国 际 电 信 联 盟

ITU-T

国际电信联盟

电信标准化部门

Y.2701

(04/2007)

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

下一代网络 – 安全

第1版本下一代网络（NGN）的安全性要求

ITU-T Y.2701建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
体系、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
下一代网络	
框架和功能体系模型	Y.2000–Y.2099
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务体系	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2701建议书

第1版本下一代网络（NGN）的安全性要求

摘要

通过将ITU-T X.805建议书“提供端到端通信的系统的安全体系结构”应用于ITU-T Y.2201建议书“第1版NGN的要求”和ITU-T Y.2012建议书“第1版本NGN的功能要求与体系结构”，本建议书为下一代网络（NGN）及其接口（如UNI、NNI和ANI）规定了安全性要求。

这些要求旨在为跨多个网络管理域的最终用户通信规定基于网络的安全性。客户域中的客户资产与信息安全（如用户网络）以及客户设备上对等应用性能的使用等不在本建议书的讨论范围之内。

本建议书使用基于网元（实物盒子）的信任模型。NGN提供商将部署支持ITU-T Y.2012建议书中定义的功能实体的网元。这些功能实体与特定网元的捆绑依供货商的不同而不同。因此，本建议书将不尝试说明逻辑功能实体与物理网元之间严格而固定的捆绑。

应将本建议书中的要求视为最起码的有关安全性的要求，并且为了NGN的安全，鼓励NGN提供商采取比本建议书中所规定的安全性要求更多的安全措施。

来源

ITU-T Y.2701建议书由ITU-T第13研究组（2005-2008年）于2007年4月27日按照WTSA第1号决议规定的程序批准。

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

本建议书为简明扼要起见而使用的“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，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T Y.2701建议书

第1版本下一代网络（NGN）的安全性要求

1 范围

本建议书为下一代网络（NGN）规定了安全性要求，以应对安全威胁。它通过将ITU-T X.805建议书“提供端到端通信的系统的安全体系结构”的基本原则应用于ITU-T Y.2201建议书“第1版NGN的要求”和ITU-T Y.2012建议书“第1版本NGN的功能要求与体系结构”来实现。

这些要求旨在保护以下多个网络环境中的对象：

- 网络和服务提供商的基础设施与资产（例如，NGN的资产与资源，如网元、系统、部件、接口、数据和信息）、资源、通信（即信令、管理和数据/承载的业务）和服务。
- NGN的服务与性能（例如，话音、视频和数据服务）。
- 最终用户的通信与信息（例如，私人信息）。

这些要求用于在多网络管理域上为最终用户通信提供基于网络的安全。客户域（如用户网络）中客户资产与信息的安全以及客户设备上的对等应用性能的使用，不在本建议书的讨论范围之内。

本建议书中规定的要求适用于NGN，包括多网络环境中的用户对网络接口（UNI）、网络对网络接口（NNI）和应用对网络接口（ANI）。

NGN服务提供商将部署支持[ITU-T Y.2012]中定义的功能实体的“网元”。这些功能实体与特定网元的绑定依供货商的不同而不同。因此，本建议书将不尝试说明逻辑功能实体与物理网元之间严格而固定的捆绑。

应将本建议书中的要求视为最起码的有关NGN安全性的要求，不应认为它已十分详尽。因此，为了NGN的安全，NGN网络提供商可以采取比本建议书中所规定的安全性要求更多的安全措施。

此外，本文件中的要求涵盖了通常称为IdM（“身份管理”）的某些技术方面的问题。IdM的现行定义为：“NGN提供商对某个实体的受信任属性所做的管理，如用户、设备或提供商”。这无意表示对某个人身份的属实确认。

主管部门可以要求NGN提供商在执行本建议书时考虑到国家监管和国家政策方面的要求。

1.1 X.805的原则

[ITU-T X.805] 定义了以下方面的安全性：

访问控制；

认证；

不可否认性；

数据机密性；

通信安全性；

数据完整性；

可用性；

私密性。

它还确定了以下安全威胁：

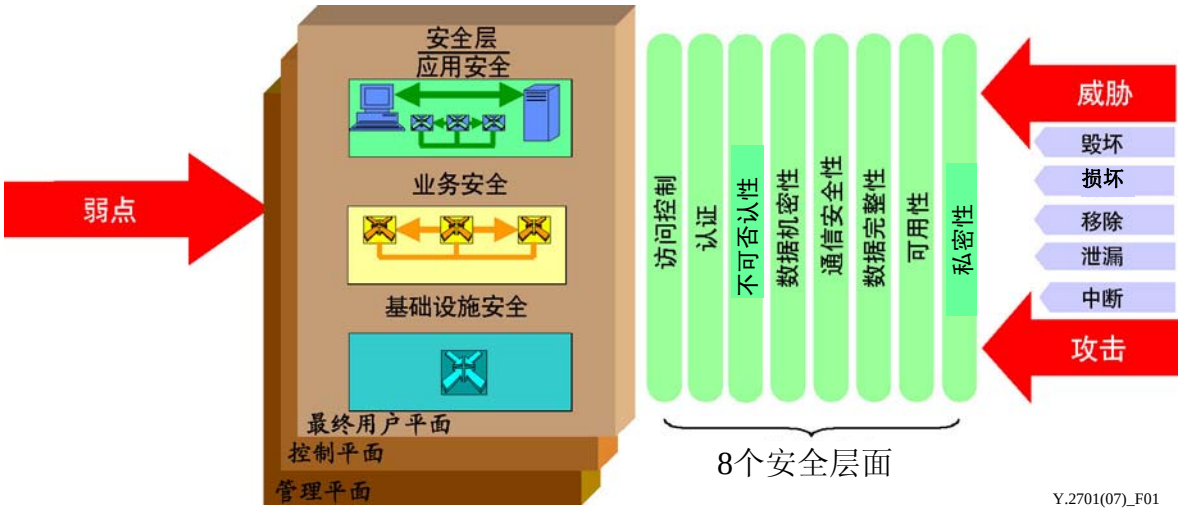


图1－X.805的安全体系结构（图3/X.805）

以上所述些安全层面和安全威胁被认为是本建议书的基础。

本建议书未进一步确定或区分X.805安全层（应用、服务或基础设施）的使用，采用本标准并不要求做出上述区分。本建议书亦未提及管理、控制和用户平面业务之间的区分，而是提醒读者注意，此分类的使用依所述协议栈中层的不同而不同。因此，需参引更多的标准来确定是否符合此类区分。本标准所述建议涉及安全层面的应用，在用于NGN网络安全性评估方面只能是挂一漏万。

1.2 假定

本建议书基于以下假定：

1) [ITU-T Y.2012]中定义的功能实体与特定网元的捆绑依供货商的不同而不同。

2) 各NGN提供商在其安全域具有具体职责。例如，履行相应的安全服务与做法，以

   a) 保护自己；

   b) 确保不损害其网络内的端到端安全；

   c) 确保NGN通信的高可用性。

3) 各网络域将建立和执行有关服务水平协议（SLA）的政策，以保障其域内的安全和网络互连的安全。现假定SLA将规定将要执行的安全服务、机制和做法，以保护互连的网络和跨UNI、ANI和NNI的通信（信令/控制业务、承载业务和管理业务）。

4) 本建议书论述基于网络的安全，它是一种分层的体系结构，包括受信任域的周边安全性、提供商设备的物理安全性以及潜在的加密的使用。

1.3 概述

本建议书组织如下：

- 第2节（参考文献）– 本节提供规范性参考文献。
- 第3节（定义和缩写词）– 本节提供本建议书中使用的定义和缩写词。
- 第4节（安全威胁与风险）– 本节重点论述对NGN环境假想的安全威胁与风险。假想的安全威胁与风险将用做指南，以制定安全方面的要求，并确定安全性能和需要支持的程序。
- 第5节（安全信任模型）– 本节描述NGN安全的信任模型。信任模型可用于发展UNI、ANI和NNI连接之间的信任关系以及安全体系结构的设计。
- 第6节（安全体系结构）– 本节描述[ITU-T Y.2012]中定义的功能性NGN体系结构与复合安全体系结构之间的关系。
- 第7节（目标和要求）– 本节描述NGN的安全性目标和一般要求，作为确定NGN安全性要求的基础。
- 第8节（具体的安全性要求）– 本节规定第7节中所定义的具体安全性要求。
- 附录一 – 应急电信服务（ETS）的安全性目标与要求。
- 参考资料。

定义本建议书旨在为NGN安全奠定一个基础。今后将为特定的安全领域提供各种配套的建议书，例如，认证和授权、证书管理、身份管理等。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，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均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

此处所示的参考文献是规范性的。资料性的参考文献可以在文末的参考资料中找到。

[ITU-T M.3016.0] ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.

[ITU-T M.3016.1] ITU-T Recommendation M.3016.1 (2005), *Security for the management plane: Security requirements.*

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

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

[ITU-T Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN release 1*.

[ITU-T Y.2201] ITU-T Recommendation Y.2201 (2007), *NGN release 1 requirements.*

3 定义和缩写词

3.1 其它文件定义的术语

本建议书使用其它文件定义的下列术语：

3.1.1 emergency telecommunications service (ETS) 应急通信服务（ETS）：一种国家服务，它在灾害发生时，为紧急救援人员提供经授权的优先电信服务，以方便其工作（见ITU-T E.107建议书）。

3.1.2 user 用户：用户包括最终用户（ITU-T Y.2091建议书）、人、注册用户、系统、设备、终端（如传真机、个人计算机）、（功能）实体、程序、应用、提供商或企业网。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 asset 资产：任何对组织及其业务、运营和连续性有价值的事物。

3.2.2 border element 边界元素：提供连接不同安全和管理域功能的网元。

3.2.3 corporate network 企业网：支持可能身处多个地点（如企业、校园）的多个用户的专用网。

3.2.4 domain border element 域边界元素：由提供商单独控制的边界元素，它为安全功能提供其它网络域。

3.2.5 network border element网络边界元素：由提供商单独控制的边界元素，它为安全功能提供终端设备。

3.2.6 security domain安全域：一组元素、一种安全政策、一个安全主管当局以及一组与安全相关的活动，其中各元素依据安全政策得到管理。安全政策将由安全主管当局进行管理。一个特定的安全域可能跨越多个安全区域。

3.2.7 security zone安全区：本建议书定义了3个安全区：

1) 受信任；
2) 受信任但很脆弱；
3) 不受信任。

通过运营控制、地点以及与其它设备/网元的连接性来定义安全区域。

3.2.8 terminal equipment border element终端设备边界元素：在客户驻地设备和服务提供商网络之间提供安全功能的边界元素。

3.2.9 trust信任：当且仅当实体X依赖实体Y以某种特殊方式来执行相关的活动时，才被认为在一系列活动方面信任实体Y。

3.2.10 trusted but vulnerable zone受信任但很脆弱的区：从NGN提供商的角度看，这是网元设备由NGN提供商负责运营（提供和维护）的安全区。设备可以由客户/订户控制，也可以由NGN提供商控制。此外，设备可以位于NGN提供商域之内或之外。它们既与受信任的区内的元素进行通信，也与不受信任的区内的元素进行通信，这就是为什么说它们是“脆弱的”的原因。它们的主要安全功能是以一种自动保护方式，保护受信任的区内的网元免受来自不受信任区的安全攻击。

3.2.11 trusted zone受信任区：从NGN提供商的角度看，这是一个NGN提供商的网元和系统处于其中且从不直接与客户设备进行通信的安全域。该域内的NGN网元的共同特性是它们完全由相关NGN提供商控制，并位于NGN提供商的驻地（提供物理安全性）内，同时它们只与“受信任”域和“受信任但很脆弱”的域内的网元进行通信。

3.2.12 un-trusted zone不受信任区：从NGN提供商的角度看，这是一个包括客户网络或可能是对等网络或最初域之外其它NGN提供商区所有网元的区域，它们与NGN提供商的边界网元相连。

3.2.13 user network用户网络：由可能连接多个用户的终端组成的专用网。

3.3 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

3G	第3代
AGW	接入网关
ANI	应用到网络接口
B2BUA	背对背用户代理
BE	边界元素
CSC-FE	呼叫会话控制功能实体
DBE	域边界元素
DNS	域名系统
ETS	应急通信服务
FE	功能实体
GW	网关
I-CSC-FE	询问呼叫会话控制功能实体
IMS	IP多媒体子系统
IP	互联网协议
ISDN	综合业务数字网
LAN	局域网
MPLS	多协议标签交换
MRP-FE	媒体资源处理功能实体
NAC-FE	网络访问控制功能实体
NAPT	网络地址与端口转换
NAT	网络地址转换

NBE	网络边界元素
NE	网元
NGN	下一代网络
NNI	网络到网络接口
OAMP	操作、管理、维护和调配
P-CSC-FE	代理呼叫会话控制功能实体
POTS	普通老式电话服务
PSTN	公众交换电话网
QoS	服务质量
RAC-FE	资源和受理控制功能实体
RAN	无线电接入网
RTSP	实时流协议
SAA-FE	服务认证与授权功能实体
S-CSC-FE	呼出呼叫会话控制服务功能实体
SIM	用户身份模块
SIP	会话起始协议
SLA	服务水平协议
SL-FE	订购定位功能实体
TAA-FE	传输认证与授权功能实体
TE	终端设备
TE-BE	终端设备边界元素
UA	用户代理
UICC	通用集成电路卡
UNI	用户到网络接口
VLAN	虚拟局域网
W-CDMA	宽带码分多址
WLAN	无线局域网
xDSL	x 数字用户线

4 安全威胁与风险

本建议书假设组成NGN的系统、部件、接口、信息、资源、通信（即信令、管理和数据/承载业务）和服务，将暴露于各种安全威胁与风险面前。这些威胁与风险将取决于诸多因素。此外，最终用户也将暴露于某些威胁（如对私人信息的未经授权的访问）面前。

NGN面临的威胁：

- 未经授权的侦察，如对系统进行远程分析，以确定其弱点（手段包括扫描、频率扫描、端口询问、查看路由表等）；
- 插入/设备接管，导致设备失控、配置审核异常和错误；
- 破坏信息和/或其他资源；
- 损坏或修改信息；
- 信息与/或其他资源被窃取、删除或丢失；
- 信息泄漏；
- 中断服务和拒绝服务

此外，很显然，NGN将工作于不同于PSTN的环境中，因此，它可能暴露于来自内部或外部的各类不同的威胁与攻击面前。NGN将直接或间接地连接至不受信任的和受信任的网络与终端设备，因此，将暴露于与连接不安全网络和客户驻地设备相关的安全风险与威胁面前。例如，一个提供商的NGN可能与图2中所示的以下对象直接或间接连接（即通过其他网络）：

- 其他服务提供商及其应用；
- 其他NGN；
- 其他基于IP的网络；
- 公众交换电话网（PSTN）；
- 企业网络；
- 用户网络；
- 终端设备；
- 其它NGN传输域。

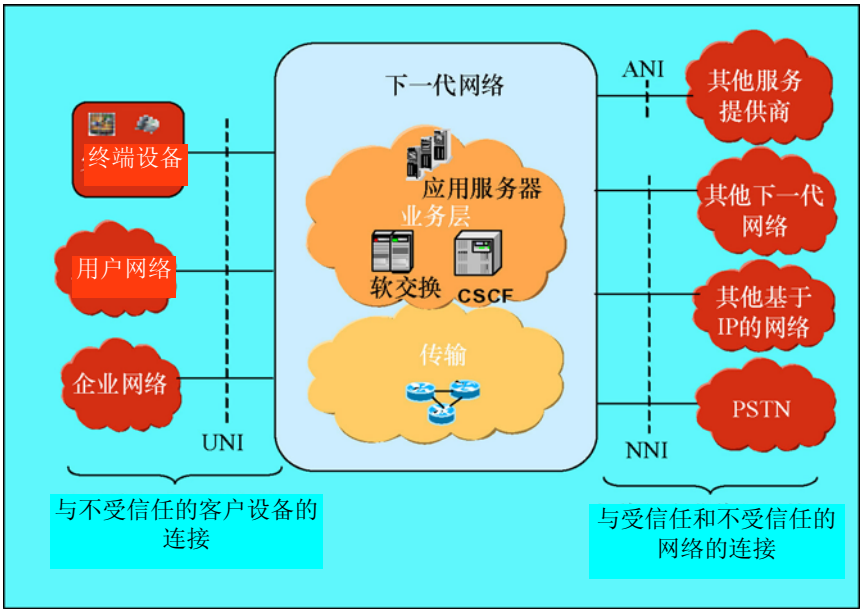


图 2－与网络和用户的连接

在发展变化的环境中，跨越多个网络提供商域的安全取决于所有提供商决定为其网络安全所做的一整套工作。对提供商网络的未经授权的访问可以轻易地导致对互连网络及其相关服务的非法利用。这只是非法利用最薄弱环节的一个例子，它与各种类型攻击一起，可以对提供商网络的完整性和服务连续性构成威胁。

各NGN提供商负责其域内的安全。各NGN提供商负责使用针对信任关系（第5节）的、网络特定的设计并实时安全解决方案，以满足其自身网络特定的需要，并在多个网络提供商域上为全球的端到端安全目标提供支持。

5 安全信任模型

本节定义NGN的安全信任模型。

NGN的功能参考架构定义了功能实体（FE）。不过，由于网络安全很大程度上取决于功能实体的捆绑方式，因此NGN的安全体系结构基于物理网元（NE），即包含一个或多个功能实体的、有形的实物盒子。这些功能实体捆绑到网元中的方式依供货商不同而不同。

5.1 单一网络信任模型

本小节定义了3种安全区：

1) 受信任区；

2) 受信任但很脆弱的区；

3) 不受信任区，

它们取决于操作控制、地点、与其他设备/网元的连接。图3所示的安全信任模型对这3种区予以具体说明。

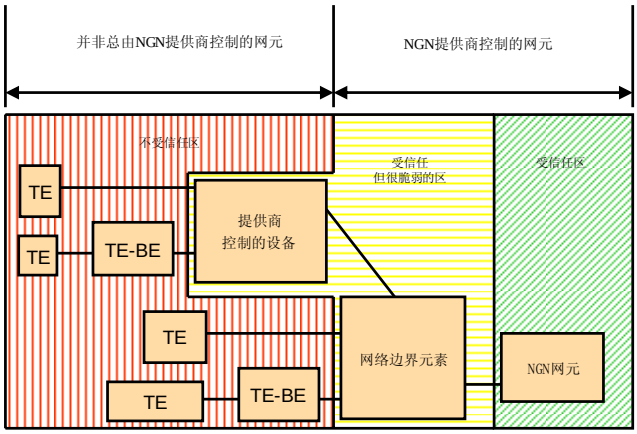


图 3 – 安全信任模型

“受信任的网络安全区”或简称为“受信任区”，是NGN提供商网元与系统所在的一个区，这些网元与系统从不直接与用户设备或其他域连接。在该区内的NGN网元的共同特点是它们完全由NGN提供商所控制，并位于NGN提供商域（它提供物理安全）内，同时它

们只与“受信任的”区和“受信任但很脆弱的”区内的元素进行通信。不应设想它们在受信任区，所以本身一定安全。

“受信任”区将得到各种方法的综合保护。这种保护的一些例子包括NGN网元的物理安全、系统总体加固、使用安全信令、OAMP消息的安全，以及为“受信任”区和“受信任但很脆弱的”区内NGN网元的通信在（MPLS/）IP网络内建立单独的虚拟专用网（VPN）。更多细节请参见第8节。

在“受信任但脆弱的网络安全区”或简称为“受信任但很脆弱的区”内，网元/设备由NGN提供商运营（调配和维护）。设备可由客户/订户所拥有，或者由NGN提供商所拥有。此外，可将设备部署在NGN提供商驻地之内或之外。这些设备既与受信任区的元素进行通信，也与不受信任的区的元素进行通信，这就是为什么说它们是“脆弱的”的原因。它们的主要安全功能是，保护受信任区内的网元免受来自不受信任区的安全攻击。

位于NGN提供商域、与受信任区之外的元素连接的元素被称作是边界元素（BE）。具体例子如下：

- UNI处的网络边界元素（NBE），它们通过接口与受信任区内NGN提供商的服务控制或传输网元相连，以便为用户/订户的服务和/或传输目的提供对NGN提供商网络的接入。
- 域边界元素（DBE）与网络边界元素相同，唯一的不同是该元素置于域的边界。
- 设备配置与引导NBE（DCB-NBE），它们通过接口与受信任区内的NGN提供商设备配置系统相连，以便配置户外设施中的用户/订户设备和NGN提供商设备。
- OAMP-NBE通过接口与受信任区内的NGN提供商的OAMP系统相连，以便提供和维护户外设施中的用户/订户设备和NGN提供商设备。
- 应用服务器/万维网服务器NBE（AS/WS-NBE），它们通过接口与受信任区内的NGN提供商的AS/WS-NBE相连，以便为用户/订户提供接入基于万维网的服务。

下面是一些由NGN提供商运营但未位于NGN提供商驻地的设备/元素，它们可能归NGN提供商控制，也可能不归NGN提供商控制：

- 接入网/技术中的户外设施；
- 基站路由器（BSR），它是一个集成了基站、无线电网络控制器和路由器功能的网元；
- 用户/订户驻地内的光单元（ONU）。

包括NBE的“受信任但很脆弱”区将由各种方法综合保护。这种保护的一些例子包括：NGN网元的物理安全、系统总体加固、对所有发往“受信任”区内的NGN网元的信令消息使用安全信令、OAMP消息的安全以及数据包过滤和防火墙等。更多细节请参见第8节。

“不受信任区”包括客户网络或可能的对等网络或最初域之外的其它NGN提供商域中的所有网元，它们与NGN提供商的边界元素相连。在包含终端设备的“不受信任”区内，设备可能不归NGN提供商控制，因此可能无法对用户执行提供商的安全政策。尽管如此，仍有必要应用某些安全措施，同时，为此目的，建议加强信令、媒体和OAMP的安全，并对位于“不受信任”区内的TE-BE进行加固。不过，由于缺少物理安全，不能认为这些保护措施都是绝对安全的。更多细节请参见第8节。

5.2 对等网络信任模型

当NGN与另一个网络相连时，信任取决于：

- 物理互连，它有多种连接方式，从安全建筑内的直接连接到通过共享设备实现的连接；
- 对等模型，在这种连接方式下，可以在两个NGN服务提供商之间直接进行业务交换，或者通过一个或多个NGN传输提供商实现业务交换。
- 业务关系，当中，服务水平协议（SLA）中可能包含惩罚性条款和/或对其他NGN提供商安全政策的信任。
- 总体而言，NGN提供商应将其它提供商视为不受信任的提供商。

图4所示为当连接网络被判为受信任时的例子。

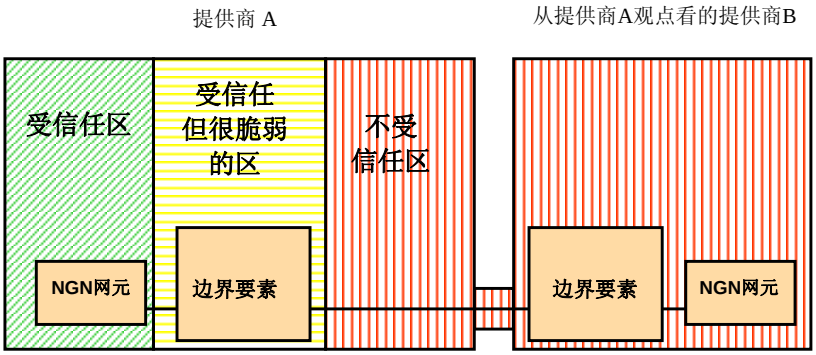


图4－对等信任模型

6 安全体系结构

6.1 功能性NGN体系结构参考文献

[ITU-T Y.2012]“第1版本NGN的功能要求与体系结构”定义了实现[ITU-T Y.2201]“第1版NGN要求”的NGN体系结构。

图5显示了NGN体系结构的功能视图。

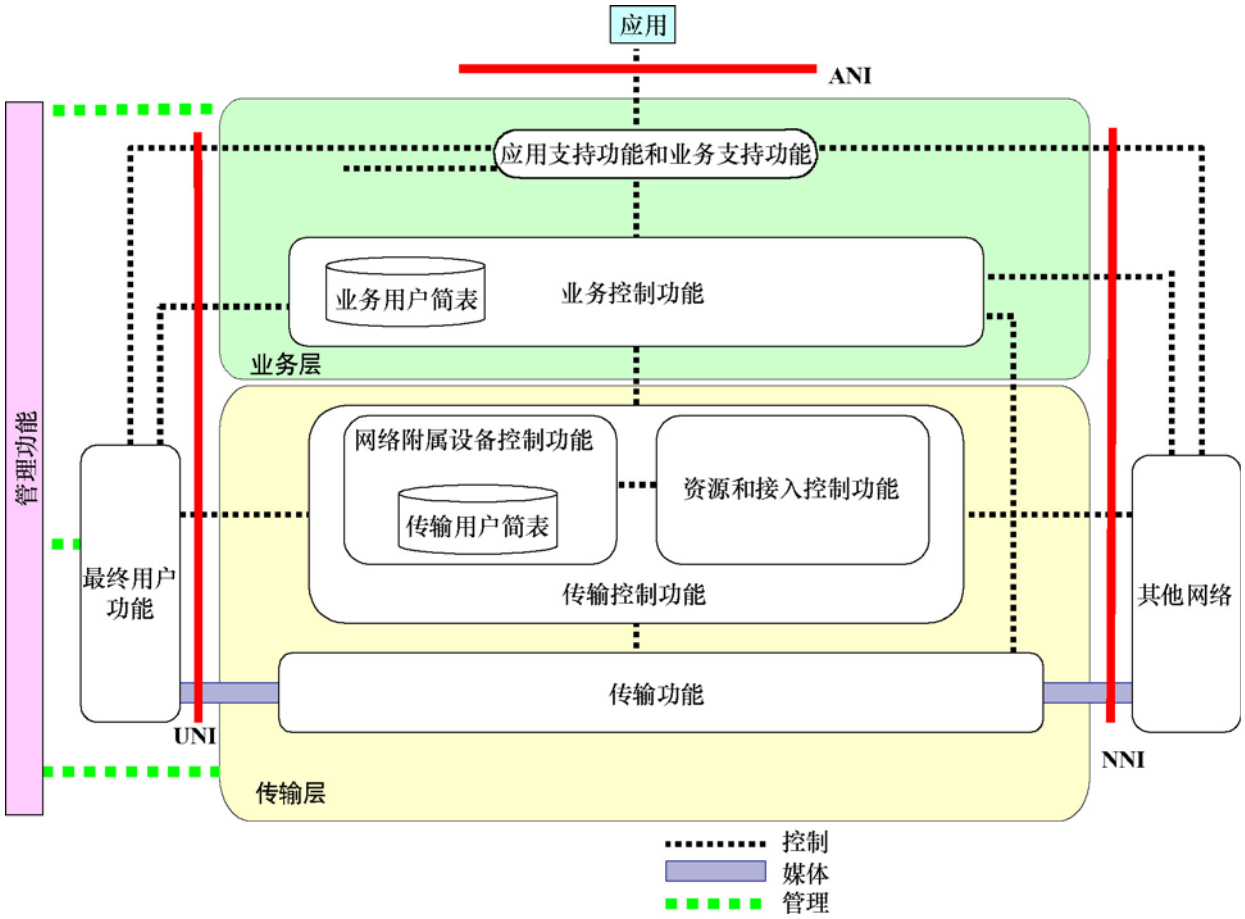


图5－NGN体系结构概述（图 1/Y.2012）

NGN支持针对最终用户功能的参考点（它被称为用户到网络接口（UNI））以及针对其他网络的参考点（它被称为网络到网络接口（NNI））。它还支持针对应用功能组的参考点，它被称为应用到网络接口（ANI），使得能够应用NGN性能来为NGN用户创建和提供应用。

在传输控制功能的控制下，包括网络附加控制功能（NACF）以及资源与接入控制功能（RACF），NGN第1版本传输层为NGN用户提供IP连接服务。

通过运用应用支持功能、业务支持功能和相关的控制功能，业务层为最终用户提供服务与应用。

最终用户功能是指那些连接于NGN接入网的功能，并且不对各种最终用户接口和最终用户网络做出任何假定。

管理功能提供管理NGN的能力，以便为NGN服务提供期望的质量、安全性和可靠性。

更多细节请参见[ITU-T Y.2012]。

6.2 映射至NGN功能性体系结构

本建议书描述了通过利用第5节中所示的信任模型实现安全的方法，也就是说，NGN由受信任域（绿色区）、不受信任域（红色区）以及之间的受信任但很脆弱域（黄色区）组成。

采用这种模式实现安全的一个关键问题是从不受信任域向受信任域传输信令、媒体、OAMP业务的方法。实现上述目的的方法多种多样，NGN提供商会在考虑其政策的情况下来决定具体方法。下面是这些方法的一些例子。

a) 在绿色区与红色区之间安装网元以终接业务（如为了SIP信令而安装B2BUA）。它接收一个来自红色区的数据包，检查之，如果不合适则丢弃之；如果合适，则复制其中必要的部分，以便为绿色区重建一个适当的数据包。在这种情况下，终接业务的网元变为黄色区的网元。

b) 对媒体层中的业务实施控制（例如，通过打开和关闭防火墙上某个特殊的端口（针孔），并保证只有经授权的网元（和用户）可以向绿色区中的设备发送业务）。在这种情况下，控制业务的网元变为黄色区内的网元。

c) 在发送和接收端采取端到端加密。

在[ITU-T Y.2012]所示的功能体系结构中（本建议书的图6），由最终用户功能产生的SIP信令（它通常是不受信任的，原因是NGN提供商不能确认该功能是否被伪造）被发往S-2、P-CSC-FE。因此，包含P-CSC-FE的网元被认为是黄色区的网元，或者，由于它的防火墙功能，被认为是绿色区的网元。如果包含S-1（S-CSC-FE）的网元与包含P-CSC-FE的网元是分开的，那么它们将被视为绿色区的网元。

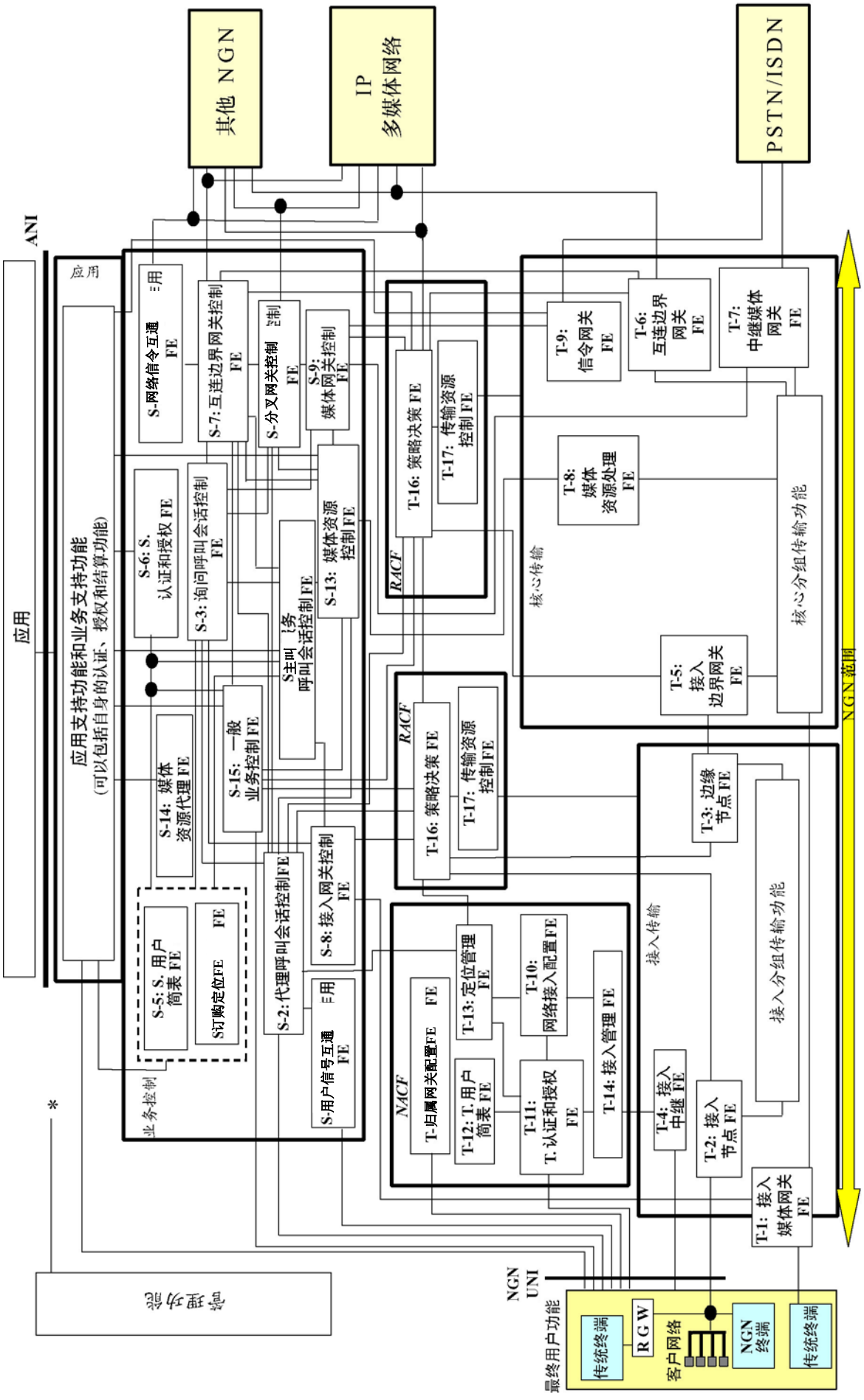


图 6——一般化的功能体系结构（图 3/Y.2012）

6.3 确定需要安全保护的NGN资源

各网络提供商有必要确定其网络内需要保护的资产、资源、信息和接口，并确定需要降低的威胁。例如，网元、接口（UNI、ANI 和NNI）、管理系统、信令、管理与媒体/承载通信。在确定需要安全保护以防威胁的NGN资源的过程中，[ITU-T Y.2012]中定义的理论分层体系结构务应与功能实体实际实现方案一起得到考虑。

下列各表提供了需要安全保护以防威胁的NGN资产、资源和接口例子，具体如下：

- 表1 – 与UNI相关的资产、资源和信息举例
- 表2 – 与传输层相关的资产、资源、信息和接口举例
- 表3 – 与服务层相关的资产、资源、信息和接口举例
- 表4 – 与管理相关的资产、资源、信息和接口举例

表1-4中所示的例子并不是详尽完整的。

表1－与UNI相关的资产、资源和信息举例

举例	目的与目标
最终用户资源： • 用户设备 • 用户网络网关 • 企业网络网关	a) 保护附着于网络的最终用户设备（如终端、用户网络和企业网关），使之免遭来自网络的攻击（如破坏、损坏、修改用户设备等攻击）。 b) 防止服务中断（如防范拒绝服务攻击），并确保服务可用性。 c) 防止对网络的未经授权访问（如未经授权的用户和用户设备）。
最终用户信息 • 订购信息 • 身份信息 • 位置信息	a) 保护信息免受损坏或修改。 b) 防止窃取、移除或丢失（如身份窃取）。 c) 防止泄漏（如对位置信息的未经授权访问）。
NGN 提供商信息 • 身份信息	a) 保护信息免受损坏或修改。 b) 防止窃取、移除或丢失（如身份窃取）。 c) 防止泄漏（如对位置信息的未经授权访问）。
UNI 接口	a) 传输层 — 为 UNI 接口上的媒体/承载业务提供安全保护。 b) 业务层（服务控制）— 为 UNI 接口上的信令和管理提供安全保护（如 SIP、HTTP、ISDN 和 H.248）。 c) 业务层（应用与业务支持）— 为 UNI 接口上的应用与服务控制功能提供安全保护（如带内信令）。

表2－与传输层相关的资产、资源、信息和接口举例

举例	目的与目标
传输层资源： • 传输网元（如 IP 路由器、MPLS 节点） • 传输链路 • 路由信息（如 DNS 服务器） • 传输用户简表信息（如传输数据库和数据存储库）	a) 保护所有的传输网元、部件和功能免受未经授权的访问威胁。 b) 保护传输网元、部件和功能的完整性。 c) 保护传输网元、部件和功能的可用性。防止服务中断（即防范拒绝服务攻击）。 d) 防止泄漏任何用户或网络私人信息。
传输层系统间通信（在网络提供商网络内的通信）	a) 为提供商网络内系统间的媒体/承载业务提供安全保护。 b) 为提供商网络内的传输控制（如 OSPF）信令和管理提供安全保护。 c) 为业务层系统（如应用服务器）和传输层系统（如 IP 路由器）间的信令提供安全保护。
传输接口与通信	a) 为传输 UNI、NNI 和 ANI 接口上的媒体/承载业务提供安全保护。 b) 为传输 UNI、NNI 和 ANI 接口上的传输控制信令（如 OSPF）和管理提供安全保护。

表3－与业务层相关的资产、资源、信息和接口举例

	举例	目的与目标
业务层 — 服务控制	业务层 — 服务控制资源 • 服务控制网元（如 CSC-FE、SL-FE、MRF-FE、网关、S/BC）	a) 保护所有的服务控制网元、部件和功能免受未经授权的访问威胁。 b) 保护服务控制网元、部件和功能的完整性，包括保护信息免遭损坏或修改。 c) 保护服务控制网元、部件和功能的可用性。防止服务中断（即防范拒绝服务攻击）。
	业务层 — 服务控制信息 • 订购信息（如包含用户简表和业务简表的数据库和数据存储库） • NGN 提供商网络信息（如包含路由、号码和地址信息的数据库和数据存储库）	a) 保护数据和信息免遭损坏或修改。 b) 防止窃取、删除或丢失（如身份窃取）。 c) 防止泄漏（如对用户与网络私人信息的未经授权访问）。
	业务层 — 服务控制系统间通信	为网络提供商网络内的系统间信令（如 CSCF 至 HSS 信令）提供安全保护（如 SIP、RADIUS、Diameter 等）。
	接口和通信	为 UNI、NNI 和 ANI 之间接口提供信令安全保护和管理

表3－与业务层相关的资产、资源、信息和接口举例

	举例	目的与目标
业务层 — 应用与服务支持	业务层 — 应用与服务支持资源： • 应用与服务支持网元和平台（如应用服务器、数据库、万维网门户）	a) 保护所有的服务支持网元、部件和功能免受未经授权的访问威胁。 b) 保护服务支持网元、部件和功能的完整性，包括保护信息免遭损坏或修改。 c) 保护服务支持网元、部件和功能的可用性。 d) 防止服务中断（即防范拒绝服务攻击）。
	业务层 — 应用与服务支持信息： • 应用与服务信息 • 订购信息	a) 保护数据和信息免受损坏或修改。 b) 防止窃取、删除或丢失（如身份窃取）。 c) 防止泄漏（如对用户与网络私人信息的未经授权访问）。
	接口	a) 为其他应用提供商的访问提供网元与资源安全保护（如 Parlay 和 OMA 网关）。 b) 为 UNI、NNI、ANI 接口提供安全保护。 c) 为 ANI 接口上的信令和管理业务量提供安全保护。

表4－与管理相关的资产、资源、信息和接口举例

举例	目的与目标
管理资源 • 传输层管理系统（如网元管理、网络管理和服务管理系统） • 业务层管理系统（如网元管理、网络管理和服务管理系统）	a) 保护所有的管理网元、部件、功能和接口，使之免受未经授权的访问威胁。 b) 保护管理网元、部件、功能和接口的完整性。这包括保护信息免遭损坏或修改。 c) 保护管理网元、部件、功能和接口的可用性。防止出现服务中断（即防范拒绝服务攻击）。
网络提供商网络内的系统间通信	a) 为网络内的管理系统间管理业务提供安全保护（如业务层）。 b) 为用户网络、网络提供商传输层和服务层之间的管理业务提供安全保护。
接口与系统间通信	a) 为内部网络管理接口和任何 UNI、NNI 及 ANI 管理接口提供安全保护。 b) 为 UNI、NNI、ANI 接口上的管理业务提供安全保护。

7 目标和要求

7.1 总的安全性目标

以下是用于指导本建议书中各项要求的总的安全性目标一览表：

- NGN的安全功能应是可扩展的、灵活的，足以满足各种需求。
- 安全要求应考虑到NGN的性能、可用性、可扩展性和成本限制条件。
- 安全方法应基于现有的、易理解的、适当的安全标准。
- NGN安全体系结构应是全球可扩展的（在网络提供商域内、跨多个网络提供商域以及在安全性提供范围内）。
- NGN安全体系结构应考虑到信令与控制业务、用户业务和管理业务量在逻辑上或物理上的独立性。
- 应可靠提供和安全管理NGN的安全性。
- NGN应为各个方面提供安全：业务、网络提供商和订购用户。
- 安全方法一般应不影响所提供服务的质量。
- 应为用户和提供商提供简单而可靠的安全服务与配置（即插即用）。
- 当使用多播功能时，应保护适当的安全水平。

- 业务发现功能应支持各种范围标准（如地点、成本等），以便实现适当的规模变化，并以适当的机制确保安全性和私密性。
- 地址解析系统应是一个只由该网络使用的专门系统，并应制定某些安全措施。该系统可以使用域内或域外的数据库。
- 应遵守[ITU-T M.3016.0]第7节所述的安全TMN管理原则和总的安全目标。

7.2 跨多个网络提供商域的安全性目标

总的目标是为多个提供商域的端到端通信提供基于网络的安全。这通过逐段转接跨越不同提供商的域方式为端到端通信提供安全来实现。图7所示为最终用户间端到端通信提供安全保护的一般网络概念。各网络部分在其安全区内具有特定的安全职责，以推动安全防护，并提高跨多个网络的NGN通信的可用性。

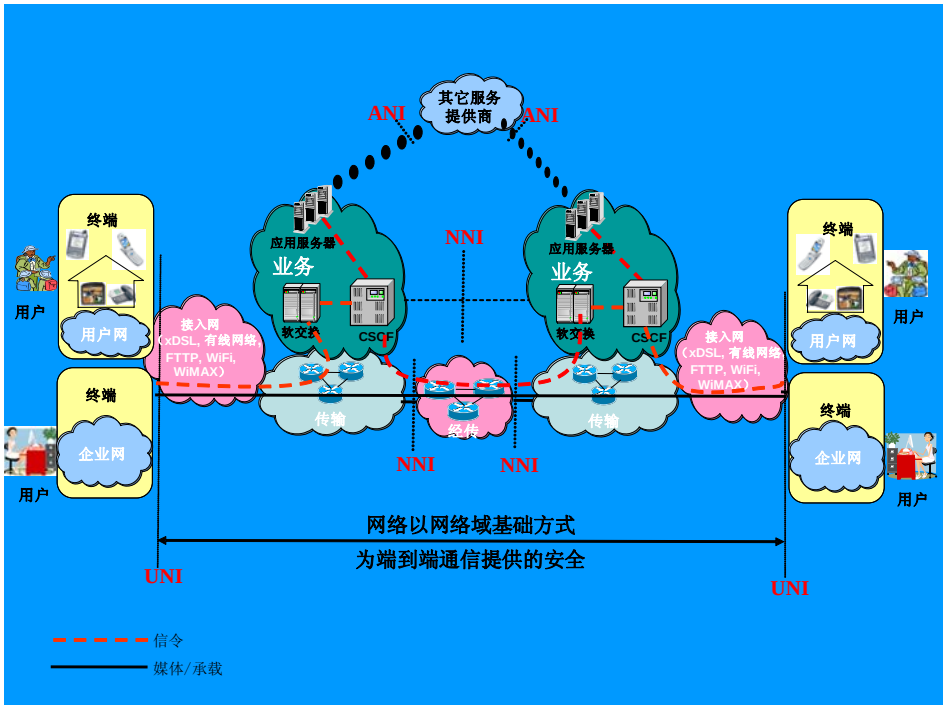


图7－跨越多个网络的通信安全

如第5.2段所述，互连NGN间的信任模型取决于物理互连、对等模型和业务关系等若干因素。

7.3 有关不同安全层面的具体要求

此处所述目标是特别针对具体安全层面的，如认证。它们通用于所有接口。

7.3.1 访问控制

NGN提供商有必要限制经授权的订购用户对网络的访问。授权可由提供接入的提供商或其它提供商在通过认证和访问控制程序、对身份确认后予以提供。

NGN有必要阻止入侵者通过伪装成经授权用户而进行的未经授权访问。

7.3.2 认证

NGN提供商有必要提供对用户、设备、网元和其他提供商进行认证的功能。这包括支持但不限于以下功能：

1) 认证传输网络接入用户的功能（例如，对最终用户设备、用户网络网关或企业网关进行认证和授权，以获得对传输网络的接入或附着于网络接入）。

2) 在服务交付之初和交付期间认证用户的服务接入功能（例如，对用户、设备或用户/设备的组合进行认证，此类认证适用于NGN服务/应用接入）。

3) 如果安全政策需要，NGN用户对每一层的NGN提供商进行认证的功能（例如，用户对连接的NGN提供商或服务提供商的身份进行认证）。

4) 作为网络服务或功能，允许用户进行对等认证的功能（例如，对被叫用户、发起实体或数据源进行认证）。

5) 为了交换信令、管理和媒体/承载业务，允许每一层上两个NGN提供商之间进行相互认证的功能（例如，对NNI接口上的直接互连和远程网络进行认证）。

6) 在ANI接口上允许对其他网络提供商进行认证的功能。将支持基于SIM和/或非基于SIM的方法。

注 – 对实体进行认证并非意在确认一个人的身份有效。

7.3.3 不可否认性

本建议书未明确定义有关不可否认性方面的安全要求。

7.3.4 数据机密性

NGN提供商有必要通过密码或其他手段来保护用户业务的机密性。

如果安全政策要求，NGN提供商有必要通过密码或其他手段来保护控制消息的机密性。

NGN提供商有必要通过密码或其它手段来保护管理业务的机密性。

7.3.5 通信安全性

NGN提供商有必要提供确保信息不被非法转移或截获的机制。

7.3.6 数据完整性

NGN提供商须有必要通过密码或其他手段来保护用户业务的完整性。

如果安全政策要求，NGN提供商须有必要通过密码或其他手段来保护控制消息的完整性。

NGN提供商须有必要通过密码或其他手段来保护管理业务的完整性。

7.3.7 可用性

NGN有必要提供安全功能，以使GN提供商能够防止或中断与不符合要求的最终用户设备之间的通信：以便减少DoS攻击、病毒或蠕虫的传播以及其他攻击。可以暂停这些功能，以便进行应急通信。NGN内容网元亦易受到病毒、蠕虫或其它攻击的威胁，因此有必要采取类似措施来隔离网络部件。

NGN应提供安全功能，以便使GN提供商能够过滤那些安全政策认为有害的数据包和业务。

NGN有必要提供支持灾难恢复功能和程序的功能。这些特殊的要求不在本建议书讨论范围之内。

7.3.8 私密性

NGN有必要提供旨在按照国家法律法规保护用户私人信息（如数据位置、身份、电话号码、网络地址或呼叫记账数据等）的功能。有关私密性的具体要求是国家事务，不在本建议书讨论范围之内。

8 具体安全性要求

本节讨论NGN基础设施中各网元的具体安全要求。不过，由于许多安全需求将与各类网元相同，因此，在以下8.1节中，将首先规定总的安全要求。

依据实现方案，可以对边界元素进行集成或分离。

8.1 NGN网元的共同安全性要求

这些要求适用于受信任区和受信任但很脆弱区内的NGN网元。不信任区内的设备有必要遵循这些要求。

以下是总的安全性要求一览表：

不同的NGN网元有必要支持互操作性（尤其是不同NGN安全机制之间的互操作性）。有必要在全世界范围内提供最起码的安全功能。

有必要在业务和传输层（用户到网络、网络到用户、网络到网络）均进行认证和授权。如果存在NAPT横向相连现象，这也应是可能的。

NGN网元有必要提供安全措施，以防止对网络资源、设备、业务和用户数据（简表）的未经授权的访问，例如，封锁未经授权的业务。

NGN基础设施有必要允许提供商限制网络拓扑结构和资源对经授权实体的可视性。

NGN基础设施有必要支持多个安全区。可能需要在不同的安全区之间实施安全隔离。

NGN基础设施有必要确保在其上传输的信令/控制流和管理流的机密性和完整性。

NGN基础设施应确保在其上传输的媒体流的机密性和完整性。

NGN有必要谨慎确保链接至管理资源（OSS、数据库等）的网元和业务资源的安全。

应使用，[ITU-T M.3016.0]第10.1节所述的安全TMN管理的安全要求，更多细节请参见[ITU-T M.3016.1]第6节。

有必要在网络边界元素（NBE或TE-BE，即在受信任但很脆弱的区中的网元）上执行安全功能。这包括根据规定的政策对数据包和信令信息实施访问控制等功能（如拒绝来自特定应用或用户的业务）。

根据所用的安全政策，敏感的NGN元素，尤其是网络边界元素，可以对传输路径实施逻辑和/或物理隔离，例如，使用逻辑上不同的接口或不同的地址计划以及使用物理上不同的真实或虚拟传输网络（如VPN和VLAN等虚拟网络），将控制和/或管理流与媒体流相隔离。

对与安全相关的数据（如身份和证书数据），网络有必要提供安全的存储器。此类存储器有必要独立于一般的数据存储库（后者包含与用户业务相关的信息）。NGN有必要提供安全政策，它包括一套规则，用于确定应对哪些业务实施保护（如基于合同）、应采取何种保护措施、应多久变换一次会话密钥以及用于确定设备安全一致性的规则。

NGN有必要支持旨在监督网络流量并就正常网络事件制定基准的功能。

NGN有必要能够检测、报告和减少异常网络事件的发生。

8.1.1 安全性政策

安全政策是一套规则，它们由管理安全服务与设施使用与供应的安全主管部门制定。NGN提供商须制定适当的安全政策，并负责将之应用于所有在其控制下的网元和设备。

8.1.2 加固和服务阻断

所有NGN网元均有必要能被配置为支持NGN提供商NGN基础设施所需的最起码服务。在所有系统和网元上，有必要能够阻断对NGN网元正确运转没有要求的任何业务或传输层端口。此外，有必要在最小权限下运行应用程序（例如，如果根权限不是必不可少的，那么不应在“UNIX/Linux”平台上作为根来运行应用程序）。支持任何NGN网元的基本操作系统（OS）均有必要能被加以特殊配置，以便提供安全和适当的加固。不得从任何“后门”（绕开通常访问控制机制的软件访问）进入任何NGN网元。

除了加固，还有必要实施物理的和逻辑的访问控制，以符合行业的最佳做法。

8.1.3 审核跟踪、捕获与日志

依照NGN提供商的安全政策，所有的NGN网均有必要能够创建审核跟踪机制，对与安全相关的事件作出记录。有必要提出一些机制，以防止经授权的或未检测的信息修改。

审核跟踪有必要能被管理，并允许将审核跟踪日志上的历史数据放置于其他媒体上（例如出于长期保存目的而置于可移动媒体上）。这种接口有必要能允许经授权的管理者将历史数据从审核跟踪日志中转移到可移动的媒体上。有必要以一种特殊的授权来保护这种能力，以便管理审核跟踪日志。

[ITU-T M.3016.0]第10.1.2.6.3节和[ITU-T M.3016.1]第6.6节和第6.7节进一步详细描述了有关安全日志和审核的更多安全要求。

8.1.4 时戳与时间源

对系统时钟和审核跟踪项时戳，NGN网元都有必要支持使用一个可信的时间源。在这种情况下，可信的时间源指的是能够验证的时间源，以便抵御未经授权的修改。可迁信任是可以接受的，也就是说，依赖于一个可信时间源的时间源本身是一个可接受的可信时间源。

8.1.5 资源分配和异常处理

各NGN网元都有必要能限制分配给服务请求的自身的重要资源数量（如内存分配）。此类限制能够将拒绝服务攻击的负面影响降至最低。在系统中，用于服务请求的资源与其他资源使用请求相互竞争。此外，各特定的NGN应用有必要能限制其自身对重要资源的使用（它分配这些重要资源来满足请求）。

这一要求旨在限制活动爆发的影响，使之不至于影响其他服务请求。这还将允许/保留应用程序（和操作系统）的性能，以便告知监控系统，应用程序和/或其平台可能受到了DoS攻击。NGN网元有必要提供一个接口，以监视资源的使用情况。

NGN网元有必要静静地抛弃任何不符合预期协议或格式要求的数据包，并且基于安全政策，能够为每一个事件建立一份日志条目。“静静地抛弃”是为了捕获并记录收到的数据包，并在接收的数据包不能响应一个抛弃指令（如错误响应）时抛弃它。

这样做的目的在于限制来自恶意或不正确数据包的潜在攻击。显然，如果日志操作中资源使用过大，以致妨碍了其他元素的运行，那么使用的明显试探性做法是停止日志，直至资源使用恢复到可接受的水平。

注：这是管理内部资源的一部分，已在上面提到。

8.1.6 代码与系统完整性和监控

网元有必要能监控：1) 其配置和软件；2) 任何变化，以便检测未经授权的改变（这两个方面均基于安全政策进行）。要求任何未经授权的变化都创建日志条目，并发出警告。基于安全政策，网元有必要完成以下工作。网元有必要能定期扫描其资源和软件，以便找出恶意软件，如病毒。网元有必要在扫描过程中发现恶意软件时发出警告。

有必要对监测进行控制，使其不至于影响到对时延敏感的实时通信，或不必要地中断连接。

[ITU-T M.3016.0]第10.1.2.6.4节详细描述了有关系统完整性的更多安全要求。

8.1.7 补丁、热补丁和补充代码

对NGN提供商的NGN网元在不受信任网络中产生的信任信号，如终端，有必要确保系统上的软件不受损害。这确保了“特洛伊[1]”木马（打电话回家）、“蠕虫”（产生无用的业务或将系统变为“僵尸”）以及其他病毒无法在NGN网元或基础OS上下载。此类病毒将危及系统的完整性、机密性和/或数据的可用性。

[1] 许多特洛伊木马是发送它们的电脑黑客的一种遥控软件设备。当它们被安全地安装在目标系统中时，它们启动一个与黑客相连的连接，通知他/她可以使用这些软件了。

NGN提供商的网元和系统有必要能对所有软件进行验证和审核。审核结果应可供OSS使用。这将便于对NGN提供商的NGN基础设施的安全状况做出分析，并为管理者和提供商提供有关需采取哪里降低威胁和风险的手段方面指南。

安全补丁应从设备供货商处获得，一经NGN提供商进行认证，即及时得到安装。

[ITU-T M.3016.1]第I.5.2节提供了关于补丁程序的更多考虑；ITU-T M.3016.1第I.5.3.9节提供了关于操作系统安全假设的更多考虑。

8.1.8 在设备内访问OAMP功能

为了保护OAMP基础设施，有必要通过一个单独的IP地址（分配自一个单独的地址块）对各内部NGN网元加以管理。各内部NGN网元应具备一个物理上或逻辑上独立的接口，专用于这种OAMP业务。当使用一个单独的接口时，NGN网元有必要静静地抛弃在OAMP接口上接收的源地址不同于OAMP地址的所有数据包。NGN网元有必要静静地抛弃在非OAMP接口上收到的使用指定给OAMP业务的源地址的所有数据包。

有必要能通过认证形式对接入OAMP功能加以控制。一旦用户通过了系统认证，内部NGN网元则有必要追踪其发生的所有变化，并提供使其恢复原状的机会。

所有与安全有关的认证应用均有必要在特定时期内被记录在审核跟踪记录中。尤其是，所有对元素的访问尝试，不管成功与否，均有必要被记录在审核跟踪。

有必要对OAMP业务实施安全的保护。如果OAMP业务（包括SNMP和NTP）在一个不受信任的网络上传输，那么则有必要对它实施安全的保护（如IPSec或MPLS等）。

8.2 对受信任区内的NGN网元的要求

应为“受信任”区中的第1版本NGN网元分派一个IP地址（从专用于内部NGN网元的地址块中分配）。所有信令都有必要使用该地址。还有必要为第1版本NGN网元分派一个IP地址（从专用于OAMP的地址块中分配），并且所有的OAMP都有必要使用该地址。

为了保护客户通信的机密性，应对信令和媒体进行保护，如进行传输加密，或确保业务只有受保护域中传输。

8.3 对“受信任但很脆弱的”域内的NGN边界网元的要求

边界网元是抵御外部攻击的主要防线，所谓外部攻击指的是来自不受信任区中设备/网元的攻击。来自“不受信任”区中设备/网元的所有业务，首先发送给边界网元，并在该网元上进行验证，然后再将其发送给“受信任”域中的目的地。采用物理上/逻辑上独立的网络性能可阻止来自不受信任区中设备/网元业务抵达任何处于“受信任”域中的网元。

网络边界元素（NBE）是抵御信令攻击的主要防线。所有来自不受信任的区中TE或TE-BE的信令业务，都在其指定的NBE上进行处理，指定的NBE再将信令重传给受信任的区中的网络设备。采用在NBE上提供物理上/逻辑上独立的网络性能可阻止不受信任区中的TE/TE-BE抵达受信任区中的任何网元，其指定的NBE除外。

与信令一样，网络边界元素（NBE）也是抵御媒体攻击的主要防线。所有来自TE/TE-BE的媒体业务都在NBE上进行处理，然后由NBE转送给媒体。只有当媒体数据包可以与一个正在进行中的受权会话相关联时，NBE才为媒体数据包选择路由，通过信任域，送往目的地。不与会话请求关联的媒体数据包是无效的，将无处可去，并被抛弃。此外，NBE将对媒体流来源进行验证，并验证数据包等级是否与会话确定的等级相一致。在NGN提供商设备内传送的媒体，要么传送给一个PSTN出入口局（用于建立PSTN连接），要么传送给另一个NBE。在第二个NBE上，对媒体进行处理，并重传给一个TE目的地。

注 – “会话”一词系指任何类型的媒体流，无论使用何种惯例建立会话。

网络边界元素有必要支持多个IP地址或多个网络接口。应从为内部第1版本NGN网元预留的地址块中分配一个IP地址（“内部”地址）。发往或来自其他内部第1版本NGN网元的所有信令和媒体，都有必要使用该地址（或该接口）。应指定一个IP地址（“外部”地址），它可以从TE设备处获得。发往或来自TE的所有信令和媒体都有必要使用该地址（或该接口）。应从为OAMP预留的地址块中指定一个IP地址（“OAMP”地址），它可以从OAMP服务器处获得。

为了保护客户通信的机密性，防止对信令业务的窃听，有必要保护所有信令消息的信令传输安全，使其安全抵达“受信任”或“受信任但很脆弱的”区中的NGN网元。在利用经过认证的安全信道，建立用于向此类NGN网元传送信令信息的、由NBE发起的所有连接。应静静地抛弃NBE在其“内部”NGN地址上、通过非安全信道收到的所有信令消息。

应通过传输加密或确保业务只在受保护网络上传输的手段保护媒体流。此外，在网络边缘的源地址保证，将确保来自外部的数据包不会声称是来自内部的NGN地址块。

应为进行中的会话（基于信令交换）由NBE在其外部地址上对收到的媒体数据包进行检查。对照预期的源地址（基于包含在信令交换中的会话描述）。NBE有必要静静地抛弃任何接收到的、不对应进行中的会话的媒体数据包。NBE还应验证数据包的等级是否与商定的会话参数相一致。NBE可以验证数据包大小是否与会话确定的大小相一致。应静静地抛弃从非本NBE有效媒体发起者的源IP地址处收到的媒体数据包。

如果客户服务协议有要求，那么NBE有必要对所有请求进行认证。当从非加密的连接上收到请求时，有必要对各个请求逐一进行认证。当从加密的连接上收到请求而该连接在建立之初未经客户端认证时，应对经该连接传送的第一个请求进行认证。当从加密的连接上收到请求且连接在建立之初已经认证时，无需进一步进行认证。注意：通过TE-BE发送的请求，将无需进行设备认证，原因是TE-BE将使用一个与NBE的加密连接。如果请求来自一个源IP地址，而该IP地址不是该NBE的一个有效请求发起者，那么应静静地抛弃它。还应静静地抛弃来自非此NBE有效请求发起者的源IP地址的安全信道请求。

8.4 对“不受信任”域内的TE边界元素的要求

对部署在客户站点的设备而言，其物理安全是个挑战。最终，务必接受这样的事实，即在很大程度上，这些设备的安全取决于客户。尽管如此，为了防范攻击、危害或其他方式的破坏，有必要对每个设备均采取合理的防范措施。为了保护客户通信的机密性，防止对信令业务的窃听，信令消息有必要在TE-BE与NBE之间使用安全的信令连接。TE-BE可以执行媒体中继功能。

8.4.1 OAMP功能

有必要对TE-BE与NGN提供商之间的所有OAMP功能实施保护，以防止确定的窃听。由于OAMP既能在带内提供，也能在带外提供，因此应对它们分别对待。

8.5 对“不受信任”域内终端设备的安全性建议

终端设备（TE）通常不受NGN提供商控制。因此，不要求NGN提供商对其安全特点或政策提出要求，这是各网络边界元素的职责，以适应客户选择的任何政策，并在这些条件下提供最好的服务。

有关NGN提供商边界元素的实际安全功能有待进一步研究。

应保护媒体业务量免遭窃听或修改。

附录一

应急通信服务（ETS）互连的安全性目标与导则

（本附录不构成本建议书的组成部分）

I.1 背景

应急通信服务（ETS）是一种国家服务，在出现灾害和紧急事件时，为经授权的ETS用户提供优先通信服务。ETS的实施是国家事务。不过，灾害/紧急事件可能超越地理界线，因此，国家/主管部门可能协定双边和/或多边协议，以连接其各自的ETS系统。这将允许在出现灾害和紧急事件时，不同国家网络之间利用双边和/或多边协议来支持ETS庇护下的优先通信服务（如话音、消息、视频和数据）。

不同国家网络（即国家/主管部门）之间的ETS通信服务需要加以保护，以应对安全威胁。为使网络能为不同国家网络（即国家/主管部门）ETS实施方案之间的端到端ETS通信服务提供安全保护，需要确立一些指南和共同的安全目标及要求。ETS通信服务的安全性和可用性将取决于涉及端到端通信的各个网络的安全。

I.2 范围/目的

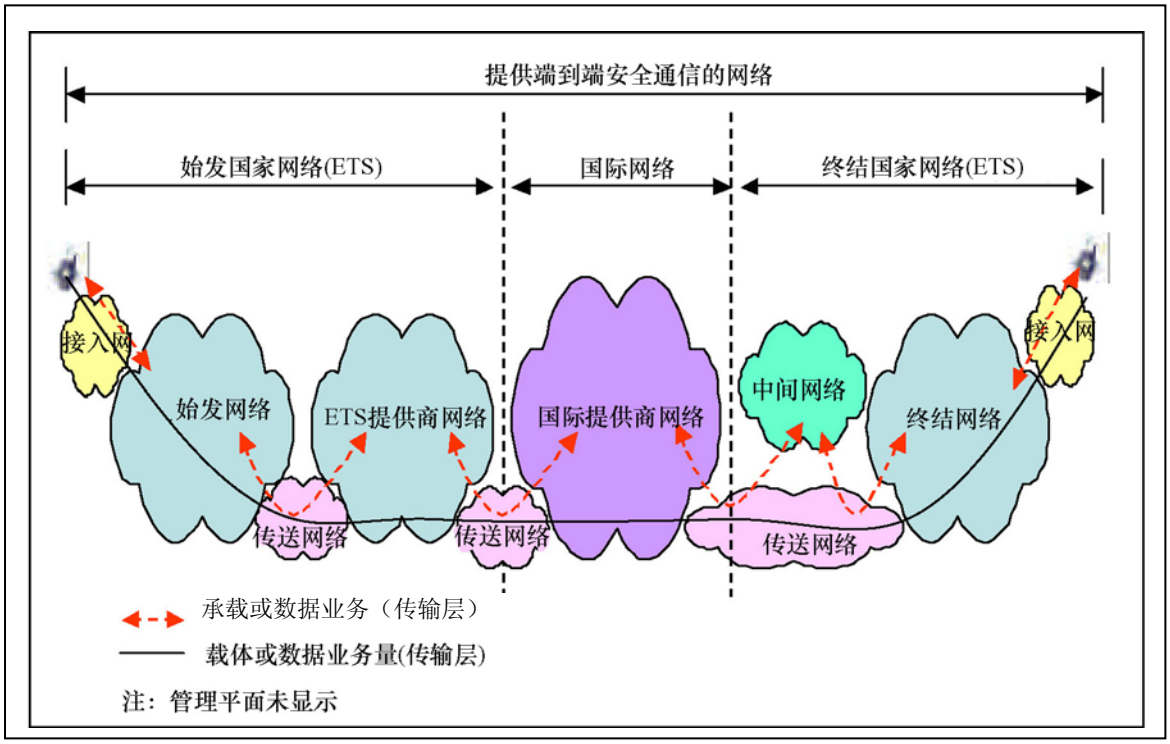
本附录提供了共同的安全目标和要求，并提供了指南，以便为在不同国家网络（即国家/主管部门）ETS实施方案之间提供ETS通信服务的网络安全性提供支持。

使用特殊最终用户设备安全功能的用户对等安全功能不在本附录的讨论范围之内。本附录的范围仅限于跨越多个网络的、以逐段转接的方式为ETS通信服务提供安全保护的网络。不过，NGN应能透明地支持此类对等功能。

本附录无意对ETS的国家实施方案强加条件。其主要目的是使网络能够为ETS通信服务提供安全保护（即安全的优先话音、视频、数据和消息通信）。

I.3 总体目标

网络的总体目标是为了能够为不同国家网络（即国家/主管部门）的ETS通信服务（如安全的优先话音、视频、数据和消息通信）提供安全保护，并保护ETS的可用性。这将涉及端到端通信的安全，它可能涉及国家和国际级网络（即国家/主管部门）的不同网络提供商域，其中，各个网络负责其域内的安全。



图I.1 – 跨越不同国家ETS实施方案的端到端通信举例

图I-1描述了两个不同国家网络之间的端到端ETS通信服务（例如，优先的话音、视频、数据和消息通信）的示例。该示例具体说明ETS端到端优先通信可能涉及多个网段和管理域（例如，接入网、始发网络、ETS提供商网络、国际提供商网络、中间网络和终接网络）。

各个网段在其域内将具有特定的安全职责，以推动ETS通信服务的端到端安全性和可用性。

以下为最起码的一套总体导则和安全规划规则，用于保护ETS的信令、承载网和与管理相关的数据以及信息：

- 各个网域都应建立和执行安全政策，并为ETS在其域内实施降低威胁和风险性能。尤其是，建议应为ETS优先通信确定和执行比一般应用服务所需的降低风险和提高安全做法更多的措施。例如，设计的这些性能和做法应有助于防止未经授权的用户使用ETS资源，并防止拒绝服务和其他类型的攻击。
- 为了确定ETS通信服务以及为了对多个网络管理域间的最终用户和网络进行身份管理与认证，各个网域都应建立信任关系、方法和程序。例如，当交付和接收ETS通信服务时，服务水平协议（SLA）应为各个域的认证建立安全政策。
- 各个网络管理域都应确立和执行安全政策，以便保护与ETS管理相关的数据和信息（例如，用户简表信息）。

I.4 总体安全功能

对ETS，建议支持以下功能：

- 保护多个网域间端到端ETS通信服务的安全功能。
- 保护多个网域间ETS通信服务可用性的安全功能。
- 提供多个网络管理域间最终用户与网络身份管理与认证的安全功能。最终用户只与ETS服务互动一次，安全机制就能将用户证书从管理域传给相关域是十分必要的。

I.5 认证、授权和访问控制

对ETS，建议支持以下最起码的认证、授权和访问控制功能：

- 保护用于认证和授权ETS用户与设备的机制的安全功能。
- 保护用于ETS最终用户与相关设备绑定的机制的安全功能。
- 保护用于在多个网域间共享认证信息的机制的安全功能（例如，确认某个最终用户已经经过认证）。
- 保护用于最终用户与实体之间相互认证的机制的安全功能。这包括ETS用户认证被叫方或通信实体的机制（例如，网站、内容服务器等）。
- 保护用于通过一个网络认证另一个网络的机制的安全功能。这包括用于认证交付ETS通信服务的网络（例如，始发网络）的机制以及用于认证接收ETS通信服务的网络（例如，中间或终接网络）的机制。
- 保护ETS信息与资源免受未经授权访问的安全功能（例如，在认证服务器和管理系统中的用户信息）。

I.6 机密性和私密性

建议支持以下最起码的机密性功能：

- 提供保护ETS信令和控制机密性的安全功能。
- 提供保护ETS承载网和数据业务机密性的安全功能（例如，话音、视频或数据）。
- 提供保护ETS最终用户和通信实体身份以及订购信息机密性的安全功能。
- 提供保护ETS最终用户位置机密性的安全功能。

建议支持以下最起码的私密性功能：

- 提供保护ETS信息私密的安全功能（例如，源自对网络活动观察的信息，如最终用户访问过的网站、最终用户的地理位置、服务提供商网络中的IP地址和设备DNS名称）。

- 提供防止对ETS使用信息进行未经授权观测的私密性保护安全功能（例如，使用规律（ETS业务量）、地点、时间、频率等）。

I.7 数据完整性

建议支持以下最起码的数据完整性功能：

- 提供保护ETS通信服务完整性的安全机制（例如，防止未经授权的修改、删除、创建或重播）。这包括提供信息篡改或修改通告的机制。
- 提供保护ETS信息完整性的安全功能（例如，优先级标记、话音、数据和视频）。
- 提供保护ETS特殊配置数据完整性的安全功能（例如，存储于政策决策功能中的优先信息、用户优先等级等）。

I.8 通信

建议支持以下最起码的功能：

- 保护ETS通信服务的授权ETS最终用户免受侵扰的安全机制（例如，防止截获、截取或重播ETS信令或承载/数据业务的机制）。

I.9 可用性

建议支持以下最起码的功能：

- 保护ETS通信服务可用性的安全机制（例如，保护ETS信令与控制以及承载/数据业务免遭拒绝服务（DoS）和其他形式的攻击）。
- 保护ETS特殊资源和信息可用性的安全机制（例如，认证/授权数据库、存储于政策决策功能中的优先信息以及用于抵御拒绝服务（DoS）和其他形式攻击的专用网络资源）。

参考资料

ITU-T建议书

[b-ITU-T E.106] ITU-T Recommendation E.106 (2003), *International Emergency Preference Scheme (IEPS) for disaster relief operations*.

[b-ITU-T E.107] ITU-T Recommendation E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS.*

[b-ITU-T E.115] ITU-T Recommendation E.115 (2007), *Computerized directory assistance*.

[b-ITU-T M.3016.2] ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.

[b-ITU-T M.3016.3] ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

[b-ITU-T M.3016.4] ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.

[b-ITU-T M.3060] ITU-T Recommendation M.3060/Y.2401 (2006), *Principles for the management of Next Generation Networks.*

[b-ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ITU-T X.1122] ITU-T Recommendation X.1122 (2004), *Guideline for implementing secure mobile systems based on PKI*.

[b-ITU-T Y.1271] ITU-T Recommendation Y.1271 (2004), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-ITU-T Y.2000-Sup.1] ITU-T Y.2000-series Recommendations – Supplement 1 (2006), *NGN release 1 scope*.

[b-ITU-T Y.2111] ITU-T Recommendation Y.2111 (2006), *Resource and admission control functions in Next Generation Networks.*

ETSI TISPAN documents

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis.*

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements.*

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture.*

ETSI/3GPP documents

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *3G security; Security architecture*.

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *3G security; Integration guidelines*.

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Key establishment between a UICC and a terminal*.

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Security Objectives and Principles*.

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G security; Access security for IP-based services*.

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *3G security; Network Domain Security (NDS); TCAP user security*.

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *3G security; Network Domain Security; IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Network Domain Security (DNS; Authentication Framework (AF)*.

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Criteria for cryptographic algorithm design process*.

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Formal Analysis of the 3G Authentication Protocol*.

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)*.

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *3G Security; Generic Authentication Architecture (GAA); System description*.

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature*.

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)*.

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security – Criteria for cryptographic Algorithm design process*.

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol*.

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description*.

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*.

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines*.

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives*.

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS)*.

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Digital cellular telecommunications system; (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)*.

ATIS/3GPP2 documents

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *IMS Security Framework*.

IPsec related IETF RFCs

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay Prevention*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains*.

[b-IETF RFC 2857] IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH*.

[b-IETF RFC 3526] IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3664] IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*.

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)*.

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*.

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use With IPsec*.

S/MIME related IETF RFCs

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification*.

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME Version 2 Certificate Handling*.

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)*.

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*.

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*.

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Cryptographic Message Syntax*.

[b-IETFB RFC 4134] IETF RFC 4134 (2005), *Examples of S/MIME Messages*.

TLS related IETF RFCs

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Upgrading to TLS Within HTTP/1.1*.

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

Miscellaneous IETF security related RFC

[b-IETF i-d.SIPUAP] IETF internet-draft work in progress, draft-ietf-sipping-config-framework-08.txt (March 6, 2006), *A Framework for Session Initiation Protocol User Agent Profile Delivery*.

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3715] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements*.

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*.

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

DNS related IETF RFCs

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Resource Records for the DNS Security Extensions*.

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Protocol Modifications for the DNS Security Extensions*.

TIA documents

[b-TIA-683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

[b-TIA-1053] TIA Standard TIA-1053 (2005), *Broadcast/Multicast Security Framework.*

[b-TIA-1091] TIA Standard TIA-1091 (2006), *IMS Security Framework.*

ARIB documents

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Common Security Algorithms*.

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	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
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	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
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、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网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
2008年，日内瓦