领域内，人的认知、感知和行为特征也是相关的，今后有可能被生物测定传感器或效应器用于认证目的。这些也被远程生物统计多模式模型所涵盖。对发生在多模式层中的相互作用进行了分类，在当中人体与电子、光学、化学或材料设备发生交互作用，获取生物测定参数，或对人体施加作用。对人进行认证，并保证其私密和安全，可依据设备与个人私密空间之间的相互作用进行规定，它构建和封装人与环境之间相互作用的模型，显性地、工程地对此类相互作用做出决定。本建议书包括对个人私密空间的说明、跨空间相互作用的特征分类、度量和说明（以定量的方式）此类相互作用的基础和衍生单元、相对相似性的度量层次结构。	SG17
X.1121	移动端对端数据通信的安全技术框架	描述了 OSI 参考模型高层中、移动网络中移动终端与开放网络中应用服务器之间的移动端对端数据通信的、移动端对端数据通信的安全威胁，以及对移动用户和应用服务提供商（ASP）的安全要求。另外，它描述了实现某种安全功能的安全技术应出现在移动端对端数据通信模型中的哪个地方。它提供了一个有关移动端对端数据通信的安全技术框架。	SG17
X.1122	基于 PKI 的安全移动系统实施指南	PKI 技术是一种安全技术，它应用于移动用户与应用服务供应商（ASP）之间、移动端对端数据通信一般模型中、移动终端与应用服务器之间的关系，或者移动用户与应用服务供应商（ASP）之间、网关模型中、移动终端与移动安全网关之间和移动安全网关与服务器之间的关系。虽然 PKI 技术是一种非常有用的、保护移动端对端数据通信的技术，但存在移动数据通信特定的特性，在构建安全移动系统（加密、数字签字、数据完整性等）时，需要对 PKI 技术进行调整。由于尚未建立构造和管理基于 PKI 技术的安全移动系统的方法，因此本建议书提供了一个构造基于 PKI 技术的安全移动系统的指南。	SG17

附 件 B

安全术语

下列 ITU-T 安全相关定义和缩写词摘自相关的 ITU-T 建议书。

ITU-T 在线 SANCHO（*Sector Abbreviations and defiNitions for a teleCommunications tHesaurus Oriented*）数据库提供 ITU-T 出版物中定义的英语、法语、西班牙语的“术语和定义”或“缩写词和首字母缩略语”。该资料是免费的在线资源，可在网页 www.itu.int/sancho 中找到。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，使用了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，可在以下网页中找到：http://www.itu.int/ITU-T/studygroups/com17/tel-security.html。

B.1 安全相关术语和定义清单

下列清单包含了最常用的安全术语，它们在当前的 ITU-T 建议书中定义。更完整的安全定义清单包含在由第 17 研究组负责维护的安全定义汇编中（见上文链接）。

术　　语	定　　义	参考文献
access control **访问控制**	1．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。 2．限制来自一个系统资源的信息流只流向授权的个人、程序、进程或网络上的其他系统资源。	X.800 J.170
access control list **访问控制列表**	实体列表及其访问权限，授予了访问资源的权限。	X.800
access control policy **访问控制政策**	定义访问条件的规则集。	X.812
access control service **访问控制业务**	访问控制业务提供了确保资源被主体以授权方式访问的方法。涉及的资源可以是物理系统、系统软件、应用和数据。可以在 TMN 的不同粒度层面上定义和实施访问控制业务：代理层面、对象层面或属性层面。访问限制含在访问控制信息中：方法用于确定哪些实体有权进行访问；允许进行什么类型的访问（读、写、修改、创建、删除）。	M.3016
accidental threats **偶然的威胁**	没有预先意图的威胁。实际的偶然威胁例子包括系统故障、操作出错和软件缺陷。	X.800
accountability **问责制**	确保能够唯一认定一个实体的动作确为该实体所为的性能。	X.800
active threat **主动威胁**	未经授权故意改变系统所含信息、或更改系统状态所带来的威胁。注 — 安全相关的主动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、拒绝服务、非授权用户对系统路由表进行的恶意更改。	X.800
adjudicator **仲裁者**	仲裁争议的实体，争议可能因拒绝接受的事件或行动而引起，也就是对证据进行评估，并确定是否发生了所争议的行动或事件。只有争议各方认可仲裁者的权威性，仲裁结果才能有效。	X.813
algorithm **算法**	一个数学过程，可用于扰乱和理清数据流。	J.93
asymmetric authentication method **非对称方法**	一种认证方法，在该方法中，两个实体并不共享所有的认证信息。	X.811
asymmetric cryptographic algorithm **非对称密码算法**	在加密或相应解密过程中对加密和解密使用不同密钥的一种算法。注 —在一些非对称密码算法中，密文解码或数字签字的生成需要使用不止一个专用密钥。	X.810
attack **攻击**	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安全机制或是使系统不正确地使用安全机制。	H.235

术　　语	定　　义	参考文献
attribute **属性**	消息处理范畴内的一个信息项、属性列表的一个组成部分，用于描述用户或分发列表，也可依据消息处理系统（或基础网络）的物理或组织结构对其进行定位。	X.400
attribute authority **属性机构**	1．通过发布属性证书指派特权的机构。 2．被一个或多个实体所信任的实体，它负责建立和签署属性证书。注 —CA 也可以是一个 AA。	X.509 X.842
attribute certificate **属性证书**	一种数据结构，由属性机构数字签字，通过证书拥有者的标识信息来绑定某些属性值。	X.509
attribute type **属性类型**	表明信息类别的一个标识符（如个人名称），是属性的一部分。	X.400
attribute value **属性值**	由属性类型表明的信息类别的一个特定实例（如一个特定的个人名称），是属性的一部分。	X.400
audit **审查**	参见“安全审查”。	X.800
audit trail **审查索引**	参见“安全审查索引”。	X.800
authenticated identity **经过认证的身份**	已通过认证保证的主体的独特标识符。	X.811
authentication **认证**	1．确认实体的过程。注 — 参见“主体”和“验证者”，以及两种不同形式的认证（数据源认证+实体认证）。认证可以是单边的，或者是双边的。单边认证只对一个主体提供身份保证。双边认证为两个主体提供身份保证。 2．向一个实体所声明的身份提供保证。 3．参见“数据源认证”和“同等实体认证”。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。 4．确认与关联建立有关的对象的身份。例如，可包括 AE、AP，以及应用的用户。注 — 定义该术语旨在表明目前的认证范围比 CCITT X.800 建议书中对等实体认证所覆盖的范围要宽。 5．验证一个实体向另一个实体所声明身份的程序。 6．旨在允许系统确认某方身份的过程。	X.811 X.811 X.800 X.217 J.170 J.93
authentication certificate **认证证书**	认证机构保证的安全证书，可用于保证实体的身份。	X.811
authentication exchange **认证交换**	1．通过信息交换方式来确保实体身份的一种机制。 2．出于认证目的的一次或多次交换认证信息传送序列。	X.800 X.811
authentication service **认证业务**	认证业务用于证明对象的身份确实是其所声明的身份。依据执行者类型和鉴定目的，可能需要以下类型的认证：用户认证、对等实体认证、数据源认证。用于实施认证业务的机制的例子包括口令和个人身份号码（PIN）（简单认证），以及基于密码的方法（强认证）。	M.3016.2
authentication token（token） **认证标记（标记）**	在一个强认证交换过程中所传送的信息，可以用来确认它的发送方。	X.509

术　语	定　义	参考文献
authenticity **真实性**	1．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。 2．确认要求的数据源能够满足接受方要求的性能。	J.170 T.411
authority **机构**	负责核发证书的实体。定义了两种类型：用于发布公开密钥证书的认证机构和用于发布属性证书的属性机构。	X.509
authority certificate **机构证书**	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。	X.509
authorization **授权**	1．授予权利，包括依据访问权利授予访问。注 — 该定义意味着能够执行某些行为的权利（如访问数据），它们授给某个进程、实体或代理人。 2．依据经认证的身份授予许可权。 3．使被允许访问者有权使用某个服务或设备的动作。	X.800 H.235 J.170
availability **可用性**	能够根据授权实体的要求进行访问和使用的性能。	X.800
cable security portal（CSP） **电缆安全入口**	一个功能要素，用于提供安全管理以及 HFC 与 Home 之间的转换功能。	J.191
call management server（CMS） **呼叫管理服务器**	IPCablecom。控制话音连接。在 MGCP/SGCP 术语中也称为呼叫代理。	J.191
capability **能力**	用作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。	X.800
certificate **证书**	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，与安全信息一同用于提供数据完整性和数据源认证服务（安全证书— X.810）。该术语指的是“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验证并签署的数值。	H.235
certificate policy **证书政策**	一套指定的规则，用于指明一个证书对于具有通用安全需求的某个特定团体与/或应用类别的适用性。例如，一个特定的证书政策可以指明在给定的价格范围内货物贸易中某种类型证书对电子数据交换交易认证的适用性。	X.509
Certificate Revocation List（CRL） **证书撤销列表**	1．表明一套证书不再被证书核发者认为有效的签字列表。除了通用术语 CRL 之外，还为 CRL 规定了一些涵盖特定领域的特殊 CRL 类型。 2．一个 CRL 包括已撤销各证书的序列号（例如，由于密钥已经受损或由于对象不再属于公司），其有效期尚未到期。	X.509 Q.817
Certification Authority（CA） **认证机构**	1．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，认证机构可以创建用户密钥。 2．可信的实体（在安全政策的范畴内），创建包含一个或多个安全相关数据类别的安全证书。	X.509 X.810
certification path **认证通路**	号码簿信息树中对象证书的一个有序序列，该序列与通路中初始对象的公开密钥一起经过处理可产生通路中最终对象的公开密钥。	X.509

术　　语	定　　义	参考文献
challenge **质询时间**	验证者产生的时间变量参数。	X.811
cipher **密码**	1．密码算法，一种数学变换。 2．在明文和密文间进行数据转换的算法。	H.235 J.170
ciphertext **密文**	经加密生成的数据。使最终数据的语义内容不可知晓。注 — 密文本身也可用作加密操作的输入，这样就可以生成超级加密的输出。	X.800
claimant **提出要求者**	出于认证目的，作为或代表一个主体的实体。提出要求者包括代表主体参与认证交换的所需功能。	X.811
cleartext **明文**	可理解的数据，其语义内容可以知晓。	X.800
compromised evidence **受损的证据**	某个时候满足要求、但对可信的第三方或仲裁者而言已不再保密的证据。	X.813
confidentiality **机密性**	防止信息提供或泄露给未经授权的个人、实体或过程的性能。	X.800
confidentiality service **机密性业务**	机密性业务提供了防止交换数据非授权透露的保护措施。有以下不同种类的机密性业务：选择性字段机密性、连接机密性、数据流机密性。	M.3016.2
content integrity **内容完整性**	1．使接受方能够验证消息的最初内容未经修改。 2．业务的该要素允许消息的发送方能够为消息的接受方提供一种手段，使接受方能利用该手段验证消息的内容未经修改。内容完整性基于逐个接收，可以使用非对称加密技术或对称加密技术。	X.400 X.400
counter-signature **连署**	添加于数据单元的数字签字，它已经过不同实体（如一个 TTP）的签署。	X.813
credentials **证明**	传送并用于建立实体所需身份的数据。	X.800
cryptanalysis **密码分析**	1．为了得到秘密变量与/或包括明文在内的敏感数据，对一个密码系统与/或它的输入和输出进行的分析。 2．在无权使用密钥的情况下恢复消息明文或加密密钥的过程。 3．在无权使用密钥（电子密码系统中的电子密钥）的情况下恢复消息明文的学科。	X.800 J.170 J.93
cryptographic algorithm **密码算法**	从一个或几个输入值计算结果的数学函数。	H.235
cryptographic chaining **密码链**	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以前的输入值或输出值。	X.810
cryptographic checkvalue **密码校验值**	对数据单元实施密码转换（参见“密码”）所生成的信息。注 — 校验值的生成可能通过一步或多步完成，它是密钥和数据单元的一个数学函数结果。通常用于检验数据单元的完整性。	X.800

术　　语	定　　义	参考文献
cryptographic system， cryptosystem 密码系统	1．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定义变换。 2．简单地说，密码系统是一个算法，它可将输入数据转换为某种不可识别的形式（加密），并可将不可识别的数据转换回其初始形式（解密）。RSA 加密技术在 X.509 中描述。	X.509 Q.815
cryptography 密码学	为隐藏信息内容、防止它受到未被发现的更改与/或防止非授权的使用而综合了数据转换原理、手段和方法的学科。注 － 密码学决定了加密和解密的使用方法。密码分析学是对密码学原理、手段和方法的攻击。	X.800
data confidentiality 数据机密性	该服务可用于保护数据不被非法泄露。认证框架支持数据机密性服务。该服务可用于防止数据被窃听。	X.509
data integrity 数据完整性	数据没有遭到以未经授权的方式改变或破坏的性能。	X.800
data origin authentication 数据源认证	1．确认所接收的数据源与所声称的相同。 2．确认主体的身份负责特定的数据单元。	X.800 X.811
decipherment 解密	相应的可逆加密的逆过程。	X.800
decryption 解密	参见“解密过程”。	X.800
delegation 授权	把特权从一个拥有特权的实体转让给另一个实体。	X.509
denial of service 拒绝服务	阻止经授权的资源访问或是延误紧急操作。	X.800
descrambling 理清	1．恢复图像/声音/数据信号的特性，以便以清晰的形式进行接收。该种恢复是一个特殊的过程，处于有条件访问系统（接收端）的控制之下。 2．扰乱功能的逆过程（参见“扰乱”），以获得可用的图像、声音和数据服务。	J.96 J.93
digital fingerprint 数字指纹	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拥有同样特性的数据项目。	X.810
digital signature 数字签字	1．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”），使数据接收方能够证明数据源和数据完整性，并防止伪造，例如接收方的伪造。 2．数据单元的一种密码转换，使数据接收方能够证明数据源和数据完整性，并防止数据的发送方和接受方免遭第三方伪造，以及防止发送方免遭接受方的伪造。	X.800 X.843
direct attack 直接攻击	基于安全机制基础算法、原理或特性中的缺陷而对系统进行的攻击。	X.814
directory service 号码簿业务	从良好定义的对象目录中搜索和查找信息的业务，它可以包含有关证书、电话号码、访问条件、地址等的信息。依据 X.500，号码簿业务提供了一个例子。	X.843

术　语	定　义	参考文献
double enveloping technique **双重封装技术**	对完整的消息可以提供额外的保护措施，包括封装参数，利用该功能可以规定消息内容自身是一个完整的消息，即双重封装技术是可用的，虽然使用内容类型变量使之可能规定消息的内容是一个内部封装。	X.402
eavesdropping **窃听**	通过监控通信来突破机密性。	M.3016.0
electronic key **电子密钥**	在用户解码器中用于控制理清过程的数据信号项。注 – 至少有三种类型的电子密钥：用于电视信号流的电子密钥、用于保护控制系统操作的电子密钥、用于在电缆系统中分发电子密钥的电子密钥。	J.93
encipherment **加密**	1．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，无法进行相应的解密操作。 2．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，通过它使密文转化为明文。	X.800 H.235
encryption **加密**	1．将明文信息转换为密文的一种方法。 2．将信号扰乱的过程，以免遭到未经授权的访问。（也见“加密”。）	J.170 J.93
end entity **端实体**	不以签署证书为目的而使用其专用密钥的证书主体，或是一个依赖方实体。	X.509
end-to-end encipherment **端对端加密**	数据在起始端系统加密，相应的解密只发生在目的端系统。（也见“逐条链路加密”。）	X.800
entity **实体**	1．一个人、一个组织、一个硬件部件或软件的一部分。 2．任何感兴趣的、具体的或抽象的事情。通常，实体可用于指代任何事情，在建模范畴中，它指的是被建模的事物。	X.842 X.902
entity authentication **实体认证**	确认主体的身份，在通信关系范畴内。注 – 主体经认证的身份只有当调用该业务时才能得到保证。通过 X.811 第 5.2.7 节中所述的方法可以确保认证的连续性。	X.811
event discriminator **事件鉴别器**	一个函数，提供对安全相关事件的初始分析，适当的话，产生一个安全审查与/或告警。	X.816
evidence **证据**	信息，其自身或当与其他信息一起使用时，可用于解决争议。注 – 证据的特定形式可以是数字签字、安全封装和安全标记。数字签字与公开密钥技术一起使用，安全封装和安全标记与秘密密钥技术一起使用。	X.813
evidence generator **证据产生器**	一个实体，它产生不可抵赖证据。注 – 该实体可以是不可抵赖业务的请求方、发起方、接收方或一起工作的多个参与方（如签署方或共同签署方）。	X.813
forgery **伪造**	一个实体，它伪造信息，并声称这些信息收自另一个实体或发往另一个实体。	M.3016.0
hash function **散列函数**	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。	X.810

术　　语	定　　义	参考文献
hide **隐藏**	一种操作，它为未受保护的数据提供机密性保护，或为已受保护的数据提供额外的机密性保护。	X.814
identity-based security policy **基于实体的安全政策**	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/对象的身份与/或属性为基础的安全政策。	X.800
indirect attack **间接攻击**	对系统的一种攻击，它不基于特定安全机制的缺陷（如绕过安全机制的攻击，或依赖于系统不正确使用安全机制的攻击）。	X.814
integrity **完整性**	1．数据没有以未经授权的方式加以改变的特性。（也见“数据完整性”。）	H.235
integrity service **完整性业务**	完整性业务提供了确保所交换数据正确性的手段，使之免遭修改、删除、创建（插入）和重播已交换数据。有以下不同种类的完整性业务：选择性字段完整性业务、不带恢复的连接完整性业务、带恢复的连接完整性业务。	M.3016.2
integrity-protected channel **完整性受保护的信道**	应用了完整性业务的通信信道。（参见“连接完整性”和“无连接完整性”。）	X.815
integrity-protected data **完整性受保护的数据**	完整性受保护的环境内数据和所有相关的属性。	X.815
integrity-protected environment **完整性受保护的环境**	可以防止未经授权的数据更改（包括创建和删除）或可以检测到未经授权的数据更改的环境。	X.815
intentional threats **故意的威胁**	指的是从利用可方便得到的监控工具所进行的不经意检查到利用专业系统知识所进行的刻意攻击的威胁。故意的威胁如果得以实现，那么可以认为是“攻击”。	X.800
intrusion resistance **入侵抵抗力**	硬件对象拒绝未经授权方对内部功能性实施物理、电子或辐射访问的能力。	J.93
IPCablecom	ITU-T 的一个项目，包括一个体系结构和一系列建议书，使得能够利用电缆调制解调器经由有线电视网络来提供实时服务。	J.160
Kerberos	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。	J.170
key **密钥**	1．控制加密/解密操作的符号序列。 2．作为被选密码算法输入值的数学值。	X.800 J.170
key distribution service **密钥分发业务**	将密钥安全分发给授权实体的业务，通过密钥分发中心进行，在 ISO/IEC 11770-1 中进行描述。	X.843
key exchange **密钥交换**	用于实体之间加密通信的实体之间公开密钥的交换。	J.170
key management **密钥管理**	依照某种安全政策，生成、存储、分发、删除、存档和应用密钥。	X.800

术　　语	定　　义	参考文献
leakage of information **信息泄露**	当通过监控传输、通过未经授权地访问储存于任何 MHS 实体中的信息或通过伪装（可以通过假冒和误用 MTS 或通过使 MTA 不正确操作）而使信息被未经授权方得到时，发生信息泄露。信息泄露威胁包括以下几方面：丢失机密性、丢失匿名性、盗用消息、业务流量分析。	X.402
link-by-link encipherment **逐条链路加密**	在通信系统的每条链路上单独应用的数据加密。（也见“端对端加密”。）注 — 逐条链路加密意味着数据在转发实体中以明文方式存在。	X.800
loss or corruption of information **信息丢失或毁坏**	所传送数据的完整性因未经授权的删除、插入、修改、重新排序、重播或延滞而受到损害。	M.3016.0
manipulation detection **处理检测**	用于检测数据单元是否被更改（偶然地或故意地）的机制。	X.800
masquerade **冒名顶替**	一个实体伪装成为另一个不同的实体。	X.800
message authentication code（MAC） **消息认证码**	用于提供数据源认证和数据完整性的密码校验值。	X.813
message origin authentication **消息源认证**	使得接受方或消息经其通过的任何 MTA 能够认证消息发送方的身份。	X.400
message sequence integrity **消息序列完整性**	1．允许发送方提供一份接收证明，以示消息序列已得到保护。 2．业务的该要素允许消息的发送方提供一份接收证明，通过这种方式，接收方可以确认从发送方发往接收方的消息序列已得到保护（消息没有丢失、没有重新排序或没有重播）。消息序列完整性的证明逐个接收方进行，可以使用非对称加密技术，或使用对称加密技术。	X.400
message sequencing **消息排序**	消息的部分或全部被重复、时移或重新排序，例如利用有效消息中的认证信息以及对有效消息进行重新排序或时移。虽然这不可能防止利用 MHS 安全业务进行的重播，但可以检测到并消除威胁的效果。消息排序包括：消息重播、消息重新排序、消息预播、消息延滞。	X.402
monitoring role **监控角色**	TTP 以此角色对行动或事件进行监控，并可信地提供有关所监控对象的证据。	X.813
mutual authentication **相互认证**	确认两个主体的身份。	X.811
non-repudiation **不可抵赖**	1．防止发送方事后否认其曾发送过信息或采取了某一行动的能力。 2．防止参与通信的若干实体中的一个否认参与过全部或部分通信。 3．一个过程，利用它，消息的发送方（如一个有关按次计费的请求）不可抵赖已经发送过消息。	J.170 H.235 J.93
notarization **公证**	向可信的第三方注册数据，允许之后确保其准确性，如内容、来源、时间和提交。	X.800

术　　语	定　　义	参考文献
notary **公证方**	向可信的第三方注册数据，以便之后确保所提供数据的准确性。	X.813
passive threat **被动威胁**	在不改变系统状态情况下出现的、未经授权的信息泄露威胁。	X.800
password **口令**	1．机密认证信息，通常由字符串组成。 2．指的是用户进入口令字符串，即指定的安全密钥，为移动用户和其基地域所共享。该用户口令和产生的用户共享秘密将用于用户认证之目的。	X.800 H.530
peer-entity authentication **对等实体认证**	1．确定关联中的一个对等实体与声明相符。 2．在通信关系期间，建立对等实体的身份证明。	X.800 M.3016.0
personal security environment（PSE） **个人安全环境**	实体专用密钥安全的本地储存、直接可信的 CA 密钥以及可能的其他数据。依据实体的安全政策或系统的要求，它可以是：例如，一个加密保护的文件或一个可以抵御篡改的硬件标志。	X.843
physical security **物理安全**	为防止资源受到故意或偶然威胁而使用的物理保护方法。	X.800
principal **主体**	1．一个实体，其身份可被认证。	X.811
privacy **保密**	1．个人控制或影响可以收集和存储的、与其相关的信息的权力，并且该个人可能泄露该信息或该信息可能泄露给该个人。 注 一 因为该术语与个人权力相关，所以它不可能非常精确，除非作为需要安全的动机，否则应避免使用它。 2．只有明确激活的各方才能解译的一种通信方式，通常通过加密和共享加密密钥来实现。	X.800 H.235
private key; secret key（deprecated) **专用密钥；** **秘密密钥（建议不用）**	1．（在公开密钥密码系统中）用户密钥对的密钥，只有该用户知晓之。 2．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）。 3．在公开密钥密码系统中使用的密钥，它属于某个单个实体，必须保密。	X.509 X.810 J.170
privilege **特权**	由某个机构指派给实体的属性或特性。	X.509
Privilege Management Infrastructure（PMI） **特权管理基础设施**	能够支持特权管理的基础设施，它支持全面的授权服务，并与公开密钥基础设施相关。	X.509
public key **公开密钥**	1．（公开密钥密码系统中）用户密钥对中公开的密钥。 2．非对称密码算法中所用的密钥，它可以公开。 3．公开密钥密码学中所用的密钥，它属于一个单独实体，并公开发布。其他实体使用该密钥来对发往密钥所有者的数据进行加密。	X.509 X.810 J.170

术　语	定　义	参考文献
public key certificate **公开密钥证书**	1．用户的公开密钥，以及其他一些信息，利用发放它的证书机构的专用密钥进行加密，不可伪造地进行提交。 2．代表所有者公开密钥（和其他可选信息）的值，由可信的机构以一种不可伪造的方式进行确认和签署。 3．实体的公开密钥与一项或多项与其身份有关的属性之间的绑定也称为数字证书。	X.509 H.235 J.170
Public Key Cryptography **公开密钥密码学**	基于两个密钥算法（秘密的和公开的）的加密技术，在该技术中，利用公开密钥对消息进行加密，但只能利用专用密钥才能对消息进行解密。也就是所知的秘密－公开密钥（PPK）系统。注 － 知道公开密钥并不能揭露专用密钥。例如：A 方设计这样一个专用密钥和公开密钥，并公开地将公开密钥传送给所有想与 A 方通信的人，但保守专用密钥的秘密。而后，任何拥有公开密钥的人都可以对发往 A 方的消息进行加密，但只有拥有专用密钥的 A 方才可以对消息进行解密。	J.93
Public Key Infrastructure（PKI） **公开密钥基础设施**	能够支持公开密钥管理的基础设施，它支持认证、加密、完整性或不可抵赖服务。	X.509
Registration Authority（RA） **注册机构**	1．负责鉴别和认证证书对象的实体，但不是 CA 或 AA，因此不签署或核发证书。注 － RA 可以为证书应用过程、撤销过程或两个过程提供帮助。 2．有资格并可信任的、执行注册业务的机构。	X.842 X.843
relay attack **转发攻击**	对认证过程的攻击，它首先截获交换 AI，而后立即予以转发。	X.811
relying party **依赖方**	在做决定时依赖证书中数据的用户或代理。	X.509
replay **重播**	重复某个消息或消息的一部分，以便产生未经授权的效果。例如，可以由另一个实体来重播包含认证信息的合法消息，以便认证它（是某某，而实际上它不是某某）。	X.800
repudiation **抵赖**	1．参与通信的一个实体否认曾参与过全部或部分通信。 2．参与过通信交换的一个实体随后否认该事实。 3．（在 MHS 情况下）MTS 用户或 MTS 可能在之后否认提交、接收或发送过消息，并且包括：拒绝发送、拒绝提交、拒绝传输。	X.800 M.3016.0 X.402
reveal **揭密**	移去某些或所有先前所用之机密性保护措施的操作。	X.814
revocation certificate **撤销证书**	由安全机构核发的安全证书，用于指明某特定的安全证书已宣布无效。	X.810
revocation list certificate **撤销列表证书**	确定安全证书列表已宣布无效的安全证书。	X.810
routing control **路由控制**	路由处理过程中规则的应用，以便选择或避免特定的网络、链路或中继。	X.800
rule-based security policy **基于规则的安全政策**	以适用于所有用户的全局规则为基础的安全政策。这些规则通常依赖于对所访问资源敏感度以及对用户、用户群或代表用户行事之实体相应属性拥有情况的比较。	X.800

术　　语	定　　义	参考文献
seal **封印**	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（即它不提供不可抵赖）。当封印与数据元相关时，该数据元被称作加封的数据。注 — 尽管封印本身不提供不可抵赖，但一些不可抵赖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。）	X.810
secret key **秘密密钥**	对称密码算法所用的密钥。秘密密钥的所有权是有限的（通常限于两个实体）。	X.810
security **安全**	术语“安全”用于表示最大限度地减少资产和资源的弱点。资产指的是任何有价值的事物。弱点指的是任何可被用于侵犯系统或其所含信息的薄弱之处。威胁指的是对安全构成的潜在侵犯。	X.800
security administrator **安全管理员**	负责定义或强制执行安全政策中一部分或多个部分的人。	X.810
security alarm **安全警报**	当检测到安全相关事件（安全政策将之定义为告警条件）时产生的消息。安全告警旨在适时地引起适当实体的注意。	X.816
security association **安全联盟**	两个或多个实体之间的一种关系，对之存在属性（状态信息和规则）来管理涉及这些实体的安全业务的供应。较低层通信实体之间的关系，对之存在相应的安全联盟属性。	X.803 X.802
security audit **安全审查**	对系统记录和行为的独立评估和检查，目的是测试系统控制的合适性，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、政策和程序提出修改建议。	X.800
security audit trail **安全审查索引**	为便于进行安全审查而收集并可能使用的数据。	X.800
security auditor **安全审查员**	允许访问安全审查索引并建立审查报告的个人或进程。	X.816
security authority **安全机构**	1．负责定义、实施或强制执行安全政策的实体。 2．安全域内负责管理安全政策的实体。 3．负责实施安全政策的管理员。	X.810 X.841 X.903
security certificate **安全证书**	由安全机构或可信第三方发布的一套与安全相关的数据，与安全信息一起用于提供数据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。X.800 系列中采用术语“安全证书”是为了避免与 X.509 产生术语冲突。	X.810
security domain **安全域**	1．服从公共安全政策的用户和系统集。 2．服从单个安全政策的资源集。	X.841 X.411
security exchange **安全交换**	开放系统间应用协议控制信息的一次传送或传送序列，作为操作一个或多个安全机制的一部分。	X.803
security information（SI） **安全信息**	执行安全业务所需的信息。	X.810
security label **安全标志**	绑定于资源上的标志（可能是一个数据单元），它命名或指定了该资源的安全属性。	X.800

术　　语	定　　义	参考文献
security management **安全管理**	安全管理，包括用于建立、维护和终止系统安全方面问题的所有行为。覆盖的主题包括：安全业务的管理、安全机制的安装、密钥管理（管理部分）、身份建立、密钥、访问控制信息、安全审查索引和安全告警管理。	M.3016
security model **安全模型**	一个用于描述安全业务（用于抵御对 MTS 的潜在威胁）和安全要素（用于支持这些业务）的框架。	X.402
security policy **安全政策**	1．掌管安全业务和设施使用和供应的安全机构所设定的一套规则。 2．提供安全业务的一套标准。注 – 参见“基于身份的安全政策”和“基于规则的安全政策”。完整的安全政策有必要解决 OSI 范围之外的许多问题。	X.509 X.800
security rules **安全规则**	本地信息，它假定所选的安全业务规定了将要使用的基础安全机制，包括操作机制所需的所有参数。注 – 安全规则是安全交互规则的一种形式，如在高层安全模型中所定义的那样。	X.802
security service **安全业务**	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。	X.800
security state **安全状态**	开放系统中持有的状态信息，在提供安全业务时所需。	X.803
security token **安全标记**	受一个或多个安全业务保护的、在通信实体之间传送的一组数据，与安全信息一起用于提供这些安全业务。	X.810
security transformation **安全转换**	一组函数（系统安全函数和安全通信函数），它们依据用户数据项一同工作，以便在通信或储存期间以一种特殊的方式来保护这些数据项。	X.803
selective field protection **选择性字段保护**	对于将要被传送的消息中特定字段的保护。	X.800
sensitivity **灵敏度**	表明资源价值或重要性的特性。	X.509
shared secret **共享秘密**	指密码算法使用的安全密钥，可能源自口令。	H.530
shield **遮蔽**	将数据转换为完整性受保护的数据。	X.815
signature **签字**	参见“数字签字”。	X.800
simple authentication **简单认证**	通过简单的口令安排实现的认证。	X.509
Source of Authority（SOA） **源机构**	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。	X.509
spamming **滥发**	向系统过度发送未经授权数据的拒绝服务攻击。一种特定的情况是在 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；将消耗宝贵的系统资源来处理。	H.235
strong authentication **强认证**	通过密码证书获取的认证。	X.509
symmetric authentication method **对称认证方法**	一种认证方法，其中的两个实体共享公共的认证信息。	X.811
symmetric cryptographic algorithm **对称密码算法**	实施加密的一种算法，或实施解密的相应算法；算法中，对加密和解密要求同样的密钥。	X.810

术　　语	定　　义	参考文献
threat **威胁**	潜在的安全侵犯。	X.800
time stamping service **时戳业务**	用于证明电子数据在某个准确的时刻存在的业务。注 — 时戳业务是有用的，为了支持长期的签字确认，它或许是不可缺少的。	X.842
traffic analysis **业务量分析**	通过对业务流量的分析（有、无、数量、方向和频度）而得出的信息推论。	X.800
traffic flow confidentiality **业务流机密性**	防止业务流分析的一种机密性服务，即对信息提供保护措施的一种安全服务，它可以来自对业务流量的分析。	X.800
traffic padding **业务流填充**	产生杂散的通信实例、杂散的数据单元与/或数据单元内杂散的数据。	X.800
trapdoor **暗门**	某个行动的结果，在该行动中，对系统的一个实体进行了修改，使得攻击者能够根据指令或在某个预定的事件或事件序列上产生非授权的效果。例如，对口令确认进行修改，这样，除了其通常的作用之外，它还认可攻击者的口令。	X.800
Trojan horse **特洛伊木马**	引入系统后，除了其授权的功能之外，特洛伊木马还具有非授权的功能。将消息拷贝给非授权信道的转发也称为特洛伊木马。	X.800
trust **信任**	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。	X.810
trusted entity **可信实体**	可以违反安全政策的实体，该实体或者做一些它不该做的事，或者没有做它该做的事。	X.810
trusted functionality **可信功能性**	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。	X.800
trusted third party （TTP） **可信第三方（TTP）**	（在某种安全政策的范畴内）就某些安全相关活动而言（被其他实体）得到信任的某个安全机构或其代理。	X.810
unauthorized access **未经授权的访问**	一个实体试图违反有效的安全政策访问数据。	M.3016
unshield **揭开**	将完整性受保护的数据转换为最初受遮蔽的数据。	X.815
user authentication **用户认证**	证明用户或应用进程的身份。	M.3016
validate **验证**	对完整性受保护的数据进行检验，以检测完整性的损坏情况。	X.815
verifier **验证者**	作为或代表要求具备经认证身份的一个实体。验证者包括认证交换中所需的功能。	X.811
vulnerability **弱点**	任何可用于侵犯系统或其所含信息的薄弱之处。	X.800
X.509 certificate **X.509 证书**	作为 ITU-T X.500 标准号码簿的一部分而制定的一种公开密钥证书规范。	J.170

B.2 安全相关首字母缩略语

缩写词	定 义
AA	[X.509] 属性机构
ACI	[SANCHO] 访问控制信息
AE	[M.3010] 应用实体
AES	[H.235] [J.170] 高级加密标准算法
APS	[SANCHO] 自动保护交换
ASN.1	[H.680] 抽象句法记法一
ASON	[SANCHO] 自动交换光网络
ASP	[X.805] [X.1121] 应用服务提供商
CA	[H.234] [H.235] [J.170] [X.509] 认证机构。一个接受实体证书申请、认证申请、核发证书并负责维护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，并负责控制通信中线路一侧的功能。
CME	[X.790] 一致性管理实体
CMIP	[M.3010] 通用管理信息协议
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 术语中也称为呼叫代理（这是应用服务器的一个例子）。
CORBA	[SANCHO] 公共对象请求代理体系结构
COS	[SANCHO] 服务等级
CP	证书政策
CPS	[SANCHO: X.842] 证书生效声明 [SANCHO: Q.817] 证书政策声明
CRL	[H.235] [X.509] 证书撤销列表
DCN	[SANCHO] 数据通信网络
DES	[SANCHO] 数据加密标准，数字加密标准
DHCP	[SANCHO] 动态主机配置协议
DOCSIS	[SANCHO] 数据电缆传输服务接口规范
DSA	[X.509] 号码簿系统代理 [SANCHO] 数字签字算法
DSL	[SANCHO] 数字用户回路
DSP	[SANCHO] 数字信号处理器 [SANCHO] 号码簿服务协议
FDS	[SANCHO] 欺诈探测系统
FEAL	[T.36] 快速数据加密算法，是一个算法族，它通过一个 64 比特的秘密密钥将 64 比特明文映射为 64 比特密文块，它类似于 DES，但功能要简单得多。简单快速的设计，使之非常适合于简单的微处理器（如智能卡）。（A. Menezes 等，应用密码学手册，CRC 出版社，1997）。
FIGS	[M.3210.1] 欺诈信息收集系统
GK	[H.235] [H.510] [H.530] 网守、网闸
GW	[H.235] 网关

缩写词	定　义
HFC	[SANCHO] 光纤/同轴混合缆
HFX	[T.30] [T.36] Hawthorne 传真密码
HKM	[T.30] [T.36] Hawthorne 密钥管理算法
ICN	信息通信网
ICT	信息通信技术
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 年创立的一种加密算法，使用具有 128 比特密钥的块密码（64 比特的块和 128 比特的密钥），被普遍认为具有非常高的安全性，是最著名的算法之一。在它投入使用后的几年中，尽管进行了诸多尝试力图击破它，但尚未见到有关实质性攻击的报告：（http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html）。
IKE	[J.170] 互联网密钥交换，是用于协商并为 IPsec 中 SA 产生密钥的一种密钥管理机制。
IKE–	[J.170] 一种记法，用于表示 IKE（互联网密钥交换）的使用，它用准共享密钥来进行认证。
IKE+	[J.170] 一种记法，用于表示需要公共密钥认证的 IKE（互联网密钥交换）。
IMT-2000	[M.3210.1] 国际移动电信 2000
IP	[X.805] 网际协议
IPsec	[H.235] [H.530] [J.170] [X.805] 网际协议安全（IPsec，IPSec）
IVR	[J.170] 交互式话音应答系统
LAN	[M.3010] 局域网
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，以确保完整性，也可记为 MIC。 [J.170] 媒体访问控制，是数据链路层的子层，通常运行于物理层之上。
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] 管理信息服务
MS	[M.3210.1] 管理系统 消息储存 复用段
MSP	[SANCHO] 复用段保护
MS-SPRing	复用段共享保护环
MTA	[J.170] 媒体终端适配器 多媒体终端适配器 消息传送代理
NAT	[H.235] 网络地址解析
OAM&P	[SANCHO] 运营、管理、维护和提供服务

缩写词	定　义
OS	[M.3010] [X.790] 运营系统
OSF	[M.3010] 运营系统功能
OSI	[SANCHO] 开放系统互连
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。
PDA	个人数据助理
PKI	[H.235] [H.530] [X.509] [J.170] 公开密钥基础设施。一个用于发放公开密钥证书的过程，包括标准、认证机构、机构间的通信，以及用于管理认证过程的协议。
PKINIT	[J.160] 公开密钥加密法初始认证 [J.191] 用于初始认证的公开密钥加密法
PMI	[X.509] 特权管理基础设施
QoS	[SANCHO] 服务质量
RA	注册机构
RADIUS	[J.170] 远程认证拨入用户业务
RAS	[SANCHO] 注册、准入和状态 [SANCHO] 注册、准入和状态协议
RBAC	[X.509] 基于角色的访问控制
RKS	[J.170] 记录保存服务器，用于收集并关联各种不同事件消息的设备。
RSA	[H.235] [T.30] [T.36] Rivest, Shamir and Adleman（公开密钥算法）
RTP	[H.225.0] [H.235] [J.170] 实时协议
SHA1	[H.235] 安全散列算法 No.1
SG	信令网关
SIP	[J.170] [X.805] 会话初始协议。应用层控制（信令）协议，用于创建、更改和终止与一个或多个参与者的会话。
SNC	[SANCHO] 子网连接
SNMP	[J.170] [X.805] 简单网络管理协议
SoA	[X.509] 源机构
SRTP	[H.235] 安全实时传输协议
SS7	[J.170] [X.805] 七号信令系统，以电话网络实施带外呼叫信令的一种体系结构和一系列协议。
SSL	[H.235] [X.805] 安全套接字层
TFTP	[SANCHO] 简单文件传输协议
TGS	[J.160] 许可证核发服务器
TLS	[H.235] 传送层安全性
TMN	[M.3010] [M.3210.1] [X.790] 电信管理网
TTP	[X.810] 可信第三方
UDP	[J.170] 用户数据报协议
VA	验证机构
VoIP	[X.805] IP 话音
VPN	[X.805] 虚拟专用网

附 件 C

研究组和安全相关研究课题清单

ITU-T 的标准化工作是通过研究组（SG）完成的，研究组中的 ITU-T 成员代表制定国际电信各不同领域的建议书（标准）。研究组以研究课题的形式推动其工作。每个研究组在某个特定电信标准化领域中开展其技术研究。以下是 2005-2008 年研究期中各 ITU-T 研究组的名称和任务清单，以及涉及安全工作的研究课题。

第 2 研究组	业务提供、网络及其性能的运营方面 业务定义、编号和路由牵头研究组
负责以下方面的研究：业务提供的原则，业务竞争的定义和运营要求；编号、命名、寻址要求及资源分配，包括预留和分配的标准及程序；路由及互联要求；人为因素；网络运营方面的问题及相关性能要求，包括网络流量管理、业务质量(业务工程、运营性能及业务测量)；传统电信网络与演进中的网络之间互联的运营方面的问题；评估运营机构、产品制造公司及使用者有关网络运营的反馈意见。	
与安全有关的研究课题：	
— **课题 1/2** — 电信编号、命名及寻址方案应用，以及包括业务定义在内的有关编号的业务和运营问题	
— **课题 4/2** — 电信网络业务质量运营问题	

第 3 研究组	包括相关电信经济及政策问题在内的资费及结算原则
负责与国际电信业务的资费及结算原则有关的研究，并研究与电信经济及政策问题有关的研究课题。为此，第 3 研究组应特别促进其各成员之间的合作，目的是在提供高效业务的情况下确定尽可能低的价格，并考虑在合理的基础上保持独立的电信财务管理的必要性。	
与安全有关的研究课题： 无	

第 4 研究组	电信管理 电信管理牵头研究组
负责有关电信业务、网络及设备管理的研究，包括支持下一代网络(NGN)及电信管理网(TMN)框架的应用和发展。另外还负责与指派、传输相关的运营程序及测试和测量技术和设备有关的其他电信管理的研究。	
作为管理活动的牵头研究组，第 4 研究组安全方面的工作涉及下述领域： 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（也称为管理平面）安全的具体要求，特别是随着网络趋于融合； c） 保护管理信息和安全参数管理安全的协议和模型。	
电信网络的管理根据不同层次上的抽象定义为，从管理网络单元的信息到用户服务管理。管理系统之间以及管理系统与网络单元之间的信息交换安全要求依赖于管理网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有的建议书中予以定义，并且另外的建议书也正在制定中。 最近批准的 M.3016 系列取代了原先的 ITU-T M.3016 建议书。该系列建议书说明了在 TMN 语言的范畴内安全的相关性和适用性。该系列建议书为特定组织利用可用的机制制定相应的规范提出了一个框架，而不是为避免威胁而规定一系列服务。 M.3016 系列涵盖了 TMN 中的下述威胁：冒名顶替、窃听、未经授权的访问、信息缺失或损毁、抵赖、伪造和拒绝服务。该系列建议书还涵盖了下述安全特性：机密性、数据完整性、责任制和可用性。	
与安全有关的研究课题：	
— **课题 6/4** — 管理原则和结构（M.3010，M.3016 系列，M.3400）	
— **课题 7/4** — 商务—商务及客户—商务管理界面要求（M.3320）	
— **课题 10/4** — 与应用具体相关的信息模型（M.3210.1）	
— **课题 11/4** — 管理界面协议（Q.813，Q.815，Q.817）	

第 5 研究组	电磁环境影响的保护
负责有关保护电信网络和设备不受干扰和雷击影响的研究，还负责与电信装置和设备(包括移动电话)产生的电磁场有关的电磁兼容性(EMC)、生命安全及对健康的影响的研究。	
在完成其任务时，第 5 研究组已对若干课题进行了研究，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。电磁威胁涉及恶意的、人为的高能瞬变现象，例如高空电磁脉冲（HEMP）和高能微波（HPM）。另外，电磁安全可能涉及因设备意外无线电发射造成的电信网络信息泄露。	
恶意威胁和相应消除技术的特性类似于应用于自然或无意电磁干扰的技术的特性。HEMP 与雷击产生的电磁脉冲有些相似。屏蔽和过滤技术在减小设备无意中的无用无线电能量发射的同时，也极大地降低了无意识能量泄露的可能性。因此，与免遭雷击和控制电磁干扰（EMI）相关的、第 5 研究组的传统研究活动，适用于保护网络安全免受恶意的人为威胁。在当前研究其内，研究组安全方面的工作是按照新的 15/5 号研究课题《电磁环境下电信信息系统的安全性》开展的。	
电磁威胁涉及恶意的、人为的高能瞬变现象，例如高空电磁脉冲（HEMP）和高能电磁（HPEM）发生器产生的发射，包括高能微波（HPM）和超宽带（UWB）干扰源。另外，电磁安全可能涉及因设备意外无线电发射造成的电信网络信息泄露。	
与安全有关的研究课题：	
— **课题 2/5** — 与宽带接入网络有关的电磁兼容性（为减少信息泄露的可能性而对宽带接入系统无用发射的控制）	
— **课题 4/5** — 通信设备抗干扰能力（设备对雷击的抵抗性改善了设备对 HEMP 感应电涌的抵抗性）	
— **课题 5/5** — 电信系统雷电保护（用于防雷的技术还为网络设备提供了一定程度的防止 HEMP 和 HPE 的能力）	
— **课题 6/5** — 全球环境下电信系统的连接配置和接地（合适的屏蔽和接地措施还有助于网络设备防止 HEMP 和 HPE）	
— **课题 12/5** — 对现有电磁兼容性建议书的维护和增补（电信设备的 EMC 提高了设备的抗导电能力以及抗辐射 HEMP 环境和抗辐射 HPE 环境的能力。同样，电信设备的 EMC 减少了信息泄露的可能性）	
— **课题 15/5** — 电磁环境下电信信息系统的安全性（防雷设备提高了设备对 HEMP 感应电涌的抵抗性）	

第 6 研究组	户外设施
第 6 研究组负责研究户外设施相关的问题，例如建筑、安装、连接、终接、防腐蚀和环境影响引起的其他形式的破坏，除电磁过程之外的、所有类型的公众电信地面线缆和相关设施。	
与安全有关的研究课题：	
— **课题 1/6** — 外部设施的环境和安全程序	
— **课题 6/6** — 光导纤维缆网络的维护	

第 9 研究组	综合宽带有线网络与电视及声音传送 综合宽带有线及电视网络牵头研究组

负责以下方面的研究：

a） 线缆和混合网的使用，主要用于将电视和声音节目传输到户，如综合宽带网络也用于承载话音或其他时间临界服务、电视点播、交互式服务等。

b） 电信系统在电视、声音节目的馈给、一次传输、二次传输和类似数据业务中的使用。

作为综合宽带有线及电视网络牵头研究组，第 9 研究组对宽带网络和业务面临的威胁和弱点进行评估，确定安全目标，评估应对措施，并规定安全体系结构。

安全相关的活动集中于以下一些领域：

a） *安全宽带业务*：为宽带接入网提供安全服务。即，电缆调制解调器的认证、加密密钥管理、传输数据的私密性和完整性、电缆调制解调器软件的安全下载。

b） *安全 VoIP 业务*：IPCablecom 是一个在使用 IP 协议的有线电视网络上承载实时交互服务的特殊工程，尤其是 IP 语音和视频。IPCablecom 提供的安全业务包括：对服务供应商的多媒体终端适配器（MTA）认证、对 MTA 的服务供应商认证、安全设备供应和配置、安全设备管理、安全信令和安全媒体。

c） *安全家庭联网业务*：增强型电缆调制解调器能够提供家庭联网业务，例如防火墙和网络地址转换。提供给增强型电缆调制解调器的安全服务包括：对服务供应商的多媒体终端适配器（MTA）认证、对 MTA 的服务供应商认证、安全设备供应和配置、安全设备管理、包过滤/防火墙功能性、安全防火墙管理、增强型电缆调制解调器软件的安全下载。

d） *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）规范中定义的安全业务。

与安全有关的研究课题：

— **课题 3/9** — 用于防止非授权拷贝和非授权再分配的有条件接入方法和实践（用于数字有线电视家庭分配的“再分配控制”）（J.93，J.96）

— **课题 8/9** — 使用网际协议（IP）的数字业务与应用和/或分组数据的有线电视传输（J.112）

— **课题 9/9** — 有线电视网上的语音和图像 IP 应用（J.160，J.170，J.191）

— **课题 10/9** — 宽带用户住地网上有线业务的扩展

第 11 研究组	信令的要求及协议 信令和协议、智能网络牵头研究组
负责研究各种网络中与网际协议（IP）相关功能、某些移动性相关功能、多媒体功能有关的信令要求和协议，包括与 NGN 的融合，以及对现有的涉及 BICC、ATM、N-ISDN 和 PSTN 接入和网络互联信令协议的建议书进行增补。 目前第 11 研究组的大部分建议书都是为基于 TDM 的可信网络开发的，这种网络中的点对点连接可以保证通信的安全。第 11 研究组认识到在网络中引入 IP 技术会带来新的安全问题。由于认识到要以安全的方式在这种处于变化的网络中引入 IP 技术以及有必要在网中提供信令与控制信息能力，第 11 研究组于 2004 年提出了一套有关信令要求和协议的研究课题，考虑了这些新的安全问题。	
与安全有关的研究课题：	
— **课题 1/11** — 新兴 NGN 环境下网络信令和控制功能结构	
— **课题 7/11** — 支持 NGN 环境下附件的信令和控制要求及协议	

第 12 研究组	性能及业务质量 业务质量和性能牵头研究组
负责关于终端和网络的端对端传输性能的建议书，涉及文本、数据、语音和多媒体应用的感性质量及用户的接受程度。虽然该项工作包括所有网络（例如基于 PDH、SDH、ATM 和 IP 的那些网络以及 NGN）和所有电信终端（例如手持设备、免提设备、头戴设备、移动设备、视听设备和互动话音响应设备）的相关影响，但特别关注的是 IP QoS、互操作性和 NGN 的影响，另外还涉及性能愈资源管理方面的工作。	
与安全有关的研究课题：	
— **课题 10/12** — 话音、数据和多媒体业务传输规划及性能考虑	
— **课题 13/12** — 多媒体 QoS/QoE 性能要求和评价方法	
— **课题 17/12** — IP 网络性能	

第 13 研究组	下一代网络 *NGN 和卫星问题牵头研究组*
负责与下一代网络的体系结构、演变和融合有关研究，包括框架与功能性体系结构、NGN 信令要求、NGN 项目的跨研究组管理协调并形成规划、实施方案与部署模型、网络与服务能力、互操作性、IPv6 的影响、NGN 的移动性以及网络融合与公众网方面的问题。	
由于认识到安全是 NGN 的一个关键特性，第 13 研究组已经确立了一个关于安全的专门研究课题：15/13 号研究课题“NGN 安全”。该课题集中研究 NGN 特有的安全问题，提出 NGN 安全解决方案。第 13 研究组的一个根本目标是推出一套标准，竭尽可能，在原有网络向 NGN 过渡时确保电信基础设施的安全。 第 13 研究组还决定在每个新的和最终修订的建议书中纳入一个有关安全问题的章节，列出建议书中涉及安全问题的段落。 第 13 研究组正在与其他研究组和其他批准开发组织协作，致力于 NGN 安全相关事项的研究。对第 13 研究组的安全研究而言，IETF（互联网、安全和传送领域）、3GPP 与 3GPP2 以及 DSL 论坛都是与此有关的特别重要的外部标准开发组织。	
与安全有关的研究课题：	
— **课题 2/13** — NGN 新兴业务要求和实施方案	
— **课题 3/13** — NGN 原则和功能结构	
— **课题 4/13** — NGN 业务质量要求和框架	
— **课题 5/13** — NGN 的 OAM 及网络管理	
— **课题 6/13** — NGN 移动性及固定—移动融合	
— **课题 7/13** — NGN 环境下网络和业务互操作	
— **课题 8/13** — NGN 业务方案和实施模型	
— **课题 9/13** — IPv6 对 NGN 的影响	
— **课题 10/13** — 卫星与地面及下一代网络(NGN)的互操作性	
— **课题 12/13** — 帧中继（X.272）	
— **课题 13/13** — 公众数据网络	
— **课题 14/13** — 多业务数据网络（MSDN）的协议和服务机制	
— **课题 15/13** — NGN 安全 安全相关任务包括： • 领导第 13 研究组内及与其他研究组进行的 NGN 特有的安全项目层面问题的研究。认识到第 17 研究组作为电信安全牵头研究组的整体作用，在 NGN 安全协调问题上为第 17 研究组提出建议和提供协助。 • 确定在 NGN 环境的范畴内如何应用 ITU-T X.805 建议书《提供端对端通信的系统的安全体系结构》。 • 确保形成的 NGN 体系结构符合工人的安全原则。 • 确保 AAA 原则按照要求纳入整个 NGN。	

第 15 研究组	光传输网及其他传输网络基础设施 接入网络传输牵头研究组 光技术牵头研究组

第 15 研究组是 ITU-T 负责研究光和其他传输网络基础设施、系统、设备、光纤及相应控制平面技术标准，促进向智能传输网演进的牵头组。这包括开发用于用户住所、接入部分、通信网络的都市和长途部分的相关标准。

14/15 号研究课题负责说明管理和控制要求，以及支持传输设备的信息模型。14/15 号研究课题遵循 ITU-T 为规定这些要求和模型而建立的 TMN 概念和框架。安全管理是五个关键性 TMN 管理功能类别中的一个。安全管理已纳入 14/15 号研究课题的研究范围，并正在研究中。

a） 传输设备管理的要求：G.7710/Y.1701、G.784 和 G.874 分别描述了在一个传输网络单元（它适用于多数技术）中的设备管理功能（EMF），尤其对 SDH NE 和 OTN NE。所述的应用用于日期与时间、故障管理、配置管理、计费管理、性能管理和安全管理。这些应用形成对 EMF 功能和及其需求的说明。在这些建议书中的安全管理要求目前正在研究中。

b） 数据通信网络体系结构和要求：G.7712/Y.1703 定义了数据通信网络（DCN）的体系结构要求，它支持与电信管理网（TMN）有关的分布式管理通信、与自动交换传输网络（ASTN）有关的分布式信令通信，以及其他分布式通信（例如 Orderwire 或语音通信、软件下载）。不同的应用（例如 TMN、ASTN 等）要求基于分组的通信网络在不同的网络单元间传输信息。例如，TMN 需要一个像管理通信网络（MCN）那样的通信网络，用于在两个 TMN 部件（例如 NEF 部件和 OSF 部件）之间传输管理信息。ASTN 需要一个像信令通信网络（SCN）那样的通信网络，用于在两个 ASTN 部件（例如 CC 部件）之间传输信令消息。G.7712/Y.1703 参考了 M.3016 系列中的 MCN 安全要求。SCN 安全要求在 G.7712/Y.1703 中定义。

c） 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）提供了有关分布式呼叫和连接管理的要求。该建议书中的要求为实现自动呼叫操作和连接操作规定了接口间的通信。规定了安全属性和其他属性，以便验证呼叫和连接操作（例如，这可能包括允许进行呼叫请求认证的信息，可能还包括进行呼叫请求完整性检测的信息）。

第 15 研究组	光传送网及其他传送网基础设施 接入网络传输牵头研究组 光技术牵头研究组
d） 自动交换光网络（ASON）中的路由体系结构和要求：G.7715/Y.1706 规定了路由功能的要求和体系结构，用于建立 ASON 框架中的交换连接（SC）和软永久连接（SPC）。该建议书涵盖的主要领域包括：ASON 路由体系结构，以及包括通路选择、路由属性、抽象消息和状态图的功能部件。该建议书参考了 ITU-T M.3016 系列建议书和 X.800 中的安全考虑因素。特别地，依据有关路由协议的上下文，它说明了在 ITU-T M.3016 系列建议书中定义的、有关机密性、数据完整性、可说明性和可用性的、总的安全目标，它们可以具有不同的重要等级。提议之路由协议的安全分析应描述以下基于 ITU-T X.800 建议书的问题，即伪装、窃听、未经授权的访问、信息丢失或破坏（包括重播攻击）、抵赖、伪造和拒绝服务。	
e） ASON 管理的框架：G.7718/Y.1709 描述了 ASON 控制平面的管理方面问题，以及管理层与 ASON 控制平面之间的相互作用问题。将包括：故障管理、配置管理、会计管理、性能管理和控制平面部件安全管理要求。	
与安全有关的研究课题：	
— **课题 3/15** — 光传送网的一般特性（G.911）	
— **课题 9/15** — 传送设备和网络保护/恢复（G.808.1，G.841，G.842，G.873.1）	
— **课题 14/15** — 传送系统和设备的管理和控制	

第 16 研究组	多媒体终端、系统及应用 多媒体终端、系统和应用以及普遍应用（“一切电子化”，例如电子医疗保健和电子商务）牵头研究组

第 16 研究组是有关多媒体终端、系统和应用以及有关普遍应用（“一切电子化”，例如电子医疗保健和电子商务）的牵头研究组。（2/16 工作组的）25/16 号研究课题涵盖了“下一代网络的多媒体安全”，负责解决以下安全问题。

像经由分组交换网络的电话、IP 话音、交互式（电视）会议和协调这类高级多媒体（MM）应用、MM 消息、音频/视频流及其他应用，在异构网络环境中面临着各种各样严峻的安全威胁。滥用、恶意篡改、窃听和拒绝服务攻击只是一小部分潜在的严重风险，特别是在 IP 网络上。

已认识到，这些应用具有共同的安全需求，可以通过普通的安全措施来满足；例如通过网络安全或网络层面的认证。然而，MM 应用通常具有专用的安全需求，可以通过应用层的安全措施很好地来满足。25/16 号研究课题关注的是下一代网络中 MM 应用的应用安全问题（NGN-MM-SEC），并酌情通过采取补充的网络安全措施来满足。

与安全有关的研究课题：

— **课题 1/16** — 多媒体系统、终端和数据会议（H.233，H.234）

— **课题 2/16** — 在分组交换网络上传输实时音频、视频和数据（H.323）

— **课题 4/16** — 在 ITU-T 定义多媒体系统平台高端的高级多媒体通信业务（H.350.2）

— **课题 25/16** — 下一代网络的多媒体安全(NGN-MM-SEC)（H.235.x 系列）

— **课题 29/16** — 多媒体系统和业务的移动性（H.530）

第 17 研究组	安全、语言及电信软件 电信安全、语言和描述技术牵头研究组

第 17 研究组负责与安全、开放系统通信应用（包括联网）和号码簿有关的研究，还负责技术语言问题、技术语言的应用方法以及涉及电信系统软件方面的其他问题。

ITU-T 第 17 研究组是有关电信安全问题的牵头研究组。ITU-T 安全标准化工作通过 4/17 号研究课题管理下的新的 ITU-T 安全项目进行协调。作为这项工作的一部分，提出了一个有关安全问题的国际电联建议书目录，汇编了摘自已经批准的 ITU-T 建议书的安全定义，并不断予以更新。2002 年 5 月在韩国的首尔、2004 年 10 月在巴西的弗洛里亚诺波利斯、2005 年 3 月在俄罗斯的莫斯科、2005 年 10 月在瑞士的日内瓦举办了安全问题研讨会和网络安全报告会。其他研讨会将按照需要组织。

依据 1/17 工作组的职能，ITU-T X.509 建议书《公开密钥和属性证书框架》为公开密钥基础设施（PKI）和特权管理基础设施（PMI）提供了基础。X.509 正不断完善，以便满足新的需求。2/17 工作组负责已有的关于核心安全体系结构、框架和协议的建议书，尤其是 X.800 系列中的那些建议书。在上一个研究周期中起草了一套新的关于安全的建议书，包括为提供端对端网络安全而规定了一个安全体系结构的 X.805。该体系结构可适用于各种不同种类的网络，而与网络的基础技术无关。它可以作为一个工具，确保在提出建议书中能够完备地考虑到安全问题，并可用于网络的安全评估。另一个基础的建议书是 X.1051，它规定了电信领域内信息安全管理系统（ISMS）的要求。在电信组织总的运营风险范畴内，它规定了建立、实施、运营、监控、评估、维护和改进已归档之 ISMS 的要求。X.1081 是一个框架建议书，奠定了未来远程生物统计规范的基础。X.1121 和 X.1122 关注的主要是移动端对端数据通信。X.1121 从移动用户和应用服务提供商的角度分析了移动环境中的安全威胁和保护措施。X.1122 对构建基于公开密钥基础设施（PKI）技术的安全移动系统提出了指导意见。在国际电联网站的第 17 研究组网页上可以查到最新资料（见 http://www.itu.int/ITU-T/studygroups/com17/ tel-security.html）。

与安全相关的课题：

1/17 工作组 开放系统技术

— **课题 1/17** — 具有业务质量管理设备的端对端多播通信

该研究课题考虑端对端多播通信的需求、体系结构、群组与会话管理以及多播通信协议。为了完成各成员间的安全群组通信，探讨了将安全协议扩展到端对端多播通信协议的问题。正在进行的工作关注的是相关安全机制对多播通信协议的应用以及安全通信程序的构建。

— **课题 2/17** — 号码簿服务、号码簿系统及公开密钥/属性证书

该研究课题负责对 X.509 的开发和维护。X.509 涵盖了公开密钥证书、属性证书、证书撤销以及用于支持基础设施（公开密钥基础设施和特权管理基础设施）的规范。公开密钥证书和支撑基础设施是进行认证的基础，特别适用于数字签字。

— **课题 16/17** — 国际化域名

安全问题是有关国际化域名（IDN）工作的一部分。16/17 号研究课题在于确定现有的表明 IDN 基本原则的技术文献，包括涉及伴随着 IDN 的实施而产生的电信网安全风险的文献。完成这一任务要征询相关实体的意见，包括 ISO/IEC、UNICODE 协会、IETF、ICANN 和 CENTR。

2/17 工作组 电信安全

— **课题 4/17 —** 通信系统安全项目

该研究课题专门用于确定并协调和组织 ITU-T 内全部通信安全活动。在其他研究组和其他标准开发组织的协作下，关于安全的研究课题将采用自上而下的方式。该项目的努力方向是在项目与战略层面让重点更为突出。

— **课题 5/17 —** 安全结构和框架

为了获得低成本、高效益的综合安全解决方案，以便能够用于多供应商环境中的各类网络、服务和应用，网络安全应围绕标准的安全体系结构和标准的安全技术进行规划。考虑到通信环境遭遇的安全威胁和目前在应对安全威胁的措施方面取得的进展，该项目考察的是新的安全要求和解决方案，以及如何制定安全体系结构和框架以反映不断发展的环境。

— **课题 6/17 —** 网络安全

该研究课题考虑国际标准化范畴内的网络安全问题。该课题特别考察网络安全的以下几个方面：

- 弱点信息的分发、共享和泄露过程。
- 网络空间中事故处理操作的标准程序。
- 保护关键网络基础设施的战略。

— **课题 7/17 —** 安全管理

该研究课题的目的是开发一套关于安全管理的 ITU-T 建议书，同时考虑与 ISO/IEC JTC 1 协作的必要性。该课题重点特别放在识别和管理电信系统的中的风险，并使电信运营商的信息安全管理系统（ISMS）与现有的 ISMS 标准挂钩。

— **课题 8/17** — 远程生物统计

该研究课题以目前采用生物统计技术开展的个人识别与认证工作为基础，正在从事的该课题研究与其他标准开发组织正在承担的工作有密切合作关系。该课题特别关注如何用有安全保障的远程生物统计方法改进用户的识别与认证，以及怎样识别出电信中的生物统计技术问题。

— **课题 9/17** — 安全通信服务

移动通信具有一些特殊的性质（如空中传输、移动设备计算能力有限且存储空间小），因此提供安全是一项特别困难的任务，需要特别关注与研究。该研究课题考察怎样识别和规定移动通信或网络服务中的安全通信服务，怎样识别和处理通信服务面临的威胁，支撑安全通信服务的技术有哪些，以及怎样维护通信服务之间的安全连接。

— **课题 17/17** — 通过技术措施应对垃圾邮件

该研究课题关注反垃圾邮件的技术需求、框架、指导原则和新技术。作为这项工作的一部分，正在开发一套关于应对电子邮件垃圾和多媒体应用中的垃圾的建议书，同时考虑了与其他 ITU-T 研究组协作以及与其他标准开发组织合作的必要性。

3/17 工作组 语言和电信软件

— **课题 10/17** — 抽象句法记法一（ASN.1）及其他数据语言

该研究课题维护和增强了 ASN.1 及其规则，包括用于生成 X.509 数字证书或数字签字的 DER（特异编码规则）。ASN.1 是信息表示法的一个重要组成部分，能以可靠的编码/解码和签字/验证方式表示信息。该课题不断改进 ASN.1，以便满足当今电信环境中不断变化的要求。

第 19 研究组	移动电信网络 *移动电信网络和移动性牵头研究组*
负责研究移动电信网络的网络问题，包括国际移动通信网（IMT-2000）和超 IMT-2000、无线互联网、移动网与固定网融合、移动性管理、移动多媒体功能、网间互联、互操作性，以及负责修订现有 ITU-T IMT-2000 建议书。	
与安全有关的研究课题：	
— **课题 1/19** — 业务和网络容量要求和网络结构	
— **课题 3/19** — 确认现有的和演化中的 IMT-2000 系统（Q.1741.1，Q.1741.2 ，Q.1741.3，Q.1742.1，Q.1742.2，Q.1742.3）	
— **课题 5/19** — 演化中的 IMT-2000 网络与演化中的固定网络的融合	

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.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：访问控制框架
X.813 – 开放系统安全框架：不可抵赖框架
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：安全审查和告警框架

网络管理安全

M.3010 – 电信管理网的原则
M.3016.x – TMN 安全（由几部分组成的建议书）
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 – 日志控制功能
X.736 – 安全告警报告功能
X.740 – 安全审查索引功能
X.741 – 访问控制的对象和属性

电信安全

X.805 – 提供端对端通信的系统的安全体系结构
X.1051 – 信息安全管理系统 — 电信需求（ISMS-T）
X.1081 – 一个用于规范远程生物统计安全保障问题的框架
X.1121 – 移动端对端通信的安全技术框架
X.1122 – 基于 PKI 实施安全移动系统的指南

电视和有线电视系统

J.91 – 确保远程国际电视传输私密性的技术方法
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

协议

X.273 – 网络层安全协议
X.274 – 传送层安全协议

多媒体通信

H.233 – 视听业务的机密性系统
H.234 – 视听业务的加密密钥管理和认证系统
H.235.x – H.323 安全（由几部分组成的建议书）
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 的号码簿服务体系结构
H.530 – H.510 中有关 H.323 移动性的对称安全程序

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 – 支持数字签字应用的 TTP 服务规范

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 – 使用三类传真终端的安全能力
T.503 – 四类传真文件交换的文件应用概况
T.563 – 四类传真设备的终端特性

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 – 公开密钥和属性证书框架
X.519 – 协议规范

消息处理系统（MHS）

X.400/F.400 – 消息处理系统和服务概述
X.402 – 总的体系结构
X.411 – 消息传送系统：抽象服务定义和程序
X.413 – 消息储存：抽象服务定义
X.419 – 协议规范
X.420 – 人际消息系统
X.435 – 电子数据交换消息系统
X.440 – 话音消息系统

可从国际电联网页 http://www.itu.int/publications/bookshop/how-to-buy.html 获取 ITU-T 建议书（该网页含有关于免费获取少量 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：

远程生物统计、安全管理、移动性安全、网络安全、归属网安全、NGN 安全、反垃圾邮件、应急电信

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

瑞士印刷
2006年，日内瓦