中华人民共和国国家标准

GB/T 9387.2--1995

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

Information processing system--Open Systems

Interconnection--Basic Reference Model

--Part2: Security architecture

目　　次

本标准等同采用国际标准 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》。

0　引言

GB 9387--88 为开放系统互连(OSI)描述了基本参考模型,它为协调开发现有的与未来的系统互连标准建立起一个框架。

开放系统互连基本参考模型的目的是让异构型计算机系统的互连能达到应用进程之间的有效通信。在各种不同场合都必须建立安全控制，以便保护在应用进程之间交换的信息。这种控制应该使得非法获取或修改数据所花的代价大于这样做的潜在价值，或者使其为得到所需数据而花费的时间很长，以致失去该数据的价值。

本标准确立了与安全体系结构有关的一般要素，它们能适用于开放系统之间需要通信保护的各种场合。为了安全通信而完善与开放每互连相关的现有标准或开发新标准，本标准在参考模型的框架内建立起一些指导原则与制约条件,从而提供了?个解决 OSI 中安全问题的一致性方法。知道安全方面的一些背景对于了解本标准是有益的。我们建议对安全问题不够熟悉的读者先读附录 A(参考件)。

本标准扩充了基本参考模型，涉及到了安全问题的一些方面。这些方面是通信协议体系结构的一般要素，但并没有在基本参考模型中予以讨论。

1　主题内容与适用范围

本标准的任务是:

a.提供安全服务与有关机制的一般描述，这些服务与机制可以为 GB9387--88 参考模型所配备;

b.确定在参考模型内部可以提供这些服务与机制的位置。

本标准扩充了 GB 9387--88 的应用领域,包括了开放系统之间的安全通信。对基本的安全服务与机制以及它们的恰当配置按基本参考模型作了逐层说明。此外还说明了这些安全服务与机制对于参考模型而言在体系结构上的关系。在某些端系统、设备和组织结构中，可能还需要附加某些别的安全措施，这些措施也适用一各种不同的应用上下文中。确定为支持这种附加的安全措施所需要的安全服务不在本标准的工作范围之内。开放系统互连(OSI)的安全功能仅仅涉及能让端系统之间进行信息的安全传送的通信通路的可见方面，不考虑在端系统、设备或组织内所需要的安全措施,除非牵连到在 OSI 中可见性安全服务的选择与定位。安全结构问题的这些?问题也可以进行标准化，但不在 OSI 标准的工作范围之内。

本标准对在 GB 9387--88 中定义的概念与原则作了补充，但并未改动它们。本标准既不是一个实施规范，也不是评价实际执行方案一致性的基准。

2　引用标准

GB9387--88　信息处理系统　开放系统互连　基本参考模型

GB/T 15274　信息处理系统　开放系统互连　网络层的内部组织结构

ISO 7498-4　信息处理系统　开放系统互连　基本参考模型　第4部分:管理框架

ISO7498/补篇 1　信息处理系统　开放系统互连 基本参考模型　补篇 1: 无连结方式传送

3　定义与缩略语

3.1　本标准以在GB 9387--88中建立的概念为基础，并使用在该标准中定义的下列术语:

a.　(N)连续；

b.　(N)数据传输;

c.　(N)实体;

d.　(N)业务;

e.　(N)层;

f.　开放系统;

g.　对等实体;

h.　(N)协议;

j.　(N)协议数据单元;

k.　(N)中继;

i.　路由选择;

m.　排序;

n.　(N)服务;

p.　(N)服务数据单元;

q.　(N)用户数据;　　r.　子网;

s.　OSI 资源;

t.　传送语法。

3.2　本标准使用的下列术语取自相应的国家标准(GB)和国际标准(ISO):

无连接方式传输　　(ISO 7498 补篇 1)

端系统　　(GB9387-88)

中继与路由功能　　(GB/T15274)

单元数据　　(GB 9387--88)

管理信息库　　(ISO 7498-4)

此外，还使用了下面这些缩写:

OSI: 开放系统互连;

SDU: 服务数据单元;

SMIB: 安全管理信息库;

MIB: 管理信息库。

3.3　本标准采用下列定义:

3.3.1　访问控制　access control

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。

3.3.2　访问控制表　access control list

带有访问权限的实体表，这些访问权是授予它们访问某一资源的。

3.3.3　可确认性　accountability

这样一种性质，它确保一个实体的作用可以被独一无二地跟踪到该实体。

3.3.4　主动威胁　active threat

这种威胁是对系统的状态进行故意的非授权的改变。

注: 与安全有关的主动威胁的例子可能是: 篡改消息、重发消息、插入伪消息、冒充已授权实体以及服务拒绝等。

3.3.5　审计　audit

见“安全审计”。

3.3.6　审计跟踪　audit trail

见“安全审计跟踪”。

3.3.7　鉴别　authentication

见“数据原发鉴别”与“对等实体鉴别”。

注:在本标准中，当涉及数据完整性时不使用术语“鉴别”，而另用术语“数据完整性”。

3.3.8　鉴别信息　authentication information

用以建立身份有效性的信息。

3.3.9 鉴别交换 authentication exchange

通过信息交换来保证实体身份的一种机制。

3.3.10 授权 authorization

授予权限，包括允许基于访问权的访问。

3.3.11 可用性 availability

根据授权实体的请求可被访问与使用。

3.3.12 权力 capability

作为资源标识符使用的权标,拥有它便拥有对该资源的访问权。

3.3.13 信道 channel

信息传送通路。

3.3.14 密文 ciphertext

经加密处理而产生的数据，其语义内容是不可用的。

注：密文本身可以是加密算法的输入，这时候产生超加密输出。

3.3.15 明文 cleartext

可理解的数据，其语义内容是可用的。

3.3.16 机密性 confidentiality

这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。

3.3.17 凭证 credentials

用来为一个实体建立所需身份而传送的数据。

3.3.18 密码分析 cryptanalysis

为了得到保密变量或包括明文在内的敏感性数据而对密码系统或它的输入输出进行的分析。

3.3.19 密码校验值 cryptographic checkvalue

通过在数据单元上执行密码变换(见“密码学”)而得到的信息。

注：密码校验值可经一步或多步操作后得出，它是依赖于密钥与数据单元的一个数学函数的结果，常被用来校验数据单元的完整性。

3.3.20 密码学 cryptography

这门学科包含了对数据进行变换的原理、手段和方法，其目的是掩藏数据的内容，防止对它作了篡改而不被识破或非授权使用。

注: 密码学决定在加密和解密中使用的方法。对密码原理, 手段, 或方法的攻击就是密码分析。

3.3.21 数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

3.3.22 数据原发鉴别 data origin authentication

确认接收到的数据的来源是所要求的。

3.3.23 解密 decipherment

与一个可逆的加密过程相对应的反过程。

3.3.24 解密处理 decryption

见“解密”。

3.3.25 服务拒绝 denial of service

阻止对资源的授权访问或拖延时限操作。

3.3.26 数字签名 digital signature

附加在数据单元上的一些数据, 或是对数据单元所作的密码变换(见“密码学”), 这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性, 并保护数据, 防止被人(例如接收者)进行伪造。

3.3.27 加密 encipherment

对数据进行密码变换(见“密码学”)以产生密文。

注:加密可以是不可逆的, 在这种情况下, 相应的解密过程便不能实际实现了。

3.3.28 加密处理 encryption

见“加密”。

3.3.29 端-端加密 end-to-end encipherment

数据在源端系统内进行加密, 而相应的解密仅仅发生在目的端系统之内。(见“逐链加密”)

3.3.30 基于身份的安全策略 identity-based security policy

这种安全策略的基础是用户或用户群的身份或属性,或者是代表用户进行活动的实体以及被访问的资源或客体的身份或属性。

3.3.31 完整性 integrity

见“数据完整性”。

3.3.32 密钥 key

控制加密与解密操作的一序列符号。

3.3.33 密钥管理 key management

在一种安全策略指导下密钥的产生，存储，分配，删除，归档及应用。

3.3.34 逐链加密 link-by-link encipherment

在通信系统的每段链路上对数据分别进行加密。(见“端-端加密”)

注: 逐链加密意味着在中继实体中数据将以明文形式出现。

3.3.35 操作检测 manipulation detection

用来检测数据单元是否被修改过的一种机制。(这种修改或是偶然发生的,或是故意进行的。)

3.3.36 冒充 masquerade

一个实体伪装为另一个不同的实体。

3.3.37 公证 notarization

由可信赖的第三方对数据进行登记，以便保证数据的特征如内容,原发，时间,交付等的准确性不致改变。

3.3.38 被动威胁 passive threat

这种威胁对信息的非授权泄露而未改变系统状态。

3.3.39 口令 password

机密的鉴别信息，通常由一串字符组成。

3.3.40 对等实体鉴别 peer-entity authentication

确认有关的对等实体是所需的实体。

3.3.41 物理安全 physical security

为防范蓄意的和意外的威胁而对资源提供物理保护所采取的措施。

3.3.42 策略 policy

见“安全策略”。

3.3.43 私密 privacy

一种个人权限，它控制和影响与这些个体有关的哪些信息可以被收集，存储以及这些信息可以被谁泄露和泄露给谁。

注：由于这一术语涉及到私人权限，不可能精确地予以限定，因此，除了作为要求安全保护的一种动机外，应避免使用。

3.3.44 抵赖 repudiation

在一次通信中涉及到的那些实体之一不承认参加了该通信的全部或一部分。

3.3.45 路由选择控制 routing control

在路由选择过程中应用规则，以便具体地选取或回避某些网络、链路或中继。

3.3.46 基于规则的安全策略 rule-based security policy

这种安全策略的基础是强加于全体用户的总体规则。这些规则往往依赖于把被访问资源的敏感性与用户、用户群、或代表用户活动的实体的相应属性进行比较。

3.3.47 安全审计 security audit

为了测试出系统的控制是否足够，为了保证与已建立的策略和操作堆积相符合，为了发现安全中的漏洞，以及为了建议在控制、策略和堆积中作任何指定的改变，而对系统记录与活动进行的独立观察和考核。

3.3.48 安全审计跟踪 security audit trail

收集起来并可用来使安全审计易于进行的数据。

3.3.49 安全标记 security label

与某一资源(可以是数据单元)密切相联的标记，为该资源命名或指定安全属性。

注：这种标记或约束可以是明显的，也可以是隐含的。

3.3.50 安全策略 security policy

提供安全服务的一套准则。(见“基于身份的安全策略”与“基于规则的安全策略”)

注:一种完备的安全策略势将涉及超出 OSI 范围之外的许多事项。

3.3.51 安全服务 security service

由参与通信的开放系统的层所提供的服务，它确保该系统或数据传送具有足够的安全性。

3.3.52 选择字段保护 selective field protection

对将被传输的消息中的特定字段实施的保护。

3.3.53 敏感性 sensitivity

资源所具有的一种特征，它意味着该资源的价值或重要性，也可能包含这一资源的脆弱性。

3.3.54　签名　signature

见“数字签名”。

3.3.55　威胁　threat

一种潜在的对安全的侵害。

3.3.56　通信业务分析　traffic analysis

通过对通信业务流的观察(出现、消失、总量、方向与频度)，而对信息作出推断。

3.3.57　通信业务流机密性　traffic flow confidentiality

抵抗通信业务分析的一种机密性服务。

3.3.58　通信业务填充　traffic padding

制造通信的假实例，产生欺骗性数据单元或数据单元中的伪数据。

3.3.59　可信功能度　trusted functionality

就某种标准，例如按某种安全策略确立的准则而言，这种功能被认为是正确无误的。

4　记法

本标准中使用的层次记法与 GB 9387--99 中确定的相同。

如果不作另外说明，“服务”一词就用来指安全服务?

5　安全服务与安全机制的一般描述

5.1　概述

本章讨论包括在 OSI 安全体系结构中的安全服务以及实现这些服务的机制。下面描述的安全服务是基本的安全服务。实际上，为了满足安全策略或用户的要求，它们将应用在适当的功能层上，通常还要与非 OSI 服务与机制结合起来使用。一些

特定的安全机制能用来实现这些基本安全服务的组合。实际建立的系统为了直接引用的方便可以执行这些基本的安全服务的某些特定的组合。

5.2　安全服务

下面所列被认为是在 OSI 参考模型的框架中能提供的可选的安全服务。其中的鉴别服务需要有鉴别信息，它包括用于鉴别而存储在当地的信息和经传送而得到的数据(凭证)两部分。

5.2.1　鉴别

这种安全服务提供对通信中的对等实体和数据来源的鉴别，分述如下:

5.2.1.1　对等实体鉴别

这种服务当由(N)层提供时，将使(N+1)实体确信与之打交道的对等实体正是它所需要的(N+1)实体。

这种服务生在连接建立或在数据传送阶段的某些时刻提供使用，用以证实一个或多个连接实体的身份。使用这种服务可以确信(仅仅在使用时间内): 一个实体此时没有试图冒充别的实体，或没有试图将先前的连接作非授权地重演。实施单向或双向对等实体鉴别是可能的，可以带有效期检验，也可以不带。这种服务能够提供各种不同程度的保护。

5.2.1.2　数据原发鉴别

这种服务当由(N)层提供时，将使(N+1)实体确信数据来源正是所要求的对等(N+1)实体。数据原发鉴别服务对数据单元的来源提供确认。这种服务对数据单元的重复或篡改不提供保护。

5.2.2　访问控制

这种服务提供保护以对付 OSI 可访问资源的非授权使用。这些资源可以是经 OSI 协议访问到的 OSI 资源或非 OSI 资源。这种保护服务可应用于对资源的各种不同类型的访问(例如: 使用通信资源; 读、写或删除信息资源; 处理资源的执行)或应用于对一种资源的所有访问。

这种访问控制要与不同的安全策略协调一致(见 6.2.1.1 条)。

5.2.3　数据机密性

这种服务对数据提供保护使之不被非授权地泄露; 分述如下:

5.2.3.1　连接机密性

这种服务为一次(N)连接上的全部(N)用户数据保证其机密性。

注:在某些使用中和层次上，保护所有数据可能是不适宜的，例如加速数据或连接请求中的数据。

5.2.3.2　无连接机密性

这种服务为单个无连接的(N)SDU 中的全部(N)用户数据保证其机密性。

5.2.3.3　选择字段机密性

这种服务为那些被选择的字段保证其机密性，这些字段或处于(N)连接的(N)用户数据中，或为单个无连接的(N)SDU 中的字段。

5.2.3.4　通信业务流机密性

这种服务提供的保护，使得通过观察通信业务流而不可能推断出其中的机密信息。

5.2.4　数据完整性

这种服务对付主动威胁，可取如下所述的各种形式之一。

注：在一次连接上，连接开始时使用对等实体鉴别服务，并在连接的存活期使用数据完整性服务就能联合起来为在此连接上传送的所有数据单元的来源提供确证，为这些数据单元的完整性提供确证，而且，例如使用顺序号，还能另外为数据单元的重复提供检测。

5.2.4.1　带恢复的连接完整性

这种服务为(N)连接上的所有(N)用户数据保证其完整性，并检测整个 SDU 序列中的数据遭到的任何篡改、插入、删除或重演(同时试图补救恢复)。

5.2.4.2　不带恢复的连接完整性

与 5.2.4.1 条的服务相同，只是不作补救恢复

5.2.4.3　选择字段的连接完整性

这种服务为在一次连接上传送的(N)-SDU 的(N)用户数据中的选择字段保证其完整性，所取形式是确定这些被选字段是否遭到了篡改、插入、删除或重演。

5.2.4.4　无连接完整性

这种服务当由(N)层提供时，对发出请求的那个(N+1)实体提供完整性保证。

这种服务为单个的无连接 SDU 保证其完整性，所取形式可以是确定一个接受到的 SDU 是否遭受了篡改。另外，在一定程度上也能提供对重演的检测。

5.2.4.5　选择字段无连接完整性

这种服务为单位无连接的 SDU 中的被选字段保证其完整性，所取形式为确定被选字段是否遭受了篡改。

5.2.5　抗抵赖

这种服务可取如下两种形式，或两者之一。

5.2.5.1　有数据原发证明的抗抵赖

为数据的接收者提供数据来源的证据。这将使发送者谎称未发送过这些数据或否认它的内容的企图不能得逞。

5.2.5.2　有交付证明的抗抵赖

为数据的发送者提供数据交付证据。这将使得接收者事后谎称未收到过这些数据或否认它的内容的企业不能得逞。

5.3　特定的安全机制

下面所列的这些安全机制可以设置在适当的(N)层上，以便提供在 5.2 条中所述的某些服务。

5.3.1　加密

5.3.1.1　加密既能为数据提供机密性，也能为通信业务流信息提供机密性，并且还成为在下面所述的一些别的安全机制中的一部分或起补充作用。

5.3.1.2　加密算法可以是可逆的，也可以是不可逆的。可逆加密算法有两大类:

a.对称(即秘密密钥)加密。对于这种加密，知道了加密密钥也就意味着知道了解密密钥，反之亦然;

b.非对称(例如公开密钥)加密。对于这种加密，知道了加密密钥并不意味着也知道解密密钥，反之亦然。这种系统的这样两个密钥有时称之为“公钥”与“私钥”。不可不逆加密算法可以使用密钥，也可以不使用。若使用密钥，这密钥可以是公开的，也可以是秘密的。

5.3.1.3　除了某些不可逆加密算法的情况外，加密机制的存在便意味着要使用密钥管理机制。密钥管理方法上的一些准则将在 8.4 条中给出。

5.3.2　数字签名机制

这种机制确定两个过程:

a.对数据单元签名;

b.验证签过名的数据单元。

第一过程使用签名者所私有的(即独有的和机密的)。第二个过程所有的规程与信息是公之于众的，但不能够从它们推断出该签名者的私有信息。

5.3.2.1　签名过程涉及到使用签名者的私有信息作为私钥，或对数据单元进行加密，或产生出该数据单元的一个密码校验值。

5.3.2.2　验证过程涉及到使用公开的规程与信息来决定该签名是不是用签名者的私有信息产生的。

5.3.2.3　签名机制的本质特征为该签名只有使用签名者的私有信息才能产生出来。因而，当该签名得到验证后，它能在事后的任何时候向第三方(例如法官或仲裁人)证明:只有那私有信息的唯一拥有者才能产生这个签名。

5.3.3　访问控制机制

5.3.3.1　为了决定和实施一个实体的访问权，访问控制机制可以使用该实体已鉴别的身份，或使用有关该实体的信息(例如它与一个已知的实体集的从属关系),或使用该 实体的权力。如果这个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图，另外还可能产生一个报警信号或记录它作为安全审计跟踪的一个部分来报告这一事件。对于无连接数据传输，发给发送者的拒绝访问的通知只能作为强加于原发的访问控制结果而被提供。

5.3.3.2　访问控制机制，可以建立在使用下列所举的一种或多种手段之上:

a.访问控制信息库，在这里保存有对等实体的访问权限。这些信息可以由授权中心保存，或由正被访问的那个实体保存。这信息的形式可以是一个访问控制表，或者等级结构或分布式结构的矩阵。还要预先假定对等实体的鉴别已得到保证;

b.鉴别信息，例如口令，对这一信息的占有和出示便证明正在进行访问的实体已被授权;

c.权力: 对它的占有和出示便证明有权访问由该权力所规定的实体或资源;

注: 权力应是不可伪造的并以可信赖的方式进行运送。

d.安全标记: 当与一个实体相关联时，这种安全标记可用来表示同意或拒绝访问，通常根据安全策略而定;

e.试图访问的时间;

f.试图访问的路由;

g.访问持续期。

5.3.3.3　访问控制机制可应用于通信联系中的一端点，或应用于任一中间点。

涉及原发点或任一中间点的访问控制是用来决定发送者是否被授权与指定的接收者进行通信，或是否被授权使用所要求的通信资源。

在无连接数据传输目的端上的对等级访问控制机制的要求在原发点必须事先知道，还必须记录在安全管理信息库中(见6.2条与8.1条)。

5.3.4　数据完整性机制

5.3.4.1　数据完整性有两个方面：单个数据单元或字段的完整性以及数据单元流或字段流的完整性。一般来说，用来提供这两种类型完整性服务的机制是不相同的，尽管没有第一类完整性服务，第二类服务是无法提供的。

5.3.4.2　决定单个数据单元的完整性涉及两个过程，一个在发送实体上，一个在接收实体上。发送实体给数据单元附加上一个量，这个量为该数据的函数。这个量可以是如象分组校验码那样的补充信息，或是一个密码校验值，而且它本身可以被加密。接收实体产生一个相应的量，并把它与接收到的那个量进行比较以决定该数据是否在转送中被篡改过。单靠这种机制不能防止单个数据单元的重演。在网络体系结构的适当层上，操作检测可能在本层或较高层上导致恢复作用(例如经重传或纠错)。

5.3.4.3　对于连接方式数据传送，保护数据单元序列的完整性(即防止乱序、数据的丢失、重演、插入和篡改)还另外需要某种明显的排序形式，例如顺序号、时间标记或密码链。

5.3.4.4　对于无连接数据传送，时间标记可以用来在一定程度上提供保护，防止个个数据单元的重演。

5.3.5　鉴别交换机制

5.3.5.1　可用于鉴别交换的一些技术是：

a.使用鉴别信息，例如口令，由发送实体提供而由接收实体验证；

b.密码技术；

c.使用该实体的特征或占有物。

5.3.5.2　这种机制可设置在(N)层以提供对等实体鉴别。如果在鉴别实体时,这一机制得到否定的结果，就会导致连接的拒绝或终止，也可能使在安全审计跟踪中增加一个记录，或给安全管理中心一个报告。

5.3.5.3　当采用密码技术时，这些技术可以与“握手”协议结合起来以防止重演(即确保存活期)。

5.3.5.4　鉴别交换技术的选用取决于使用它们的环境。在许多场合，它们将必须与下列各项结合使用:

a.时间标记与同步时钟;

b.两方握手和三方握手(分别对应于单方鉴别和相互鉴别);

c.由数字签名和公证机制实现的搞抵赖服务。

5.3.6　通信业务填充机制

通信业务填充机制能用来提供各种不同级别的保护，抵抗通信业务分析。这种机制只有在通信业务填充受到机密服务保护时才是有效的。

5.3.7　路由选择控制机制

5.3.7.1　路由能动态地或预定地选取，以便只使用物理上安全的子网络、中继站或链路。

5.3.7.2　在检测到持续的操作攻击时，端系统可希望指示网络服务的提供者经不同的路由建立连接。

5.3.7.3　带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继或链路。连接的发起者(或无连接数据单元的发送者)可以指定路由选择说明,由它请求回避某些特定的子网络、链路或中继。

5.3.8　公证机制

有关在两个或多个实体之间通信的数据的性质，如它的完整性、原发、时间和目的地等能够借助公证机制而得到确保。这种保证是由第三方公证人提供的。公证人为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。当这种公证机制被用到时，数据便在参与通信的实体之间经由受保护的通信实例和公证方进行通信。

5.4　普遍性安全机制

在本条说明的几种安全机制不是为任何特定的服务而特设的，因此在后面的第7章中，在任一特定的层上，对它们都不作明确的说明。某些这样的普遍性安全机制可认为属于安全管理方面(见第8章)。

5.4.1　可信功能度

5.4.1.1　为了扩充其他安全机制的范围，或为了建立这些安全机制的有效性必须使用可信功能度。任何功能度，只要它是直接提供安全机制，或提供对安全机制的访问都应该是可领事的。

5.4.1.2　用来保证可对这样的硬件与软件寄托信任的手段已超出本标准的范围,而且在任何情况下，这些手段随已察觉到的威胁的级别和被保护信息的价值而改变。

5.4.1.3　一般说来，这些手段的代价高而且难于实现。能大大简化这一难题的办法是选取一个体系结构，它允许安全功能在这样一些模块中实现，这些模块能与非安全功能分开来制作，并由非安全功能来提供。

5.4.1.4　应用于一个层而对该层之上的联系所作的任何保护必须由另外的手段来提供，例如通过适当的可信功能度。

5.4.2　安全标记

包含数据项的资源可能具有与这些数据相关联的安全标记，例如指明数据敏感性级别的标记。常常必须在转送中与数据一起运送适当的安全标记。安全标记可能是与被传送的数据相连的附加数据，也可能是隐含的信息，例如使用一个特定密钥加密数据所隐含的信息，或由该数据的上下文所隐含的信息，例如数据来源或路由来隐含。明显的安全标记必须是清晰可辨认的，以便对它们作适当的验证。此外，它们还必须安全可靠地依附于与之关联的数据。

5.4.3　事件检测

5.4.3.1　与安全有关的事件检测包括对安全明显的检测，也可以包括对“正常”事件的检测，例如一次成功的访问(或注册)。与安全有关的事件的检测可由OSI内部含有安全机制的实体来做。构成一个事件的技术规范由事件处置管理来维护(见8.3.1条)。对各种安全事件的检测，可能引起一个或多个如下动作:

a.在本地报告这一事件;

b.远程报告这一事件;

c.对事件作记录(见5.4.3条):

d.进行恢复(见5.4.4条)。

这种安全事件的例子为:

a.特定的安全侵害;

b.特定的选择事件;

c.对事件发生次数计数的溢出。

5.4.3.2　这一领域的标准化将考虑对事件报告与事件记录有关信息的传输，以及为了传输事件报告与事件记录所使用的语法和语义的定义。

5.4.4　安全审计跟踪

5.4.4.1　安全审计跟踪提供了一种不可忽视的安全机制，它的潜在价值在于经事后的安全审计得以检测和调查安全的漏洞。安全审计就是对系统的记录与行为进行独立的品评考查，目的是测试系统的控制是否恰当，保证与既定策略和操作堆积的协调一致，有助于作出损害评估，以及对在控制、策略与规程中指明的改变作出评价.安全审计要求在安全审计跟踪中记录有关安全的信息，分析和报告从安全审计跟踪中得来的信息。这种日志记录或记录被认为是一种安全机制并在本条中予以描述，而把分析和报告视为一种安全管理功能(见8.3.2条)。

5.4.4.2　收集审计跟踪的信息，通过列举被记录的安全事件的类别(例如对安全要求的明显违反或成功操作的完成)，能适应各种不同的需要。

已知安全审计的存在可对某些潜在的侵犯安全的攻击源起到威摄作用。

5.4.4.3　OSI安全审计跟踪将考虑要选择记录什么信息，在什么条件下记录信息，以及为了交换安全审计跟踪信息所采用的语法和语义定义。

5.4.5　安全恢复

5.4.5.1　安全恢复处理来自诸如事件处置与管理功能等机制的请求，并把恢复动作当作是应用一组规则的结果。这种恢复动作可能有三种:

a.立即的;

b.暂时的;

c.长期的。

例如:

立即动作可能造成操作的立即放弃，如断开。

暂时动作可能使一个实体暂时无效。

长期动作可能是把一个实体记入“黑名单”，或改变密钥。

5.4.5.2　对于标准化的课题包括恢复动作的协议，以及安全恢复管理的协议(见8.3.3条)。

5.5　安全服务与安全机制间关系的实例

对于每一种服务的提供，表1标明哪些机制被认为有时是适宜的，或由一种机制单独提供，或几种机制联合提供。此表展示了这些关系的一个概貌，而且也不是一成不变的。在表中引述的服务和机制在5.2条与5.3条中作了描述，在第6章将对这些关系作更充分的说明?

表1

	机制							
	加密	数字签名	访问控制	数据完整性	鉴别交换	通信业务填充	路由控制	公证
服务								
对等实体鉴别	Y	Y	•	•	Y	•	•	•
数据原发鉴别	Y	Y	•	•	•	•	•	•
访问控制服务	•	•	Y	•	•	•	•	•
连接机密性	Y	•	•	•	•	•	Y	•
无连接机密性	Y	•	•	•	•	•	Y	•
选择字段机密性	Y	•	•	•	•	•	•	•
通信业务流机密性	Y	•	•	•	•	Y	Y	•
带恢复的连接完整性	Y	•	•	Y	•	•	•	•
不带恢复的连接完整性	Y	•	•	Y	•	•	•	•
选择字段连接完整性	Y	•	•	Y	•	•	•	•
无连接完整性	Y	Y	•	Y	•	•	•	•
选择字段无连接完整性	Y	Y	•	Y	•	•	•	•
抗抵赖，带数据原发证据	•	Y	•	Y	•	•	•	Y
抗抵赖，带交付证据	•	Y	•	Y	•	•	•	Y

说明：Y——这种机制被认为是适宜的，或单独使用，或与别的机制联合使

用。

- ——这种机制被认为是不适宜的。

6　服务、机制与层的关系

6.1　安全分层原则

6.1.1　为了决定安全服务对层的分配以及伴随而来的安全机制在这些层上的配置用到了下列原则:

a.实现一种服务的不同方法越少越好;

b.在多个层上提供安全服务来建立安全系统是可取的;

c.为安全所需的附加功能度不应该不必要地重复 OSI 的现有功能;

d.避免破坏层的独立性;

e.可信功能度的总量应尽量少;

f.只要一个实体依赖于由位于较低层的实体提供的安全机制，那么任何中间层应该按不违反安全的方式构作;

g.只要可能，应以不排除作为自容纳模块起作用的方法来定义一个层的附加安全功能;

h.本标准被认定应用于由包含所有七层的端系统组成的开放系统，以及中继系统。

6.1.2　各层上的服务定义可能需要修改以便满足安全服务的请求，不论所要求的安全服务是由该层提供或下面提供。

6.2　保护(N)服务的调用、管理与使用模型

本条应与第 8 章结合起来读，该章包含了对安全管理问题的一般讨论。本条说明安全服务与机制能够由管理实体通过管理接口使之激活，或由服务调用使之激活。

6.2.1　通信实例保护特点的确定

6.2.1.1　概述

本条说明对于面向连接无连接通信实例保护的调用。在面向连接通信的情形，请求和获准保护通常是在连接建立时刻。在无连接服务调用的情形，请求和获准保护是对每个“单元数据”请求进行的。

为了简化下面的说明，“服务请求”一词将用来指连接建立或单元数据请求。对被选数据调用保护能够通过请求选择字段保护来达到。例如，可以这样进行：建立几个连接，每个连接带有不同类型或级别的保护。

这种安全体系结构适应多种安全策略，包括基于规则的，基于身份的，或二者兼而有之的安全策略。这一安全体系结构也适应多种保护：行政管理强加的，动态选定的，或二者兼有的。

6.2.1.2　服务请求

对于每个(N)服务请求，(N+1)实体可以请求安全保护以达到所要求的目标。(N)服务请求将与参数以及附加的相关信息(如敏感性信息或安全标记)一起指明安全服务以达到这一目标安全保护。

在每个通信实例之先，(N)层必须访问安全管理信息库(SMIB)(见 8.1 条)。SMIB 保存有与所涉及的(N+1)实体相关联的行政管理强加保护要求的信息。还需要可信功能度来实施这些行政管理强加的安全要求。

当为面向连接通信事例时，安全特点的提供可以要求对所需的安全服务进行协商。机制与参数的协商过程可以作为一个单独的过程，或作为正常的连接建立过程的一部分。

当协商是作为一个单独的过程实现时，取得一致的结果(即为了提供这样的安全服务而必需的安全机制的类型和安全参数)便进入安全管理信息库(见 8.1 条)。

当协商是作为正常的连接建立过程的一部分实现时，(N)实体之间协商的结果将暂时存储在 SMIB 之中。在进行协商之前，(N)实体将访问 SMIB 以获得协商所需要的信息。

如果服务请求违反了记录在 SMIB 中为该(N+1)实体所作的行政管理强加的要求，(N)层将拒绝这一服务请求。

(N)层也将给被请求的保护服务添加上安全服务，这一所要求的安全服务在 SMIB 中是作为“委托者”而被定义的，以达到这一目标安全保护。

如果(N+1)实体不指明一个目标安全保护，那么(N)层将遵循与 SMIB 相一致的安全策略。这可能是使用在 SMIB 中为这个(N+1)实体定义的区段内缺省安全保护而继续进行通信。

6.2.2　提供保护服务

在已决定了行政管理强加与动态选取安全要求相结合之后，如在 6.2.1 条中所述，该(N)层将试图最低限度地达到目标保护。这将由下述方法实现，或用其一，或两者兼用。

a.在(N)层中直接调用安全机制;

b.从(N-1)层请求保护。这时，经可信功能度和/或(N)层中特定的安全机制的结合保护的范围必须扩展到该(N)服务。

注：这并不一定意味着(N)层中所有的功能度必须是可信任的。

因此，(N)层决定它是否能达到受请求的目标保护。如果它不能达到，通信就不发生。

6.2.2.1　受保护(N)连接的建立

下面的讨论是讲在(N)层内提供服务(与之相对的是对(N-1)服务的依赖)。

在某些协议中，为达到满意的目标保护，操作的顺序是至关重要的。

a.出访问控制

(N)层可以担负出访问控制，即它可以在本地(从 SMIB)决定是否可以试图建立保护(N)连接，或是禁止建立。

b.对等实体鉴别

如果目标保护包含了对等实体鉴别，或者如果知道(从 SMIB)目的地的(N)实体将要求对等实体鉴别，那么就必须发生鉴别交换。这可以利用两方或三方握手来提供所需的单方或相互鉴别。

有的时候，此种鉴别交换可结合到通常的(N)连接建立规程中去。在别的情况下，鉴别交换可以与(N)连接的建立分开来单独完成。

c.访问控制服务

目的(N)实体，或中间实体可以强加访问控制约束。如果特定的信息为一个远程访问控制机制所要求，那么始发(N)实体便在(N)层协议中，或经由管理信道提供这一信息。

d.机密性

如果全机密服务或选择性机密服务被选定，就一定得建立一个保护(N)连接。这必须包括建立恰当的工作密钥和协商对于此次连接的密码参数。在鉴别交换中这可以预定，或由一个单独的协议来完成。

e.数据完整性

如果选定了全部(N)用户数据的完整性，带或不带恢复，或选定了选择字段的完整性，就一定得建立一个保护(N)连接。这可能是为提供机密性服务而建立的同一个连接，而且它可以提供鉴别。同样的考虑适用于对保护(N)连接的机密性服务。

f.抗抵赖服务

如果选定了数据原发证明的抗抵赖，就必须建立适当的密码参数，或者建立带公证实体的保护连接。

如果选定了交付证明的抗抵赖，就必须建立适当的参数(它不同于对数据原发证明的抗抵赖所要求的参数)，或者建立带有公证实体的保护连接。

注：保护(N)连接的建立可能由于在密码参数上没有遵守协议而失败(可能包括不占有恰当的密钥)，或者由于遭到一个访问控制机制的拒绝而失败。

6.2.3　保护(N)连接的操作

6.2.3.1　在保护(N)连接的数据传送阶段，必须提供经协商的保护服务。

在(N)服务范围内，下列各项可见的:

a.对等实体鉴别(间隔进行);

b.选择字段的保护;

c.报告主动攻击(例如,当数据操作已在进行，而且正在提供的服务为“不带恢复的连接完整性”时，见5.2.4.2条)。

此外，还可能需要:

a.安全审计跟踪记录;

b.事件检测与处理。

6.2.3.2　对选择性应用能起作用的服务为:

a.机密性;

b.数据完整性(可能与鉴别一起);

c.抗抵赖(接收方或发送方)。

注：①为了标明选来作服务应用的那些数据项，有两种办法。第一种办法是使用“粗体”。预先假定表示层将识别某些字体，知道它们要求应用某种保护服务。第二种办法是用某种形式的标志符去标记那些对它们将应用指定的保护服务的数据项。

②可以认为提供抗抵赖服务的选择应用的一个理由可能来自下述情况:在双方(N)实体就某一数据项的最后版本取得相互认可之前，某种形式的协商对话在联系中发生。这时，所指的接受者可以要求发送者把抗抵赖服务(带数据原发和交付证据)应用于该数据项的最后同意的版本。发送者请求并获得这些服务,将这些数据项发送出去，然后接收通知：该数据项已被收到并为接收者所承认。这种抗抵赖服务使数据项的发出者与接受者确信该数据已被成功地发送。

③两种抗抵赖服务(即数据原发证明和交付证明)由发出者调用。

6.2.4　提供保护无连接数据传输　　不是所有在面向连接协议中可用的安全服务都能用于无连接协议。具体地说，抗删除、插入与重演攻击的保护，如果需要，必须在面向连接的更高的层次上提供。对重演攻击的有限的保护可由时间标记机制提供。此外，一些其他的安全服务不能提供面向连接协议能够达到的同样的安全强度。

适宜于无连接数据传输的保护服务如下:

a.对等实体鉴别(见 5.2.1.1 条)；

b.数据原发鉴别(见 5.2.1.2 条)；

c.访问控制服务(见 5.2.2 条)；

d.无连接机密性(见 5.2.3.2 条)；

e.选择字段机密性(见 5.2.3.3 条)；

f.无连接完整性(见 5.2.4.4 条)；

g.选择字段无连接完整性(见 5.2.4.5 条)；

h.带数据原发证明的抗抵赖(见 5.2.5.1 条)。

提供的这些服务机制为加密、签名机制，访问控制机制，路由选择机制,数据完整性机制和公证机制(见 5.3 条)。

无连接数据传输的发出者将必须保证它发出的单个 SDU 包含了使它在目的地被接受所需的全部信息。

7　安全服务与安全机制的配置

本章规定在OSI基本参考模型的框架内提供的安全服务，并简要说明实现它们的方式。任何一个安全服务都是按要求来选择提供的。

本章中在识别某一具体的安全服务时是由一个特定层选择提供的，除非特别说明，这种安全服务就由运行在该层的安全机制来提供。如第6章中所述，多个层能提供特定的安全服务。这样的层不总是从它们本身提供这些安全服务，而可以使用在较低层中提供的适当的安全服务。即使在一个层内没有提供安全服务，该层的服务定义也可能需要修改以便容许安全服务的请求传递到较低层。

注：①普通性安全机制(见5.4条)不在本章中讨论。

②为各种应用选取加密机制的位置在附录C(参考件)中讨论。

7.1　物理层

7.1.1　服务

在物理层上或单独或联合提供的安全服务仅有：

a.连接机密性；

b.通信业务流机密性。

通信业务流机密性采取两种形式：

(1)全通信业务流机密性。它只在某些情况下提供，例如，双向同时、同步、点对点传输；

(2)有限通信业务流机密性。它能为其他传输类型而提供，例如异步传输。

这些安全服务只限于对付被动威胁，能应用于点对点，或多对等实体通信。

7.1.2　机制

数据流的总加密是物理层上主要的安全机制。

一种只能用于物理层的，特有的加密形式为传输安全(即展宽频谱安全)。

物理层保护是借助一个操作透明的加密设备来提供的。物理层保护的目标是保护整个物理服务数据比特流，以及提供通信业务流的机密性。

7.2　数据链路层

7.2.1　服务

在数据链路层上提供的安全服务仅为：

a.连接机密性;

b.无连接机密性。

7.2.2 机制

加密机制用来提供数据链路层中的安全服务[见附录C(参考件)]。

链路层的这些附加安全保护功能度是在为传输而运行的正常层功能之前、和为接收而运行的正常层功能之后执行，即是说，安全机制基于并使用了所有这些正常的层功能。

在数据链路层上的加密机制对链路层协议是敏感的。

7.3 网络层

网络层是在内部组织起来提供执行下列操作的协议:

a.子网访问;

b.与子网有关的收敛;

c.与子网无关的收敛;

d.中继与路由选择。

7.3.1 服务

执行与OSI网络服务相关联的子网访问功能，该功能的协议可以提供下列安全服务:

a.对等实体鉴别;

b.数据原发鉴别;

c.访问控制服务;

d.连接机密性;

e.无连接机密性;

f.通信业务流机密性;

g.不带恢复的连接完整性;

h.无连接完整性。

这些安全服务可以单独或联合提供。与提供OSI网络服务相关联从端系统到端系统的中继与路由选择操作的协议能提供的安全服务与执行子网访问操作的协议所提供的相同。

7.3.2 机制

7.3.2.1　执行与 OSI 网络服务相关联的子网访问协议和从端系统到端系统的中继与路由选择操作的协议使用相同的安全机制。路由选择在这一层上执行，所以路由选择控制也在这一层执行。上面列举的那些安全服务以如下机制予以提供:

a.对等实体鉴别服务由密码导出的或受保护的鉴别交换、受保护口令交换与签名机制的适当配合来提供;

b.数据原发鉴别服务能够由加密或签名机制提供;

c.访问控制服务通过恰当使用特定的访问控制机制来提供;

d.连接机密性服务由加密机制和路由选择控制提供;

e.无连接机密性服务由加密机制与路由选择控制提供;

f.通信业务流保密服务由通信业务填充机制,并配以网络层或在网络层以下的一种机密性服务或路由选择控制来获得;

g.不带恢复的边疆完整性服务通过使用数据完整性机制，有时结合加密机制来提供;

h.无连接完整性服务通过使用数据完整性机制，有时配合上加密机制来提供。

7.3.2.2　执行与从端系统到端系统 OSI 网络服务相关联的子网访问操作的协议中的机制提供跨越单个子网的服务。

子网管理强制实现的子网保护将应用在子网访问协议的支配之下，但通常在正常的子网传输功能之前和正常的子网接收功能之后应用。

7.3.2.3　跨越一个或多个互连网络的服务机制由执行端系统到端系统、与提供 OSI 网络服务相关联的中继与路由选择操作的协议来提供。

这些机制将在传输时的中继与路由功能之前和接收时的中继与路由选择功能之后调用。在路由选择控制机制的情形，从 SMIB 导出适当的约束信息，然后数据与这些必要的路由选择约束一起被传递给中继与路由选择功能。

7.3.2.4　网络层中的访问控制能够为多种目的服务。例如，它允许端系统去控制网络连接的建立和拒绝不需要的呼叫。它也允许一个或多个子网去控制网络层资源的使用。在某些情况下，这后一目的与使用网络的费用有关。

注:网络连接的建立常可能导致子网管理上的收费。通过控制访问和选取反向付费或其他网络特定参数能使费用降到最低限度。

7.3.2.5　一特定子网的要求可能把访问控制机制强加在执行从端系统到端系统与提供OSI网络服务相关联的子网访问操作的协议上。当访问控制机制是由执行从端系统到端系统、与提供OSI网络服务相关联的中继与路由选择操作的协议提供时，既可用它们来控制中继实体对子网的访问，也可用来控制对端系统的访问。显而易见，访问控制的这种隔离程度是相当粗糙的，只能在网络层实体之间进行区分。

7.3.2.6　如果通信业务填充与网络层中的一种加密机制配合起来使用(或是从物理层来的机密性服务)，将会使通信业务流的机密性达到相当高的水准。

7.4　运输层

7.4.1　服务

在运输层上可以单独或联合提供的安全服务如下:

a.对等实体鉴别;

b.数据原发鉴别;

c.访问控制服务;

d.连接机密性;

e.无连接机密性;

f.带恢复的连接完整性;

g.不带恢复的连接完整性;

h.无连接完整性。

7.4.2　机制

上面列举的那些安全服务以如下机制予以提供:

a.对等实体鉴别服务是由密码导出的或受保护的鉴别交换、受保护口令交换与签名机制的适当配合来提供的;

b.数据原发鉴别服务由加密或签名机制提供;

c.访问控制服务通过适当使用特定的访问控制机制来提供;

d.连接机密性服务由加密机制提供;

e.无连接机密性服务由加密机制提供;

f.带恢复的连接完整性服务的提供是使用数据完整性机制，有时由加密机制与之配合;

g.不带恢复的连接完整性服务的提供是使用数据完整性机制，有时由加密机制与之配合；

h.无连接完整性服务是使用数据完整性机制，有时配合上加密机制来提供的。

这些保护机制将按使得安全服务可以为单个运输连接所调用的方式运行。保护的结果将是此运输连接个体能被隔离于所有其他运输连接之外。

7.5 会话层

7.5.1 服务

表示层将提供设施以支持经应用层向应用进程提供下列安全服务:

a.连接机密性;

b.无连接机密性;

c.选择字段机密性;

在表示层中的设施也可以支持经应用层向应用进程提供下列安全服务:

d.通信业务流机密性;

e.对等实体鉴别;

f.数据原发鉴别;

g.带恢复的连接完整性;

h.不带恢复的连接完整性;

j.选择字段连接完整性;

k.无连接完整性;

选择字段无连接完整性; m.

n.数据原发证明的抗抵赖;

p.交付证证明的抗抵赖。

注: 由表示层提供的设施依赖于只能运行在数据传送语法编码上的机制,也包括，例如，基于密码技术的设施。

7.6.2 机制

对于下面所列的安全服务，支持机制可以设置在表示层上，如果这样，就可以用来与应用层安全机制相配合以提供应用层安全服务。

a.对等实体鉴别服务能够由语法变换机制(例如加密)支持;

b.数据原发鉴别服务能够由加密或签名机制支持;

c.连接机密性服务能够由加密机制支持;

d.无连接机密性服务能够由加密机制支持;

e.选择字段机密性服务能够由加密机制支持;

f.通信业务流机密性服务能够由加密机制支持;

g.带恢复的连接完整性能够由数据完整性机制支持，有时由加密机制与之配合;

h.不带恢复的连接完整性服务能够由数据完整性机制支持，有时由加密机制与之配合;

j.选择字段连接完整性服务能够由数据完整性机制支持，有时由加密机制与之配合;

k.无连接完整性服务能够由数据完整性机制支持，有时由加密机制与之配合;

m.选择字段无连接完整性服务能够由数据完整性机制支持，有时由加密机制与之配合;

n.数据原发证明的抗抵赖服务能够由数据完整性、签名与公证机制的适当结合来支持;

p.交付证明的抗抵赖服务能够由数据完整性，签名与公证机制的适当结合来支持。

应用于数据传送的加密机制，当它设置在较高层时，将包含在表示层中。

上面所列的某些安全服务也能由完全包含在应用层中的安全机制来选择提供。

只有那些机密性安全服务能够由包含在表示层的安全机制完全提供。

在表示层中的安全机制发送时运行于传送语法变换的最后阶段，接收时运行于该变换过程的初始阶段。

7.7　应用层

7.7.1　服务

应用层可以提供一项或多项下列基本的安全服务，或单独提供，或联合提供;

a.对等实体鉴别;

b.数据原发鉴别;

c.访问控制服务;

d.连接机密性;

e.无连接机密性;

f.选择字段机密性;

g.通信业务流机密性;

h.带恢复的连接完整性;

j.不带恢复的连接完整性;

k.选择字段连接完整性;

m.无连接完整性;

n.选择字段无连接完整性;

p.数据原发证明的抗抵赖;

q.交付证明的抗抵赖。

在实开放系统中，认定的通信各方的鉴别对OSI资源和非OSI资源(例如，文件、软件、终端、打印机等)的访问控制提供支持。

在一次通信事例中要决定特定的安全要求，包括数据机密性，完整性与鉴别，可以由OSI安全管理，或由应用层管理按在SMIB中的信息以及应用进程提出的请求来作出。

7.7.2 机制

在应用层中的安全服务借助下列机制予以提供:

a.对等实体鉴别服务能够通过在应用实体之间传送的鉴别信息来提供，这些信息受到表示层或较低层的加密机制的保护;

b.数据原发鉴别服务能够通过使用签名机制或较低层的加密机制予以支持;

c.对一个实开放系统的与OSI有关的那些方面——例如与特定系统或远程应用实体通信的能力——的访问控制服务，可由在应用层中的访问控制机制与在较低层的访问控制机制联合起来提供;

d.连接机密性服务能够通过使用一个较低层的加密机制予以支持;

e.无连接机密性服务能够通过使用一个较低层的加密机制予以支持;

f.选择字段机密性服务能够通过使用在表示层上的加密机制予以支持;

g.一种有限的通信业务流机密性服务能够通过使用在应用层上的通信业务填充机制并配合一个较低层上的机密性服务予以支持;

h.带恢复的连接完整性服务能够通过使用一个较低层的数据完整性机制予以支持(有时要加密机制与之配合);

j.不带恢复的连接完整性服务能够通过使用一个较低层的数据完整性机制予以支持(有时要加密机制相配合);

k.选择字段连接完整性服务能够通过使用表示层上的数据完整性机制(有时配合上加密机制)予以支持;

m.无连接完整性服务能够通过使用一个较低层的数据完整性机制予以支持(有时要加密机制相配合);

n.选择字段无连接完整性服务能够通过使用表示层上的数据完整性机制(有时配合上加密机制)予以支持;

p.数据原发证明的抗抵赖服务能够通过签名机制与较低层的数据完整性机制的适当结合予以支持，并与第三方公证相配合;

q.交付证明的抗抵赖服务能够通过签名机制与较低层数据完整性机制的适当结合予以支持，并与第三方公证相配合。

如果一种公证机制被用来提供抗抵赖服务，它将作为可信任的第三方起作用。为了解决纠纷，它可以有一个用数据单元的传送形式(即传送语法)中继的数拓单元记录。它可以使用从较低层提供的保护服务。

7.7.3　非OSI安全服务

应用进程本身基本上可以提供所有这些服务，并使用同种类的机制，这些机制在本标准中是适当地放置在体系结构的不同层上加以描述的。这种使用不在OSI服务、协议定义及OSI体系结构的范围之内，但并不与之冲突。

7.8　安全服务与层的关系的实例

表2表明在参考模型的各个层上能够提供哪些特定的安全服务。在5.2条中可找到对这些安全服务的描述。一种安全服务设置在一个特定层上的理由在附录B(参考件)中给出。

表2

服务 \ 层	1	2	3	4	5	6	7
对等实体鉴别	•	•	Y	Y	•	•	Y

数据原发鉴别	•	•	Y	Y	•	•	Y
访问控制服务	•	•	Y	Y	•	•	Y
连接机密性	Y	Y	Y	Y	•	•	Y
无连接机密性	•	Y	Y	Y	•	•	Y
选择字段机密性	•	•	•	•	•	•	Y
通信业务流机密性	Y	•	Y	•	•	•	Y
带恢复的连接完整性	•	•	•	Y	•	•	Y
不带恢复的连接完整性	•	•	Y	Y	•	•	Y
选择字段连接完整性	•	•	•	Y	•	•	Y
无连接完整性	•	•	Y	Y	•	•	Y
选择字段无连接完整性	•	•	•	•	•	•	Y
抗抵赖，带数据原发证据	•	•	•	•	•	•	Y
抗抵赖，带交付证据	•	•	•	•	•	•	Y

说明：Y——服务应该作为提供者的一种选项被并进入该层的标准之中。

• ——不提供。

——应该指出，就第 7 层而言，应用进程本身可以提供安全服务。

注：①表 2 并不指明表中各项具有同等的重要性，相反在表中项目间存在相当大的等级差别。

②网络层中安全服务的配置说明于 7.3.2 条中。在网络层中安全服务的位置对将被提供的服务的性质与范围有很大影响。

③表示层包含许多支持应用层提供安全服务的安全设施。

8　安全管理

8.1　概述

8.1.1　OSI 安全管理涉及与 OSI 有关的安全管理以及 OSI 管理的安全两个方面。OSI 安全管理与这样一些操作有关，它们不是正常的通信情况但却为支持与控制这些通信的安全所必需。

注:通信服务的有效性决定于网络设计、或网络管理协议，或两者兼而有之。对此需要作适当的选择，以防止服务的拒绝。

8.1.2　由分布式开放系统的行政管理强加的安全策略可以是各种各样的，OSI 安全管理标准应该支持这样的策略。从属于单一的安全策略、受单个授权机构管理的多个实体有时构成的集合称之为“安全域”。安全域以及它们的相互作用是有待进一步开拓的重要领域。

8.1.3　OSI 安全管理涉及到 OSI 安全服务的管理与安全机制的管理。这样的管理要求给这些服务与机制分配管理信息，并收集与这些服务和机制的操作有关的信息。例如，密钥的分配，设置行政管理强加的安全选择参数，报告正常的与异常的安全事件(审计跟踪),以及服务的激活与停活。安全管理并不强调在呼叫特定的安全服务的协议中(例如连接请求的参数中)传递与安全有关的信息。

8.1.4　安全管理信息库(SMIB)是一个概念上的集存地，存储开放系统所需的与安全有关的全部信息。这一概念对信息的存储形式与实施方式不提出要求。但是每个端系统必须包含必需的本地信息使它能执行某个适当的安全策略。SMIB 在端系统的一个(逻辑的或物理的)组中执行一种协调的安全策略是必不可少的,在这一点上，SMIB 是一个分布式信息库。在实际中，SMIB 的某些部分可以与 MIB 结合成一体，也可以分开。

注:SMIB 能有多种实现办法，例如: a)数据表; b)文卷; c)嵌入实开放系统软件或硬件中的数据或规则。

8.1.5　管理协议，特别是安全管理协议，以及传送这些管理信息的通信信道潜在着抗攻击的脆弱性。所以应加以特别关心以确保管理协议与信息受到保护,不致削弱为通常的通信实例提供的安全保护。

8.1.6　安全管理可以要求在不同系统的行政管理机构之间交换与安全有关的信息,以便使 SMIB 得以建立或扩充。在某些情况下，与安全有关的信息将经由非 OSI 通信通路传递，局部系统的管理者也将采用非 OSI 标准化方法来修改 SMIB。在另外一些情况下，可能希望在一个 OSI 通信通路上交换这样的信息，这时这些信息将在运行于实开放系统中的两个安全管理应用之间传递。该安全管理应用将使用这些通信信息来修改 SMIB。SMIB 的这种修改可以要求事先给适当的安全管理者授权。

8.1.7　应用协议将为在 OSI 通信信道上交换与安全有关的信息作出规定。

8.2　OSI 安全管理的分类

有三类 OSI 安全管理活动:

a.系统安全管理;

b.安全服务管理;

c.安全机制管理。

此外，还必须考虑到 OSI 管理本身的安全(见 8.2.4 条)。对这几类安全管理所执行的关键功能概述如下。

8.2.1　系统安全管理

系统安全管理涉及总的 OSI 环境安全方面的管理。下列各项为属于这一类安全管理的典型活动:

a.总体安全策略的管理，包括一致性的修改与维护;

b.与别的 OSI 管理功能的相互作用;

c.与安全服务管理和安全机制管理的交互作用;

d.事件处理管理(见 8.3.1 条);

e.安全审计管理(见 8.3.2 条);

f.安全恢复管理(见 8.3.3 条)。

8.2.2　安全服务管理

安全服务管理涉及特定安全服务的管理。下列各项为在管理一种特定安全服务时可能执行的典型活动:

a.为该种服务决定与指派目标安全保护;

b.指定与维护选择规则(存在可选情况时)，用以选取为提供所需的安全服务而使用的特定的安全机制;

c.对那些需要事先取得管理同意的可用安全机制进行协商(本地的与远程的);

d.通过适当的安全机制管理功能调用特定的安全机制，例如，用来提供行政管理强加的安全服务;

e.与别的安全服务管理功能和安全机制管理功能的交互作用。

8.2.3　安全机制管理

安全机制管理涉及的是特定安全机制的管理。下列各项为典型的安全机制管理功能，但并未包罗无遗:

a.密钥管理;

b.加密管理;

c.数字签名管理;

d.访问控制管理;

e.数据完整性管理;

f.鉴别管理;

g.通信业务填充管理;

h.路由选择控制管理;

j.公证管理。

上列各项安全机制管理功能在8.4条中详加讨论。

8.2.4 OSI管理的安全

所有OSI管理功能的安全以及OSI管理信息的通信安全是OSI安全的重要部分。这一类安全管理将借助对上面所列的OSI安全服务与机制作适当的选取以确保OSI管理协议与信息获得足够的保护(见8.1.5条)。例如，在管理信息库的管理实体之间的通信一般将要求某种形式的保护。

8.3 特定的系统安全管理活动

8.3.1 事件处理管理

在OSI中可以看到的属于事件处理管理的方面为远程报告那些违反系统安全的明显企图，以及对用来触发事件报告的阈值的修改。

8.3.2 安全审计管理

安全审计管理可以包括:

a.选择将被记录和被远程收集的事件;

b.授予或取消对所选事件进行审计跟踪日志记录的能力;

c.所选审计记录的远程收集;

d.准备安全审计报告。

8.3.3 安全恢复管理

安全恢复管理可以包括:

a.维护那些用来对实有的或可疑的安全事故作出反应的规则:

b.远程报告对系统安全的明显违反;

c.安全管理者的交互作用。

8.4　安全机制的管理功能

8.4.1　密钥管理

密钥管理可以包括:

a.间歇性地产生与所要求的安全级别相称的合适密钥;

b.根据访问控制的要求，对于每个密钥决定哪个实体应该接受密钥的拷贝;

c.用可靠办法使这些密钥对实开放系统中的实体实例是可用的，或将这些密钥分配给它们。

要知道某些密钥管理功能将在OSI环境之外执行。这包括用可靠手段对密钥进行物理的分配。

用于一次联系中的工作密钥的交换是一种正常的层协议功能。工作密钥的选取也可以通过访问密钥分配中心来完成，或经管理协议作事先的分配。

8.4.2　加密管理

加密管理可以包括:

a.与密钥管理的交互作用;

b.建立密码参数;

c.密码同步.

密码机制的存在意味着使用密码管理，和采用共同的方式调用密码算法。由加密提供的保护的辨别水准决定于OSI环境中哪些实体独立地使用密钥。一般说来，这反过来又决定于安全体系结构，特别地由密钥管理机制决定。

为获得对加密算法的共同调用可使用密码算法寄存器，或在实体间进行事前的协商。

8.4.3　数字签名管理

数字签名管理可以包括:

a.与密钥管理的交互作用;

b.建立密码参数与密码算法;

c.在通信实体与可能有的第三方之间使用协议。

注:一般说来，数字签名管理与加密管理极为类似。

8.4.4　访问控制管理

访问控制管理可涉及到安全属性(包括口令)的分配，或对访问控制表或权力表进行修改。也可能涉及到在通信实体与其他提供访问控制服务的实体之间使用协议。

8.4.5　数据完整性管理

数据完整性管理可以包括:

a.与密钥管理的交互作用;

b.建立密码参数与密码算法;

c.在通信的实体间使用协议。

注:当对数据完整性使用密码技术时，数据完整性管理便与加密管理极为类似。

8.4.6　鉴别管理

鉴别管理可以包括把说明信息，口令或密钥(使用密钥管理)分配给要求执行鉴别的实体。它也可以包括在通信的实体与其他提供鉴别服务的实体之间使用协议。

8.4.7　通信业务填充管理

通信业务填充管理可包括维护那些用作通信业务填充的规则。例如,这可以包括:

a.预定的数据率;

b.指定随机数据率;

c.指定报文特性，例如长度;

d.可能按日时间或日历来改变这些规定。

8.4.8　路由选择控制管理

路由选择控制管理涉及确定那些按特定准则被认为是安全可靠或可信任的链路或子网络。

8.4.9　公证管理

公证管理可以包括:

a.分配有关公证的信息;

b.在公证方与通信的实体之间使用协议;

c.与公证方的交互作用。

附录 A

有关 OSI 中安全问题的背景信息

(参考件)

A1　背景情况

本附录提供:

a.有关 OSI 安全的信息，以便对本标准有一个更广泛的了解;

b.各种安全特点与要求在体系结构意义上的背景。

OSI 环境中的安全仅仅是数据处理与数据通信安全的一个方面。在 OSI 环境中所采取的保护措施要有效，就需要有 OSI 之外的某些措施予以支持。例如，对在系统之间流动的信息可以加密，但如果在对这些系统本身的访问上不设置物理上的安全限制，加密就可能是徒劳的。而 OSI 只涉及系统的互连。为了 OSI 安全措施的有效性，它们将与不属于 OSI 范围的措施配合起来使用。

A2　对安全的要求

A2.1　安全的含义是什么?

这里的“安全”一词是用来指将财富与资源的脆弱性降到最低限度。财富是指任何有价值的东西。脆弱性是指可利用侵害系统或系统内信息的任何弱点。威胁乃是对安全潜在有的侵害。

A2.2　在开放系统中要求安全的原因

国际标准化组织(ISO)认为为了提高 OSI 体系结构的安全性有必要制定一系列标准。这种必要性来源于:

a.社会对计算机的依赖性在增长，这些计算机是通过数据通信来访问或连接的，它们要求保护以抵御各种威胁;

b.在一些国家中出现了“数据保护”法规，迫使供应商表明系统的完整性与保密性;

c.各种组织对现存的和未来的安全系统而言，使用 OSI 标准的愿望随着需要而增强。

A2.3　需要保护的是什么?

一般说来，下列各项可以要求保护:

a.信息与数据(包括软件，以及与安全措施有关的被动数据，例如口令)；

b.通信和数据处理服务；

c.设备与设施。

A2.4　威胁

对数据通信系统的威胁包括：

a.对通信或其他资源的破坏；

b.对信息的讹用或篡改；

c.信息或其他资源的被窃，删除或丢失；

d.信息的泄露；

e.服务的中断。

可以将威胁分为偶发性与故意性两类，也可以是主动威胁或被动威胁。

A2.4.1　偶发性威胁

偶发性威胁是指那些不带预谋企图的威胁。偶发性威胁的实例包括系统故障，操作失误和软件出错。

A2.4.2　故意性威胁

故意性威胁的范围可从使用易行的监视工具进行随意的检测到使用特别的系统知识进行精心的攻击。一种故意的威胁如果实现就可认为是一种“攻击”。

A2.4.3　被动威胁

被动威胁是指这样的威胁：它的实现不会导致对系统中所含信息的任何篡改，而且系统的操作与状态也不受改变。使用消极的搭线窃听办法以观察在通信线路上传送的信息就是被动威胁的一种实现。

A2.4.4　主动威胁

对系统的主动威胁涉及到系统中所含信息的篡改，或对系统的状态或操作的改变。一个非授权的用户不怀好意地改动路由选择表就是主动威胁的一个例子。

A2.5　几种特定类型的攻击

下面简要列举在数据处理与数据通信环境中特别关心的几种攻击。在下列各条中，出现“授权”与“非授权”两个术语。“授权”意指“授予权力”。这个定义包含的两层意思为：这里的权力是指进行某种活动的权力(例如访问数据)；这样的

权力被授予某个实体、代理人或进程。于是，授权行为就是履行被授予权力(未被撤消)的那些活动。关于授权概念详见 A3.3.1 条。

A2.5.1　冒充

冒充就是一个实体假装成一个不同的实体。冒充常与某些别的主动攻击形式一起使用，特别是消息的重演与篡改。例如，鉴别序列能够被截获，并在一个有效的鉴别序列发生之后被重演。特权很少的实体为了得到额外的特权可能使用冒充装扮成具有这些特权的实体。

A2.5.2　重演

当一个消息，或部分消息为了产生非授权效果而被重复时例出现重演。例如，一个含有鉴别信息的有效消息可能为另一个实体所重演，目的是鉴别它自己(把它当作其他实体)。

A2.5.3　消息篡改

当数所传送的内容被改变而未发觉，并导致一种非授权后果时例出现消息篡改。例如，消息“允许约翰·斯密司读机密文卷“帐目”被篡改为“允许弗雷德·布劳恩读机密文卷“帐目”。

A2.5.4　服务拒绝

当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行它们的正当功能的时候便发生服务拒绝。这种攻击可能是一般性的，比如一个实体抑制所有的消息，也可能是有具体目标的，例如一个实体抑制所有流向某一特定目的的端的消息，如安全审计服务。这种攻击可以是对通信业务流的抑制,如本例中所述，或产生额外的通信业务流。也可能制造出试图破坏网络操作的消息，特别是如果网络具有中继实体，这些中继实体根据从别的中继实体那里接收到的状态报告来作出路由选择的决定。

A2.5.5　内部攻击

当系统的合法用户以非故意或非授权方式进行动作时例出现内部攻击。多数已知的计算机犯罪都和使系统安全遭受损害的内部攻击有密切的关系。能用来防止内部攻击的保护方法包括:

a.对工作人员进行仔细审查;

b.仔细检查硬件、软件、安全策略和系统配制,以便在一定程度上保证它们运行的正确性(称为可信功能度);

c.审计跟踪以提高检测出这种攻击的可能性。

A2.5.6　外部攻击

外部攻击可以使用的办法如:

a.搭线(主动的与被动的);

b.截取辐射;

c.冒充为系统的授权用户，或冒充为系统的组成部分;

d.为鉴别或访问控制机制设置旁路。

A2.5.7　陷井门

当系统的实体受到改变致使一个攻击者能对命令，或对预定的事件或事件序列产生非授权的影响时，其结果就称为陷井门。例如，口令的有效性可能被修改，使得除了其正常效力之外也使攻击者的口令生效。

A2.5.8　特洛伊木马

对系统而言的特洛伊木马，是指它不但具有自己的授权功能，而且还有非授权功能。一个也向非授权信道拷贝消息的中继就是一个特洛伊木马。

A2.6　对威胁、风险与抵抗措施的评估

系统的安全特性通常会提高系统的造价，并且可能使该系统难于使用。所以,在设计一个安全系统之前,应该明确哪些具体威胁需要保护措施来对付。这叫做威胁评估。一个系统易受攻击的地方是多方面的，但只有其中的几个方面是可被利用的,这或是因为攻击者缺乏机会，或是因为得到的结果不值得去作这种努力和冒被检测到的风险。虽然关于威胁评估的详情细节不属本附录的范围，但大致来说包括:

a.明确该系统的薄弱环节;

b.分析目的在于利用这些薄弱环节进行威胁的可能性;

c.评估如果每种威胁都成功所带来的后果;

d.估计每种攻击的代价;

e.估算出可能的应付措施的费用;

f.选取恰当的安全机制(可能要使用价值效益分析)。

非技术性措施，例如交付保险，对于技术性安全措施而言在价值上也可能是一种有效的选择。技术上要做到完全安全好比要做到安全的物理保护，同样是不可能。所以，目标应该是使攻击所化的代价足够高而把风险降低到可接受的程度。

A3　安全策略

本章讨论安全策略，问题包括：需要一个规定恰当的安全策略；安全策略的作用；使用中的策略方法；和为了应用于具体情况而作的改进。然后将这些概念应用于通信系统。

A3.1　对安全策略的需要和安全策略的目的

安全的整个领域既复杂又广泛。任何一个相当完备的分析都将引出许许多多不同的细节，使人望而生畏。一个恰当的安全策略应该把注意力集中到最高权力机关认为须得注意的那些方面。概括地说，一种安全策略实质上表明；当所论的那个系统在进行一般操作时，在安全范围内什么是允许的，什么是不允许的。策略通常不作具体规定，即它只是提出什么是最重要的，而不确切地说明如何达到所希望的这些结果。策略建立起安全技术规范的最高一级。

A3.2　策略规定的含义：精确化过程

由于策略是很一般性的，因而这一策略如何与某一具体应用紧密结合，在开始是完全不清楚的。完成这一结合的最好办法经常是让这一策略经受一个不断精确化的改进过程，在每个阶段加进从应用中来的更多的细节。为了知道这些细节应当是什么就需要在总策略的指导下对该应用领域进行细致的考查和研究。这种考查应该决定出由于试图将策略的条件强加于应用而出现的问题。这一精确化过程将产生出用直接从应用中抽取来的确切语言重新表述的总策略。这个重新表述的策略使得易于去决定执行的细节。

A3.3　安全策略的组成部分

对于现存的安全策略有两个方面，它们都建立在授权行为这一概念之上。

A3.3.1　授权

已讨论过的所有威胁都与授权行为或非授权行为的概念有关。在安全策略中包含有对“什么构成授权”的说明。在一般性的安全策略中可能写有“未经适当授权的实体，信息不可以给予、不被访问、不允许引用、任何资源也不得为其所用”。按授权的性质以区分不同的策略。基于所涉及的授权的性质可将策略分为两种，即

基于规则的策略和基于身份的策略。第一种策略使用建立在不多的一般属性或敏感类之上的规则，它们通常是强加的。第二种策略涉及建立在特定的、个体化属性之上的授权准则。假定某些属性与被应用实体永久相关联；而其余属性可以是某种占有物(例如权力)，它们可传送给另外的实体。人们也可以将授权服务分为行政管理强加的授权服务与动态选取的授权服务两类。一个安全策略将决定那些系统安全要素，它们总是加以应用的，有效的(例如，基于规则的与基于身份的安全策略组成部分)，以及用户在认为合适时可选择使用的系统安全要素。

A3.3.2　基于身份的安全策略

安全策略的这一基于身份的方面，在一定程度上与“必需认识”的安全观念相当。它的目的是过滤对数据或资源的访问。基本上有两种执行基于身份策略的基本方法，视有关访问权的信息为访问者所拥有，还是被访问数据的一部分而定。前者的例子为特权标识或权力，给予用户并为代表该用户进行活动的进程所使用.后者的例子为访问控制表(ACL)。在这两种情况中，数据项的大小可以有很大的变化(从完整的文卷到数据元素)，这些数据项可以按权力命名,或带有它自己的 ACL。

A3.3.3　基于规则的安全策略

在基于规则的安全策略中的授权通常依赖于敏感性。在一个安全系统中,数据或资源应该标注安全标记。代表用户进行活动的进程可以得到与其原发者相应的安全标记。

A3.4　安全策略，通信与标记

标记的概念在数据通信环境中是重要的。带有属性的标记发挥多种作用。有在通信期间要移动的数据项，有发起通信的进程与实体；有响应通信的进程与实体；还有在通信时被用到的系统本身的信道和其他资源。所有这一切都可以设法用它们的属性来标记。安全策略必须指明属性如何能被使用以提供必要的安全。为了对那些特别标记的属性建立适当的安全意义可能需要进行协商。

当安全标志既附加给访问进程，又附加给被访问数据时，那么应用基于身份访问控制所需要的附加信息应是有关的标记。当一个安全策略是建立在访问数据的用户的身份之上时，不论是直接的或是通过进程，这时安全标记应该包含有关该用户的身份信息。用于特定标记的那些规则应该表示在安全管理信息库中的一个安全策略中，

如果需要，还应与端系统协商。标记可以附带属性，指明其敏感性，说明处理与分布上的隐蔽处，强制定时与定位，以及指明对该端系统特有的要求。

A3.4.1　进程标记

在鉴别中，完全识别发起与响应一个通信实例的那些进程或实体带有所有相应的属性，一般说来是特别重要的。所以，安全管理信息库(SMIB)将包含足够的信息说明对任一行政管理强加策略而言是重要的那些属性。

A3.4.2　数据项标记

当通信事例中数据项在移动时，每一个都与它的标记紧紧地接合在一起。(这种约束是有意义的，而且在某些基于规则的实例中，要求将此标记做成数据项的一个特别部分，然后交付应用)。保持数据项完整的技术也将保持准确性以及标记的耦合。这些属性能为 OSI 基本参考模型数据链路层中的路由选择控制功能所使用。

A4　安全机制

一种安全策略可以使用不同的机制来实施，或单独使用，或联合使用，取决于该策略的目的以及使用的机制。一般说来，一种机制属于下面(有重叠的)三类之一:

a.预防;

b.检测;

c.恢复。

下面讨论适合于数据通信环境的安全机制。

A4.1　密码技术与加密

密码学是许多安全服务与机制的基础。密码函数可用来作为加密，解密,数据完整性，鉴别交换，口令存储与检验等等的一部分，借以达到保密、完整性和鉴别的目的。用于机密性的加密把敏感数据(即受保护的数据)变换成敏感性较弱的形式。当用于完整性或鉴别时，密码技术被用来计算不可伪造的函数。

加密开始时在明文上实施以产生密文，解密的结果或是明文，或是在某种掩护下的密文。使用明文作通用的处理在计算上是可行的；它的语义内容是可以理解的。除了以特定的方式(例如本原解密或恰切匹配)在计算上是不能处理密文的，它的语义内容已隐藏起来。有时故意让加密是不可逆的(例如截短或数据丢失)，这时不希望导出原来的明文，例如口令。

密码函数使用密码变量，并作用于字段、数据单元或数据单元流上。两个密码变量为：密钥，它指导具体的变换；初始变量，为了保持密文外表的随机性在某些密码协议中需要它。密钥通常必须处于机密性状态，而且加密函数与初始变量可能加大延迟和提高带宽消耗。这使得把“透明的”和“可选的”密码技术加到现存系统中去变得复杂了。

不论对于加密或解密而言，密码变量可以是对称的，或非对称的。用在非对称算法中的密钥在数学上是相关的；一个密钥不能从另一个计算出来。这种算法有时称为公开密钥算法，这是因为可使一个密钥公之于众而另一个保持秘密。

当不知道密钥也能在计算上恢复明文时，密文可受到密码分析。如果使用一个脆弱的或是有缺陷的密码函数就会发生这种攻击。窃听和通信业务流分析可能导致对密码系统的攻击，包括消息和字段的插入、删除与更改，先前有效密文的播放，以及冒充。所以密码协议的设计要抗攻击，有时还要抗通信业务流分析。对付通信业务流分析的一种具体办法即“通信业务流机密性”，目的是掩蔽数据及其特征的出现或不出现。如果密文被中继，那么在中继站和网关上地址必须是明文。如果数据只在每个链路上是加密的，而在中继内或网关内被解密(因而易受攻击)，这种体系称为用的是“链路加密”。如果只有地址(及类似的控制数据)在中继或网关内是明文，这种体系称为“端到端加密”。从安全观点看来更希望有端到端加密，但在体系结构上带来相当大的复杂性，特别是如果包含有频带内电子密钥分配(一种密钥管理功能)，更是如此。链路加密与端到端加密可以联合起来使用以达到多种安全目标。数据完整性经常是借计算密码校验值来实现的。这种校验值可以在一步或多步内导出，而且是密码变量与数据的数字函数。这些校验值与要受到保护的那些数据相关联。这种密码校验值有时称为操作检测码。

密码技术能够提供，或有助于提供保护以防止：

a. 消息流的观察和篡改；

b. 通信业务流分析；

c. 抵赖；

d. 伪造；

e. 非授权连接；

f. 篡改消息。

A4.2　密钥管理方面

密码算法的使用就意味着要进行密钥管理。密钥管理包括密码密钥的产生、分配与控制。密钥管理方法的选取是基于参与者对使用该方法的环境所作的评估之上。对这一环境的考虑包括要进行防范的威胁(组织内部的和外部的),所使用的技术,提供的密码服务的体系结构与定位，以及密码服务提供者的物理结构与定位。关于密码管理需要考虑的要点包括:

a.对于每一个明显或隐含指定的密钥，使用基于时间的“存活期”，或使用别的准则;

b.按密钥的功能恰当地区分密钥以便可以按功能使用密钥，例如，打算用来作机密性服务的密钥就不应该用于完整性服务，反之亦然;

c.非 OSI 的考虑， 例如密钥的物理分配和密钥存档。

对于对称密钥算法，有关密钥管理要考虑的要点包括:

a.使用密钥管理协议中的机密性服务以运送密钥;

b.使用密钥体系。应该允许有各种不同情况，如:

1)“平直的”密钥体系，只使用加密数据密钥，从一个集合中按密钥的身份或索引隐含地或明显地进行选取;

2)多层型的密钥体系;

3)加密密钥的密钥决不应该用来保护数据，而加密数据的密钥也决不应该用为保护加密密钥的密钥。

c.将责任作分解使得没有一个人具有重要密钥的完全拷贝。

对于非对称密钥算法，有关密钥管理要考虑的要点包括:

a.使用密钥管理协议中的机密性服务以运送秘密密钥;

b.使用密钥管理协议中的完整性服务，或数据原发证明的抗抵赖服务以运送公钥。这些服务可以通过使用对称或非对称密码算法提供。

A4.3　数字签名机制

数字签名这一术语是用来指一种特别的技术，能够用它来提供诸如抗抵赖与鉴别等安全服务。数字签名机制要求使用非对称密码算法。数字签名机制的实质特征为:不使用私有密钥就不能造成签过名的那个数据单元。这意味着:

a.签过名的数据单元除了私有密钥的占有者外，别的个人是不能制造出来的;

b.接受者不能造出那签过名的数据单元。

所以，只需使用公开可用的信息就能认定数据单元的签名者只能是那些私有密钥的占有者。因而在当事人后来的纠纷中，就可能向一个可靠的第三方证明数据单元签名者的身份，这个第三方是被请来对签过名的数据单元的鉴别作出判决的。这种类型的数字签名称为直接签名方案(见图 A1)。在别的情况下，
可能需要再加一条特性(c)：

c.发送者不能否认发出过那个签过名的数据单元。

在这一情形，一个可信赖的第三方(仲裁人)向接受者证明该信息的来源与完整性。这种类型的数字签名有时称为仲裁签名方案(见图 A2)。

注:发送者可能要求接受者事后不能否认接受过该签名数据。这可用交付证明的抗抵赖服务来完成，方法是将数字签名机制、数据完整性机制与公证机制作适当的结合。

A4.4　访问控制机制

访问控制机制是用来实施对资源访问加以限制的策略的机制，这种策略把对资源的访问只限于那些被授权用户。技术包括使用访问控制表或矩阵(通常包含被控制项与被授权用户(例如人群或进程)的身份)，口令，以及权力，标记或标志，可以用对它们的占有来指示访问权。在使用权力的地方，权力应该是不可伪造的，而且用可靠的方式传递。

A4.5　数据完整性机制

数据完整性机制有两种类型:一种用来保护单个数据单元的完整性，另一种既保护单个数据单元的完整性，也保护一个连接上整个数据单元流序列的完整性。

A4.5.1　消息流的篡改检测

讹误检测技术，与通常通信链路和网络所引入的对比特错、码组错与顺序错的检测相关联，也能用来检测消息流的篡改。但如果协议的头标与尾标不受完整性机制的保护，那么一个知情的入侵者就可能成功地旁路这些检测。因而,成功的检测消息流的篡改只有使用讹误检测技术并配合以顺序信息才能达到。这不能防止消息流的篡改但将提供攻击的通知。

A4.6　鉴别交换机制

A4.6.1　机制的选取

适合于各种不同场合的鉴别交换机制有多种选择与组合。例如:

a.当对等实体以及通信手段都可信任时，一个对等实体的身份可以通过口令来证实。该口令能防止出错，但不能防止恶意行为(特别不能防止重演)。相互鉴别可在每个方向上使用不同的口令来完成;

b.当每个实体信任它的对等实体但不信任通信手段时，抗主动攻击的保护能够由口令与加密联合提供，或由密码手段提供。防止重演攻击的需要双方握手(用保护参数)，或时间标记(用可信任时钟)。带有重演保护的相互鉴别，使用三方握手就能达到;

c.当实体不信任(或感到它们将来可能不信任)它们的对等实体或通信手段时可以使用抗抵赖服务。使用数字鉴名机制和公证机制就能实现抗抵赖服务。这些机制可与上面 b 中所述的机制一起使用。

A4.7　通信业务填充机制

制造伪通信业务和将协议数据单元填充到一个定长能够为防止通信业务分析提供有限的保护。为了使保护成功，伪通信业务级别必须接近实际通信业务的最高预期等级。此外，协议数据单元的内容必须加密或隐藏起来，使得虚假业务不会被识别而与真实业务区分开来。

A4.8　路由选择控制机制

传送数据的路由警告说明(包括一整条路径的说明)可用来保证数据只在物理上安全的路由上传输，或保证敏感数据只在具有适当保护级别的路由上传输。

A4.9　公证机制

公证机制建立在可信任的第三方(公证人)的概念之上，以确保在两个实体间交换的信息的某些性质不致变化，例如，它的来源、完整性、或它被发出或收到的时间。

A4.10　物理安全与人员可靠

物理安全措施总是必需的以便获得完全的保护。物理安全的代价高，经常力求通过使用别的(更廉价的)技术把对它的需要降到最低限度。对物理安全与人员可靠方面的考虑不在 OSI 的范围之内，尽管所有系统将最终依靠某种形式的物理安全和对操作系统人员的信赖。为了保证正确的操作和明确人员的责任,应该确定好操作规程。

A4.11　可信任的硬件与软件

用来对实体的功能的正确性建立信任的方法包括:形式证明法，验证与证实,对已知的试图进行的攻击进行检测和记录，由一个可信任的人员在安全的环境中建造实体。预防也是需要的以保证实体例如在维护与改进时不会被偶然地或故意地修改,致使在它的运行期内危害安全。如果要保持安全，也必须对系统的某些实体建立功能正确性的信任，但用来建立信任的方法不在 OSI 的范围之内。

附录 B

第 7 章中安全服务与机制配置的理由

（参考件）

B1　概述

在第 7 章中已指明在不同层上所提供的安全服务，本附录对此说明一些理由。在标准的 6.1.1 条中提出的那些安全分层原则指导了这一选择过程。

一种特定的安全服务如果被认为在不同层上对总的通信安全的影响是不同的,便在多个层上提供(例如，在第一层与第四层上的连接机密性)。但是，考虑到现存的 OSI 数据通信机能(如多链路规程，多路复用功能，强化一个无连接服务为面向连接服务的不同方法)，以及为了让这些传输机制得以运行，允许一种特定服务在另一层上也被提供可能是必要的，尽管它们对安全的影响不能认为有什么不同。

B2　对等实体鉴别

第 1 层与第 2 层：没有。在这些层上对等实体鉴别被认为是无用的。

第 3 层：有。在一些单独的子网上和为了路由选择，或在网际上。

第 4 层：有。第四层中端系统到端系统的鉴别，在一个连接的开始前和持续过程中能够用来作两个或多个会话实体的相互鉴别。

第 5 层：没有。于第四层或更高层重复提供这一服务没有好处。

第 6 层：没有。但加密机制能支持在应用层的这种服务。

第 7 层：有。对等实体鉴别应该由应用层提供。

B3　数据原发鉴别

第 1 层与第 2 层：没有。在这些层上数据原发鉴别被认为是无用的。

第 3 层与第 4 层：数据原发鉴别能够端到端地提供于第 3 层和第 4 层的中继与路由选择作用之中，如下所述：

a.在建立连接时提供对等实体鉴别，并在连接存活期基于加密的连接鉴别,事实上也就提供了数据原发鉴别服务；

b.即使不提供 a 项中的服务，基于加密的数据原发鉴别也能通过对已经位于这两层中的数据完整性机制增加非常小的一点额外开销而提供。

第 5 层：没有。于第 4 层或第 7 层重复提供这一服务没有好处。

第 6 层：没有。但加密机制能支持在应用层提供这一服务。

第 7 层：有。可能要与表示层中的机制相配合。

B4　访问机制

第 1 层与第 2 层：在一个遵守完全的 OSI 协议的系统中，在第 1 层或第 2 层不能提供访问控制机制，这是因为没有可用于这样一种机制的端设备。

第 3 层：根据特定子网的要求，访问控制机制强加于子网访问作用之上。当由中继与路由选择作用执行时，在网络层中的访问机制既能用于控制中继实体对子网的访问，又能用于控制对端系统的访问。显然，这种访问粒度是非常粗糙的，它仅网络层的实体之间有所不同。

网络连接的建立往往会导致在子网管理上的费用。通常可通过访问控制、选用反向记费、或选用其他网络或子网特定参数来使费用降低到最低限度。

第 4 层：有。访问控制机制能够在每个运输连接端到端的基础之上而被使用。

第 5 层：没有。于第 4 层或第 7 层重复提供这一服务没有好处。

第 6 层：没有。第 6 层上这是不适宜的。

第 7 层：有。应用协议和应用进程能提供而向应用的访问控制业务。

B5　在(N)连接上全(N)用户数据的机密性

第 1 层：有。由于成对插入透明性的电气转换设备能给出物理连接上的完全机密性，所以应该提供。

第 2 层：有。但不给第 1 层或第 3 层的机密性提供更多的安全利益。

第 3 层：有。用于某些个体子网上的子网访问，以及网际上的中继与路由选择。

第 4 层：有。因为单个运输连接给出端到端运输机制并提供会话连接的隔离。

第 5 层：没有。在第 3、4、7 层的机密性上它不提供额外利益，在这一层上提供这一服务看来是不适宜的。

第 6 层：有。因为加密机制提供纯语法变换。

第 7 层：有。与较低层的机制相配合。

B6　在单个的无连接(N)-SDU 中全(N)用户数据的机密性

除第 1 层外，理由的说明与全用户数据的机密性相同。在第 1 层没有无连接服务。

B7　SDU 的(N)用户数据和选择字段的机密性

这种机密性服务由表示层中的加密来提供，并且根据数据的语义由应用层中的机制调用。

B8　通信业务流机密性

全通信业务流机密性只能在第 1 层实现。在物理传输通路中插入一对加密设备就能办到。假定传输通路是双向同时同步的，以便加密设备的插入将使物理媒体上的全部传输(甚至传输的出现)成为不易识别。

在物理层之上，全通信业务流安全是不可能的。在一个层上使用完全的 SDU 机密性服务，并在一个高层上注入伪通信业务能部分地产生这种机密性的某些效果。这样一种机制是高代价的，可能要耗用大量的载波与切换能力。

如果在第 3 层提供通信业务流机密性，那么将使用通信业务填充和路由选择控制。路由选择控制采用消息绕过不安全的链路或子网，可提供有限度的通信业务流机密性。但是把通信业务填充结合在第 3 层会使网络得到更好的利用，例如避免不必要的填充与网络拥塞。

在应用层上通过制造伪信息，并与防止识别这些伪通信业务的机密性相结合能提供有限度的通信业务流机密性。

B9　在(N)连接上(带差错恢复)全(N)用户数据的完整性

第 1 层与第 2 层：第 1 层与第 2 层不能提供这种服务。第 1 层没有检测或恢复机制，而第 2 层机制只运行在点对点基础上而不是端到端的，所以提供这种服务被认为是不适宜的。

第 3 层：没有。因为差错恢复不是普遍可用的。

第 4 层：有。因为这提供了真正的端到端运输连接。

第 5 层：没有。因为差错恢复不是第 5 层的功能。

第 6 层：没有。但加密机制能支持应用层中的这种服务。

第 7 层：有。与表示层中的机制相配合。

B10　在(N)连接上(无差错恢复)全(N)用户数据的完整性

第 1 层与第 2 层：第 1 层与第 2 层不能提供这种服务。第 1 层没有检测或恢复机制，第 2 层只能运行在点对点基础上而不是端到端的，所以提供这种服务被认为是不适宜的。

第 3 层：有。起到单个子网的子网访问，以及网际上的路由选择与中继作用。

第 4 层：有。对于这种情况，在检测到主动攻击之后停止通信是可取的。

第 5 层：没有。因为在第 3、4 层或第 7 层的数据完整性之上，它不提供额外的好处。

第 6 层：没有。加密机制能支持应用层中的这种服务。

第 7 层：有。与表示层中的机制相配合。

B11　在(N)连接上(不带恢复)传送的(N)-SDU 的(N)用户数据中选择字段的完整性

选择字段的完整性能够由表示层中的加密机制提供并与应用层中的调用机制与检测机制相配合。

B12　单个无连接(N)-SDU 中全(N)用户数据的完整性

为了把功能重复减少到最低限度，无连接传送的完整性应该只在那些提供不带恢复的完整性的层上提供，即网络层，运输层和应用层。这样的完整性机制可能只有非常有限的效用，这一点必须认识到。

B13　单个无连接(N)-SDU 中选择字段的完整性

选择字段的完整性能够由表示层中的加密机制提供并与应有层中调用机制与校验机制相配合。

B14　抗抵赖

数据原发与交付抗抵赖服务能够由一个涉及在第 7 层上作中继的公证机制提供。

使用用于抗抵赖的数字签名机制要求在第 6 层与第 7 层之间进行密切合作。

附录 C

应用选取加密的位置

(参考件)

C1　大多数应用将不要求在多个层上加密，加密层的选取主要取决于下述的几个主要问题：

1)如果要求全通信业务流机密性，那么将选取物理层加密，或传输安全手段(例如，适当的扩频技术)。足够的物理安全，可信任的路由选择以及在中继上的类似机能够满足所有的机密性要求。

2)如果要求高粒度保护(即对每个应用联系可能提供不同的密钥)，和抗抵赖或选择字段保护，那么将选取表示层加密。由于加密算法耗费大量的处理能力，所以选择字段保护可能是重要的。在表示层中的加密能提供不带恢复的完整性，抗抵赖，以及所有的机密性。

3)如果希望的是所有端系统到端系统通信的简单块保护，或希望有一个外部的加密设备(例如为了给算法和密钥以物理保护，或防止错误软件)，那么将选取网络层加密。这能够提供机密性与不带恢复的完整性。

注：虽然在网络层不提供恢复，但运输层的正常的恢复机制能够用来恢复网络层检测到的攻击。

4)如果要求带恢复的完整性，同时又具有高粒度保护，那么将选取运输层加密。这能提供机密性，带恢复的完整性或不带恢复的完整性。

5)对于今后的实施，不推荐在数据链路层上加密。

C2　当关系到这些主要问题中的两项或多项时，加密可能需要在多个层上提供。

附加说明：

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准由复旦大学负责起草。

本标准主要起草人刘光奇、张根度。