国 际 电 信 联 盟

ITU-T M.3016.1

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：安全需求

ITU-T M.3016.1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.3016.1建议书

管理平面的安全：安全需求

摘　要

本建议书确定了电信管理中管理平面的安全需求。主要关注于网元（NE）和管理系统（MS）的管理平面安全特性，NE和MS属于电信基础设施中的一部分。

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.3016.1（2005年）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需求，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。尽管目前这些需求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需求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：轮廓文稿。

ITU-T M.3016.1建议书

管理平面的安全：安全需求

1 范围

ITU-T M.3016.1-3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、业务和机制，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 1-3建议书不指定某项安全需求、业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需求。主要关注于网元（NE）和管理系统（MS）的管理平面安全特性，NE和MS属于电信基础设施中的一部分。

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。

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。

1.1 目标

ITU-T M.3016.0建议书明确了管理网络安全的多个目标，并明确了对网络造成威胁的方面，介绍了达到这些目标的风险。本建议书所定义的安全需求源自上述安全目标，并且定义了安全服务以应对这些威胁。在定义安全服务时，将使用基于特定算法的安全机制。本系列建议书中的其他建议书都建立在ITU-T M.3016.0建议书概述所建立的体系结构上。各建议书细化了管理平面中所需安全的各个不同的步骤。

1.2 与X.805所定义的安全体系的关系

ITU-T X.805建议书定义了端到端的网络安全体系结构。X.805所定义的安全体系结构将一个复杂的端到端的网络安全特性集，从逻辑上划分成三个不同的结构组件，分别为：安全空间、安全层次和安全平面（见图2/X.805）。一个安全空间包括一系列的安全措施，用来针对某个特定的网络安全特性。ITU-T X.805建议书定义了三个安全层次，分别为：基础设施安全层、业务安全层和应用安全层，每一层都构建在另一层的基础之上，以提供基于网络的安全解决方案。一个安全平面包括一类网络活动，这些网络活动由安全空间来保护。X.805建议书定义了三个安全平面，分别为管理平面、控制平面和端用户平面。为提供一个完整的解决方案，安全措施（如访问控制、鉴权等）需要应用到网络基础设施、网络业务和网络应用的每一类网络活动中（如管理平面活动、控制平面活动和端用户平面活动等）。本建议书则主要关注于网元（NE）与管理系统（MS）的管理平面中的安全特性，NE与MS属于网络基础设施的一部分。

1.3 与E.408所定义的电信网络安全需求的关系

ITU-T E.408建议书提供了一个安全需求的概述，确定了一个通用的威胁电信网络安全的框架（包括固定网络和移动网络、涉及话音业务和数据业务等），同时给出了如何制定安全对策的指南，这些安全对策

可用来减轻各种威胁所带来的风险。这是一个通用的建议书，不针对某一个特定的网络需求。M.3016.x系列建议书确定了电信网络的安全需求、安全服务和安全机制，即电信管理中的管理平面。

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 G.8080/Y.1304 (2001), *Architecture for the automatically switched optical network* (*ASON*), plus Amendment 2 (2005).

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

— ITU-T Recommendation M.3013 (2000), *Considerations for a telecommunications Management network.*

— ITU-T Recommendation M.3016.0 (2005), *Security for the Management Plane： Overview*.

— ITU-T Recommendation M.3016.2 (2005), *Security for the Management Plane： Security services*.

— ITU-T Recommendation M.3016.3 (2005), *Security for the Management Plane： Security mechanism*.

— ITU-T Recommendation M.3016.4 (2005), *Security for the Management Plane： Profile proforma*.

— ITU-T Recommendation X.509 (2000), *Information Technology – Open Systems Interconnection： The Directory： Public-key and attribute certificate frameworks*, plus Technical Cor.1 (2001), Technical Cor.2 (2002) and Technical Cor.3 (2003).

— ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*, plus Amendment 1 (1996), *Layer Two Security Service and Mechanisms for LANs*.

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

— IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

3 术语和定义

本建议书采用ITU-T G.8080/Y.1304建议书中规定的下列术语：

— 控制平面；

— 管理平面；

— 传送平面。

本建议书采用ITU-T M.3010建议书中规定的下列术语：

— 管理系统；

— 网元。

本建议书采用ITU-T M.3013建议书中规定的下列术语：

— 网元管理系统.

本建议书采用ITU-T X.509建议书中规定的下列术语：

— 强鉴权。

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。

本建议书规定下列术语：

3.1 关键的安全管理活动，包括但不限于如下方面：

a） 定义和分配用户权限；

b） 增加和删除用户 ID；

c） 去活某特定用户 ID，使之不能作为登录 ID；

d） 初始化和重新设置登录口令；

e） 初始化和修改密钥；

f） 设置系统登录口令的有效期限；

g） 设置每个登录用户 ID 允许的登录失败的次数限制；

h） 去除锁定，或者修改系统的锁定定时器值；

i） 设置系统的去活定时器值；

j） 设置系统的安全日志和告警配置；

k） 管理系统安全日志流程；

l） 升级安全软件；

m） 终止任何用户或系统会话。

4 缩写词和首字母缩略语

本建议书采用下列缩写词：

AAA	鉴权,授权与计费
ACS	访问控制服务器
ALE	年度损失期望值
ANSI	美国国家标准协会
CO	中心局
CORBA	公共对象请求代理体系
CSI	公共安全协同能力
DoS	拒绝服务
EMS	网元管理系统
FTP	文件传输协议
HAZMAT	危险物资

HTTP	超文本传输协议
IETF	互联网工程任务组织
IP	互联网协议
IPsec	互联网协议安全
ISO/IEC	国际标准化组织/国际电子技术委员会
ITU-T	国际电信联盟电信化标准部门
LAES	合法授权的电子监测
MS	管理系统，含任何EMS、NMS或OSS[1]
NE	网元
NE/MS	网元或管理系统
NMS	网络管理系统
NTP	网络时间协议
OAM&P	操作、管理、维护和指配
OASIS	先进的结构化信息标准组织
OEM	原始设备制造厂商
ORB	对象请求代理
OS	操作系统
OSS	运营支持系统
RFC	征求意见
SAML	安全声明标记语言
SNMP	简单网络管理协议
SOAP	简单对象访问协议
SSH	安全外壳
SSL	安全套接层
TCP	传输控制协议
TLS	传输层安全
TMN	电信管理网
XML	扩展标记语言

5 约定

在ITU-T M.3016.1-3建议书中，用一个描述符来表示不同的需求、服务和机制。描述符的组成包括下述三个字母，后带一个数字：

— REQ：表示需求；

[1] 在电信管理网体系的任何层上，OSS通常可在与MS相同的上下文中使用。

— SER：表示服务；

— MEC：表示机制。

6 安全需求

本节包括操作、管理、维护和指配（OAM&P）的安全需求，以及**管理平面**的运营支持系统（OSS）的安全需求。

图1/M.3016.0描绘了安全目标、网络威胁、风险、安全需求以及业务之间的关系。并且描述了如何将“安全需求”从“网络威胁”和“安全目标”中分离出来，并由一系列的安全服务实现的过程。这些对抗网络威胁的“安全服务”将使用“安全机制”，而安全机制又将使用“安全算法”来实现。表1（即M.3106.0建议书中的表4）给出了安全需求和安全服务间的关系。本节中所描述的安全需求根据表1来组织，如下所示：

— 身份认证；

— 受控访问和授权；

— 机密保护;

— 数据完整性保护；

— 可追溯性；

— 安全日志和审计；

— 安全告警上报。

注 — 违反安全后的恢复是需要再研究的领域。

表1/M.3016.1－安全需求和安全服务间的映射
（表4/M.3016.0）

功 能 需 求	安 全 服 务
身份认证	用户鉴权 对等实体鉴权 数据来源鉴权
受控访问和授权	访问控制
机密保护 — 存储的数据	访问控制 机密性
机密保护 — 传输中的数据	机密性
数据完整性保护 — 存储的数据	访问控制
数据完整性保护 — 传输中的数据	完整性
可追溯性	不可否认
活动记录到日志中	审计跟踪
安全告警上报	安全告警
安全审计	审计跟踪

6.1 身份认证

鉴权在**管理平面**的安全中有两个目的：

1） 它确保各通信方的身份合法，是两个系统间建立一个具有完全的数据完整性和机密性的私有通信的基础；

2） 它提供登录到一个管理系统中的基本机制，和/或对任何系统中的管理活动进行审计的基本机制。

6.1.1 用户鉴权、口令和用户ID

用户**鉴权**涉及网络管理中包括的所有客户的**鉴权**。在这种情况下，**鉴权**证实了合法用户的身份，同时也预防了非法用户的伪装入侵。通过适当的**鉴权**，使得跟踪用户活动成为可能，并且限制了用户进行任何未授权的活动或扮演任何未授权的角色，6.3节将对此展开论述。

对**鉴权**的最低需求是使用用户ID和静态的**复杂口令**。还有一些另外的机制，这些机制使用的历史可能与NE/MS管理的历史同样长，并且要确保其提供的安全层次至少与用户ID和静态**复杂口令**所提供的安全层次一样强壮，这些可能被考虑过的另外的机制包括：

— 一个用户 ID 和使用一个口令生成器的**双重鉴权** [2]；

— 使用一个灵便卡的**双重鉴权**，该灵便卡中以一种受保护的方式存储有证书。

需求 1： NE/MS 登录、记录日志和审计时，应当支持强**鉴权**。

需求1提出了安全需求。通用的**鉴权**机制的描述由ITU-T M.3016.3建议书给出。所期待的是**鉴权**技术和个人签名技术可以继续得到改进。

可靠的个人签名协议仍然需要面对信任书实体的挑战；然而，一个用户可能不必一定要敲入信任书，因为这些信任书是以某种方式被安全隐藏的（如Kerberos）。

下面的需求可维护口令的复杂性，并在审计和记录日志时起到相应的作用。

需求 2： 每个 NE/MS 都应当根据组织策略强制进行**鉴权**。

需求 3： 每个 NE/MS 都应当根据组织策略支持为**鉴权**制定的最低复杂度的规则。

需求 4： NE/MS 应当防止其他的用户在用户不知情的情况下修改已登录用户的口令。

需求 5： 每个 NE/MS 应当自动确保任何一个新的登录口令都不同于之前设置的口令。不同的程度应当可以根据组织策略进行配置。

一般来说，由于口令都是通过一个单向的加密方式存储的，因此旧口令的入口也需要允许NE/MS判断新旧口令间的不同程度。

需求 6： 每个 NE/MS 应当防止口令的重新使用。防止口令重复使用的参数，应当可以根据组织策略进行配置。

需求 7： 每个用户 ID 应当拥有其自己设置的登录口令。

需求 8： 口令应当可以根据用户自身需求进行修改，但两次修改间需要有相隔一个最小的时间间隔。最小时间间隔应当可以根据组织策略进行配置，并且应当由**系统安全管理员**进行设置。

---

2 本节不讨论动态口令，因为已经超出了本建议书的范围。

需求 9： 每个 NE/MS 应当支持多层次的口令控制。某些用户可以被锁定（如：根据口令的有效期限或登录失败次数等），而另一些用户不能被锁定。

6.1.2 缺省鉴权

关于合理地使用缺省口令已经在安全文献中被详细讨论过了。在历史上，缺省的口令可以是直接编写在程序中的硬编码、也可以与每个软件版本和每次升级相关。如下所述为缺省鉴权的需求：

需求 10： 应当应用如下情况中的一种：

- 配置软件应当为新版本或新升级后的软件中的每个应用程序产生一个唯一的独特的初始化口令[3]。
- 如果一个缺省的口令在使用，系统应当要求在设备投入使用前将该缺省的口令替换为一个唯一的独特的口令。
- 如果设备在交货时尚无口令或是一个空口令，则在设备投入使用前的初始化过程中应当被分配一个唯一的独特的口令。

需求 11： 系统登录口令的有效期限应当可配置，如果该功能仍包括在应用程序中。当有效期限过期时，受影响的应用程序的登录口令应当被重新设置为‘需求 10’中所定义的初始的缺省状态。在这种情况下，所有用户修改口令的权限将被收回，仅一个用户除外，即系统中或应用实例中拥有最高级别安全权限的用户。

需求 12： 系统去活定时器值应当可配置，如果该功能仍包括在应用程序中。当系统去活定时器激活时，应当阻止给定用户 ID 对系统的访问，该用户的登录过程将被去激活，不能够登录到系统中。

需求 13： 系统限制用户登录的连续失败次数应当可配置，如果该功能仍包括在应用程序中。当系统限制的用户登录连续失败次数到达时，‘需求 12’中定义的系统去活定时器将开始被调用。

6.2 受控访问和授权

每个NE/MS必须支持“最小权限”思想（即：一个人处于某种角色中，将可被授权去读数据、修改数据或是发起**管理活动**等，且这些活动仅可用于该角色所被允许的功能中）。本节定义了通过良好的系统安全管理实现“最小权限”的基本需求。

6.2.1 安全管理

每个NE/MS必须确保仅仅是授权用户才被允许管理系统安全资源。所有的管理活动都需要与用户角色相关联，而这些用户角色被分配给每一个特定的用户。本建议书仅讨论其中的一部分类型的用户角色，尽管其他类型的具有各种不同权限级别的用户角色也可能存在，主要是讨论关于关键的安全**管理活动**，目标是确保仅有授权的、具有相应权限的用户能够管理关键的安全资源。

需求 14： 每个 NE/MS 应当支持多用户定义类型的用户角色，且**管理活动**被分配到每个用户角色。

---

[3] 这类似于每个新购买的CD都带有一个唯一的口令。

用户角色可能会导致角色的层次性，即每个被分配有不同的或较小任务的用户角色，将比权限多的用户角色拥有更少的权限。这种层次性的例子是：一个用户角色拥有执行所有**管理活动**的能力，类似于计算机中的“超级用户”；而另一个用户角色仅仅支持读操作，以便完成对设备的监视，类似一个操作员。

需求 15： 每个 NE/MS 应当支持一个缺省的用户类型，该用户类型拥有最小的或受限的**管理活动**。

需求 16： 每个 NE/MS 应当支持如下**关键的安全管理活动**，但不局限于此：

- 定义和分配用户和用户组的权限。
- 维护登录到系统中的 ID 的所有操作请求的记录。
- 增加和删除用户 ID。
- 去活和激活某个特定的用户 ID 可作为登录 ID 使用。
- 初始化和设置登录口令。
- 初始化和修改密钥。
- 设置系统的登录口令的有效期限。
- 设置每个登录用户 ID 允许的登录失败的次数限制。
- 去除锁定，或者修改系统的锁定定时器值。
- 设置系统的去活定时器值。
- 设置系统的安全日志和告警配置。
- 监视所有的系统安全日志。
- 管理系统安全日志流程。
- 升级安全软件。
- 终止任何用户或系统会话。
- 向其他角色的特定用户委托安全授权。
- 设置口令的复杂性规则。

需求 17： 每个 NE/MS 应当支持如下的应用程序安全**管理活动**，但不局限于此：

- 定义和分配应用程序级别的新用户和新用户组权限。
- 维护登录到应用程序中的 ID 的所有操作请求的记录。
- 增加和删除应用程序级用户 ID。
- 监视所有的应用程序级安全日志。
- 配置应用程序级安全日志和告警。
- 管理应用程序级安全日志流程。
- 终止用户应用程序会话。

6.2.2 NE/MS的使用和操作

本节所定义的需求可应用于对NE/MS的远端访问和本地控制台访问。这些必选的需求是对实际存储有用户ID和口令的NE/MS的基本要求。许多NE/MS都倾向于使用一个集中式的访问控制服务器（ACS）来存储用户ID和口令。本建议书所描述的必选需求可应用到存储有用户ID和口令的NE/MS，也可应用到存储在ACS中的用户ID和口令。

需求 18： NE/MS 应当以一种经过鉴权的方式进行时间同步（如 NTP 第 3 版）。

需求 19： 对于一个 NE/MS，每个**管理活动**应当与一个单独的授权会话相关联。

需求 20： 每个会话应当通过合法的**鉴权**而建立，对鉴权的描述见需求 1。

需求 21： 一个 NE/MS 与一个 ACS 间为传送经**鉴权**后的信任书而进行通信时，应当通过一个**可信任的路径**。

需求 22： NE/MS 应当使用**访问控制**和隔离措施来允许、拒绝、或其他的方法来控制用户、用户组或远端系统对 NE/MS 的访问，并且应当提供相应功能来限制用户为完成他们的任务而进行的对数据、事务和设备的必要的访问。访问许可应当包括但不限于：只读和读写。

6.2.3 登录过程

需求 23： NE/MS 应当具备能力为每个独立的用户分配一个登录到某个应用程序或某个主机系统的唯一的用户 ID。

需求 24： 必要时，NE/MS 应当具备下述能力：当一个账户建立后初次访问系统时，或者口令被重置后初次访问系统时，系统应自动强制用户修改口令。

注 — 下述需求（需求25）要求在对网元（NE）进行管理时和对管理系统（MS）进行管理时要有所区分。对网元的管理，要求在进行配置改变时，需要通过多种机制来监视设备，这些机制可能需要是同步的。而对MS来说，这不是必须的。

本需求的目的是管理用户对NE/MS所有可用资源的消耗能力。操作人员应当在需要时为各种不同情况调整NE的缺省值，并且应当监视和调查任何企图要超出这些限定的情形，如可能指示操作不足或企图进行有害的行为等。

需求 25： NE/MS 在适当时候，应当防止、控制或限制同一个用户 ID 同时有多个激活使用。同时激活的会话个数应当能够以每个用户 ID 为基础进行配置。

需求 26： NE/MS 应用程序不应当要求具有**超级用户**的访问权限，以使工作能够正常进行。

需求 27： NE/MS 应当具备能力在登录过程的适当时候将用户上次成功**鉴权**的时间和日前显示给该用户。

需求 28： 在任何一个逻辑访问被允许之前，都应当在初始入口屏幕上显示一个客户化的所有权信息声明和不允许非法侵入的警告信息。设备应当支持的最短长度为 1600 个字符。应当提供一个缺省的信息。

下述为警告语的一个示例：

> 警告！本计算机系统和网络为私有的，并拥有所有权，仅授权用户可访问。任何非授权使用本计算机系统或网络将被严格禁止，并可能付诸法律、对雇员进行惩罚甚至解雇、或终止提供/服务合同。所有者，或其代理人，可能监视计算机系统或网络的任何活动或通信。所有者，或其代理人，可能查询存储在计算机系统或网络中的任何信息。用户在访问或使用本计算机系统或网络时，意味着同

意由于法律或其他目的而进行的监视和信息查询。用户应保证不将私密信息进行传输或存储在本计算机系统或网络中，包括存储在本地或远端的硬盘上，或本计算机系统或网络所使用的其他媒质上。

建议每个实体都显示适当的警告语。

需求 29： 任何一个失败的登录尝试都应当报告给用户，除非登录程序失败或不可用。有些信息，如“不合法的用户 ID”或“不合法的口令”不应报告给用户。

需求 30： 当一个用户超出登录连续失败次数的门限时，NE/MS 应当**锁定**该用户账号，不允许再登录。**锁定**应当包括控制台界面。不应当**锁定**初始支持所有管理活动的缺省账号。

需求 31： NE/MS 不应当具备旁路登录**鉴权**和登录过程的机制。

需求 32： NE/MS 不应当在任何媒体上显示明文的信任书，如口令信息等，包括不能显示在终端屏幕上、不能打印、不能存储在日志记录中等。

需求 33： NE/MS 应当根据配置的门限值强制执行口令的更换。

对需求33的一个通用的，可被接受的实现是，对系统来说当用户使用旧的口令被鉴权通过后，马上要求用户设置一个新的口令。另一个可选方案是，系统可能会要求一个管理者适当地修改口令。如果一个账号很久没有被使用，该账号可被认为处于休眠状态。

需求 34： 如果一个登录口令已经超出了该系统有效期限的限制，则 NE/MS 应当锁定该用户 ID，不允许登录，直到口令被正确修改。

需求 35： 如果一个账号处于休眠状态的时间超出了所配置的门限值，每个 NE/MS 应当产生一个告警警报。

需求 36： 如果一个账号处于休眠状态的时间超出了所配置的门限值，每个 NE/MS 应当在产生去活警报后将该账号去活。去活程序不应当包括**系统管理员**账号、**系统安全管理员**账号和**超级用户**账号。

需求 37： 为了将一个**去活**的登录 ID 重新激活，需要一个适当的已登录的管理员，且该管理员应分配有关键的安全管理活动权限，由该管理员为此登录 ID 初始化并重新设置一个登录口令。

重新激活登录ID的权限可被配置为一个系统范围内角色一级的参数。

需求 38： 为了重新设置一个已**锁定**的登录，并且删除**锁定**条件，需要一个适当的已登录的管理员，且该管理员应分配有关键的安全管理活动权限，由该管理员为此登录 ID 去除锁定，或者修改系统的锁定定时器值。

为一个登录ID去除**锁定**的权限可被配置为一个系统范围内角色一级的参数。

6.2.4 退出过程

需求 39： 每个正常的登录**会话**应当可被用户或去活的系统退出。

需求 40： 当某一个**会话**从最后一次激活后，处于不工作的时间已经超出了系统配置的去活定时器值，则NE/MS 应当退出该正常的登录**会话**。

6.2.5 应用

需求 41： 一个用户的角色类型应当在执行和退出任何 NE/MS 应用程序的过程中保持不变。

用户不能够使用一种控制序列机制，如从Shell到**超级用户**方式；或者，如果一个应用程序失败，它不能将该用户处于拥有更多权限的角色中。如果用户要使用不同的角色，必须重新被鉴权（重新登录）。

6.3 机密性保护

本节指定了加密算法和密钥管理需求，以保证系统和网络的安全。在机密性和完整性业务中，常使用对称算法。对称算法的密钥应当在与鉴权紧密绑定在一起的过程中进行交换。在支持鉴权和密钥交换的业务中，非对称算法也有可能使用。用来产生、存储、分配、销毁和废除这些密钥的方法是非常重要的。另外，某些因素，如密钥长度、密钥选择、算法选择等，对特定密码系统安全的健壮性具有直接的影响。

受保护的鉴权和数据机密性都基于密码基础。密码系统使用一种特定的标准的公开算法，因此允许进行大范围的深入研究，且易于实现。密码系统的“健壮性”基于密码系统所使用的算法，以及使用的密钥长度（即：健壮性归结为解码工程师要发现或猜出某个特定算法所使用的密钥值所需的时间长度）。

安全协议（如IPsec，SSL，SSH）提供具有代表性的鉴权、完整性和机密性机制。其他协议的安全扩展，如简单网络管理协议第三版（SNMPv3）[4]、公共对象请求代理体系（CORBA）、边界网关协议（BGP），以及开放最短路径优先（OSPF）等协议被设计用来提供**鉴权**和完整性。**受保护的鉴权**和完整性在NE/MS之间是必需的，并且在认为适当的地方，机密性也是需要的。

6.3.1 对称加密算法

对称的或安全的加密指的是一个密码系统，在该系统中加密和解密是相同的。对称密码系统要求为每一个共享唯一密钥的个体进行初始排列。密钥必须通过某种安全的方法分发给每个个体，或者由内部产生（如基于一个共享的安全根密钥），因为知道加密方法就意味着知道解密方法，反之亦然。

需求 42： 对于所有的对称型加密应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。

---

[4] SNMPv3也可能提供机密性。

6.3.2 非对称加密算法

在一个非对称的密码系统中，加密和解密的方法是相关但不相同的。其中一个是公开的，而另一个是私有的。公开密钥不同于私有密钥，且没有任何可行的方法从公开密钥中生成私有密钥。公开密钥被广泛地分布，而私有密钥总是保持秘密。非对称加密的使用主要局限于两方面，一是为密钥交换而进行的对称密钥加密中，二是用于数字签名的消息摘要签署中。在密钥交换中，接收方的公开密钥被使用，而在消息摘要签署中，签署方的私有密钥被使用。

需求 43： 对于所有的非对称型加密应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。

需求 44： 对于所有的密钥交换应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。

6.3.3 密钥管理

完全地管理密钥资料是困难和复杂的，因为密钥的管理包括：期满终止、可靠交换、可靠发布、以及密码生成等。IETF RFC 1750（*Randomness Recommendations for Security*）提供了附加的指南。

6.3.4 通信

可靠的通信是现代网络中**管理平面**安全的基础。附件A中讨论了为实现可靠的管理通信所需要的体系结构和协议。本节所定义的必选需求可应用于电信管理网（TMN）中的所有接口。TMN在ITU-T M.3010建议书（电信管理网的原则）中描述。

需求 45： 对于 NE/MS 中每一个携带了任何管理信息流的物理的或逻辑的接口，为保证**管理信息流**的可靠性，NE/MS 均应当配置具有**强鉴权**和密钥保护，以提供机密性、完整性和重放保护。

需求 46： 任何以纯文本方式传输的口令应当必须通过一个**可信任的路径**传输，除非使用一次性的口令机制。如果使用了一次性口令机制，则口令可被以纯文本方式传输，直到不存在中介主机为止。

6.4 数据完整性保护

6.4.1 数据完整性算法

为保证任意长度消息的数据完整性，必须使用加密的消息摘要算法与哈希函数。

需求 47： 对于所有对称的安全的数据完整性应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。

需求 48： 对于所有非对称的安全的数据完整性应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。

6.4.2 NE/MS开发与交付

一个NE/MS的安全依赖于它的整个生命周期。安全是一个产品在概要设计阶段需要考虑的问题，在详细设计、开发、部署和退役等各个阶段仍然是需要考虑的问题。在整个生命周期中进行适当的控制和测试是提供可接受的安全级别的关键所在。第I.5.2节和I.5.3节讨论了附加的在生命周期中需要考虑的事项。

需求 49：所有的软件在交付给业务提供商或其他用户时应适当地包括：密码**鉴权**和完整性保护机制，如数字签名或对称的消息**鉴权**，该内容在 ITU-T M.3016.3 建议书中定义。

需求 50：所有的 NE/MS 在接收软件时应当具备能力解释密码**鉴权**和完整性保护机制，并且在适当的时候检验资源和软件的完整性。

需求 51：所有的软件升级，包括打补丁时，均应当通过**可信任的路径**传输给接收的 NE/MS。

NE/MS应当能够通过电子化方法检测当前软件和硬件的修订级别，并且验证正确的软件/固件配置。

6.5 责任制

责任制的目标是确保任何实体对它所发起的任何操作负责。

需求 52：所有的 NE/MS 应当提供能力确保每个实体不能否认其所执行的任何操作以及由此引起的结果。

另见需求49和需求50所定义的与NE/MS开发和交付相关的责任制需求。

6.6 安全日志和审计

重要的是，每个NE/MS都应当提供足够的能力允许调查、审计、实时检测、分析和保护等活动，这样才可能采取合适的补救措施。本节考虑了安全审计日志，然而安全审计日志的内容和格式的详细定义不在本建议书的定义范围之内。

注意，调查和分析活动可能包括与安全无关的OAM&P消息，以及存储在本节所描述的安全审计日志中的信息。将与安全无关的OAM&P消息，有时也被称为“最新变化”的消息，记入日志，对于可审计的任何活动来说是必须的。

需求 53：NE/MS 应当可以将任何修改了安全属性和业务、访问控制参数、设备配置参数等的活动记入日志。

需求 54：NE/MS 应当提供能力以配置那些**关键的安全管理活动**，并且将其记入安全日志。

需求 55：NE/MS 应当具备能力将下述信息记入日志，包括每次登录尝试和相应的结果；每次退出或会话结束（包括远端或本地控制台）；每次导致调用需求 12 中定义的系统去活定时器的登录尝试以及相应的结果。

建议在加上序列标签并经由NE/MS密码鉴权后，将审计日志的条目发送给一个不变的审计服务器。

需求 56：NE/MS 应当能够通过一个**可信任的路径**进行远端日志记录。

需求 57：每个日志条目均应包括如下信息：

- 要记入日志的事件或活动的描述；
- 发起活动的用户或过程的身份及安全级别；
- 活动发生的日期和时间；
- 适当时（如登录时），给出网络资源和目的地信息；
- 活动的成功或失败指示。

6.7 安全告警上报

某些事件需要上报为安全告警，如参见需求35。然而，确定什么事件需要进行上报不在本建议书的定义范围之内。

需求 58：所有的 NE/MS 均应当提供能力针对选中的事件产生告警通知。

需求 59：所有的 NE/MS 均应当提供能力允许用户定义产生告警通知的事件选择条件。

6.8 DCN的保护

为保护管理基础设施，和通用意义上的数字通信网（DCN），对于网络操作员来说，检查流出DCN和流入DCN的业务流（如从对端网络和客户处来的业务流），并对之采取相应的措施是非常有用的。如，当检测到外面网络发来的分组数据的源IP地址和DCN的地址空间相匹配时，则不允许该分组数据流入DCN。

需求 60：所有基于分组连接的 NE/MS 应当阻止与 DCN 安全策略不匹配的业务流。

附 件 A

安全需求、业务和机制间的映射表

本附件提供了安全需求与ITU-T M.3016.2建议书中所定义的安全服务，以及ITU-T M.3016.3建议书中所定义的安全机制之间的映射表。

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 1：	NE/MS 登录、记录日志和审计时，应当支持强鉴权。	**服务 1，服务 2， 服务 3，服务 8**	**机制 1-机制 13**
需求 2：	每个 NE/MS 都应当根据组织策略强制进行**鉴权**。	**服务 1，服务 2， 服务 3**	**机制 1-机制 6**
需求 3：	每个 NE/MS 都应当根据组织策略支持为**鉴权**制定的最低复杂度的规则。	**服务 1，服务 2， 服务 3**	**机制 1-机制 6**
需求 4：	NE/MS 应当防止其他的用户在用户不知情的情况下修改已登录用户的口令。	**服务 8**	**机制 7-机制 11**
需求 5：	每个 NE/MS 应当自动确保任何一个新的登录口令都不同于之前设置的口令。不同的程度应当可以根据组织策略进行配置。	**服务 1**	**机制 7-机制 11**
需求 6：	每个 NE/MS 应当防止口令的重新使用。防止口令重复使用的参数，应当可以根据组织策略进行配置。	**服务 1**	**机制 7-机制 11**
需求 7：	每个用户 ID 应当拥有其自己设置的登录口令。	**服务 1**	**机制 7-机制 11**

续表

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 8：	口令应当可以根据用户自身需求进行修改，但两次修改间需要有相隔一个最小的时间间隔。最小时间间隔应当可以根据组织策略进行配置，并且应当由**系统安全管理员**进行设置。	**服务 1**	**机制 7-机制 11**
需求 9：	每个 NE/MS 应当支持多层次的口令控制。某些用户可以被锁定（如：根据口令的有效期限或登录失败次数等），而另一些用户不能被锁定。	**服务 1，服务 2,** **服务 3，服务 4**	**机制 20-机制 23**
需求 10：	应当应用如下情况中的一种： • 配置软件应当为新版本或新升级后的软件中的每个应用程序产生一个唯一的独特的初始化密码（这类似与每个新购买的 CD 都带有一个唯一的口令）。 • 如果一个缺省的口令在使用，系统应当要求在设备投入使用前将该缺省的口令替换为一个唯一的独特的口令。 • 如果设备在交货时尚无口令或是一个空口令，则在设备投入使用前的初始化过程中应当被分配一个唯一的独特的口令。	**服务 1，服务 2，** **服务 3**	**机制 7-机制 11**
需求 11：	系统登录口令的有效期限应当可配置，如果该功能仍包括在应用程序中。当有效期限过期时，受影响的应用程序的登录口令应当被重新设置为‘需求 10’中所定义的初始的缺省状态。在这种情况下，所有用户的修改口令权限将被收回，仅一个用户除外，即系统中或应用实例中拥有最高级别安全权限的用户。	**服务 4**	**机制 7-机制 11**
需求 12：	系统去活定时器值应当可配置，如果该功能仍包括在应用程序中。当系统去活定时器激活时，应当阻止给定用户 ID 对系统的访问，该用户的登录过程将被去激活，不能够登录到系统中。	**服务 4**	**机制 7-机制 11**
需求 13：	系统限制用户登录的连续失败次数应当可配置，如果该功能仍包括在应用程序中。当系统限制的用户登录连续失败次数到达时，‘需求 12’中定义的系统去活定时器将开始调用。	**服务 4**	**机制 7-机制 11**
需求 14：	每个 NE/MS 应当支持多用户定义类型的用户角色，且**管理活动**被分配到每个用户角色。	**服务 4**	**机制 20-机制 23**
需求 15：	每个 NE/MS 应当支持一个缺省的用户类型，该用户类型拥有最小的或受限的**管理活动**。	**服务 4**	**机制 20-机制 23**

续表

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 16：	每个 NE/MS 应当支持如下**关键的安全管理活动**，但不局限于此： • 定义和分配用户和用户组的权限。 • 维护登录到系统中的 ID 的所有操作请求的记录。 • 增加和删除用户 ID。 • 去活和激活某个特定的用户 ID 可作为登录 ID 使用。 • 初始化和设置登录口令。 • 初始化和修改密钥。 • 设置系统的登录口令的有效期限。 • 设置每个登录用户 ID 允许的登录失败的次数限制。 • 去除锁定，或者修改系统的锁定定时器值。 • 设置系统的去活定时器值。 • 设置系统的安全日志和告警配置。 • 监视所有的系统安全日志。 • 管理系统安全日志流程。 • 升级安全软件。 • 终止任何用户或系统会话。 • 向其他角色的特定用户委托安全授权。 • 设置口令的复杂性规则。	**服务 4，服务 8**	**机制 20-机制 23**
需求 17：	每个 NE/MS 应当支持如下的应用程序安全**管理活动**，但不局限于此： • 定义和分配应用程序级的新用户和新用户组权限。 • 维护登录到应用程序中的 ID 的所有操作请求的记录。 • 增加和删除应用程序级用户 ID。 • 监视所有的应用程序级安全日志。 • 配置应用程序级安全日志和告警。 • 管理应用程序级安全日志流程。 • 终止用户应用程序会话。	**服务 4，服务 8**	**机制 20-机制 23**
需求 18：	NE/MS 应当以一种经过鉴权的方式进行时间同步（如 NTP 第 3 版）。	**服务 8**	**不适用**
需求 19：	对于一个 NE/MS，每个**管理活动**应当与一个单独的授权会话相关联。	**服务 4**	**机制 20-机制 23**
需求 20：	每个会话应当通过合法的**鉴权**而建立，对鉴权的描述见需求 1。	**服务 1，服务 2，服务 3**	**机制 1-机制 12**
需求 21：	一个 NE/MS 与一个 ACS 间为传送经**鉴权**后的信任书而进行通信时，应当通过一个**可信任的路径**。	**服务 5，服务 6**	**机制 19**

续表

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 22：	NE/MS 应当使用**访问控制**和隔离措施来允许、拒绝、或其他的方法来控制用户、用户组或远端系统对 NE/MS 的访问，并且应当提供相应功能来限制用户为完成他们的任务而进行的对数据、事务和设备的必要的访问。访问许可应当包括但不限于：只读和读写。	**服务 4**	**机制 20-机制 23**
需求 23：	NE/MS 应当具备能力为每个独立的用户分配一个登录到某个应用程序或某个主机系统的唯一的用户 ID。	**服务 1，服务 2，服务 3**	**机制 7-机制 11**
需求 24：	必要时，NE/MS 应当具备下述能力：当一个账号建立后初次访问系统时，或者口令被重置后初次访问系统时，系统应自动强制用户修改口令。	**服务 4**	**机制 7-机制 11**
需求 25：	NE/MS 在适当时候，应当防止、控制或限制同一个用户 ID 同时有多个激活使用。同时激活的会话个数应当能够以每个用户 ID 为基础进行配置。	**服务 1，服务 2，服务 3，服务 4**	**机制 7-机制 11**
需求 26：	NE/MS 应用程序不应当要求具有**超级用户**的访问权限，以使工作能够正常进行。	**服务 4**	**机制 20-机制 23**
需求 27：	NE/MS 应当具备能力在登录过程的适当时候将用户上次成功**鉴权**的时间和日前显示给该用户。	**服务 4，服务 8**	**机制 7-机制 11**
需求 28：	在任何一个逻辑访问被允许之前，都应当在初始入口屏幕上显示一个客户化的所有权信息声明和不允许非法侵入的警告信息。设备应当支持的最短长度为 1600 个字符。应当提供一个缺省的信息。	**服务 4**	**不适用**
需求 29：	任何一个失败的登录尝试都应当报告给用户，除非登录程序失败或不可用。有些信息，如“不合法的用户 ID”或“不合法的口令”不应报告给用户。	**服务 8**	**机制 7-机制 11**
需求 30：	当一个用户超出登录连续失败次数的门限时，NE/MS 应当**锁定**该用户账号，不允许再登录。**锁定**应当包括控制台界面。不应当**锁定**初始支持所有管理活动的缺省账号。	**服务 4**	**机制 7-机制 11**
需求 31：	NE/MS 不应当具备旁路登录**鉴权**和登录过程的机制。	**服务 1，服务 2，服务 3**	**机制 7-机制 11**
需求 32：	NE/MS 不应当在任何媒体上显示明文的信任书，如口令信息等，包括不能显示在终端屏幕上、不能打印、不能存储在日志记录中等。	**服务 8**	**机制 7-机制 11**
需求 33：	NE/MS 应当根据配置的门限值强制执行口令的更换。	**服务 4**	**机制 7-机制 11**
需求 34：	如果一个登录口令已经超出了该系统有效期限的限制，则 NE/MS 应当**锁定**该用户 ID，不允许登录，直到口令被正确修改。	**服务 4**	**机制 7-机制 11**
需求 35：	如果一个账号处于休眠状态的时间超出了所配置的门限值，每个 NE/MS 应当产生一个告警警报。	**服务 4，服务 8，服务 9**	**机制 7-机制 11** **机制 33-机制 37**

续表

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 36：	如果一个账号处于休眠状态的时间超出了所配置的门限值，每个 NE/MS 应当在产生去活警报后将该账号去活。去活程序不应当包括**系统管理员**账号、**系统安全管理员**账号和**超级用户**账号。	**服务 4，服务 8**	**机制 7-机制 11** **机制 20-机制 23**
需求 37：	为了将一个**去活**的登录 ID 重新激活，需要一个适当的已登录的管理员，且该管理员应分配有关键的安全管理活动权限，由该管理员为该登录 ID 初始化并重新设置一个登录口令。	**服务 4**	**机制 7-机制 11** **机制 20-机制 23**
需求 38：	为了重新设置一个已**锁定**的登录，并且删除**锁定**条件，需要一个适当的已登录的管理员，且该管理员应分配有关键的安全管理活动权限，由该管理员为该登录 ID 去除锁定，或者修改系统的锁定定时器值。	**服务 4**	**机制 7-机制 11** **机制 20-机制 23**
需求 39：	每个正常的登录**会话**应当可被用户或去活的系统退出。	**服务 4**	**机制 33-机制 37**
需求 40：	当某一个**会话**从最后一次激活后，处于不工作的时间已经超出了系统配置的去活定时器值，则 NE/MS 应当退出该正常的登录**会话**。	**服务 4**	**机制 7-机制 11**
需求 41：	一个用户的角色类型应当在执行和退出任何 NE/MS 应用程序的过程中保持不变。	**服务 4**	**机制 20-机制 23**
需求 42：	对于所有的对称型加密应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。	**服务 5，服务 6**	**机制 24-机制 26**
需求 43：	对于所有的非对称型加密应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。	**服务 5，服务 6**	**机制 27-机制 28**
需求 44：	对于所有的密钥交换应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。	**服务 5，服务 6**	**机制 38-机制 40**
需求 45：	对于 NE/MS 中每一个携带了任何管理信息流的物理的或逻辑的接口，为保证**管理信息流**的可靠性，NE/MS 均应当配置具有**强鉴权**和密钥保护，以提供机密性、完整性和重放保护。	**服务 2，服务 3，服务 5，服务 6**	**机制 24-机制 32**
需求 46：	任何以纯文本方式传输的口令应当必须通过一个**可信任的路径**传输，除非使用一次性的口令机制。如果使用了一次性口令机制，则口令可被以纯文本方式传输，直到不存在中介主机为止。	**服务 1，服务 2，服务 3，服务 5，服务 6**	**机制 19**
需求 47：	对于所有对称的安全的数据完整性应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。	**服务 5**	**机制 29-机制 30**
需求 48：	对于所有非对称的安全的数据完整性应用程序，算法的健壮性应当与国家的、工业的或组织的策略相一致。	**服务 5**	**机制 31-机制 32**
需求 49：	所有的软件在交付给业务提供商或其他用户时应适当地包括：密码**鉴权**和完整性保护机制，如数字签名或对称的消息**鉴权**，该内容在 ITU-T M.3016.3 建议书中定义。	**服务 7**	**机制 29-机制 32**

续表

M.3016.1 安全需求		M.3016.2 安全服务	M.3016.3 安全机制
需求 50：	所有的 NE/MS 在接收软件时应当具备能力解释密码**鉴权**和完整性保护机制，并且在适当的时候检验资源和软件的完整性。	**服务 7**	**机制 29-机制 32**
需求 51：	所有的软件升级，包括打补丁时，均应当通过**可信任的路径**传输给接收的 NE/MS。	**服务 5，服务 6**	**机制 19**
需求 52：	所有的 NE/MS 应当提供能力确保每个实体不能否认其所执行的任何操作以及由此引起的结果。	**服务 7**	**机制 29-机制 32**
需求 53：	NE/MS 应当可以将任何修改了安全属性和服务、访问控制参数、设备配置参数等的活动记入日志。	**服务 8**	**机制 33-机制 37**
需求 54：	NE/MS 应当提供能力以配置那些**关键的安全管理活动**，并将其记入安全日志。	**服务 4**	**机制 33-机制 37**
需求 55：	NE/MS 应当具备能力将下述信息记入日志，包括每次登录尝试和相应的结果；每次退出或会话结束（包括远端或本地控制台）；每次导致调用需求 12 中定义的系统去活定时器的登录尝试以及相应的结果。	**服务 8**	**机制 33-机制 37**
需求 56：	NE/MS 应当能够通过一个**可信任的路径**进行远端日志记录。	**服务 5，服务 6，服务 8**	**机制 33-机制 37** **机制 19**
需求 57：	每个日志条目均应包括如下信息： • 要记入日志的事件或活动的描述； • 发起活动的用户或过程的身份及安全级别； • 活动发生的日期和时间； • 适当时（如登录时），给出网络资源和目的地信息； • 活动的成功或失败指示。	**服务 8**	**机制 33-机制 37**
需求 58：	所有的 NE/MS 均应当提供能力针对选中的事件产生告警通知。	**服务 9**	**机制 41**
需求 59：	所有的 NE/MS 均应当提供能力允许用户定义产生告警通知的事件选择条件。	**服务 9**	**机制 41**
需求 60：	所有基于分组连接的 NE/MS 应当阻止与 DCN 安全策略不匹配的业务流。	**服务 10**	**机制 42**

附 录 一

附加的安全考虑

后续章节中所详细描述的安全过程从实质上来说仅仅是一个指南。它们不在本建议书所定义的详细需求的范围之内，但在提供一个安全系统时，它们仍然需要被考虑到。在某些情况下，在语言使用中用到了必选口气，然而也仅是为提供一些信息，读者可将其作为一个示例看待。在本附录中提及的协议和建议书还需要继续讨论和投稿。本附录没有任何倾向包括或不包括当前存在的或即将形成的任何标准中的内容。

I.1 应用于企业的操作、管理、维护和指配

当今企业的发展已经远远不同于过去传统的孤立的企业网络。企业发展多地域的商务，横跨大范围的地理区域，因此需要与客户及商务伙伴间进行外网连接。企业必须允许商务伙伴和客户能够访问内部数据，并且基于这些数据进行商务决策。

企业网络可以由企业自身进行开发和管理，也可以从网络提供商处购买作为一个被管理的网络。由网络提供商开发的业务使得企业可以在一个更大的网络环境中管理他们自身的网络部分。

随着产业的发展，企业希望能够访问到告警和性能数据、希望能够配置不同的网络组件等的需求显得越来越必要，因此适当的安全机制应考虑到。这些机制必须提供足够的保护控制，不仅保护企业的被管理网络，还应当保护网络提供商自身的内部网络。内部网络可能与这些企业网络相连接，也可能是电信网络基础设施的一部分。总的来说，本附录所描述的操作、管理、维护和指配的安全需求可完全应用于企业及业务提供商/网络提供商。

I.2 公共对象请求代理体系，简单网络管理协议，扩展标识语言和简单对象访问协议

下述关于公共对象请求代理体系（CORBA），简单网络管理协议（SNMP），扩展标识语言（XML）和简单对象访问协议（SOAP）的安全考虑应当引起重视。另外，还有其他的协议也同样适用，如块数据扩展交换协议。尽管没有提议要对这些协议进行修改，但下述的讨论可用来增强安全性。

I.2.1 CORBA

CORBA的安全服务包括责任人（人或对象）的安全鉴权功能、责任人访问对象的授权功能、安全审计、通信安全、不可否认、以及管理等。然而，所有的这些功能都使用可能对大多数应用程序来说都是具有杀伤力的，一般来说，从可用性和简单性角度出发，应用程序可能仅要求具备基于传输层安全（TLS）（和其之前的安全套接层SSL）技术的通信安全和系统级鉴权功能。甚至有一些应用程序可能没有安全要求。因此下述的几种需求情况可以反映三种可能的选择：

— 没有安全；

— 对象请求代理（ORB）使用 TLS（或 SSL）提供通信安全和系统级鉴权，从实质上说是“会话”安全；

— ORB 使用 CORBA 的安全服务，为用户组或个人用户在访问每个对象或操作时提供通信安全、鉴权、不可否认和访问控制列表。

在CORBA体系框架下附加的安全信息在ITU-T Q.816建议书（基于*CORBA*的*TMN*业务）和ITU-T Q.816.1建议书（基于*CORBA*的*TMN*服务：支持粗粒度接口的扩展）中有定义。

如果CORBA应用于网元/管理系统（NE/MS）间的接口，则应当应用CORBA的安全机制。CORBA安全实现的一致性级别应当明确。下述的讨论提供了关于CORBA安全的指南，而不是尝试去对标准进行推断。当提供基于CORBA的产品或系统时，基本的安全级别如下所述：

— 级别 0：不提供应用级的安全，程序不考虑安全。应当提供鉴权、密码、数据完整性、对象调用授权、审计跟踪、以及安全域管理。

— 级别 1：程序可能考虑安全，即程序在访问一些附加业务时可能会调用一个应用编程接口（API），附加业务如签名验证、对象访问检查、以及写入审计记录等。

— 级别 2：支持数字签名，以保证对事务处理的签名和不可否认。在跨不同的组织间进行操作时，如在商务对商务（B2B）的上下文中，或对等设备网络管理中，这种要求是非常重要的。

公共安全协同能力（CSI）规范通过对规范的整理定义了在使用通用ORB间协议（GIOP）/互联网ORB间协议（IIOP）时安全协同能力的标准：

— CSI 级别 1：初始责任人的身份需要从发送方传递到接收方。

— CSI 级别 2：初始责任人的身份需要从发送方传递到接收方，但是该身份可以委托给另外的对象，因此另外的对象能够模仿用户。

— CSI 级别 3：除将初始责任人的身份传递外，在从客户方传递到目的方时，初始责任人的属性还可以包括其他授权信息，如角色或用户组内的成员。

对提供方来说应负责：

— 完全熟悉所选择的 ORB 技术的安全能力；

— 确保符合本建议书中其他部分所描述的安全需求。

正如其名称所隐含的，CORBA处理的是对象。对象安全指的是通过执行一系列的访问控制规则来防止对对象的非授权使用。CORBA安全确保了用户对他们所针对对象进行的操作是负责任的，并且确保了对象的可用性。

对象安全不同于许多其他方面的安全。通常，开发者不必知道安全的细节，因为安全一般在更晚些的阶段应用，就好像是最后的包装纸。正因为此，某些方面是至关重要的。在CORBA中，名字是可以重复使用的，或根本就不存在，仅有引用存在。可能在定义某个对象的策略时，不需要知道该对象的名字。相类似的，也可能在定义某个对象的策略时，该对象拥有多个名字，因此应用策略时必须不考虑使用名字来确保对象安全。

典型的面向对象系统会具有数万个对象，对每个单独的对象定义安全性是不合理的，因此应当将对象分成组，然后为每个组中具有类似安全需求的对象定义安全策略。

— 端到端鉴权：CORBA 能够将用户的上下文传递到另一个应用程序。在这些系统间建有强壮的可靠关系的场合下，不经过其他验证即接受这些信息是可能的。然而，在不存在其他机制的场合下，为保证另外系统的安全性，与 CORBA 安全紧密耦合是非常必要的。端到端的鉴权是非常重要的，并且提供商是否支持该特性是值得检测的。

— 访问控制：CORBA 支持基于角色的登录思想。且系统总是按照这种特性进行开发，因为这不仅能够降低管理成本，而且还可以简化系统，即配置时会更少出错。

— 加密：在 CORBA 中使用加密法必须遵从本建议书中所规定的需求。在完整性、机密性和登录鉴权时完整地使用加密法应当作为 CORBA 的一种特性，尤其当跨越各种类型的网络进行通信时。

— 策略管理：CORBA 策略管理应负责设置如下信息：域、用户、角色对象访问策略、消息保护策略即审计策略。在域和对象命名设计的各个方面都应当清晰明确。在角色定义时，应清晰定义以确保各职责间有适当的隔离。

I.2.2 SNMP安全

SNMP，一个广泛应用的管理方法，用以管理各种基于处理器的设备，提供如下能力：

— 获取设备配置参数；

— 设置设备配置参数；

— 从被管理设备向中心分析系统发送告警。

在许多已经部署的SNMP版本中，有重大的安全漏洞。在版本1和版本2中，口令（即公共字符串）是通过纯文本方式传递的。另外，尽管已经检测了客户方互联网协议（IP）地址的合法性，一个普通的攻击者仍然能够进行IP地址的欺骗。SNMP的版本1和版本2在一些网络中产生了重大的安全漏洞，因此，SNMP版本1和版本2应当仅仅被用作最后的选择。ITU-T第4研究组（SG4）认为应当建立下面两个新的协议栈：

— SNMPv3 或具有基于传输控制协议之上的 TLS 的 V2C（无访问控制）；和

— SNMPv3，且具备基于用户数据报协议（UDP，作为前转协议）之上的用户安全模式。

在部署SNMP时，版本3是首选的级别。SNMP版本3具有更多的安全机制，应当可被应用到所有的新系统中，版本3提供保护以阻止修改数据、模仿、消息重排，机密性损失等。应考虑下面所述的对策以确保SNMPv3可以安全地访问NE：

— 当一个 SNMP 代理接收到未知源发来的命令时，应当向管理者发出告警信息。

— 应当使用访问控制，以确保 SNMP 消息是由授权的管理者发出的。从其他任何源发来的 SNMP 消息均应被拒绝，并且应根据适当的安全策略进行处理。需要时，可以在设备范围或整个网络范围内锁定非授权请求。

— 不能使用缺省的公共字符串。

— 入侵访问和错误访问应当被记入日志。

— SNMPv3 缺省使用数据密码标准，也可使用更安全的算法。

— 使用 SNMPv3 时，至少应当具备 AuthNoPriv，即提供鉴权但没有传输的机密性保护。一般来说，使用 AuthPriv 更合适（既有鉴权，又有传输的机密性保护）。

— SNMP 代理的日志应当被激活。

— 任何没有明确要求的业务或能力都应去激活，包括 SNMP。

I.2.3 XML

XML标准提供了定义数据结构的语言，当前版本是1.0。版本1.1正处于建议书的检查阶段。先进的结构化信息标准组织（OASIS）安全服务技术委员会正在致力于通过协调各方面的特性扩展XML的安全功能。OASIS正准备将安全声明标识语言（SAML）定稿。SAML基于如下四个声明：

— 鉴权 — 发行者已经对数据进行了鉴权；

— 属性 — 特定的统一的资源标识符，或是定义属性的扩展方案；

— 决议 — 鉴权后，上报合法性；和

— 授权 — 实体被允许访问资源。

XML声明必须包括如下内容：

— 基本信息 — 声明的唯一标识符或名称，一般还包括发行日期、时间和有效期限；

— 要求 — 描述声明使用方法的文件；

— 条件 — 声明可能基于某种条件下有效或无效；和

— 建议 — 提供附加的信息，如用于进行策略决策的声明。

I.2.4 SOAP

SOAP1.1版本是万维网（WWW）协会发布的建议书。SOAP是一种消息格式，而不局限于某个特定的协议。它一般使用超文本传输协议（HTTP），但也可以使用其他协议，如SMTP或文件传输协议（FTP）。当SOAP使用HTTP时，防火墙查看SOAP时，将其认为是HTTP，通常会允许其通过。潜在地，SOAP应该能够被防火墙过滤掉，尽管防火墙并没有意识到是SOAP。然而这种过滤并不简单，很易于出错。过滤是一种挑战，因为加密将所传输数据（即XML）的内容和上下文都隐藏了，而且SOAP没有一种统一的寻址方案或内部结构（即头和方法的名称都是可选的）。

I.3 合法授权的电子监测

电信运营商们应当重视下述的关于合法授权的电子监测（LAES）方面的安全考虑。

LAES活动的安全实施应当是健壮的，并且对任何关键的网元（NE）、运营支持系统（OSS）或具有下文所述的某些例外情况的管理系统（MS）来说都应当是一样的。这些实施是保证LAES活动机密性的必要条件。

— 仅有授权的职员可以参与 LAES 活动。

— LAES 信息，包括目标方身份、法律执行代理、通话内容和通话识别信息等，都应当受到保护不被泄漏给未授权的个人。

— 仅有授权个人可以访问 LAES 命令和过程。

— 需要维护一个最新的授权个人列表，这些授权个人可以访问、维护和管理 LAES 活动、过程和程序。

— LAES 安全活动、策略和程序需要完整地编制文档，并且对授权个人来说是可用的。

— 应当维护 LAES 相关的安全日志和活动记录，并将其存储在可靠的设备中。

— 需要根据文件规定的程序严格执行，以识别和鉴别法律执行代理和处理 LAES 请求。

I.4 物理安全考虑

在物理安全中应当重视下述考虑。在准备安全需求时，物理安全是一个重要的组成部分。许多安全的体系结构都假定物理环境是受保护的，安全的。同时，所有的NE也都是放在一个中心局机房中，在这些机房中，职员们工作在一起，对设备进行操作、指配、管理和维护。职员之间互相认识，外来人员是不可能不被注意地访问这些地点的。然而，当前的环境是很不同的，无线设备可以安装在一个不可靠的环境外部。另外，许多，如果不是大多数的话，中心机房是无人值守的，并且在大部分时间是黑暗的。巡检职员和中心局派遣的职员会定期执行升级和维护任务。当前，每天24小时、每周7天（24/7）的安全守护是很少见的。中心局还有可能被外部人员作为存放工具和设备的便利场所。下面所述为安全的设施的特性：

— 所有人员的进入和退出都应当被记入日志和记录。

— 设备供应商和协作人员应被审查，且他们的进入和退出都应当被记入日志和记录。

— 对 NE 的物理访问应局限于授权职员。

— 同场合工作人员应与负有责任的业务提供商具有相同的访问需求。

— 如果没有受保护的鉴权，即使某人从物理上能够合法地访问中心局，他也不能够从逻辑上访问 NE，控制台，设备的 OSS 等。

— 应监测到未授权的访问，并对其即时进行响应。

— 水、电、电信网络等基础服务应是可用的。

— 场所应处于监视中，包括随机的安全巡检人员的监测，监测和记录门窗开关的告警系统的监测，活动探测器的监测，入侵探测器的监视等，对于一些关键的地点还需要有远端录像监测。

— 监测媒体和日志的保持时长应该有规定。保持时长根据风险级别的不同应不同。

下面的章节提供了关于物理安全的附加信息。关于物理安全问题的详细讨论见《国家通信系统》“公共交换网络安全评估指南”2000年9月。

I.4.1 建筑物的物理安全

各组织常常会根据设施中资产的重要性程度来实现不同级别的机房访问控制。通常，大的企业会单独建立一个高度安全的设施，来存放关键的物理组件，如交换机、数据中心等。所存放的资产的重要性决定了安全的级别。这种判断在发现阶段和资产的评估讨论过程中都在进行。下面各小节包括了为安装高价资产或关键资产的设施进行评估的各条款。对于不太重要的设施，评估工作可以投入少一些。全部的物理安全评估必须决定所需要的保护级别，以及需要实施的相关保护机制的质量。

I.4.1.1 通用建筑物安全

尽管一个建筑物的门和窗常被认为是最主要的进入点，然而根据威胁的不同种类，其他各点（如空气通风孔、入水口、入气口、通信入口、电线入口，以及下水管道等）也必须考虑到。附加的入口点也需要被考虑到，如中心局电缆室，以及其他可能存在引起损害因素的地点。更近一步而言，在本建筑物与公共建筑物之间的缓冲空间必须被考虑到。草坪、景观、照明设备、以及栅栏等应被认为起到第一层的外围保护作用，因为他们可以减缓或阻止对建筑物的偷偷靠近。物理的屏障，如邮筒或大的景观植物等能够被用来阻止汽车、卡车或其他可能引起潜在的破坏性入侵的交通工具的靠近。外部的照相机、及其他监测装置等也可加强或扩大这个缓冲空间的作用。

I.4.1.2 保安、加锁和识别证件

建筑物的保安可保护建筑物的外围，有时也保护内部区域。对于关键设施，必须确保如下内容：

— 所有的供出入该设施的门在任何时候必须或者是加锁的，或者是有保安守卫的。

— 任何不常使用的门，如紧急出口，应有警告器。检查评估时必须确保告警功能正常，且存在对告警做出响应的流程。

— 门应被正确安装，不能够从外部将其移走（如应保护铰链和门闩等不能从外部被损坏）。

— 在出入的高峰期间，入口和出口应有保安守卫。在非高峰期间，门应当被监控，并应存在其他方式的访问控制（如刷卡、打卡、使用钥匙等）。

— 使用某种方式进入未守卫的门时，应要求对进入者进行识别。

— 通过钥匙或其他途径提供访问的无守卫大门应当具备机制防止“尾随”。可以使用陷阱、旋转门或监视器等方式防止尾随发生，或当尾随发生时发出告警信息[5]。

— 对雇佣的保安人员的资格限定、培训以及使用的保持质量的方法等应当是足够的和适当的。尤其对合同保安服务尤其重要，目前这种方法使用很普遍。

— 职员、现场的设备提供商、合同人员、以及其他授权个人在建筑物中应随时持有并显示证件。

— 应为非职员的参观者提供一个临时证件，如参观通行证，并要求明确地显示。

— 应当定义相应的流程和条件，在某些条件下，参观者可以不被陪同地进入和工作，而在另一些条件下，参观者必须有陪同人员。

— 职员的证件应显示一个彩色照片。照片应足够大，当保安需要看时，不需要职员将证件交给保安即可看清。并且应保证照片不能够被改变或替换。照片应当清晰，使保安可以与佩带者进行比对。

— 证件应清晰地显示职员的姓名和其他标识信息（如工号、条形码等）。

— 证件应具有标志或指示以区分职员和其他进入建筑物的非职员。

---

[5] 尾随指的是一个未授权人员跟随一个已授权人员进入打开的门的一种行为。

— 证件应持久耐用，应尽可能地抗磨损、抗损害、抗修改等。

— 证件可包括电子或磁性信息，以可能被读卡器识别。

— 证件可能包括一个灵便卡，可嵌入一些附加信息，如个人信息数据、X.509 建议书中定义的证书等。

— 证件的鉴权和授权系统应当与一个中心安全目录相联系，以允许对访问权限的及时修改和删除。

— 证件应具备能力限制访问公司的某些区域，相反的，适当时候可以设置为具有全权访问权限。

— 应设置一个地址，当证件丢失并被非职员捡到后，可不需要邮资便能将证件邮寄到该地址。

— 公司或建筑物安全应当具备措施将丢失的证件，或者佩带者已经不再允许进入建筑物或公司的证件去活或使之无效。

— 当佩带者终止雇佣，应有相应人员（管理者、建筑物保安、公司安全人员等）保留或毁坏证件，以防止非法使用。

保安不是唯一的对建筑物的内部安全负责的人。授权的所有人经常通过警戒和消极的监测来加强建筑物的安全。将对职员进行评估以决定是否赋予职员权力来挑战非授权人员对受控领域的入侵。一个深入的测试对判断保安或职员在物理安全的重要性方面是否经过正确的培训，以及培训的程度如何，是有价值的。检查者可能企图偷偷通过，或者说服保安通过，或者引诱职员提供方法通过无保安守卫的入口等。

I.4.1.3 物理钥匙和逻辑钥匙的管理

传统的物理钥匙很少在重要设施中使用，因为他们很难盘点并回收，且他们不能提供审计用户踪迹的功能。通常，物理钥匙的使用仅局限于建筑物内部，如储藏室、保管室、电线存储室等。然而，也经常发现在商务活动和安装时使用物理钥匙作为进入建筑物或访问建筑物内部关键区域的首选方式。在这种情况下，下述的预防措施是重要的：

— 必须有严格的流程将钥匙批准分发给个人，包括钥匙的控制，并将访问和分发情况记入日志；

— 钥匙需要各自编号；

— 应维护并审计所有钥匙及其所有者的记录清单；

— 当钥匙丢失后，换锁的标准必须适当；

— 必须对钥匙的记录清单执行周期性审计，并且处理协调矛盾的流程必须适当；

— 当访问不再需要时或授权发生变化后，回收钥匙的流程应适当。

逻辑钥匙（如刷的卡）的程序必须采用相同的标准进行评估。使用逻辑钥匙可简化钥匙的回收、进出记录、以及授权等流程，因为这些系统提供一个中心设备来监视钥匙的使用、分配钥匙权限，去活钥匙等。同样，必须有适当的流程确保当有人离职，或人员访问需求发生变化后，应通知到那些负责维护钥匙清单和经授权可对数据库进行操作的人员。对于具有暗码的锁，一种特殊的逻辑锁，应进行评估以确保暗码不能通过佩带方式识别，也不能将暗码写下来。当入口授权发生变化时，暗码应被修改。

I.4.1.4 设施的功能分离和多层次访问控制

物理安全应用到建筑物的内部区域和周围外部区域。访问那些被认为是敏感的和关键的内部区域时应当受控，由于某些原因，访问他们的内容时是受限的（如包括敏感的数据、经验或设备等），通常：

— 关键的计算机和网络设施应放在具有独立的物理访问控制机制的区域。仅准许确实有必要进行访问的人员访问。

— 必须有适当的流程确保当私有信息不被使用时，应将其保存在一个安全的设施中。常规保存这些资料的办公室和文档室应加锁。保存私有信息的橱柜也应当加锁。

— 所有可能的对关键计算机和网络设施（如控制台、操作中心等）的访问点应当被控制，采用的控制方式应与施加在设施本身的控制方式相适应。

— 应当维护一个上述受控区域的访问记录表。

— 存储关键信息的媒质应加密，或是存放在上锁的、限制访问的区域中。

— 关键系统的物理地址不应当透露给任何不必知情的人员。

对建筑物内部区域的控制可通过隔离角色和职责的方式得到增强，如行政工作人员不应要求访问机构内的计算机房，类似的，工程人员一般不应要求访问文档控制室。应检查评估现存的隔离方式是否合适。另外，如果风险程度需要时，可使用双重入口钥匙或暗码锁。

I.4.2 建筑物公共设施

一个机构的运行很大程度上依赖于公共设施是否有效，如水、能源、电信设施和废物处理等。

I.4.2.1 公用设施（水、能源、电信和废物处理）

没有水、能源、电信和废物处理等公共设施、一个机构则根本不能有效的运行。对这些公共设施的依赖程度经常被低估。评估时，应评价该机构对于这些公共设施发生中断时所计划采取的反应措施。因为公共设施对商务的连续运转非常关键，因此下述步骤是很基本的：

— 能源的供给应当备份，且应放在地理上隔离的地方，以防止能源的意外损失。

— 应急能源应保证连续运转，且应保证比能源断供期的平均时长要更长。发电能力应保证在应急供应将耗尽前得到部署（移动发电机可以是自有的，或承包的）。

— 必须有足够的现场水储藏量（或传输设施），以支持设施中关键部件的连续运转。

— 外部通信必须是主用—备用方式、或是足够强壮以保证在危机时候可正常运行，内部通信也同样，其能力必须足以处理危机级别的业务量。

— 卫生间和下水道设施应在危机时仍正常运作，或应具备适当的快速处理污水的临时安排。

— 计算机机房及其他对环境有要求的区域的空调应当备份，以预防机器失效或出现过载危险。

— 无论何时在使用害怕泄漏或损坏的材料时，上锁的容器应当随时可用。检查时，应跟踪这些材料可能的泄漏路径以确保容器是关闭的。

评估的兴趣在于这些公共设施在建筑物内部的分布。评估时，应当评价公共设施在业务中断时的整体抵抗力，范围从公用设施提供商生成公共服务，到建筑物内部路径的分布。

I.4.2.2 应急设施

检查时，应当评价是否有适当的应急设施，如着火检测和抑制设施、能源调节装置、空气调节装置、通风孔、及关键系统连续运转所必须的其他环境保护系统。这些系统必须发挥作用，以允许：

— 用户撤离建筑物；

— 设备被保护（至少坚持到消防人员或其他人员到来）；

— 设施应保证结构完整；

— 尽可能地保护建筑物内部不受外部环境影响。

应急设施在安全被破坏后是重要的，在发生意外事故或自然灾害时也是同等重要，正如上节所建议的那样。

I.4.2.3 冗余传送和关键设施的物理保护

关键的计算机和通信系统设施应在不影响运行成本、性能和安全的前提下尽可能地在地理上分散放置。另外，通信链路的路由（如重要的局间中继、信令链路等）应当冗余，且在地理上分布，这样在必要时，通信可以很快地通过物理上分布的备用路由重新选路。提供业务的通信网应当以这样的方式设计：即当单点发生故障时，不会有大范围的影响或严重的掉线。

I.4.3 环境和地理上的威胁

应检查关键场所，以确定由于其所在区域可能引起的任何风险，如可能的自然灾害、严重的事故（如化学制品溢出、煤气泄漏等）、能源中断以及相应的问题等。检查时，还应考虑环境因素的影响，如太热或太冷、盐和污染的损害、以及飓风气候等。

地理上的问题包括当地人员的反应（如是否有敌对行为），本地应急服务的响应、提供给现场职员和去工作途中职员的安全性级别等。由于人类的行为和动机会根据局面的动荡情况、政治问题、宗教观点、以及其他因素等发生变化，应当根据预先定义的时间表周期性地重复进行检查和评估。当这些风险存在时，尽管要放弃设施常是不切实际的，但还是应当备份或重新部署这些处于高风险设施中的关键系统和资源。

应当开发一套商务连续性和灾难恢复计划，以指引如何应对上述威胁和问题所引起的事件。计划应包括命令、控制和通信流程，并且应经常进行检查。运行恢复计划还应包括指配和签约承包，以快速响应危险物资（HAZMAT）事件。这些计划还应当考虑到要完全恢复到一个安全的环境可能会在长期的一段时间内不能正常访问设施。潜在的补救措施可能是重新部署到一个备份的设施，或是在过渡期间，由经过危险物资（HAZMAT）培训或装备的人员来操作该设施。

I.4.4 同场合工作流程

当设备属于处于同一个物理场所的不同提供商时，同场合工作是一种流行的情况。从物理安全评估的目的出发，应特别关注的是，提供这样的访问常意味着竞争者（有时是多个竞争者）会要求访问主机提供商的物理组件和设施。在检查评估时应当注意如下：

— 应使用物理屏障来隔离关键设备，然而，同场合工作人员会与对此负责的业务提供商具有相同的访问需求。

— 应具备适当的钥匙分配、计费和审计流程。应具备适当的过程以确保人员的变化能够通过同场合的公司监测到。

— 关键设备和设施不应引起别人的注意。传统的清晰标识重要设备和传输设施的方式（俗称红色标注 [6]）在一个开放环境中已经变为一个潜在的危险，应当避免。

I.5 开发过程

I.5.1 引导程序，安装和故障模式

在引导程序、安装和故障模式的安全流程中，应重视如下考虑：

从最初安装到实现的整个生命周期中，必须完成一些独特的工作。为明确这个问题，必须首先理解开发过程中存在的威胁。这些威胁参见ANSI T1.233-2004（操作、管理、维护和指配－电信管理网接口安全框架）和ISO/IEC 10181建议书（开放系统互连－开放系统安全框架）。通用的开放系统连接性会带来如下威胁：

— 引导程序病毒；

— 未授权的访问；

— 伪装；

— 数据完整性威胁；

— 机密性威胁；

— 拒绝服务；和

— 抵赖。

I.5.2 打补丁过程

业务提供商会与设备提供商签署协议，由设备提供商开发并提供应用程序和安装应用程序的平台，或者，有时仅提供应用程序软件。在后一种情况下，由业务提供商自己将软件安装在他们之前购买的平台上。

设备提供商在普通的软件升级之间，开发补丁程序来修正或修改操作系统（OS）或应用程序，或者二者兼有。在经过适当的测试后，补丁程序将发布给业务提供商。在某些情况下，根据合同规定，应用软件开发者可能打包发布补丁。每6个月发布一次比较常见。

操作系统的补丁不应影响应用程序的运行，但情况并不总是如此。因此，当一个平台提供商发布了一个操作系统补丁时，业务提供商应负责与应用软件提供商证实该发布的操作系统补丁不会影响应用系统的运行。

---

6 有红色标注意味着警告人员该电路非常重要，必须认真看护不能损坏。

当一个应用程序提供商既提供应用程序，又提供硬件平台，但他又不是硬件平台的原始设备制造厂商（OEM）时，硬件平台的操作系统安全补丁由原始设备制造厂商（OEM）发布，在这种情况下，应用程序提供商和业务提供商双方应共同负责注意到该发布的安全补丁，并组织对补丁及时进行测试，以验证该补丁不会影响到应用程序。

为了让应用程序提供商检查评估，必须给打了安全补丁的应用程序分配优先级（按周或按月）。同样，必须建立一个例行程序，当业务提供商与应用程序提供商间交换一个关于安全补丁方面的关注点时，应用程序提供商可通过一种畅通的方式迅速给出适当的响应。另外，应用程序提供商应确保补丁的安装不会破坏之前安装的安全补丁。

当安全补丁的测试发现对应用程序有影响时，应及时采取适当的矫正措施来确定问题，并明确计划来纠正引起应用程序故障的条件，随后再提供安全补丁。

在实现操作系统或应用程序软件的补丁时，应重视如下安全考虑：

— 设备提供商和系统集成商应为经营者提供安全参考文件和培训手册，包括详细的操作系统和应用程序安全功能和流程，以及用户访问流程。

— 应当检验操作系统安全和其他补丁对 NE 和 MS 应用程序是一致的。

— 操作系统软件：仅有 OEM 批准的补丁才可被应用到运行的网元或管理平台操作系统上。

— 管理应用软件：仅有初始管理应用程序提供商批准的补丁才可被应用到运行的管理应用系统上。

— 重大影响的补丁必须及时发布，不必拘泥于定期的补丁分发程序。

— 对软件或配置数据的所有下载或上载都必须通过强壮的数据源鉴权和强壮的完整性保护。理想情况下，通过软件提供商的数字签名，两者都必须提供。另外，软件提供商还可以选择软件或配置数据加密。

— 关于如何获取或合并系统及每个网元中运行的应用软件的最新的安全补丁的流程描述，应当在交付的同时提供。

— 关于在批准向业务提供商发布补丁前对每个安全补丁的测试过程的描述，应当在交付的同时提供。

— 系统软件版本和安全维护补丁版本的后向兼容程度应在交付的同时明确。

— 系统软或过程必须记录所应用的补丁和升级。补丁和升级状态应可被审计。

I.5.3 开发生命周期的安全

一个产品或业务的安全依赖于整个生命周期过程。安全是一个产品在概要设计阶段需要考虑的问题，在详细设计、开发、部署和退役等各个阶段仍然是需要考虑的问题。对于处理敏感信息的产品或业务，甚至可能在产品和业务退役后仍需考虑安全。在整个生命周期中进行适当的控制和测试是提供可接受的安全级别的关键所在。

I.5.3.1 人员管理

安全的一个常被忽略的基本问题是职员的可信赖性。所有进行设计、开发和测试的职员都必须是可信赖的：

— 在关键软件组件的开发和测试中有关的所有职员，包括合同人员，转包者，顾问和雇员等，都必须经过背景检查。

I.5.3.2 安全意识和培训

所有的人员都必须明白安全策略和流程，并明白保护信息资产的必要性。安全中的最弱环节往往是同人相关的。安全意识和培训将很大程度地加强这些最弱环节。安全意识将减少职员进行非授权行为的尝试次数，提高保护控制的有效性，并且帮助避免对计算资源的欺骗、浪费和滥用。

— 应当对所有的职员进行安全意识和培训，包括合同人员，转包者，顾问和雇员等。

I.5.3.3 风险管理

风险管理是信息安全的基础。风险管理被定义为与“事件”相关的确认、分析、控制和损失最小化。确认风险的最主要的步骤包括确认正在实施的威胁、推断已经发生了的威胁、威胁发生的可能频率、以及已经发生威胁的可能性等。风险管理不仅包括保护成本效益的风险分析，还包括对保护的实现、检查和维护。

风险分析将确定风险，并提供相应对策的成本效益理由。这些信息用来影响整个生命周期阶段的决策过程，包括场所的选择、建筑物的设计、建设决定等。为了决定某个安全措施是否正确，需要测定年度损失期望值（ALE）。（安全措施实施前的ALE）–（安全措施实施后的ALE）=安全措施的值。注意：安全措施实施应包括每年为操作和维护所需的费用。

— 应为每个新的产品或业务执行风险分析。风险分析应包括一个正式文档描述了采用的分析方法及分析的结果。报告中至少应明确所有可访问的数据和数据所有者（即公司、互联网业务提供商），风险数据或业务的数量和质量，并确定该威胁对 NE 或 OSS 的潜在的上行或下行影响。

I.5.3.4 需求

— 在产品或业务的需求收集阶段，安全需求应被编制到文档中。

I.5.3.5 设计

— 应在设计阶段明确安全需求，而不是在开始开发后才加进去。

— 应执行安全设计评估，以定位影响安全的设计缺陷。

— 所有的系统访问点都必须很好地编制文档，并且应支持标识和鉴权。

— 违反安全策略对秘密通道或活动通道进行维护是不被允许的。

I.5.3.6 职责分离

在一个可靠的环境中无害的功能，应用到一个不可靠的环境中时，能够产生安全弱点。例如：一个脚本解释器被设计用来检查文档，而一个不可靠的文档能够恶意地利用脚本解释器中的功能，如拷贝文件或删除文件。

— 系统应至少支持三种用户级别：用户、系统管理员/操作员和安全管理员。

— 每种功能应当拥有最小级别的权力来执行工作职责。

I.5.3.7 实现

— 任何可再使用的信息资源（即文件、内存、临时存储器等）在再使用前应当经过净化。

— 开发者应当遵循最佳的安全编程经验（即管理缓冲器，这样不会发生缓冲区溢出）。

— 应对开发、测试和支持环境执行周期性的安全审计。

— 开发环境不应用于非公司的商务活动。

— 在开发、测试和支持系统中，不应输入、使用或分布公共领域的软件，除非其源代码可用，且该源代码已经经过检查，不含恶意代码。

I.5.3.8 文件编制

— 文档应在适当位置标记所有者标识。

— 提供给最终用户的文档必须描述对用户不透明的安全功能，解释功能，并提供使用指南。

— 系统管理员指南应包括如下：

- 关于在运行安全模式时需要受控的功能和权限的警告；
- 审计功能的文件使用；
- 检查和维护审计日志的流程；
- 详细的审计日志结构；
- 审计日志备份和删除流程；
- 可用于审计日志的空闲空间检测的流程。

I.5.3.9 操作系统

操作系统必须能够提供有效的硬件和软件控制，以便对被管理的数据和资源提供适当的保护。对于一个计划的安全体系结构，假设操作系统会对被管理的数据和资源提供所需的安全级别。对于特定的业务提供商的需求来说，这种假设可能需要被检查。如果操作系统不能满足安全提供商的安全需求，则应用软件可能需要被安装在另一个能够提供更高安全级别的操作系统中。

— 操作系统必须安装相应的安全补丁。

— 操作系统必须能够可靠地配置，且在经过有限的安全访问权限配置后才可交付。有许多文献和网元都讨论了操作系统的安全，给出这些列表已超出了本建议书的范围，有几个示例如

Common Criteria 和 OS Protection Profiles。[7, 8, 9]

— 操作系统缺省仅需要激活一个最小的业务集。

I.5.3.10 软件工程

安全是软件工程的一个组成部分。为了开发一个可靠的产品，必须使用可靠的编程技巧和可靠的协议。在最好的安全协议和机制中，会存在不可靠的编程技巧。如果程序员没有正确地管理缓冲区，可能会发生缓冲区溢出，这样可能会提供给用户不适当的更多的权限。

— 软件提供商应遵循正式的文档开发程序，如由软件工程协会开发的能力成熟度模式（CMM）。应该在设计、开发、测试和软件发行时均遵循可靠的基于最佳经验的编程方法。

I.5.3.11 可用性和性能

可用性和性能是安全系统的组成部分。性能的降级到一个点后，系统就不可用了。

— 设计、开发和实现应当使得 DoS 侵袭的影响最小化。

— 设计、开发和实现应确保高可用性。

— 网络的体系机构和实现应不存在失效单点。

I.5.3.12 系统软件

用来操作和维护计算机系统的软件（操作系统，应用程序和管理系统等）必须能被安全地配置和维护。应执行测试以确保组件和安全特性已被健壮地实现并正确地配置。

— 系统软件和中间件产品必须被安全地安装和配置，包括安全补丁的安装。软件必须在经过有限的安全访问权限配置后才可交付。

I.5.3.13 传输

— 应由业务提供商来决定采用哪种可靠的数据传输选择方式。可靠的传输方式选择应在客户方到服务方，及服务方到客户方两个方向都是可用的。

I.5.3.14 安全存储

— 应向业务提供商提供数据安全存储的配置权力。业务提供商应当能够指定哪些领域需要安全地存储。

I.5.3.15 软件保证

软件保证应从两个方面明确：安全特性的测试和潜在的违反安全策略的测试。

— 软件开发组和软件测试组的职责必须分离。

— 安全测试计划、测试流程和测试结果应编制为文档。

---

[7] Common Criteria是一个正规安全评估的国际公认标准（http://www.commoncriteria.org/）。

[8] 信息保证技术框架论坛，操作系统保护框架http://www.iatf.net/protection_profiles/operating_systems.cfm

[9] 国家标准和技术协会，计算机安全资源中心http://csrc.nist.gov/

— 所有的安全特性必须被测试到。

— 测试应当包括定位对安全策略的违反（如对访问控制的攻击）。

— 作为测试的一部分，应检验新开发的系统或应用程序不会对已存在的体系结构、公共网络和系统等带来攻击。

— 应执行对安全编程技巧的检验，检验可通过源代码检查或通过软件工具。

— 所有的安全缺陷必须被修正、删除或抑制，且系统应被重新测试。

I.5.3.16 包装和交付

必须在产品的整个生命周期使用一个软件配置管理系统，来维护控制源代码和文档的变化。

— 开发人员不必维护软件配置管理系统。

— 开发人员不应当访问产品系统，除非在受控的紧急指配下，且应被批准并记入日志。

— 仅有授权的代码和代码的修改能够被加到已经交付的源基线中。

— 所有的修改必须编制文档并被检查评估。

— 必须存在工具或流程来从源代码中产生一个新的系统版本。

— 必须存在工具或流程来保护源代码不被未授权的修改。

— 必须存在工具或流程来检验所使用的源代码模块具有适当的版本和级别。

— 产品必须包含完整性机制，可以检验已安装的软件是否与交付的软件相一致（即没有做非授权的修改）。

— 当机械扫描工具有效时，在操作系统或应用软件升级或进行重大修改后，必须对弱点进行完全扫描。

— 安全缺陷的补救或“修理”必须及时提供，并与威胁相适应。

— 必须存在主数据库包含所有交付软件的拷贝。软件必须具有版本号和与操作系统和硬件相适应的规格说明书。

I.5.3.17 安全安装、配置和操作

— 应当为软件定义安全配置参数。

— 应当为软件定义安全操作流程，并编制文档。

— 软件的所有的远端支持应当通过可靠的方式执行。

— 所有随同系统交付的缺省的用户 ID 应在交付时处于去活状态，需要管理员/软件安装人员使用显式地动作来激活。

— 所有的安装过程应可靠，不应当依赖信任关系（即共享驱动器）。

附 录 二

框架和设计指南

II.1 框架和模型

在本建议书的上下文中提到“让某事安全”意思是保护它（如计算机、网络、数据或其他资源等）不受未授权的访问、使用或操作。数据丢失、拒绝服务（DoS）、剽窃服务等仅仅是由于安全事故引起的结果。系统和网络管理者需要保护系统和它的组件单元不受内部或外部用户的攻击。尽管安全是多方面的（范围包括操作、物理、通信、过程和人员等），这里关注的是由于部署配置和技术中固有的共同弱点而引起的安全问题。威胁包括，但不限于：泄漏、未授权使用、信息元素修改、拒绝服务。表II.1列出了一些安全威胁。

表II.1/M.3016.1—威胁

威胁类别（注）	威胁示例
未授权访问	黑客 带有攻击性的未授权系统访问 剽窃服务
伪装	会话重放 劫持会话 普通人的攻击
系统完整性威胁	未授权操作系统配置文件 未授权操作系统数据
通信完整性威胁	在运输途中未授权操作数据
机密性威胁	窃听 记录和泄漏会话 违反私密性
拒绝服务	传输控制协议（TCP）SYN 流 残缺分组攻击 分布式的 DoS
注 — 引自美国国家标准协会（ANSI）T1.233-1993（R1999）（操作、管理、维护和指配－电信管理网接口安全框架）和国际标准化组织（ISO）7498-2：1989（信息处理系统－开放系统互连－基本参考模型－第 *2* 部分：安全体系结构）	

这些安全威胁在一个包含了安全服务的物理系统或网元平台或应用程序中，可能减到最小或得到减轻（如ISO 7498-2：1989，“信息处理系统－开放系统互连－基本参考模型－第2部分：安全体系结构”中所定义的），因为执行了如下特性：

— 识别和**鉴权**；

— 授权**访问控制**级别；

— 数据完整性；

— 私密性和机密性；

— 不可否认。

本建议书明确了管理平面的安全，即安全特性是用来确保网络能够被管理，且以一种安全的方式进行管理。但即使遵循了本建议书中所包括的建议，仍然可能存在一些弱点。下面的风险就处于其中，并且可能危害到管理平面：

— 授权用户或攻击者的不恰当的行为。这些行为可能是恶意的或是意外的。

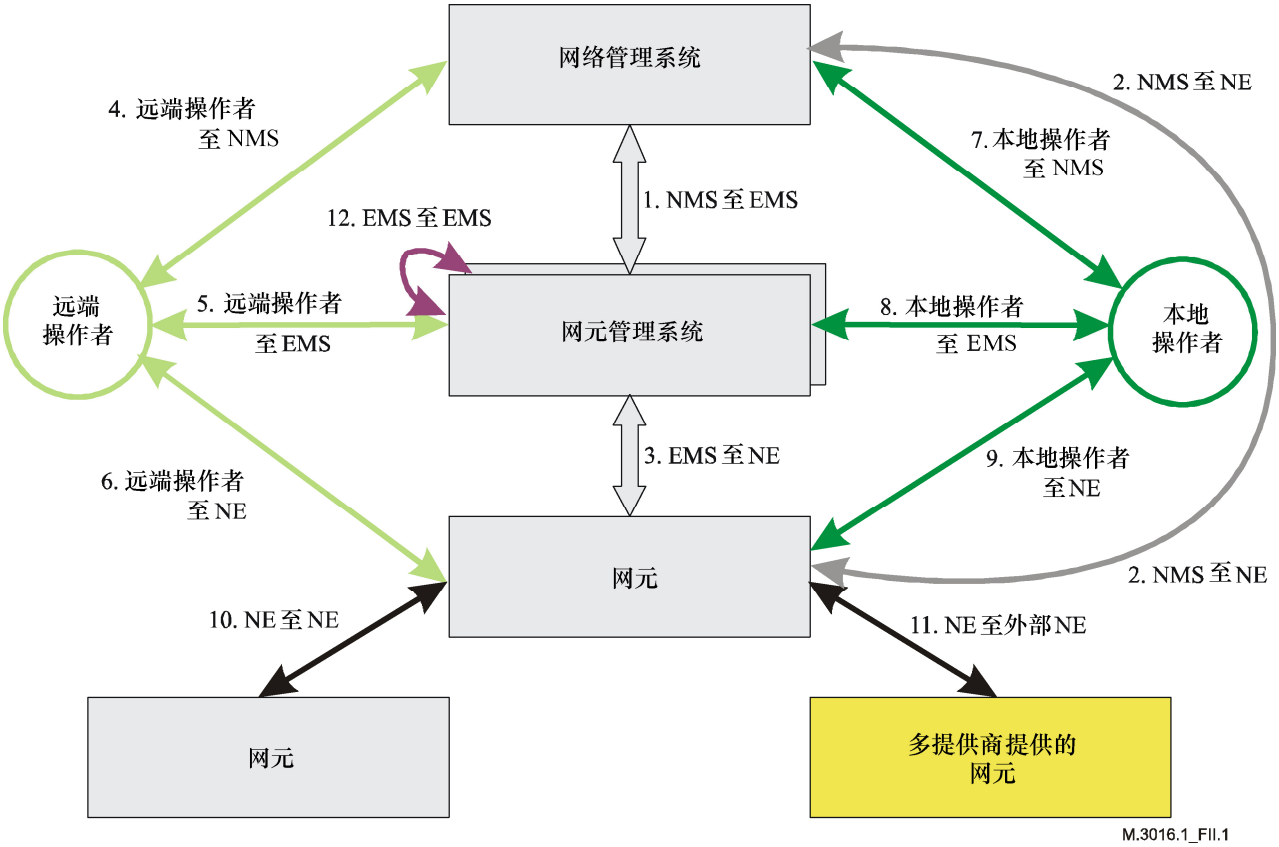
— 控制平面安全的桥梁（如：信令、路由、命名和发现协议）。

— 特定协议的弱点的影响。

— 不良件（如：病毒、特洛伊木马、蠕虫、或其他内嵌代码）。一旦这些不良件成功地危害到任何 NE/MS，它们可能会利用安全的网络通信链路向其他 NE/MS 组件进行攻击。这些攻击将可能一直持续，直到网络管理员检测到并采取措施将其终止。

本建议书关注的是管理业务流的安全，尤其是通过网络传送最终用户的业务流时。图II.1描述了一个参考模型，用来说明网络管理安全方案。该参考模型用来检测整个网络中的逻辑通信路径，以及在每条路径通信中使用的协议数量。使用该参考模型，可以监测每条路径的威胁和弱点，并能够应用适当的安全机制。

图II.1中，在参考模型的底部显示了多提供商提供的NE。为这些NE提供特定管理功能的网元管理系统（EMS）显示在NE的上面。网络管理系统（NMS）显示在参考模型的顶部。NMS提供对NE和EMS的全面的管理，还包括特定的业务管理应用和事务管理应用，如配置和计费系统。参考模型中还显示了远端和本地操作者，以及与其他系统相连的通信路径。



图II.1/M.3016.1－网络管理安全参考模型

安全参考模型（图II.1）也可用于电信管理网（TMN）定义的接口。电信管理网在ITU-T M.3010建议书（电信管理网原则）中定义，TMN被定义为一个管理体系结构，包括对电信设备、网络和业务的计划、指配、安装、维护、操作和管理。

II.2 设计指南

表II.2表示设计指南的目标是为了满足本建议书第6节定义的需求，来减轻表II.1中所提到的威胁。

表II.2/M.3016.1－设计指南

指　南	描　述
隔离	将管理业务流与客户业务流分离开来。
有效的安全策略	需求和支持的体系结构必须允许策略是可定义的、灵活的、可实施的、可验证的、可靠的和可用的。
强**鉴权**，授权和计费（AAA）	对鉴权实体间完全授权的会话进行可靠的计费。
给定成本的最高收益	实现标准化的、广泛实现了的并广泛部署的安全机制可以改善安全性，因此应评估安全机制的使用历史。
改进路径	考虑增强和改进网络管理安全性的下一步，以更进一步地满足技术和机制的发展而提出的需求，或者是新定义的安全需求。

指　南	描　述
技术可行性	需求必须与当今的产品、解决方案和可用技术相适应
常规过程	需求应当与运行良好的标准的网络管理操作流程相适应。
开放标准	使用标准的，或即将由标准化组织进行标准化的思想和观念（如 IP 安全－IPsec，数字签名等）。这些开放标准的所有方面均应重视，包括系统、协议、模型、算法、密钥尺寸和编码等。

附　录　三

M.3016.x系列建议书中使用的术语语义

下列术语用在需求陈述中时，以**黑体**形式出现。

III.1　**访问控制**：防止对资源的未授权使用，包括防止以一种未授权的方式使用资源。摘自 ANSI T1 233-1993（R1999）第 3.1 节。[10]

III.2　**访问控制服务器（ACS）**：一个辅助网元，对基于**复杂口令**的 MS 执行访问鉴权，如果 NE 不能直接执行此功能时，则部署该网元。

III.3　**应用程序管理员**：一种角色，负责 NE/MS 应用程序的正确操作、维护和使用。应用程序管理员的任务包括升级应用程序软件。[11]

III.4　**应用程序安全管理员**：一种角色，负责 NE/MS 应用级安全特性的正确操作、维护和使用。具有 NE/MS 应用实例的最高级别的安全授权，其任务包括：

— 定义和分配应用程序级别的新用户和新用户组权限；

— 维护和记录所有请求登录到应用程序的登录 ID；

— 增加和删除应用程序级别的用户；

— 监视所有的应用程序安全日志；

— 配置应用程序安全日志和告警；

— 管理应用程序安全日志流程；

— 终止用户应用程序会话。

III.5　**鉴权**：**鉴权**是对声称的身份进行检测验证。

III.6　**复杂口令**：当一个口令是由字母、数字和特殊字符等组合而成时，要通过一般的工程方法或自动方法猜出来是很困难或是不可能的，则该口令被认为是“复杂的”。

---

[10] 摘自ANSI T1 233-1993(R1999)《操作、管理、维护和指配－电信管理网接口安全框架》第3.1节。

[11] 如果**超级用户**必须完成该任务的话，该任务也可能是**系统管理员**的功能。必须开发一个过程来控制对**超级用户**帐户的访问。

III.7 **控制平面：控制平面**执行呼叫控制和连接控制功能。通过信令，**控制平面**建立和释放连接，也可能在失效时恢复连接。[12]

III.8 **关键的安全管理活动：系统安全管理员**负责关键的安全管理活动，允许对一个系统（NE/MS）的安全特性进行正确的激活、维护和使用。**关键的安全管理活动**包括，但不限于如下所述：

— 定义和分配用户权限；

— 增加和删除用户 ID；

— 去活某些特定的 ID，使之不能作为登录 ID；

— 初始化和设置登录口令；

— 初始化和修改密钥；

— 为登录口令设置系统的有效期限；

— 为每个登录 ID 设置系统的登录失败次数限制；

— 去除锁定，或修改系统的锁定定时器值；

— 设置系统的去活定时器值；

— 设置系统安全日志和告警配置；

— 管理安全日志流程；

— 升级安全软件；

— 终止用户或系统会话。

III.9 **去活/去活的：**指的是一个用户 ID 处于一种状态，在这种状态下，用户 ID 不能用作登录 ID，直到该 ID 被另外一个具有适当授权权限的用户 ID（如**系统安全管理员**或**应用程序安全管理员**）激活后才可以登录。

III.10 **网元管理系统（EMS）：**在网元管理级执行操作系统功能的系统。

III.11 **密钥长度：**不同的加密算法根据其被解开的难易程度有不同的安全级别。一个加密算法如果不可能通过计算来解开，则认为该算法是强壮的，即该算法有足够的复杂度，不可能利用当前的或可预见的未来的可用资源在一个“合理的”时间内解开。计算复杂度一般由处理复杂度来衡量，或者由攻击所需的时间和内存空间来衡量。尽管针对某种特定算法和密钥长度的攻击复杂度保持不变，但计算能力却一直在提高。应设计好的加密算法，使得即使计算能力在未来多年内继续发展，也不可能解出来。作为新技术和编码方法快速发展的结果，针对某种应用程序的适当的密钥长度也在不断的变化中。

III.12 **锁定/加锁**：指的是一个用户 ID 处于一种状态，在该状态下，用户 ID 不能被用于登录，直到锁定状态被一个或多个适当的活动移除。适当的活动包括，但不限于如下所述：

— 超出定时门限后（如 60 分钟后），自动进行重设；

---

[12] 见ITU-T G.8080/Y.1304建议书《自动交换光网络ASON的体系结构》，2001年11月（ITU-T电子书店中有）。

— 成功地执行了预先定义的重设过程后（如所有者正确回答了一系列问题后），自动进行重设；或者

— 通过另一个具有适当授权权限用户（如**系统安全管理员**或**应用程序安全管理员**）的特定操作进行重设。

III.13 **管理活动**：由**系统管理员**或代表**系统管理员**采取的活动。

III.14 **管理通信**：**管理活动**的任何通信行为。

III.15 **管理平面**：**管理平面**为**传送平面**，**控制平面**和整个系统执行管理功能。它也为所有平面提供协调功能。ITU-T M.3010 建议书（电信管理网的原则）中定义的性能、故障、配置、计费和安全管理功能域由**管理平面**来执行。[13]

III.16 **网元（NE）**：参见 ITU-T M.3010 建议书。

III.17 **网络管理系统（NMS）**：在网络管理层中执行操作系统功能的系统。

III.18 **网元/管理系统（NE/MS）**：一个组合术语，用来描述电信网络中的所有元素，包括网元、网元管理系统和运营支持系统等。

III.19 **受保护的鉴权**：包括**强鉴权**，**双重鉴权**，**可信任的路径鉴权**，第三方密码鉴权（如 Kerberos），或是一次性口令鉴权。

III.20 **会话**：机器与机器间或人与机器间的一系列的操作，这些操作都与一个唯一的过程或用户 ID 相关。

III.21 **强鉴权**：**强鉴权**是一种**鉴权**，依赖于对密码技术的使用（如公共密钥编码，对称型密钥编码，数字签名和数字散列技术等）。**强鉴权**应包括双向鉴权，以防止主动的攻击。

III.22 **强加密**：当一个黑客利用可用的计算资源尝试各种可能的密钥组合办法试图解开加密信息时，这种攻击是很严重的。在这种情况下，平均尝试一半的密钥组合即有可能发现正确的密钥。尝试使用一半的密钥组合所用时长是衡量一种加密算法强壮性的度量值。因此，在任何时候，**强加密**机制采用的算法和密钥，应使得任何黑客使用当前的技术解密至少需要超出两年的时间。

III.23 **系统管理员**：一种角色，负责 NE/MS 操作系统级别的过程和流程，包括操作平台的安装和维护，平台中软件的安装，以及控制**超级用户**的授权等。其任务可能包括：

— 协调新平台的安装；

— 定义和分配操作系统级别的新用户和新用户组权限；

— 维护和记录所有请求登录到操作系统的登录 ID；

— 增加和删除操作系统级别的用户；

---

13 TMN体系结构在ITU-T M.3010建议书《电信管理网的原则》中有定义，关于管理平面的附加的详细信息在ITU-T M系列建议书中提供。G.8080/Y.1304建议书《自动交换光网络*ASON*的体系结构》2001年11月（在国际电联电子书店中有）。

— 去活某些特定的 ID，使之不能作为登录 ID（bin、sys、uucp）；

— 安装操作系统升级版本和补丁；

— 给操作系统安装应用程序和数据库软件；

— 监视所有的系统日志；

— 维护和监视超级**用户口令**的访问和修改；

— 控制对**超级用户**账号的访问，当商务需要时，允许适当的访问；

— 管理系统日志流程；

— 向其他角色的特定用户委托管理授权，包括**应用程序管理员**；

— 终止任何用户和系统会话。

III.24 **系统安全管理员**：一种角色，负责 NE/MS 系统安全特性的正确操作、维护和使用。具有 NE/MS 系统/应用实例的最高级别的安全授权，其任务包括：

— 定义和分配操作系统级别的新用户和新用户组权限；

— 维护和记录所有请求登录到操作系统的登录 ID；

— 增加和删除操作系统级别的用户；

— 去活某些特定的 ID，使之不能作为登录 ID（bin、sys、uucp）；

— 监视所有的系统安全日志；

— 初始化和修改密钥；

— 为登录口令设置系统的有效期限；

— 为每个登录 ID 设置系统的登录失败次数限制；

— 去除锁定，或修改系统的锁定定时器值；

— 设置系统的去活定时器值；

— 配置系统安全日志和告警；

— 管理系统安全日志流程；

— 向其他角色的特定用户委托安全授权，包括**应用程序安全管理员**；

— 终止任何用户或系统会话。

III.25 **传送平面**：**传送平面**为用户信息从一个网元传递到另一个网元提供双向的或单向的传送，也可以提供一些控制和网络管理信息的传送。**传送平面**是分层的，等同于 ITU-T G.8080/Y.1304 建议书（自动交换光网络 ASON 的体系结构）中定义的传送网络。

III.26 **可信任的路径**：一种机制，通过该机制任何用户/操作者到系统，或者系统到系统之间的操作都是安全可靠的。该机制仅能够被用户/操作者或系统激活，不能被伪造。**可信任的路径**可以是一个专用的物理路径（如终端之间与系统相连），也可以是一个包括完整性和重放保护的加密路径).（如“安全的”虚拟专用网，安全套接层 SSL 隧道，安全外壳 SSH 等）。[14]

---

14 摘自国家计算机安全中心，NCSC-TG-004-88，计算机安全术语集，1998年10月（http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf）。

III.27 **双重鉴权：双重鉴权**术语一般用来描述一种**鉴权**过程，该过程要求不仅拥有一个物理实体（令牌或卡），还要求知道密码（如口令或密语）。

参 考 资 料

本参考资料中的书目为附录I和II中涉及的论题提供了附加信息。

— ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*

— ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation,* (available from the ANSI X9 Electronic Standards Store, http：//webstore.ansi.org/ansidocstore/ dept.asp?dept_id=80).

— ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry： The Elliptic Curve Digital Signature Algorithm (ECDSA),* (available from the ANSI X9 Electronic Standards Store, http：//webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).

— ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*

— ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.

— ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*

— ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*

— ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.

— ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

— ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Elements – Implementation Agreements Version 1.1,* (available at ftp：//ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

— BARRETT (D.), SILVERMAN (R.)： SSH, The Secure Shell： The Definitive Guide, *O'Reilly*, January 2001.

— BELLOVIN (S.)：An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.

— BLEICHENBACHER (D.)：Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.

— BONEH (D.)： Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, February 1999, (available at http：//www.ams.org/notices/199902/boneh.pdf).

— BONEH (D.), JOUX (A.), NGUYEN (P.)： Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.

— Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, September 1999.

— General Requirements (GR)-815, *Generic Requirements for Element/Network System Security*, March 2002 (available at Telcordia Information SuperStore, http ： //telecom-info.telcordia.com/site-cgi/ido/index.html).

— GR-1194, *Bellcore Operations Systems Security Requirements*, December 1998, (available at Telcordia Information SuperStore, http：//telecom-info.telcordia.com/site-cgi/ido/index.html).

— GUTMANN (P.)： Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998, (available at http：//www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/ gutmann.pdf).

— Information Assurance Technical Framework Forum (IATF), http：//www.commoncriteria.org/ and http：//www.iatf.net/protection_profiles/profiles.cfm.

— IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*, (available at IEEE Standards Online, http：//standards.ieee.org/catalog/olis/ busarch.html).

— IETF RFC 768, *User Datagram Protocol*, J. Postel, August 1980 (available at http：//www.ietf.org/rfc/rfc0768.txt?number=768).

— IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*, (available at http：//www.ietf.org/rfc/ rfc0791.txt?number=791).

— IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*, (available at http：//www.ietf.org/rfc/rfc0792.txt?number=792).

— IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification*, (available at http：//www.ietf.org/rfc/rfc0793.txt?number=793).

— IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, (available at http：//www.ietf.org/rfc/rfc0826.txt?number=826).

— IETF RFC 859 (1983), *Telnet Status Option,* (available at http：//www.ietf.org/rfc/rfc0859.txt?number=859).

— IETF RFC 959 (1985), *File Transfer Protocol (FTP),* (available at http：//www.ietf.org/rfc/rfc0959.txt?number=959).

— IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (available at http：//www.ietf.org/rfc/rfc1157.txt?number=1157).

— IETF RFC 1288 (1991), *The Finger User Information Protocol,* (available at http：//www.ietf.org/rfc/rfc1288.txt?number=1288).

— IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* (available at http：//www.ietf.org/rfc/rfc1905.txt?number=1905).

— IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One： Format of Internet Message Bodies,* (available at http：//www.ietf.org/rfc/rfc2045.txt?number=2045).

— IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1,* (available at http：//www.ietf.org/rfc/rfc2202.txt?number=2202).

— IETF RFC 2222 (1997), *Simple 鉴权 and Security Layer (SASL),* (available at http：//www.ietf.org/rfc/rfc2222.txt?number=2222).

— IETF RFC 2246 (1999), *The TLS Protocol Version 1.0,* (available at http：//www.ietf.org/rfc/rfc2246.txt?number=2246).

— IETF RFC 2271 (1998), *An Architecture for Describing SNMP Management Frameworks,* (available at http：//www.ietf.org/rfc/rfc2271.txt?number=2271).

— IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP),* (available at http：//www.ietf.org/rfc/rfc2272.txt?number=2272).

— IETF RFC 2273 (1998), *SNMPv3 Applications,* (available at http：//www.ietf.org/rfc/rfc2273.txt?number=2273).

— IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, (available at http：//www.ietf.org/rfc/rfc3414.txt?number=3414).

— IETF RFC 2275 (1998), *View-based 访问控制 Model for the Simple Network Management Protocol* (*SNMP)*, (available at http：//www.ietf.org/rfc/rfc2275.txt?number=2275).

— IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, (available at http：//www.ietf.org/rfc/rfc2401.txt?number=2401).

— IETF RFC 2402 (1998), *IP 鉴权 Header,* (available at http：//www.ietf.org/rfc/rfc2402.txt?number=2402).

— IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, (available at http：//www.ietf.org/rfc/rfc2406.txt?number=2406).

— IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* (available at http：//www.ietf.org/rfc/rfc2451.txt?number=2451).

— IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1,* (available at http：//www.ietf.org/rfc/rfc2616.txt?number=2616).

— IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method,* (available at http：//www.ietf.org/rfc/rfc2631.txt?number=2631).

— IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core,* (available at http：//www.ietf.org/rfc/rfc3080.txt?number=3080).

— IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP,* (available at http：//www.ietf.org/rfc/rfc3081.txt?number=3081).

— ISO 7498-2：1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2： Security Architecture,* (available at ISO Online Store, http：//www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1 =35&ICS2=100&ICS3=1).

— ITU-T Recommendation M.3010 (2000), *Principles for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).

— ITU-T Recommendation M.3013 (2000), *Considerations for a Telecommunications Management Network,* (available at ITU Electronic Bookshop).

— JANSEN (W.A.)： A Revised Model for Role Based Access Control, *NIST-IR 6192*, July 1998, (available at http：//csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

— JONSSON (J.), KALISKI (B.)： On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, August 2002.

— KELSEY (J.), SCHNEIER (B.), FERGUSON (N.)： Yarrow-160： Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual*

Workshop on Selected Areas in Cryptography, Springer-Verlag, August 1999, (available at http：//www.counterpane.com/yarrow-notes.html).

— KRAWCZYK (H.)： Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, August 2002.

— LENSTRA (A.), VERHEUL (E.)： Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

— National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*. October 1988, (available at http：//csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

— National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000, (available at http：//www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_ sep00.pdf).

— Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, March 2002, (available at http：//cgi.omg.org/docs/formal/02-03-11.pdf).

— Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* March 2001, (available at http：//cgi.omg.org/docs/formal/01-03-08.pdf).

— Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, September 2001, (available at http：//www.pcis.org/library.cfm?urlSection=WG).

— RESCORLA (E.)： SSL and TLS, Addison-Wesley, 2001.

— SCHNEIER (Bruce.)： Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

— SILVERMAN (R.)： The Mythical MIPS Year, *IEEE Computer*, August 1999.

— SILVERMAN (R.)： A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, April 2000.

— VAUDENAY (S.)： Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, April-May 2002.

— World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, February 1998, (available at http：//www.w3.org/TR/1998/REC-xml-19980210).

— World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, May 2000, (available at http：//www.w3.org/TR/SOAP/).

— WU (T.)： The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, March 1998, (available at http：//www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

— YLÖNEN, T.： SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, July 1996, (available at http：//www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

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