国 际 电 信 联 盟

ITU-T M.3016.2

国际电信联盟
电信标准化部门

(04/2005)

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：安全服务

ITU-T M.3016.2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.3016.2建议书

管理平面的安全：安全服务

摘　要

本建议书确定了电信管理中管理平面的安全服务。主要关注于网元（NE）和管理系统（MS）管理平面的安全特性，NE和MS是电信基础设施的一部分。

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4月13日批准了ITU-T M.3016.2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”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

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

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

目 录

引言

电信网是全球通信和经济的重要基础设施。为控制此基础设施的管理功能提供适当的安全是必需的。电信网络管理安全有很多标准存在。然而遵循程度较低，而且在不同的电信设备和软件组件中是不一致的。本建议书确定了安全服务，允许设备提供商、代理及业务提供商能够实现一个安全的电信管理基础设施。尽管目前这些安全服务和安全机制已经代表了当前对技术状态的理解，但技术在不断发展中，条件也会发生变化，为了更加成功，本建议书必须根据条件的变化而发展。本建议书应作为一个基础，业务提供商可能包括附加的安全服务和机制来满足他们特定的超出本建议书所涉及的需要。

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.3016.2建议书

管理平面的安全：安全服务

1 范围

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。

本建议书确定了电信管理中管理平面的安全服务需求。主要关注于网元（NE）和管理系统（MS）管理平面的安全特性，NE和MS是电信基础设施的一部分。

本建议书为通用建议书，不是针对电信管理网（TMN）中的某一个特定接口的安全需求。

本建议书将不定义安全需求或是支持安全服务需求的安全机制。

本建议书是M.3016.x系列建议书的一部分。安全需求、安全机制和简表文稿在M.3016.x系列建议书的其他部分中确定。

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), *Telecommunication networks security requirements*.

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

— ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 定义

本建议书采用ITU-T X.800建议书中规定的下列术语：

— 访问控制；

— 鉴权；

— 机密性；

— 数据完整性；

— 不可否认。

4 缩写

本建议书采用下列缩写：

MS 管理系统

NE 网元

OAM&P 操作、管理、维护和指配

OSI 开放系统互连

TMN 电信管理网

5 约定

在ITU-T M.3016.1，M.3016.2和M.3016.3建议书中，使用描述符来标识不同的需求、服务和机制。描述符由三个字母后带一个数字组成：

— REQ 表示需求；

— SER 表示服务；

— MEC 表示机制。

6 安全服务

图1描述了安全目标、威胁、风险、安全需求和安全服务之间的关系。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”。

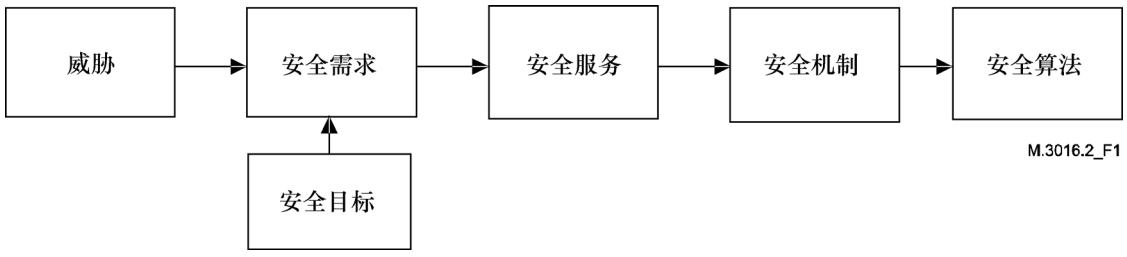

图1/M.3016.2－安全框架

下面的表1复制自ITU-T M.3016.0建议书（ITU-T M.3016.0建议书中的表4）。该表概述了安全需求和安全服务间的关系，并且作为本系列建议书中其他建议书组织的基础。例如，ITU-T M.3016.1建议书讨论

了安全功能需求，本建议书（ITU-T M.3016.2建议书）讨论了安全服务、ITU-T M.3016.3建议书讨论了适应安全服务的特定的安全机制。

本节仅定义了标准解决方案所涵盖的安全服务，其他可能的服务（如拒绝服务的检测）将不予考虑。

表1/M.3016.2－安全需求和安全服务间的映射

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

表2简要描述了本节的组织：

表2/M.3016.2－第6节的组织

节　　号	内　　容
6.1	讨论鉴权服务，包括用户鉴权、对等实体鉴权和数据源鉴权。
6.2	讨论访问控制服务。
6.3	讨论数据机密性服务。
6.4	讨论数据完整性服务。
6.5	讨论不可否认服务。
6.6	讨论审计跟踪服务。
6.7	讨论安全告警服务。

6.1　鉴权

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（PINs）（简单鉴权）和基于密码的方式（强鉴权）。

鉴权在确保**管理平面**的安全中有两个用途：

1） 确保了通信各方的身份，提供了建立通信双方间具有完全的数据完整性和机密性的私密通信的基础；和

2） 提供了记录事件日志到管理系统中，和/或在任何系统中对管理活动进行审计的基本机制。

下述各层可提供该服务（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。

6.1.1 用户鉴权

用户鉴权所关注的是对网络管理活动中包含的客户的**鉴权**。通过这种方式，**鉴权**证明了合法用户的身份，同时阻止了非法用户的伪装侵袭。通过适当的**鉴权**，使得跟踪活动，并限制用户进行非授权操作，扮演非授权角色成为可能。

服务1：每个提供用户访问的NE/MS应当支持强鉴权服务以验证身份。

应当注意的是，本建议书没有要求独立的签名服务，但在后续的建议书中可能会要求提供。然而，如果建立签名服务后，协议仍然会对信任书实体提出挑战。一个用户如果以某种方式安全隐藏的话（如一个Kerberos机制），他可能不必输入信任书。

6.1.2 对等实体鉴权

对等实体**鉴权**关注的是对通信的对等实体的**鉴权**，通信的实体可能包括应用程序、系统或设备。**鉴权**认证了对等实体的身份，并且阻止了非法设备的伪装侵袭。

对等实体**鉴权**在系统间（如系统到系统、应用程序到应用程序）进行数据通信时提供**鉴权**，是建立具有完全的数据完整性私密通信的基础。在数据通信过程中，对发送实体的**鉴权**使得消息的接收者可以确定消息源。在一个安全的通信通道中，基于密码的**鉴权**应当与每个消息相联系，来将发送实体的身份与消息绑定起来。接收者检查消息中提供的密码信息，来验证发送实体的真实身份。

服务2：每个提供系统间数据通信的NE/MS均应当支持对通信的对等实体**鉴权** ，并且应当使用X.509建议书规定的基于信任书的系统来进行**鉴权**或进行**受保护的鉴权**。

6.1.3 数据源鉴权

数据源**鉴权**是建立证据，以验证系统实体的身份，该实体声称其为所接收的数据的来源。这种**鉴权**证实了数据源确实是所声称的数据源。该服务经常与数据完整性服务一起提供。该服务独立于源端和接收端的任何连接，并且所怀疑的数据可能是过去任何时间所发起的。

服务3：每个提供系统实体身份与数据源证明的NE/MS应当提供数据源**鉴权**服务。

6.2 访问控制

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。根据空闲超时、或修改口令等要求，可能需要再鉴权。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）；

— 将时间与已鉴权实体和他们鉴权所使用的令牌相联系起来的方法。

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。

服务4：每个NE/MS应当支持管理联盟、管理通知和被管资源访问控制服务。

6.3 数据机密性

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**。

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

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。

— 连接与无连接机密性

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。

服务5：每个NE/MS应当提供数据机密性服务以保护面向连接和无连接的数据交换的非授权泄漏，并且对所选择的字段提供机密性。

6.4 数据完整性

一个TMN应当能够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）和重现。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。

数据完整性服务要求使用仅有通信双方知道的加密值。多个协议都使用该加密值创建一个HMAC-MD5 摘要，这个摘要被加到每个消息中。

服务6：每个NE/MS应当支持数据完整性服务来保护交换数据不被修改、删除、插入和重现。

6.5 不可否认

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。

服务7：每个NE/MS应当支持不可否认服务，以确保没有实体能够否认他们的行为和由这些行为引起的后果。

6.6 审计跟踪

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。同时，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。

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。

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。

重要的是，每个NE/MS应提供足够的能力允许调查、审计和实时检测并分析事件，这样才能够实施正确的补救措施。本节考虑了安全审计日志，然而， 安全审计日志的更详细的内容和格式不在本建议书的定义范围之内。

注意：调查和分析事件可能包括对与OAM&P 消息相关的非安全事件的调查，同时也包括对本节所描述的存储在安全审计日志中的信息的调查。将与OAM&P 消息相关的非安全事件，有时又称为“最新修改”的消息记入日志，对所有可审计的行为来说是必须的。

服务8：NE/MS应当能够将任何修改了安全属性和服务、访问控制、设备配置参数、每次登录企图以及相应的引起系统调用去活计时器的结果、以及任何需要审计的事件记录到日志中。每个NE/MS应当支持对这些日志进行审计的能力。

建议由NE/MS对审计日志记录加上顺序标签，并进行密码鉴权后，将审计日志记录发送到一个不能变更的审计服务器中。

6.7 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。

服务9：每个NE/MS应当支持告警通知服务提醒安全管理员与安全相关的操作条件。

6.8 分组检测

一个TMN应当提供能力对基于分组的，流向任何TMN设备管理平面的流量进行分组检测。用户应当能够定义过滤条件，过滤条件可以基于资源和目的网络地址，协议和分组的源端口及目的端口等来定义。

分组检测是一个过程，根据确定的匹配条件来检查每个流经网元的分组的头。可针对分组检测后的结果执行某种操作。

服务10：每个NE/MS应当支持分组检测服务，来保护TMN的管理平面中没有不匹配安全策略的业务流。

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