国 际 电 信 联 盟

ITU-T M.3016.0

国际电信联盟
电信标准化部门

(05/2005)

M系列：电信管理，包括TMN和网络维护
电信管理网

管理平面的安全：概述

ITU-T M.3016.0建议书

国际电信联盟

ITU-T M系列建议书

电信管理，包括 TMN 和网络维护

引言与维护和维护组织的一般原则	M.10-M.299
国际传输系统	M.300-M.559
国际电话电路	M.560-M.759
公共信道信令系统	M.760-M.799
国际电报系统和相片传真传输	M.800-M.899
国际租用一次群和超群链路	M.900-M.999
国际租用电路	M.1000-M.1099
移动电信系统和业务	M.1100-M.1199
国际公众电话网	M.1200-M.1299
国际数据传输系统	M.1300-M.1399
标志和信息交换	M.1400-M.1999
国际传送网	M.2000-M.2999
电信管理网	**M.3000-M.3599**
综合业务数字网	M.3600-M.3999
公共信道信令系统	M.4000-M.4999

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T M.3016.0建议书

管理平面的安全：概述

摘　要

本建议书给出了确定电信管理网安全威胁的概述和框架，并且概述了如何在电信管理网功能体系的上下文内应用安全服务。

来　源

ITU-T 第4研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于2005年5月22日批准了ITU-T M.3016.0建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

ITU-T M.3016.0建议书

管理平面的安全：概述

1 范围

本建议书给出了确定电信管理网（TMN）安全威胁的概述和框架，并且概述了如何在电信管理网功能体系的上下文内应用安全服务，电信管理网功能体系在ITU-T M.3010建议书中描述。

本建议书为通用建议书，不是针对电信管理网中的某一个特定接口的安全需求。

本建议书将不定义新的安全服务，而是使用在其他ITU-T建议书和ISO标准中已经定义的安全服务。

本建议书是ITU-T M.3016.x系列建议书的一部分，该系列建议书将为持续发展的网络的管理平面安全提供指南和建议：

ITU-T M.3016.0建议书 — 管理平面的安全：概述。

ITU-T M.3016.1建议书 — 管理平面的安全：安全需求。

ITU-T M.3016.2建议书 — 管理平面的安全：安全服务。

ITU-T M.3016.3建议书 — 管理平面的安全：安全机制。

ITU-T M.3016.4建议书 — 管理平面的安全：简表文稿。

ITU-T M.3016.1、M.3016.2和M.3016.3建议书为提供适当的管理功能安全定义了一系列安全需求、服务和机制，这些管理功能是支持电信基础设施所必需的。由于不同的行政部门和组织机构对安全有不同级别的要求，ITU-T M.3016 1、M.3016.2和M.3016.3建议书不指定某项安全需求、服务或机制为必选项或可选项。

ITU-T M.3016.4建议书中定义的文稿指定了对需求支持的必选项和可选项，以及取值范围和取值等，用来帮助各组织、行政部门及其他国家/国际机构用来实现他们各自的安全策略。

2 参考文献

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

— ITU-T Recommendation E.408 (2004), T*elecommunication networks security requirements*.

— ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

— ITU-T Recommendation M.3400 (2000), *TMN management functions*.

— ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

— ITU-T Recommendation X.741 (1995), *Information technology – Open Systems Interconnection –Systems management: Objects and attributes for access control.*

— ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

— ITU-T Recommendation X.802 (1995), *Information technology – Lower layers security model*.

— ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model.*

— ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Overview*.

— ITU-T Recommendation X.812 (1995), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Access control framework.*

— ITU-T Recommendation X.813 (1996), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Non-repudiation framework*.

— ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Confidentiality framework.*

— ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Integrity framework*.

— ITU-T Recommendation X.816 (1995), *Information technology – Open Systems Interconnection –Security frameworks for open Systems: Security audit and alarms framework.*

— ISO/IEC 9979:1999, *Information technology –Security techniques – Procedures for the registration of cryptographic algorithms*.

3 定义

本建议书没有规定新的术语。

4 缩写词和首字母缩略语

本建议书采用下列缩写词：

CCITT 国际电报电话咨询委员会
DCN 数据通信网
FC 功能类
ISO 国际标准化组织
ITU-T 国际电信联盟电信标准化部门
LLA 逻辑分层体系
MF 适配功能
NEF 网元功能
OSF 运行系统功能
OSI 开放系统互联
PIN 个人识别码
TF 转换功能

TMN　　电信管理网

TTP　　可信任的第三方

WSF　　工作站功能

5　　基本原理

TMN中的安全需求由不同的来源提出：

— **客户/用户**需要信赖网络及网络所提供的服务，包括正确的计费。

— **公共社团/权力机构**通过指令和立法等方式提出安全性要求，以确保服务的有效和隐私的保护。

— **网络操作员/服务提供者**自身也要求安全，以保护他们的业务和商业利益，并且符合他们对客户和公众应尽的职责。

TMN是用来管理电信网络的，因此，TMN的安全对电信网络的正常运转是必需的。更进一步说，电信网络可能合并需要TMN来进行管理的安全特性。ITU-T M.3400建议书列举了这些安全管理功能。

TMN安全标准应当基于国际公认的安全标准，应当重用这些标准并从中获益，而不是创建一些新的标准。安全服务和机制的前期准备和使用可能比被保护的事务的价值更加昂贵，因此，能够根据被保护的TMN事务，对安全进行定制是非常重要的。用来确保TMN事务安全的安全服务和机制应当以允许定制的方式提供。根据安全特性的大量可能的组合，需要有一个**安全简表**（见附录一）可以涵盖TMN安全应用的广泛范围。

标准化将推动**解决方案和产品的重用**，即安全可以引入得更快、而成本更低。

标准的解决方案对系统提供商和用户所带来的重大好处是相同的，即在与安全相关的TMN系统的产品开发和组件交互过程中所带来的规模效益。

在TMN实体间（在ITU-T M.3010建议书中定义）提供安全服务和机制以保护TMN事务是非常重要的，可以防止这些实体被恶意侵袭，如窃听、欺骗、信息篡改（如对信息进行修改、延迟、删除、插入、重放、改道发送、错误路由或重新排序等）、否认或伪造等。保护包括对侵袭进行预防、检测和恢复，同时对安全相关的信息进行管理。标准应当涵盖域内部接口（如Q接口和F接口）和域间接口（如X接口）。

6　　系统描述

本建议书的目标是做出抽象，以避免任何实现的细节，并且对结果达成一致意见，这些结果可用于后续映射到某种特定的实现。

TMN由功能体系结构、信息体系结构和物理体系结构（见ITU-T M.3010建议书）等术语描述。

在ITU-T M.3010建议书中指明，TMN的组成模块除了支持Q接口、X接口和F接口之外，可能还会支持其他接口。类似的，物理设备除了具备与从Q接口、X接口和F接口接收的信息相关的功能外，可能还会具备其他功能。这些额外的接口和相应的功能在TMN的定义范围之外，因此也在TMN安全标准的定义范围之外。

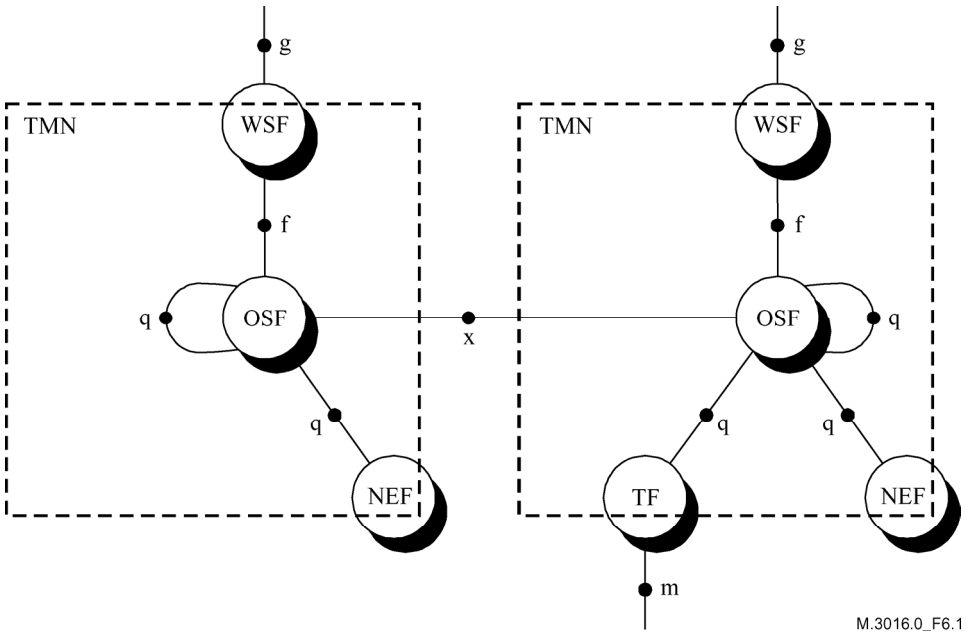

图1/M.3016.0－TMN 功能体系结构

6.1 参与者和角色

为了对TMN安全进行标准化，我们将仅考虑技术上的安全，这意味着所考虑的相关参与者为TMN的用户。一个TMN用户是一个人或一个提供TMN管理业务以完成管理操作的进程。TMN用户还能够再分类为内部用户和外部用户，根据他们是否属于运行TMN的组织（内部用户）、还是访问TMN的外部用户。

每次，TMN用户访问一个管理业务，该TMN用户都将会扮演一种角色。在一些情况下，TMN用户和角色之间是一对一的关系，即TMN用户总是扮演同样的角色。而在另外一些情况下，特定的TMN用户和其可能扮演的角色之间是一对多的关系。

如下给出了一些通用角色的高层分类：

— 网络操作员（私有的或公共的）；

— 业务提供者（承载业务提供者或增值业务提供者）；

— 业务用户/业务客户；

— 业务端用户；

— 设备供应商/软件供应商；

— 可信任的第三方（即被双方均信任的第三方，按照国家的相关法律和规定运转，提供证明、鉴权和相关服务的第三方）。

在为TMN提供安全保护时，仅控制所谓的TMN用户的行为是远远不够的，还必须考虑到企图非法侵袭TMN的可能的入侵者。

一些安全措施要求具备参与者来扮演可信任的第三方（TTP）角色。一个重要的安全问题是这些参与者如何被允许与TMN进行交互。

6.2 安全域

ITU-T M.3010建议书引入了逻辑分层体系（LLA）的概念，在这种概念中，管理功能被划分为不同的层次。每一个功能层仅关心整个管理活动中被清晰界定的一个子集。每一个功能层在运行系统功能（OSF）的控制下，是一个分离的管理域，称为一个OSF域。被OSF控制的网元功能（NEF）是OSF域的一部分。一个TMN就这样由一个或多个OSF域组成，这些不同的OSF域能够分离、交互、重叠或包含。

一个安全域被定义为归属于单个安全策略和单个安全部门的实体或组件的集合。常规假设一个TMN即为一个独立的安全域。一般来说该假设是成立的，但将其作为一个通用的假设可能不正确。在更大的包括很多不同管理系统的TMN中，TMN的不同组件可能会归属于不同的安全策略和安全需求，因此，更合适的说法为：TMN安全域包括一个独立的OSF域或一个OSF域的集合。

使用这个假设，将应用如下所示的安全域间关系和安全域内关系：

可能的安全域内关系：

— q (OSF-NEF, OSF-OSF)。

可能的安全域间关系：

— x (OSF-OSF)；

— f (WSF-OSF, WSF-MF)；

— q (OSF-OSF, OSF-TF)。

注意：上述关系指的是安全域，而不是管理域。注意一个重要情况，q参考点可能会涉及安全域内的关系，也可能涉及安全域间的关系。安全域内关系和安全域间关系的主要不同在于两个相关实体间信任程度的不同。

7 TMN通用的安全目标

本节的目的是描述在TMN环境中实施安全措施的终极目标。主要关注于要达到什么样的安全，而不是如何达到。

安全目标应当源自操作员或其他参与者的利益、业务关系、法律或制度约束以及合同约束等。

TMN的安全目标包括：

— 仅有合法的参与者能够访问和操作TMN中的资产。

— 合法的参与者应当能够访问和操作他们被授权访问的资产。

— 所有的参与者应当对他们自己，也仅仅是对他们自己在TMN中的活动负有责任。

— 应当保护TMN的可用性，不进行非授权的访问和操作。

— 应当能够从TMN中查询到安全相关的信息。

— 如果检测到安全入侵，应当以一种受控方式进行处理，使得危害降到最低。

— 在检测到一个安全漏洞后，应当恢复到正常的安全级别。

— TMN的安全体系应当提供一定的灵活性，以支持不同的安全策略，如具有不同强度的安全机制。

术语“访问资产”应理解为不仅指操作某些功能的可能性，也指对信息的查阅。

上述通用的安全目标由企业管理视点和语言来进行描述，而下述各节需要使用更技术性的术语来描述可实现的安全服务和功能。两种语言的映射并不总是明显的。

可以显示，达到了下述安全目标，则可以达到本节上述所提及的TMN安全目标中的前5个。

— 机密性；

— 数据完整性；

— 责任制；

— 可用性。

第9节描述的威胁和风险，第6节描述的功能需求将基于这些更专业的术语，这些专业术语的定义，见第9节。

8 法律问题

TMN的安全基础设施必须能够适应政府法律、契约规定、条约以及规章制度等的约束。这些约束可能包括一些强制的安全服务（如确保客户信息的私密性），也可能包括不允许使用某种安全机制（如某些加密类型），并且/或者支持由执法机构进行安全方面的窃听等。

9 威胁和风险

本节的目的是探究对TMN的威胁和风险。而不是试图对风险进行评估或者对单个的TMN实例的威胁进行分析。这些是各供应商在不影响互操作的基础上可以自行进行不同处理的本地问题。

威胁是一种潜在的对安全的破坏。根据TMN中确定的通用安全目标，威胁可针对四种不同类型的目标：

— **机密性**（已存储信息和传送中信息的机密性）；

— **数据完整性**（保护已存储信息和传送中信息的完整性）；

— **责任制**（任何实体应对自身发起的任何操作负责）；和

— **可用性**（所有合法的实体应当能够对TMN设施进行正确的访问）。

本建议书区分了三种不同类型的威胁：

— 意外威胁：威胁的发起者没有任何恶意的企图；

— 管理威胁：威胁源自缺少安全方面的管理；和

— 故意威胁：威胁由一个恶意的实体发起，企图袭击通信本身，或是网络资源。

意外威胁和管理威胁应被TMN标准化工作所重视，因为他们的后果同故意威胁相同。为了对威胁做更准确的分析，考虑到TMN的体系结构，本建议书关注于TMN不同参与者之间通信时存在的故意威胁。这种方法的目的是能够给出一个更简短的威胁列表，可以直接用于TMN的标准化工作。对TMN的某种威胁的分析应当明确下述基于ITU-T X.800建议书所定义的几个方面：

— **冒充（“欺骗”）：**一个实体伪装成另外一个不同的实体；

— **窃听**：通过监视通信而违反了机密性；

— **未授权访问**：某个实体试图违反安全策略强制访问数据；

— **信息丢失或破坏**：传输过程中的信息完整性被未授权地删除、插入、修改、重新排序或延迟等破坏；

— **否认**：包含在一个通信交互过程中的实体随后否认自己的行为；

— **伪造**：一个实体伪造信息，并且声明该信息是从另一个实体接收来的，或是要发向另一个实体；

— **拒绝服务**：拒绝服务发生在当一个实体执行自己的功能失败时，或阻止其他实体执行他们各自的功能时。这种行为包括拒绝访问TMN，或者通过将TMN通信溢出而拒绝通信。在一个共享网络中，这种威胁能够被识别为伪造额外的业务流量导致网络溢出，或者是通过延迟其他用户的业务流量而阻止其他用户使用网络。

表1给出了威胁和目标间的映射关系。

表1/M.3016.0－威胁和目标间的映射

威　　胁	机　密　性	数据完整性	责　任　制	可　用　性
冒充	x	x	x	x
窃听	x			
未授权访问	x	x	x	x
（传输中的）信息丢失或破坏		x		x
否认			x	
伪造		x	x	
拒绝服务				x

对一个系统的某种潜在的威胁可以是无损害的，除非该系统中有一个相应的弱点，且在某一时刻该弱点被暴露了出来。每一种威胁都意味着一种风险。对风险的评估可以分为两部分：对每种威胁发生的可能性进行评估和对该威胁可能造成的后果进行评估。威胁和风险的评估必须是一个循环反复的过程：即当一个对策建立时，可能会引发新的威胁，如当使用加密措施时可能会引出对密钥的威胁。

10　　安全需求和服务

图2描述了安全目标、威胁、安全需求和安全服务间的关系。该图描述了如何从“威胁”和“安全目标”中提出“安全需求”，并随之由一系列的“安全服务”来实现的过程。这些对抗威胁的“安全服务”会用到“安全机制”，而“安全机制”又会用到“安全算法”。

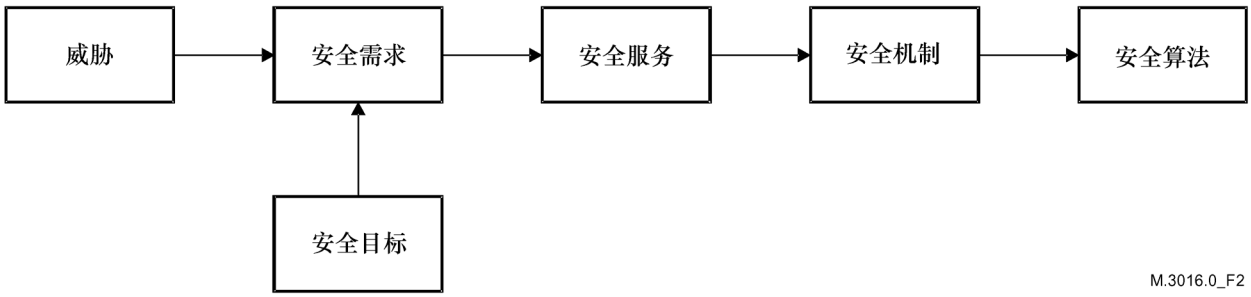

图2/M.3016.0－安全框架

第10.1节列出了这些安全需求。除非有其他说明，本建议书中的“需求”并不意味着这些功能在每个TMN中都是必选的，更确切的含义是，“需求”意味着根据某TMN的某种特定的应用和/或接口需求，一个功能可以由该TMN管理者定义为必选项。实际的选择依赖于操作者在安全策略中所规定的安全目标。

除了安全需求和安全服务，本节还规定了对安全服务进行管理的通用需求（见10.2节）和将安全服务综合到TMN体系结构中的体系结构需求（见10.3节）。管理需求和生命周期需求是重要的，但不会影响到体系结构，因此不在本节的定义范围之内。

10.1 安全需求和相应的服务

本节描述了一系列通用的功能需求和用来对抗TMN威胁的相应的服务。

10.1.1 功能需求、威胁和安全目标间的映射关系

本节将明确安全功能需求以涵盖第9节中所列的威胁，如表2所示。另外，安全需求被映射到第7节中所描述的安全目标，如表3所示。表2中所列的需求限于通用的需求，且对组件和体系结构有切实的影响。

表2/M.3016.0－功能需求和威胁间的映射

功能需求	冒充	窃听	未授权访问	信息丢失或破坏	否认	伪造	拒绝服务
身份认证	x		x				
受控访问和授权			x				x
机密性保护		x	x				
数据完整性保护				x			
责任制					x	x	
活动日志	x		x		x	x	x
告警上报	x		x	x			x
审计	x		x		x	x	x

这里所使用的目标是第7节定义的4个正式目标，在表3中每个目标占用一列，指出了与正在讨论的目标相匹配的功能需求集。

10.1.2 功能需求和相应服务的描述

对表2和表3中列出的每一项功能需求，将会在后续文字中有更深入的讨论，对每一个需求，还会明确其相应的安全服务。注意到，任何一个功能需求并不会自动地调用ISO中所定义的安全服务。而实际上，在许多情况下二者是同时发生的。

表3/M.3016.0－安全目标和功能需求间的映射

功能需求	机　密　性	数据完整性	责　任　制	可　用　性
身份认证	x	x	x	
受控访问和授权	x	x	x	x
机密性保护	x			
数据完整性保护		x		
责任制			x	
活动日志			x	x
告警上报	x	x	x	x
审计			x	x

10.1.2.1 身份认证

一个TMN应当提供能力确定并验证TMN中每个参与者所声称的身份。

参与者可以是人员或TMN中的实体。被验证的身份可提供责任制的基础，并且是满足本节所列的大多数安全需求的基础。

支持本需求的安全服务是**鉴权**。鉴权服务交付证据以确保对象或实体的身份确实是其所声称所具有的身份。根据参与者类型的不同和鉴权目标的不同，可能需要下述鉴权类型：

— 用户鉴权，认证使用人员或应用进程的身份；

— 对等实体鉴权，认证一个通信关系中对等实体的身份；

— 数据源鉴权，认证对某特定数据单元负责的身份。

使用鉴权服务可对当时某特定实例的身份进行认证。为确保持续的认证，鉴权必须重复进行，或者与完整性服务相联系。

完成鉴权服务所使用的机制可以包括：口令、个人识别码（PIN）（简单鉴权）和基于密码的方式（强鉴权）。

10.1.2.2 受控访问和授权

一个TMN应当提供能力确保参与者不对信息和资源进行未授权地访问。

符合本需求的安全服务是**访问控制。**访问控制服务提供途径以确保资源被实体以一种授权方式进行访问。有关的资源可能是物理系统、系统软件、应用程序或数据。访问控制服务可被定义和实现为不同的TMN粒度级别：代理者级别、对象级别或属性级别。访问限制体现在访问控制信息中，访问控制信息标明：

— 确定哪个实体被授权可以进行访问的方法；

— 什么类型的访问被允许（读、写、修改、创建、删除）。

更详细的TMN访问控制可划分为如下三种类型：

— 管理协会访问控制

该服务使得访问控制处于管理协会级别，意思是访问权限与协会自身相关，即建立协会的权力。

— 管理通知访问控制

该服务使得访问控制与通知相关，即确保通知仅发送给授权接收这些通知的实体。

— 被管资源访问控制

该服务提供与资源本身相关的访问控制。

需要在实体被允许访问资源前，对试图进行访问的实体身份进行检测。这意味着访问控制的使用总是需要与鉴权服务的使用结合起来。

10.1.2.3 机密性保护

一个TMN应当提供能力确保已存储数据和传送中数据的机密性。

支持该需求的安全服务是：对已存储数据的**访问控制**和对传送中数据的**数据机密性**。对某种类型的已存储数据可能也要求**数据机密性**，如口令。

机密性服务提供对交互数据的保护，以避免其被未授权的泄漏。应区分下述机密性服务的类型：

— 选择字段机密性；

— 连接机密性；

— 数据流机密性。

10.1.2.4 数据完整性保护

一个TMN应当保护已存储数据和传送中数据的完整性。

支持该需求的安全服务是：对已存储数据的**访问控制**和**数据完整性**，和对传送中数据的**数据完整性。**

完整性服务提供方式以确保交换数据的正确性，保护交换数据不被修改、删除、创建（插入）和延迟。应区分下述完整性服务的类型：

— 选择字段完整性；

— 无恢复连接完整性；

— 有恢复连接完整性。

10.1.2.5 责任制

一个TMN应当提供能力使得某实体不能否认其所执行的任何操作以及由此引起的任何后果。

支持该需求的服务是**不可否认**服务，该服务将个人（或实体）与其所执行的操作捆绑起来。不可否认服务能够提供方式证明数据交换确实发生了。它有两种形式：

— 不可否认：有源端证据；

— 不可否认：有交付证据。

另一个更通用，也可能弱一些的责任制的实现是通过将**鉴权、访问控制**和**审计跟踪**等服务适当地合并起来。

10.1.2.6 活动日志，告警上报和审计

这些需求涵盖了对TMN中与安全相关的行为进行存储和分析的需要。另外，告警通知应当基于某些可调整的事件进行上报。相应的服务是**审计跟踪**和**告警上报**。以下各小节中将详细讨论每个需求。

10.1.2.6.1 活动日志

一个TMN应当提供能力存储关于系统活动的信息，使得追踪个人或实体的这些信息成为可能。

一个日志可以看作是记录的储藏室：是OSI从实际开放系统中抽象出的日志资源。记录中包含被记入日志的信息。

对于许多管理功能来说，有必要保存已经发生的事件信息、或对不同的资源已经执行或试图执行的操作信息。

更进一步说，当这些信息被从日志中检索出时，管理者应当能够判断出这些记录是否有丢失，或这些存储在日志中的记录的特性在任何时候是否被修改过。

10.1.2.6.2 安全告警上报

一个TMN应当提供能力针对选择的事件产生告警通知。应当允许用户定义选择条件。

安全审计控制功能是一种系统管理功能，描述了安全事件采集通知。由该系统管理功能定义的安全告警通知提供了与安全相关的操作条件信息。

10.1.2.6.3 安全审计

一个TMN应当提供能力分析记入日志的安全相关的事件数据，以检测这些事件是否违反了安全策略。

审计应当独立地对系统记录和事件进行回顾和检查，检查是否有足够的系统控制，以确保与建立的安全策略和操作流程相一致，并且检测出安全的漏洞。审计结果应明确在控制、策略和流程方面应做哪些改变。

表4给出了需求和安全服务间的关系。本节仅定义了由标准解决方案涵盖的安全服务，另外一些可能的服务（如拒绝服务的检测）不予考虑。

表4/M.3016.0－安全需求与安全服务间的映射

功能需求	安全服务
身份认证	用户鉴权 对等实体鉴权 数据源鉴权
受控访问和授权	访问控制
机密性保护 – 已存储数据	访问控制 机密性
机密性保护 – 传送中数据	机密性
数据完整性保护 – 已存储数据	访问控制
数据完整性保护 – 传送中数据	完整性
责任制	不可否认
活动日志	审计跟踪
安全告警上报	安全告警
安全审计	审计跟踪
DCN 的保护	分组检测

注 — 下述需求不同于表4之前所描述的需求类型，甚至要作为标准化工作的候选项可能也不是很显然。但不管怎样，在设计阶段以及实现上述TMN核心需求的阶段，下述需求仍然应当被重视。

10.1.2.6.4 系统完整性

一个基本情况是，实现安全功能的软件和硬件环境决定着所要求的安全级别。

环境还包括对运行系统和故障排除系统的正确配置。

这些方面并不是安全简表自身的组成成份，但是它们必须与这些安全规范一起进行规定，以保证现实世界环境中功能的强壮性。

10.1.2.6.5 可用性备注

可用性需求不是由某个安全服务或有限的安全服务集就能够满足的。这里列出的所有安全服务应当组成一个集合来共同维持可用性。然而，安全服务自身不可能确保可用性：可用性还需要硬件和软件的可靠性支持（不论从设计观点还是从实现观点均是如此）。

10.1.2.7 DCN的保护

一个TMN应当提供对DCN的保护，包括从客户端和网络对端发来的业务流。

一个TMN应当将DCN业务流与其他类型的业务流隔离开来，尤其是对于分组方式的DCN。

10.2 安全管理的需求

一个TMN应当包含TMN安全服务的信息模型和对其的管理能力。

详细的安全管理需求规定了应当引入什么样的管理应用，以及这些管理应用应当如何设计。 这么做是为了向安全管理者提供适当的工具，使之以一种有效和正确的方式来监测和控制安全服务。安全管理的目标和目的可以通过电信系统的三个不同级别来描述，分别对应于系统安全的管理，安全服务和安全机制。

与TMN中安全服务管理相关的操作和信息需要从安全观点来特殊考虑。如密码系统中的密钥、鉴权信息和访问控制列表等，这些示例所要求的保护强度可能会高于网络管理所要求的保护强度。

对安全的管理应当与ITU-T M.3400建议书中所定义的安全管理功能相一致。

在一个系统出现安全漏洞后，应当支持将系统恢复到安全状态。

无论何时，当出现安全漏洞时，TMN都应当能够以一种受控方式处理这种情况，这意味着该漏洞不应当引发TMN严重的可用性劣化。

10.3 体系结构需求

适合TMN框架而采取的安全措施应当满足的最重要的需求包括：

— 安全措施应当基于TMN功能模型所定义的原则。

— 安全措施应当符合面向对象的数据和TMN的信息模型。

— 安全措施应当应用于TMN的所有域，包括公共部分和私有部分。

— 解决方案应当能够根据TMN规模的大小进行调整。

— 解决方案应当符合相关的TMN参考点的内部体系结构。

— 解决方案应当明确所涉及到所有外部和内部TMN用户。

— 解决方案应当考虑到健壮性。

— 解决方案应当支持当用户或应用程序增加或删除时进行重配置。

安全域和其他功能域发生冲突是不可避免的，例如计费数据的完整性和机密性一定要与电话记录单所需要的超大信息流量相适应。一个值得信赖的安全需求集需要考虑对其他功能域特性的影响。

当分析某一个特定的TMN场景时，可能会出现更深的体系结构方面的需求。

10.4 安全服务和OSI分层

本节描述了由OSI的哪一层来提供安全服务，并显示了他们如何以一种适当的方式提供给TMN。

假设：当我们说OSI的某一层提供安全服务时，是指将安全服务提供给该层之上的一层。在ITU-T X.800建议书中定义了各层所能够提供的服务，应以该建议书为基础对各种可能性进行限制。

10.4.1 用户鉴权

该服务依赖于与用户的交互。因此，在OSI参考模型定义范围之外。

10.4.2 鉴权（对等实体和数据源）

下述各层能够提供该服务（根据ITU-T X.800建议书）：

— 网络层（验证传输层两端实体的身份）；

— 传输层（验证会话层两端实体的身份）；

— 应用层（验证两端应用进程的身份）；

— OSI之外：在应用进程自身内。

考虑到TMN的需求是要通过访问控制对管理者和代理者，以及鉴权链路进行认证和鉴权，因此建议该服务所在的OSI协议栈的层次为应用层和应用进程自身。

10.4.3 访问控制

— 管理协会访问控制

该服务可用于存在管理协会的OSI层。可以用在应用层（对应用进程的访问控制）或在应用进程自身。

协会访问控制可以在网络层提供，例如使用X.25闭合用户群业务。此外，协会访问控制可以由应用层或应用进程自身提供。

— 管理通知访问控制

由于应用进程自身能够区分类似管理者和代理者的（应用进程）实体，因此该服务可用于应用层或应用进程自身。

— 管理资源访问控制

由于应用进程自身能够区分类似管理者和代理者的（应用进程）实体，因此该服务可用于应用层或应用进程自身。

10.4.4 安全告警，审计跟踪和恢复

这些服务与其他的服务是相关的，因此这些服务存在于其他服务所在的层。

10.4.5 完整性

— 选择字段完整性

由于应用进程自身能够区分不同的字段，因此该服务可用于应用层或应用进程自身。

— 有恢复连接完整性

该服务可由传输层、应用层或应用进程提供。

— 无恢复连接完整性

该服务可由网络层、传输层、应用层或应用进程提供。

10.4.6 机密性

— 选择字段机密性

由于应用进程自身能够区分不同的字段，因此该服务可用于应用层或应用进程自身。

— 连接和无连接机密性

考虑到需要端到端的机密性，不包括物理层和数据链路层，机密性可由网络层、传输层、表示层、应用层或应用进程提供。

— 数据流机密性

该服务可由网络层、传输层、应用层或应用进程提供。

10.4.7 不可否认

— 不可否认 — 有源端证据；

— 不可否认 — 有交付证据。

该服务可用于表示层、应用层或应用进程自身。

总结如表5所示。

表 5/M.3016.0－安全服务与OSI参考模型的关联

	层 次						
服 务	**1**	**2**	**3**	**4**	**5**	**6**	**7**
用户鉴权	–	–	–	–	–	–	+
对等实体鉴权	–	–	+	+	–	–	+
数据源鉴权	–	–	+	+	–	–	+
管理协会访问控制	–	–	+	–	–	–	+
管理通知访问控制	–	–	–	–	–	–	+
被管资源访问控制	–	–	–	–	–	–	+
安全告警，审计跟踪和恢复	+	+	+	+	+	+	+
选择字段完整性	–	–	–	–	–	–	+
有恢复连接完整性	–	–	–	+	–	–	+
无恢复连接完整性	–	–	+	+	–	–	+
选择字段机密性	–	–	–	–	–	–	+
连接/无连接机密性	–	–	+	+	–	+	+
数据流机密性	–	–	+	+	–	+	+
不可否认 – 有源端证据	–	–	–	–	–	+	+
不可否认 – 有交付证据	–	–	–	–	–	+	+

10.5 安全管理

安全管理包括与系统安全相关的所有创建、维护和终止等活动。

包括的主题有：

— 安全服务的管理；

— 安全机制的安装；

— 密钥管理（管理部分）；

— 身份、密钥、访问控制等信息的建立；

— 安全审计跟踪和安全告警的管理。

附 录 一

功能类和安全分简表

I.1 安全措施分组

安全措施可分组为“功能类”（FC）。下述定义不含安全措施的强壮性：

一个功能类是与不同功能级别的需求相适应的安全措施的集合。

I.1.1 功能类在域间的应用情况

TMN的安全不应当仅仅是消极地受域间行为的影响。在域间安全策略中，应当定义域的交互规则。这些规则将定义在什么情况下，应当采用哪些安全措施。为了促进交互的域间达成共识，这些安全措施可以被定义为一种特定的功能类。

I.1.2 功能类在域内的应用情况

在域内情况下，功能类能够简化安全的定义。功能类还可用作安全担保的目的。为了做到这一点，功能类应当与管理产品的厂商所声称的一个担保级别相联系起来。这与正式的评估标准有很强的联系。

一种可能情况是，为了域间交互的目的，一个操作员能够请求另一个操作员为域内交互情况而定义的特定的功能类应用。这么做的原因是，在两个域间接口上，并不是所有的威胁都能被有效地处理好。确保在TMN交互时，存在一个最小的内部安全级别是一种解决方案。TMN的安全标准不应当规定必须要求哪种功能类，但应当能够提供一种可能性，即通过定义适当的选择条款来要求某些功能类。

I.2 功能类

功能类用来定义一个精简的安全服务组，以匹配某种安全级别。本节设计了一个功能类集合作为示例，来显示如何定义一个功能类。X-接口的功能类被定义为三个不同的安全级别：

1） 最小功能类（功能类1）；

2） 基本功能类（功能类2）；

3） 高级功能类（功能类3）。

考虑到实用化目的，功能类的数量不宜太多。另一方面，又应当可能匹配各种不同组织的需求。功能类可能通过下述方式进行修改：

— 仅为X-接口定义的功能类也可能包括Q接口。

— 对所有的类来说，机密性可以是一种可选特性，原因有两个：

- 它是一种次严格的需求；
- 功能类中的必选特性可能对类的可用性具有法律上的隐含含义。

表I.1提供了功能类的概述。

表I.1/M.3016.0－安全服务的功能类

功能类1	功能类2	功能类3
强调已存储的被管资源的完整性	强调已存储的被管资源的完整性和传送中数据的完整性	功能类 2＋ 管理操作的责任制
• 鉴权（对等实体和用户） • 管理协会访问控制 • 被管资源访问控制 • 安全告警，审计和恢复	• 鉴权（对等实体和用户） • 管理协会访问控制 • 被管资源访问控制 • 数据源鉴权 • 选择字段完整性 • 连接完整性 • 安全告警，审计和恢复	• 鉴权（对等实体和用户） • 管理协会访问控制 • 被管资源访问控制 • 数据源鉴权 • 选择字段完整性 • 连接完整性 • 源不可否认 • 目的地不可否认 • 安全告警，审计和恢复
可选项： • 连接完整性 • 连接机密性	可选项： • 连接机密性 • 选择字段机密性	可选项： • 连接机密性 • 选择字段机密性

另外，应当区分适用于域间情况的功能类和适用于域内情况的功能类。两种情况下的需求是不同的，正因为此，安全措施也可能是不同的。

下文部分给出了两种不同情况的一个概述，这样读者可以认识到哪些功能类是必须的，哪些是相关的。

假设

对于每个域，都存在一个权威人士来负责决定本域中应当使用的安全措施。

应区分三种情况：

1） 由域内权威人士定义，且应用于域自身（域内）的功能类；

2） 由域内权威人士定义，且应用于域交互（域间）的功能类。这些功能类将是几个交互的域内权威人士协商的结果；

3） 由域内权威人士定义，但目的是为了其他域的内部安全需求的功能类。

在每种情况下，为不同安全级别而定义的功能类的个数能够确定下来。

安全级别的个数待研究。

构成功能类的安全措施集合待研究。

不同情况下的功能类可能是相同的，这样可以减少总的功能类数目。

还应当考虑到不同情况间的平衡问题，如当某个域间安全处于高级别时，其他域的内部安全需求可能会处于较低的级别，反之亦然。另一种可能性是，一个表示安全措施最小集的功能类，能够通过增加适当的附加措施而进行扩展。

I.3 安全简表

功能类不要求使用标准化的安全机制，只要能符合需求，任何安全机制均可应用。

为了使不同域中的安全措施能够进行交互，安全措施的制定应当符合标准。规定使用哪些特定的标准来共同提供一个功能类的描述，被称为一个安全简表。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	**电信管理，包括TMN和网络维护**
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2005年，日内瓦