国　际　电　信　联　盟

ITU-T

Y.2704

(01/2010)

国际电信联盟
电信标准化部门

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

下一代网络(NGN)的安全机制和程序

ITU-T Y.2704 建议书

ITU-T

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
未来的网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
运营商级开放环境	Y.2900–Y.2999

如果需要进一步了解细目，请查阅*ITU-T*建议书清单。

ITU-T Y.2704建议书

下一代网络(NGN)的安全机制和程序

摘要

ITU-T Y.2701建议书《下一代网络(NGN) 第一阶段的安全要求》规定了下一代网络(NGN)的安全性要求及其接口(例如UNI、NNI和ANI)。ITU-T Y.2704建议书描述了一些安全性机制，能够用来实现在ITU-T Y.2701建议书中描述的要求，并且对每一种选定的机制明确了选项组。具体地说，本建议书描述了识别、认证和授权机制；接着讨论了信令和OAMP传输安全以及媒体安全。然后讨论了与审计跟踪相关的机制，最后描述了提供机制。本建议书描述的安全机制以应用在ITU-T Y.2701建议书中定义的信任模型作为基础。

本建议书描述的系列安全机制不是全部，鼓励NGN提供商在需要的时候支持除了本建议书规定的机制以外、另外的安全工具、能力和运行措施，用于NGN的安全保护。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2704	2010-01-29	13

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)和国际电工委员会(IEC)合作制定的。

注

本建议书为简要扼起见而使用的“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”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

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

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

		页码
1	范围	1
1.1	假设	1
1.2	概述	1
2	参考文献	2
3	定义	3
3.1	其他文献规定的术语	3
3.2	本建议书规定的术语	4
4	缩写词和首字母缩略语	4
5	约定	7
6	安全风险和威胁	7
7	安全信任模型	7
7.1	单一网络信任模型	7
7.2	对等网络信任模型	9
8	识别、认证和授权	10
8.1	订户	10
8.2	网元	10
8.3	凭证在NGN安全中的应用	10
8.4	订户的识别和认证	14
8.5	最终用户的识别和认证	18
8.6	由TE-BE开展的识别和认证	20
8.7	认证器-SAA/TAA-FE接口	20
8.8	承载业务的识别和认证	21
9	信令和OAMP的传输安全	23
9.1	TLS	23
9.2	可信区和可信但脆弱的区内的IPsec	27
9.3	不可信区和可信但脆弱的区之间的密钥管理协议	31
9.4	不可信区和可信但脆弱的区之间的IPsec	31
10	媒体安全	31
10.1	SRTP	33
11	OAMP	34
11.1	网元与登录系统的接口	35
11.2	网元使用SNMP	35
11.3	安全补丁管理	35
11.4	版本管理	35
11.5	TE-BE的审计跟踪、捕获和记录	36
12	不可信区内设备供应	36

页码

附录一 – 源地址保证及其在订户识别和认证机制中的应用举例 37
I.1 与接入线路认证相关联的订户识别和认证 37
I.2 在IP连通性建立期间与明确接入认证相关的订户识别和认证 39
附录二 – 应急电信服务(ETS)的互连安全 42
II.1 背景 42
II.2 范围/目的 42
II.3 ETS安全目标和ETS互连准则 42
II.4 认证和授权 42
II.5 信令和OAMP的传输安全 43
II.6 媒体业务 43
II.7 支持主叫号码ID和主叫名称ID限制特性 43
II.8 不可追溯性 43
II.9 端对端对等加密 43
附录三 – 安全最佳做法 44
III.1 引言 44
III.2 防火墙 44
III.3 操作系统加固 45
III.4 脆弱性评估 45
III.5 侵入检测系统 46
参考资料 47

ITU-T Y.2704建议书

下一代网络(NGN)的安全机制和程序

1 范围

[ITU-T Y.2701]《下一代网络(NGN)第一阶段的安全要求》提出了下一代网络(NGN)的安全性要求及其接口(例如UNI、NNI和ANI)，包括一个信任模型。为实现这些要求而选择的安全机制将包含选项和不希望有的失配选项，因为失配选项往往引入安全脆弱性，并使互操作性的实现变得更加困难。

因此，本建议书强调了一些能够用来实现[ITU-T Y.2701]要求的重要安全机制，并为每一种选定的机制明确了选项组，以便减少互操作性和失配问题。本建议书中描述的系列机制不是全部，鼓励NGN提供商在需要的时候提供除了本建议书规定的机制以外、另外的安全工具、能力和运行措施，用于NGN的安全保护。

本建议书旨在与 [ITU-T Y.2701]一并使用，为NGN安全提供一个基础。本建议书应根据具体的安全领域酌情与其他关于安全的建议书和其他技术要求一并使用。

注 — 本建议书中描述的用于识别和认证的机制是更宽泛的通常被称做IdM(“身份管理”)的主题的一部分。

1.1 假设

本建议书基于下列假设：

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

2) 各个NGN提供商在其安全域内有具体的职责。例如，履行适当的安全服务和做法，以a)保护自己，b)确保不损害其网络内端对端的安全，c)确保NGN通信的高可用性和完整性。

3) 各网络域将建立和执行有关服务水平协议(SLA)的策略，以确保其域内的安全和网络互连的安全。假设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，它是一个分层的体系结构，包括可信域的边界安全、提供商设备的物理安全以及可能采用加密。

1.2 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) — 本节提供本建议书所用的定义。
- 第4节(缩写词和首字母缩略语) — 本节提供本建议书所用的缩写词和首字母缩略语清单。
- 第5节(约定) — 本节有意空白。

- 第6节(安全风险和威胁)— 本节提供适用于NGN的安全风险和威胁参考。
- 第7节(安全信任模型)— 本节提供[ITU-T Y.2701]定义的信任模型的概述。
- 第8节(识别、认证和授权)— 本节提供用于识别、认证和授权的机制和安全措施。
- 第9节(信令和OAMP的传输安全)— 本节提供用于信令和OAMP的加密和完整性保护的机制。
- 第10节(媒体安全)— 本节提供用于媒体(即承载业务)保护的机制。
- 第11节(OAMP)— 本节提供关于安全事件审计跟踪、捕获和记录的信息和参考文献。
- 第12节(不可信区内设备供应)— 本节提供关于不可信区内用户设备供应的信息。
- 附录一 — 源地址保证及其在订户识别和认证机制中的应用举例
- 附录二 — 应急电信服务(ETS)的互连安全性
- 附录三 — 安全最佳做法
- 参考资料

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均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和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。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T Y.2012] ITU-T Y.2012建议书 (2006)，《下一代网络(NGN)的功能要求和体系结构》。

[ITU-T Y.2701] ITU-T Y.2701建议书(2007)，《下一代网络(NGN)第一阶段的安全要求》。

[ITU-T Y.2702] ITU-T Y.2702建议书(2008)，《下一代网络(NGN)第一阶段的认证和授权要求》。

[ITU-T Y.2703] ITU-T Y.2703建议书(2009)，《下一代网络(NGN)中认证、授权和结算(AAA)的应用》。

[ITU-T Y.2720] ITU-T Y.2720建议书(2009)，《下一代网络(NGN)的身份管理框架》。

[ITU-T X.509] ITU-T X.509建议书 (2008) | ISO/IEC 9594-8:2008，《信息技术 — 开放系统互连 — 号码簿：公开密钥和属性证书框架》。

[ITU-T X.660] ITU-T X.660建议书 (2008) | ISO/IEC 9834-1:2008，《信息技术 — 开放系统互连 — OSI登记机构的操作规程：通用规程和国际对象标识符树的顶端弧》。

[ITU-T X.1035] ITU-T X.1035建议书 (2007)，《口令认证密钥交换(PAK)协议》。

[IETF RFC 4302] IETF RFC 4302 (2005)，*IP Authentication Header*。

[IETF RFC 4303] IETF RFC 4303 (2005)，*IP Encapsulating Security Payload (ESP)*。

[IETF RFC 5246] IETF RFC 5246 (2008)，*The Transport Layer Security (TLS) Protocol Version 1.2*。

3 定义

3.1 其他文献规定的术语

本建议书采用其他文献规定的下列术语。

3.1.1 asset 资产 [ITU-T Y.2701]：任何对组织及其业务、运营和连续性有价值的事物。

3.1.2 border element 边界元素[ITU-T Y.2701]：提供连接不同安全和管理域功能的网元。

3.1.3 corporate network 企业网[ITU-T Y.2701]：支持多个用户并可能在多个地点(如企业、校园)的专用网。

3.1.4 domain border element 域边界元素[ITU-T Y.2701]：完全由提供商控制的边界元素，为其他网络域提供安全功能。

3.1.5 emergency telecommunications service (ETS) 应急电信服务[b-ITU-T E.107]：国家服务，它在发生灾害和出现突发事件时向有权使用ETS的用户提供优先通信。

3.1.6 network border element 网络边界元素[ITU-T Y.2701]：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。

3.1.7 security domain 安全域[ITU-T Y.2701]：一组元素、一种安全策略、一个安全主管当局以及一组与安全相关的活动，依据安全策略管理其中各个元素。安全策略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。

3.1.8 security token 安全令牌[b-ITU-T X.810]：在相互通信的实体之间传送的，受一个或几个安全服务保护的一组数据，其中附带用于提供这些安全服务的安全信息。

3.1.9 security zone 安全区[ITU-T Y.2701]：[ITU-T Y.2701]规定了三种安全区， (1) 可信，(2)可信但脆弱的，(3) 不可信。安全区从操作控制、位置和至其他装置/网元的连通性几方面来规定。

3.1.10 terminal equipment border element 终端设备边界元素[ITU-T Y.2701]：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。

3.1.11 trust 信任[ITU-T Y.2701]：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，才认为实体X在一系列活动方面信任实体Y。

3.1.12 trusted but vulnerable zone 可信但脆弱的区[ITU-T Y.2701]：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)的一个安全区。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提供商域内或域外。它们既与可信区内的元素进行通信，也与不可信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，保护可信区内的网元免遭来自不可信区的安全攻击。

3.1.13 trusted zone 可信区[ITU-T Y.2701]：从NGN提供商的角度看，这是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一个安全域。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“可信”域和“可信但脆弱的”域内的网元进行通信。

3.1.14 un-trusted zone 不可信区[ITU-T Y.2701]：从NGN提供商的角度看，这是包括客户网络或可能是对等网络或最初域之外其他NGN提供商区的所有网元的一个区域，这些网元与NGN提供商的边界网元相连。

3.1.15 user 用户[b-ITU-T Y.2091]：用户包括最终用户，人员，订户，系统，设备，终端(例如传真机、个人计算机)，(功能)实体，进程，应用，提供商或企业网。

3.1.16 user network 用户网[ITU-T Y.2701]：由终端设备组成的可能有多个用户的某一专用网。

3.2 本建议书规定的术语

本建议书规定下列术语：

3.2.1 authenticator 认证器：认证器是一个便于订户、设备或最终用户识别和认证的网元。例如，具有背对背用户代理(B2BUA)功能或代理呼叫会话控制功能实体(P-CSC-FE)的边界元素可以是基于SIP服务的订户的认证器。

4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

3G	第3代
AGW	接入网关
AH	认证报头
AKA	认证和密钥协商
ANI	应用网络接口
AS/WS	应用服务器/万维网服务器
AuC	认证中心
B2BUA	背对背用户代理
BE	边界元素
BSR	基站路由器
CA	认证机构
COPS	公共公开策略服务

CRL	证书撤销列表
CSC-FE	呼叫会话控制功能实体
DBE	域边界元素
DNS	域名系统
DoS	拒绝服务
DTMF	双音多频
ECC	椭圆曲线密码
ESP	封装安全协议
ETS	应急电信服务
FE	功能实体
GBA	通用引导体系结构
GW	网关
HMAC	散列信息认证码
HTTP	超文本传输协议
I-CSC-FE	询问呼叫会话控制功能实体
ID	身份
IdM	身份管理
IDPS	侵入检测和预防系统
IDS	侵入检测系统
IKE	互联网密钥交换
IMS	IP多媒体子系统
IP	网际协议
ISDN	综合业务数字网
LAN	局域网
MD5	信息摘要5
MIB	管理信息库
MPLS	多协议标签交换
MRP-FE	媒体资源处理功能实体
MS	移动台
NAC-FE	网络接入控制功能实体
NAPT	网络地址和端口转换
NAT	网络地址转换
NBE	网络边界元素
NE	网元
NGN	下一代网络
NNI	网络网络接口
OAMP	运营、管理、维护和提供

OID	对象标识符
ONU	光网络单元
PAK	口令认证密钥
P-CSC-FE	代理呼叫会话控制功能实体
POTS	普通老式电话业务
PSTN	公众交换电话网
QoS	服务质量
RAC-FE	资源和接纳控制功能实体
RADIUS	远程认证拨入用户业务
RAN	无线电接入网
RTSP	实时流协议
SAA-FE	服务认证和授权功能实体
SASL	简单认证和安全层
S-CSC-FE	呼叫会话控制服务功能实体
SDP	会话描述协议
SIM	用户身份模块
SIP	会话起始协议
SLA	服务水平协议
SL-FE	签约位置功能实体
SNMP	简单网络管理协议
SRTP	安全实时协议
TAA-FE	传输认证和授权功能实体
TCP	传输控制协议
TE	终端设备
TE-BE	终端设备边界元素
TLS	传输层安全
TMN	电信管理网
TRIP	IP电话路由协议
UA	用户代理
UDP	用户数据报协议
UE	用户设备
UICC	通用集成电路卡
UMTS	通用移动通信系统
UNI	用户网络接口
URL	统一资源定位器
USIM	通用用户身份模块
VLAN	虚拟局域网

VPN 虚拟专用网

WLAN 无线局域网

xDSL x数字用户线

5 约定

无。

6 安全风险和威胁

NGN环境中所谓的安全风险和威胁见[ITU-T Y.2701]第4节。

7 安全信任模型

NGN提供商对安全机制的选择取决于适用的信任模型。本建议书假设采用在[ITU-T Y.2701]中定义的信任模型。本节提供[ITU-T Y.2701]定义的NGN安全信任模型的概述。

NGN功能参考体系结构定义了功能实体(FE)，然而，由于网络安全方面严重依赖于将FE物理上绑定在一起的方式，因而NGN安全体系结构建立在物理网元(NE)的基础上，即包含一个或多个FE的实际机箱。将这些FE绑定成NE的方式将因供货商和NGN提供商的不同而不同。

7.1 单一网络信任模型

本节规定三种安全区：

1) 可信；

2) 可信但脆弱的；

3) 不可信，

这三种安全区取决于运营控制、地点、与其他设备/网元的连接性。图1所示的安全信任模型对这三种区给予了说明。

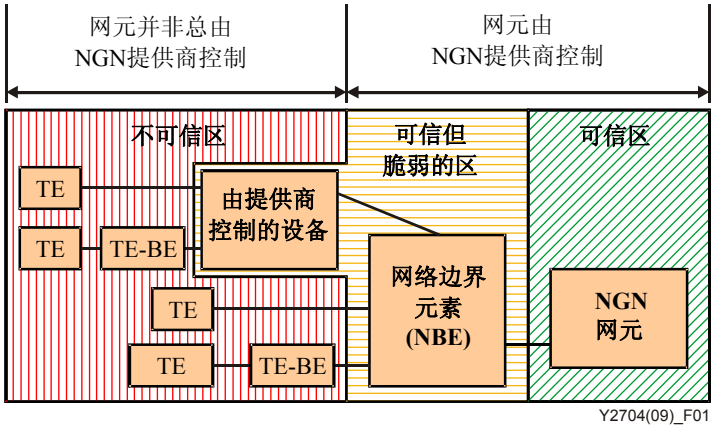


图1－安全信任模型/[ITU-T Y.2701]

“可信网络安全区”或简称为“可信区”，是NGN提供商的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：

1) 它们完全由NGN提供商所控制(以进行设备配置、维护和操作控制)；

2) 位于NGN提供商域内；且

3) 它们只与“可信”区和“可信但脆弱的”区内的其他元素进行通信。

不能因为某一网元在可信区内，就认为它一定是安全的。

“可信区”内的网元将受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、安全信令的使用、管理消息的安全，以及(MPLS/)IP网络内建立单独虚拟专用网(VPN)的使用。同样，这些方法的组合也有望适用于“可信”区内的安全通信，适用于“可信”区内与“可信但脆弱的”区内NGN网元之间的安全通信。

“可信但脆弱的网络安全区”或简称为“可信但脆弱的区”，是网元/网络设备与“不可信”区内的元素相互通信的区，这就是为什么说它们是“脆弱的”的原因。此外，它们也与“可信”区内的元素进行通信。与“可信”区内的网元一样，设备可能由NGN提供商控制，尽管设备可能位于NGN提供商驻地内，也可能位于驻地外。它们的主要安全功能是保护可信区内的网元免遭来自不可信区的安全攻击。“可信”区内与“可信但脆弱的”区内NGN网元之间的安全通信所用方法的组合可能与“可信”区内的安全通信不同。

位于NGN提供商域内、与可信区之外的元素连接的元素被称做网络边界元素(NBE)，一些网络边界元素的例子如下：

- 位于UNI处的网络边界元素(NBE)，它们为可信区内NGN提供商的服务控制或传输元素提供接口，以便为服务和/或传输目的提供用户/订户对NGN提供商网络的接入。
- 与网络边界元素类似的“域边界元素”(DBE)，不同之处是该元素处于域的边界。
- “设备配置与引导NBE”(DCB-NBE)，它们通过接口与可信区内的NGN提供商的设备配置系统相连，以便配置户外设施中用户/订户的设备和NGN提供商的设备。
- “OAMP-NBE”通过接口与可信区内的NGN提供商的OAMP系统相连，以便提供和维护户外设施中用户/订户的设备和NGN提供商的设备。
- “应用服务器/万维网服务器NBE”(AS/WS-NBE)，它们通过接口与可信区内的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。

图1所示的是与这些需要受到保护的NBE和NE的关系。

下面是一些设备/元素由NGN提供商运营但不在NGN提供商的驻地，可能受NGN提供商的控制、也可能不受NGN提供商的控制的例子：

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

包含NBE的“可信但脆弱的”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、对所有传输到“可信”区内NGN网元的信令信息采用安全信令、OAMP信息安全以及数据包过滤器和防火墙。“不可信区”包括客户网络或可能的对等网络或其他NGN提供商域中的所有网元，它们与NGN提供商的网络边界元素相连。在包含终端设备的“不可信区”内，设备不受NGN提供商的控制，也许无法对用户实施NGN提供商的安全策略。然而仍然应当尝试应用一些安全措施，最后，建议应该保护信令、介质和OAMP，并对位于“不可信区”内的TE-BE进行加固。然而，由于是与“不可信”区内网元的通信，所以不如与“可信”区内网元的通信安全。

7.2 对等网络信任模型

当NGN与另一个网络相连时，信任与否取决于：

- 物理互连，可以有多种互连方式，从安全建筑内的直接连接到两个单独的(可能是不安全的)建筑经过共享设备的连接；
- 对等模型，在这种情况下，可以在两个NGN服务提供商之间直接进行业务交换，或通过一个或多个NGN传输提供商进行业务交换；
- 网络间的业务关系，在这种情况下，服务水平协议(SLA)中可能有惩罚性条款，和/或信任其他NGN提供商的安全策略；通常，NGN提供商应把其他提供商视为不信任的提供商。

图2所示的是判定一个已连接的网络为不可信的例子。

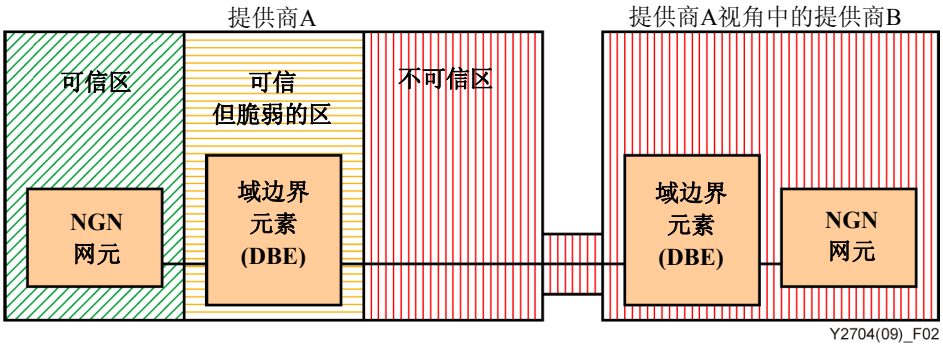


图2 – 对等信任模型/[ITU-T Y.2701]

8 识别、认证和授权

有关识别、认证、授权和身份管理(IdM)的信息参见[ITU-T Y.2701]、[ITU-T Y.2702]、[ITU-T Y.2703]和[ITU-T Y.2720]。

本节描述识别、认证和授权机制，特别是那些与基于SIP的服务有关的机制。与其他服务有关的机制有待进一步研究。

8.1 订户

一个NGN服务请求与一个订户相关联，通过识别请求和订户来确定这种联系。可能有必要根据NGN提供商和订户之间的服务水平协议(SLA)，对最终用户做更进一步的识别(以及相关的认证)。

这个过程能够通过使用一个功能元素来完成，功能元素是一个促进订户、设备或最终用户(称为认证器)识别和认证的网元。例如，具有背对背用户代理(B2BUA)功能或P-CSC-FE的网络边界元素(NBE)能够作为基于SIP服务的订户的认证器，通过在认证器和TE之间交换和验证凭证来实现识别和认证。

8.2 网元

[ITU-T Y.2701]建议应该对通信的网元进行识别和认证。

如果边界元素收到可信区内NGN网元的请求，则可以根据NGN提供商的安全策略，认为请求中包含的标识是正确的，不对其做进一步的检查。

如果边界元素收到不可信区和可信但脆弱的区内网元的请求，则建议对网元进行识别和认证并验证通信特权。通过在认证器和TE之间交换和验证凭证来实现识别和认证。

8.3 凭证在NGN安全中的应用

凭证在NGN安全中用于识别和认证设备、订户和/或最终用户。用于识别和认证设备、订户和/或最终用户的凭证在第8.3.1节中做了说明。凭证可以采取两种不同形式中的一种：X.509公开密钥证书(在第8.3.2节中描述)或共享密钥(在第8.3.3节中描述)。基于NGN提供商的策略，X.509公开密钥证书可能用于在IE和认证器(在第8.3.1节中描述)之间建立一个安全传输。基于NGN提供商的策略，共享密钥可能用于建立一个安全传输，或用于生成/验证对认证器发出的询问(在第8.3.1节中描述)的应答。

8.3.1 设备、订户和最终用户凭证

在NGN中使用了三种不同类型的凭证：

1) 设备凭证；
2) 订户凭证；和
3) 最终用户凭证。

设备凭证可能由制造商随同设备一起提供，例如，在设备制造期间，设备可能有一个由制造商“烙下”的凭证，该凭证包含如设备序列号或制造商之类的信息。设备凭证标识该设备，NGN提供商可能把设备凭证同一个特定的订户服务联系起来，以便缓解对于订户凭证的需求。在这种情况下，可以根据NGN提供商的策略，将设备发出的请求同一个特定的账户相关联。

订户凭证用于将NGN请求的发起者与一个特定的账户联系起来，将订户凭证输入到(例如通过下载、SIM等)能够接受这种订户凭证的设备，设备中安装的订户凭证将订户与该设备关联起来。设备发出的所有呼叫都将与该设备中安装凭证所属的订户相关联。多组凭证可以安装在一台设备上，在这种情况下，设备提供手段来区分与各个订户相关联的请求。

注 — NGN客户可能有一个或多个与0个或多个设备相关联的NGN订阅，此外，根据NGN提供商的策略，NGN订阅可能与一个或多个可能正在使用不同设备或共用同一个设备的最终用户(即最终用户不一定是订户)相关联。

最终用户凭证用于识别和认证网络的特定最终用户。例如，SIM卡能够识别某一项服务的最终用户；当最终用户将其SIM卡放入电话机时，这部电话机就同该用户联系起来(并且认为该电话的所有的呼叫都来自该用户)。另外一个例子是安全令牌，硬件令牌(一台物理设备)或软件令牌(安装在一台通用设备如个人计算机上的程序)，假设由某一个经过授权的用户来补充认证过程，安全令牌可能存储密码的密钥如数字签名，或生物数据如指纹，由NGN设备发起的请求被当做与安全令牌相关联的最终用户发起的请求，进行识别和认证。在某些情况下(比如上文的SIM卡)，多个最终用户可能使用与单一订户相关联的服务(如订户账户)，由最终用户发起的呼叫都由订户的账户支付。订户和最终用户可以是同一个，或单一订户可能有多个最终用户。为了利用个人服务，最终用户能够通过网络来识别和认证他们自己。可以在TE和NGN网络(认证器)之间使用最终用户凭证建立个人的传输层安全关联。为了计费，NGN提供商将最终用户凭证与某一项特定的订户服务联系起来。

8.3.2 X.509公开密钥证书作为凭证

证书是包含实体标识符、实体属性、属于该实体的公开密钥以及其他认证信息(如关于证书颁发者、证书撤销列表(CRL)、证书有效期开始/结束日期和时间等的信息)的一个数字文件。X.509公开密钥证书某些基本字段和扩展字段的说明如表1所示。X.509公开密钥证书各字段的详细说明见[ITU-T X.509]。公开密钥证书要经过一个可信第三方的数字签名，这个可信第三方通常被称做公开密钥证书的认证机构(CA)。CA计算除了*签名数值字段*以外所有字段的散列值(如使用SHA-1)，用自己的专用密钥对它进行加密，然后把签名和所用的签名算法加到证书中(在*签名数值字段*)。

表1 – X.509公开密钥证书的某些基本字段和扩展字段

字段名称	说明
主体	识别与公开密钥证书关联的实体(证书主体在号码簿中的特异名称)
序列号	证书的唯一标识符
颁发者	识别签发证书的实体(CA在号码簿中的特异名称)
有效期开始时间	证书有效期的开始日期和时间
有效期截止时间	证书有效期的结束日期和时间
公开密钥	证书持有者的公开密钥
版本	X.509公开密钥证书的编码版本
主体备用名	证书持有者的另一个标识符
CRL发布点	RL发布点的名称或哦地址
机构信息访问	用于获取CA信息的名称或地址
增强的密钥应用	证书用途说明(ITU-T | ISO/IEC定义的对象标识符(OID) [ITU-T X.660]
应用策略	能够使用证书的应用和服务(用OID表示)
证书策略	CA用于接收证书请求以及处理、授权、颁发、管理证书的策略和机制
签名算法	CA在签署证书时所用算法和散列函数的算法标识符(例如采用RSA的SHA-1)
签名数值	证书的实际签名

[ITU-T X.509]中的公开密钥证书可能被NGN网元用于建立与其他网元的安全关联，提供相互识别和认证的基础。出于同样的目的，它们也能被用于TE和认证器之间。

对于一个订户或最终用户证书，<订户账户标识符>(见第6.4.2节)，这个读取订户账户信息的标识符被认证器用于从SAA/TAA-FE获得关于凭证的更多信息。对于一个设备证书，设备供货商和设备序列号被认证器用于确定相关的<订户账户标识符>(只有当该设备已经与某一个订户相关联时才有效)，然后像上面一样用<订户账户标识符>通过SAA/TAA-FE获取关于凭证的信息。

最终用户、服务和设备证书可以用于在设备和认证器之间建立TLS连接(第9.1.2节)，或可以用于通过IKE认证建立IPsec连接(第9.2.4.3节)。

8.3.3 共享密钥作为凭证

共享密钥能够用于提高NGN接入的安全性，在这种情况下，将一份共享密钥交给订户或最终用户，一份存储在适当的功能实体如服务用户信息功能实体(SUP-FE)或传输用户信息功能实体(TUP-FE)。要求每份密钥有一个唯一的名称，该名称被认证器用来获取关于凭证的更多信息。

当使用预先共享的密钥时，系统的强度取决于共享秘密的长度，目标是不让共享秘密成为安全链条的薄弱环节，这意味着共享密钥需要含有与使用的密码同样多的熵(随机性)，换句话说，建议共享密钥应至少有128-160比特的熵。

应注意，对称密钥法与第8.3.2节所述的非对称密钥法相比，存在一些差别，并应考虑下述事项：

– 实体需要让每一通信伙伴都有一组单独的对称密钥；

– 密钥应以安全的方式提供、建立和存储；

– 实体必须依靠其伙伴来保持共享密钥的秘密。

8.3.4 SUP/TUP-FE中为各组凭证提供的信息

SUP/TUP-FE是所有设备、订户和最终用户凭证的存储库，这些凭证将用于接入NGN基础设施。为了使认证请求处理最优化，通常将SUP/TUP-FE作为认证器的一个组成部分来实现。然而，为了支持可移动性，认证器可能需要查询一个远程的SAA/TAA-FE服务器以获得关于凭证的信息，订户账户标识符或密钥名称被用于从SAA/TAA-FE提取该信息。

在FE如存储凭证的SUP/TUP-FE中，需要提供下列与各组凭证相联系的安全相关信息：

1) 订户账户标识符或密钥名称；

2) 对于这个订户是否需要最终用户识别和认证；

3) 这些凭证描述的是一个订户还是一个最终用户；以及

4) 请求中“来源”报头的容许值。

以下是凭证存储库如SUP/TUP-FE中所存储信息的一些例子。

对于一个处理号码为212-555-1111-1113和1151四条POTS线路的TE NGN设备证书：

订户账户：	123-456789
“来源”报头：	sip:212-555-111[1-3]@NGN .ngn.com
	| sip:212-555-1151@NGN .ngn.com
身份串：	sip:212-555-1111@NGN .ngn.com
凭证类型：	订户
是否需要最终用户ID：	否

对于一个分配给John Doe家庭的订户证书：

订户账户：	Doe-family
“来源”报头：	sip:*Doe@NGN .ngn.com
身份串：	sip:Doe@NGN .ngn.com
凭证类型：	订户
是否需要最终用户ID：	否

对于一个分配给John Doe家庭的预先共享的密钥：

密钥名称：	JohnDoe
密钥：	dfe56131d1958046689d83306477ecc
“来源”报头：	sip:*Doe@NGN .ngn.com
身份串：	sip: Doe@NGN .ngn.com
凭证类型：	订户
是否需要最终用户ID：	否

对于一个服务于Acme Widget公司的TE-BE：

订户账户：	Acme Widget Company
“来源”报头：	sip:*@acme.com
身份串：	sip:acme.com
凭证类型：	订户
是否需要最终用户ID：	否

对于Acme Widget公司的一个最终用户：

订户账户：	Acme Widget Company
“来源”报头：	sip:bob@acme.com
身份串：	sip:bob@acme.com
凭证类型：	最终用户

8.4 订户的识别和认证

8.4.1 总的策略

SIP中发起者的身份通常包含在“来源”报头中，然而，通过在SIP请求中使用“来源”报头进行订户标识容易遭到欺骗攻击，因此在需要对订户身份进行更高级别确认的情况下不能采用这种方式，取而代之的是将“来源”报头的数值与通过其他方式获得的订户身份进行对比。

为了使得对呼叫建立时延的影响最小，只要有可能，应从网络源地址(IP数据包报头中的源地址)或传输安全关联(发起设备和认证器之间通过如IPsec或TLS建立的关联)获得订户的识别和认证。当这些方法不能产生一个与SIP请求中“来源”报头相一致的标识时，就对该发起者发送一个询问；如果应答包含了正确的凭证则请求继续进行。关于这些程序的更多细节在以下各节中描述。

第8.4.2节中的程序描述了认证器如何根据网络源地址判定下面情况中的一种：

1) 不能通过这种方法确定订户；

2) 确定了订户且订户与请求中“来源”报头匹配；或

3) 确定了订户但订户与请求中“来源”报头不同。

第8.4.3节中的程序描述了认证器如何根据传输安全关联判定下面情况中的一种：

1) 不能通过这种方法确定订户；

2) 确定了订户且订户与请求中“来源”报头匹配；或

3) 确定了订户但订户与请求中“来源”报头不同。

认证器采取的行动见表2。

表2 – 针对各种认证结果认证器的行动

确定订户源地址	确定订户传输安全性	认证器行动
N/A	N/A	使用询问/应答
N/A	匹配	通过
N/A	不同	使用询问/应答
匹配	N/A	通过
匹配	匹配	通过
匹配	不同	使用来自网络源地址的订户身份
不同	N/A	使用询问/应答
不同	匹配	使用来自传输安全关联的订户身份
不同	不同	使用询问/应答
N/A：不适用。		

如果导致的行动是使用询问/应答，则遵循第8.4.4节中的程序。

除了第8.4.2节到第8.4.4节中描述的策略以外，通用引导体系结构(GBA)也能够用于订户的识别和认证，关于它的描述见第8.4.5节。

本建议书中描述的认证策略是典型的例子，各个NGN提供商可以选用这些策略的其中之一(如只使用在下面各节中描述的一个程序)。

8.4.2 通过网络源地址的订户识别

这是订户识别的最简单形式，完全依据IP数据包提供的源地址。认证器查询预先提供的IP地址范围到<订户账户标识符>的映射，如果请求的源地址在其中一个范围之内，认证器就认为请求来自该订户。然后使用<订户账户标识符>从SAA/TAA-FE获得订户凭证，并检验与“来源”报头数值的一致性。

如果“来源”报头的数值与订户一致，则认为“匹配”；如果“来源”报头的数值与订户不一致，则认为“不同”；如果任何预先提供的地址范围都不包含该源IP地址，则认为“不可行”。

这种订户识别方式的强度取决于假设的源地址保证，源地址保证意味着IP地址只能由该地址分配给的合法订户使用，为了实现这一点，以下两个机制对于传输处理或者传输控制FE是必需的，并且必须严格地相互配合：1)严格管理订户和分配给他/她的地址之间的映射，和2)根据该管理信息防止地址欺骗。上述机制及其配合的例子见附录一。

8.4.3 通过TLS/IPsec安全关联的订户识别

如果为发起设备和认证器之间的信令业务建立一个安全TLS传输，且采用X.509 TE-BE证书对该安全传输进行认证(见第8.3.2节)，则认证器要检查“来源”报头与由<订户账户标识符>所确定的订户容许值的一致性。

如果为发起设备和认证器之间的信令业务建立一个安全传输(IPsec或TLS)，并且采用X.509 TE NGN设备证书对该安全传输进行认证(见第8.3.1节和第8.3.2节)，则认证器会利用设备供货商和设备序列号来确定相关的<订户账户标识符>(只有当设备已经与某一个订户关联时才有效)。<订户账户标识符>用于获取订户凭证，然后检验那些凭证与“来源”报头中数值的一致性。

如果为发起设备和认证器之间的信令业务建立一个安全传输(IPsec或TLS)，并且采用X.509 TE NGN订户证书对该安全传输进行认证(见第8.3.1节和第8.3.2节)，则认证器会利用<订户账户标识符>从SAA/TAA-FE获得订户凭证，然后检验订户凭证与“来源”报头中数值的一致性。

如果为发起设备和认证器之间的信令业务建立一个安全传输(IPsec或TLS)，并且采用X.509 TE NGN最终用户证书对该安全传输进行认证(见第8.3.1节和第8.3.2节)，则认证器会利用<订户账户标识符>从SAA/TAA-FE获得订户凭证，然后检验订户凭证与“来源”报头中数值的一致性。

如果为发起设备和认证器之间的信令业务建立一个安全传输(IPsec或TLS)，并且采用预先共享的密钥对该安全传输进行认证(见第9.2.4.3.1节)，则认证器会利用密钥名称从SAA/TAA-FE获得订户凭证，然后检验订户凭证与“来源”报头中数值的一致性。

如果在发起设备和认证器之间不使用安全传输，或者使用“匿名客户端”TLS连接，则这种方法是“N/A”。

8.4.4 通过询问/应答的订户识别

询问/应答是老式用户身份/口令体制(即将用户标识和口令作为服务请求的一部分发送，存在的问题是用户标识和口令容易在后来被重放以获取欺骗性服务)的更安全版本。在询问/应答体制中，服务器发送一个询问到客户端，要求客户端使用共享密钥完成一些加密工作，将计算的结果包含在应答中，然后由服务器对其进行验证。如果交换被其他人拦截，只要服务器不再重复使用旧的询问，应答就不能被重放。

询问-应答方式有一个重要的类型，兼有基于口令认证方式的便利性和基于询问/应答体制方式的安全性。口令认证密钥(PAK)交换协议就属于这一类。PAK协议在通过Diffie-Hellman交换建立对称密钥的过程中确保了双方的相互认证，使用Diffie-Hellman交换确保了完全的前向安全-密钥建立协议的一个特性，确保在一个特定的会话以后会话密钥或者长期专用密钥的泄露不会导致任何更早的会话泄露。另外，PAK认证方式能够保护交换免于遭受中间人攻击，认证依赖预先共享的秘密，对于偷听者而言，该秘密是受到保护的(即保持不被泄露)，从而防止离线字典攻击。因此，该协议能够用于预先密钥以可能存在弱口令为基础的多种应用。PAK协议的说明见[ITU-T X.1035]和[b-TIA 683-D]。

询问/应答涉及认证器和发起端点之间附加的信息交换，计算由发起端点完成，因此可能会对用户感知的时延有影响，NGN安全的目标是只有为了获得必要级别的识别和认证绝对需要时才使用询问/应答。

如果为发起设备和认证器之间的信令业务建立一个安全传输连接(IPsec或TLS)，并且在可配置的一段时期内一个先前的具有相同“来源”报头内容的请求被认证器成功地认证，则认为认证是成功的、请求被接受。在呼叫建立信令的情况下，由于在一个新连接上一般第一个请求是“注册”，因此每次都将进行询问/应答，不会对呼叫建立时延有影响。

由于认证请求的计算强度大，因此认证器限定查询SAA/TAA-FE的频度是很有必要的，无论SAA/TAA-FE是认证器的一个主要部分还是一个独立的元素，都可以遵守本段落中规定的限制。仅仅让认证器接连不断地收到不正确的请求就能实现对一个端点的简单拒绝服务攻击 — 如果每个请求都需要在SAA/TAA-FE中进行密码运算，然后必定会延迟或停止对所有(有效或无效)请求的服务。为了抵御这样的攻击，如果有来自相同端点的待处理的授权请求，认证器可以在本地拒绝该请求。这种方式的稍微复杂一些的变形是如果认证器在过去的YYY秒内已经一共收到了至少XXX条请求，则认证器在本地拒绝该请求(XXX和YYY值在认证器中是可以配置的)。另外，认证器在对失败的授权请求做出响应之前可以故意等待一段可以配置的时间，这样也能防止各种形式的“口令破解”攻击。

8.4.4.1 采用发起设备SIP信令的询问/应答

如果发起设备正在使用SIP信令协议，则[b-IETF RFC 3261]定义的代理认证机制能够可选地用于实现询问/应答，见[b-IETF RFC 3261]的第22.2节、[b-IETF RFC 2617]的第3节和[b-IETF RFC 3310]的第3节。

认证器以407(所需的-代理-认证)回答作为对SIP请求的响应，在这个响应中包含了一个代理-认证报头：“摘要”的认证体制、“NGN.ngn.net”区域，“auth”的qop，16字节密码的当前随机数(采用十六进制)、可选“Opaque”参数的数值和取决于与客户所达成服务协议的“MD5”或“AKAv1-MD5”算法。

407响应中代理-认证报头的例子：

```
Proxy-Authenticate: Digest realm="NGN .ngn.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5
```

发起设备以一个重新产生的包含代理-认证报头的请求作为对407的响应，检验该报头包含以下信息：“摘要”的认证体制，与407响应相同的区域，与407响应相同的随机数，与407响应相同的不透明参数。此外，代理-认证报头包含一个给出密钥名称的“用户名”参数，一个与请求的Request-URI相匹配的“Uri”参数，以及一个为[b-IETF RFC 2617]或[b-IETF RFC 3310]规定散列值的“响应”参数。

在重新发出的请求中代理—认证报头的例子：

```
Proxy-Authorization: Digest username="bob", realm="NGN .ngn.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com",
response="dfe56131d1958046689d83306477ecc"
```

[b-IETF RFC 3261]中定义的“用户对用户的认证”机制也可以用于实现询问/应答，更多细节见[b-IETF RFC 3261]的第22.2节、[b-IETF RFC 2617]的第3节和[b-IETF IETF RFC 3310]的第3节。

如果请求被分流，则多个NGN NE(例如MGC-FE)和/或TE可能希望对发起设备询问。分支NE(例如S-CSC-FE)将这些询问汇集起来，把它们放在由分支NE发送到发起设备的单一响应中。当发起设备收到包含对多个询问的响应时，它会在一个请求中提供多个凭证并提交该请求。

8.4.4.2 采用发起设备非SIP信令的询问/应答

如果期望发起设备使用SIP，但发起设备采用非SIP信令协议发出请求，则认为询问/应答已经失败，该请求被拒绝。

8.4.5 通用引导体系结构(GBA)

通过引导体系结构(GBA)规定了与访问无关的引导程序。它提供最终用户和网络应用功能(NAF)相互认证的一个框架，能够用于识别和认证NGN中的订户。关于GBA的信息参见[b-ETSI TS133 220]。

8.5 最终用户的识别和认证

8.5.1 总的策略

尽管订户识别对于NGN基础设施是绝对需要的，但是最终用户识别是一项可能由订户要求的或服务所需的可选服务。通常这将提供附加的服务，如在需要发出请求的用户的身份才能提供服务的情况下个人的移动性和存在。如果订户需要这种附加级别的识别，则所有相关的端点设备必须要有支持输入附加的最终用户凭证或使用最终用户取代订户证书的能力。

认证器识别和认证最终用户有两种方式，第一种方式是通过信令交换采用的传输层安全关联，如果与一个最终用户证书(或与单一最终用户相关联的预先共享密钥)建立了该安全关联，则最终用户识别是完整的。第二种方式是通过询问/应答，适用于响应中给出的密钥名称与单一最终用户相关联的情况。对这两种方式的更多描述见以下各节。

对于正在使用NGN设备的人而言，高级的NGN设备可能有多个身份如订户证书和一个或多个最终用户证书。这样一台设备将建立到认证器的多个TLS连接，一个证书一个单独的连接，于是设备将根据期望的呼叫身份通过适当的信令连接发送请求到认证器。

让人关注的是单一用户的凭证应在该用户已经“离开”后长时间有效。如果传输安全关联是以最终用户证书为基础，则订户可能需要持续的活跃性以保持认证的有效性。没有这样的活跃性，认证器会结束安全传输连接，要求发起设备采用当前的最终用户证书(如果没有最终用户证书可用的话，可以采用订户证书或设备证书)重新建立安全传输连接。对认证器行为的详细要求见第9.1.2节和第9.2.4.3.1节，该要求以两个定时器为基础：一个定时器限定对于一个安全关联最终用户凭证为有效的绝对时间，第二个定时器限定两个相继请求之间的空闲时间。可以按订户或最终用户规定定时器数值，但是必须受NGN提供商设定的最大数值的限制。

8.5.2 通过TLS/IPsec安全关联的最终用户识别

如果为发起设备和认证器之间的信息业务建立一个安全TLS传输，并且采用X.509 TE-BE证书对该安全传输进行认证(见第8.6节)，则认证器会检验“来源”报头与证书中包含的<订户账户标识符>所确定订户容许值的一致性。

如果为发起设备和认证器之间的信令业务建立一个安全传输(IPsec或TLS)，并且采用X.509 TE NGN最终用户证书对该安全传输进行认证(见第8.6节)，则认证器会利用<订户账户标识符>从SAA/TAA-FE获得订户凭证，然后检验订户凭证和“来源”报头中数值的一致性。如果为发起设备和认证器之间的信令业务建立一个安全IPsec传输(见第8.4.4节)，并且使用预先共享的密钥对该安全传输进行认证(见第9.2.4.3.1节)，则认证器会利用密钥名称从SAA/TAA-FE获得订户凭证，然后检验订户凭证和“来源”报头中数值的一致性。

8.5.3 通过询问/应答的最终用户识别

用于最终用户识别的询问/应答程序与那些用于识别订户的询问/应答程序相同，见第8.4.4节。

唯一的扩充是认证器从SAA/TAA-FE重新获得的信息中，根据密钥名称检查是否有一个该密钥与某一个最终用户相关联的标志，如果有，则最终用户识别成功。

如果认证器已经采用了询问/应答来识别订户，并且在响应中返回的指定密钥没有确定一个最终用户，则最终用户识别失败。如果不需要通过询问/应答来识别订户，则立刻发送一个询问。

8.6 由TE-BE开展的识别和认证

TE-BE执行的识别和认证程序与认证器执行的那些识别和认证程序基本相同，不同处有两点：

1) 由于TE-BE无权使用对认证器可用的分布式SAA/TAA-FE功能，可能要给TE-BE提供识别和认证它服务的订户和最终用户所需要的全部凭证。

2) 含有“代理-授权”报头、在对认证器询问的应答中重新发出的请求，被传递给认证器而不是在TE-BE中进行处理。

8.6.1 X.509证书的使用

每个TE-BE和至少一个NBE之间存在着一个安全关联，该安全关联采用颁发给TE-BE的X.509证书建立。NBE收到的请求遵循第8.4.3节给出的识别和认证程序，该程序最低程度地验证了由TE-BE执行的识别。当需要询问/应答时(例如针对“漫游”用户)，交换将在发起端点和NBE之间，透明地穿过TE-BE。

端点和TE-BE之间的安全传输是可选的，可以预期网络源地址将足以识别大多数的请求。

端点通过TE-BE登录到NBE。

8.7 认证器-SAA/TAA-FE接口

8.7.1 ADIUS的使用及其扩展

SAA/TAA-FE包含判定点，SUP/TUP-FE是NGN基础设施中所有最终用户和设备凭证的存储库。一些SAA/TAA-FE功能如认证器，可能会分布式部署以使得认证请求性能最优化。

两个有竞争力的选择通常被用做认证器和SAA/TAA-FE之间的通信协议：RADIUS [b-IETF RFC 2865](众所周知并且得到很好的支持)和Diameter [b-IETF RFC 3588](为修正RADIUS的一些不足而定义的)。NGN基础设施的最终目标是移植到Diameter；然而要认识到服务器当前运行的通信协议都是基于RADIUS，并且为了满足这种认证功能需求，已经对基本的RADIUS协议进行了多次特别扩展。虽然本建议书的这个版本是以RADIUS和[b-IETF RFC 5090]描述的扩展为基础，本建议书将来的版本将很可能改变这个接口到以Diameter和[b-IETF RFC 4740]描述的扩展为基础。

认证器成为一个RADIUS客户端，而SAA/TAA-FE服务器成为一个RADIUS服务器，见[b-IETF RFC 2865]的定义。两者都可能实现扩展的SIP摘要认证，见[b-IETF RFC 5090]。认证器和SAA/TAA-FE服务器之间的连接可能受到具有相互认证的IPsec的保护。

根据[b-IETF RFC 4590]扩展，认证器用来自代理-认证报头的参数产生一个RADIUS请求；RADIUS服务器计算期望的响应并将它返回到认证器，然后认证器通过比较端点的实际响应和期望的响应来验证该请求。

认证器发送到SAA/TAA-FE服务器的信息的例子是：

```
Code = 1 (Access-Request)
      Identifier = 1
      Length = 164
      Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e
      Attributes:
      NAS-IP-Address = d5 89 45 26 (213.137.69.38)
      NAS-Port-Type = 5 (Virtual)
      User-Name = "bob"
      Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"
      Digest-Attributes (207) = [Realm (1) = "NGN .ngn.com"]
      Digest-Attributes (207) = [Nonce (2) = " ea9c8e88df84f1cec4341ae6cbe5a359
"]
      Digest-Attributes (207) = [Method (3) = "INVITE"]
      Digest-Attributes (207) = [URI (4) = " sip:5551212@ngn.com "]
      Digest-Attributes (207) = [Algorithm (5) = "md5"]
      Digest-Attributes (207) = [User-Name (10) = "bob"]
```

SAA/TAA-FE 服务器发送到认证器的响应例子是：

```
Code = 2 (Access-Accept)
      Identifier = 1
      Length = 20
      Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d
      Attributes:
      Digest-Response (206) = "dfe56131d1958046689d83306477ecc"
```

8.7.2 传输信令安全关联

当在建立传输信令安全关联过程中使用X.509证书时，SUP/TUP-FE存储(根据<订户账户标识符>进行检索)可能在来自该信源的请求中出现的可以接受的“来源”报头集，该报头集将与请求中提供的“来源”报头进行匹配。

如果在建立传输信令安全关联的过程中使用预先共享的密钥，则SUP/TUP-FE存储(通过密钥名称检索)可能在来自该信源的请求中出现的可以接受的“来源”报头集，该报头集将与请求中提供的“来源”报头进行匹配。

8.8 承载业务的识别和认证

有时候出于安全性增强的目的希望识别各个承载的业务流，例如，抵御欺骗攻击如欺骗或RTP介入。在NGN中，能够通过以下五部分来识别承载业务：

- 源IP地址；
- 目的IP地址；
- 源端口；
- 目的端口；及
- 协议号。

本节描述的识别机制采用了用于识别各个数据包的标识符，该机制是以一个共享密钥和使用密码散列函数、带密钥的散列信息认证码(HMAC)为基础，有关信息见[b-NIST FIPS 198-1]。

认证过程中涉及的实体–最终用户功能和接入节点FE — 见[ITU-T Y.2701]的描述，以及以UNI作为例子的图3所示。

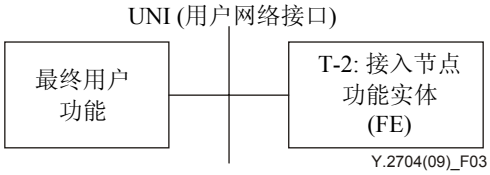


图3－与认证程序有关的NGN实体 — 以UNI为例

该机制的描述使用了以下约定：

- *F*是承载业务的标识符(由五部分组成)。
- *K*是最终用户功能和接入节点FE共同拥有的一个共享密钥。
- *P*是最终用户功能试图发送给接入节点FE的一个数据包。
- *i*由通信双方增加的数据包的序号，是一个64比特的数值。
- *t*是一个时间戳-表示以秒计的时间的64比特的数值。作为选择，它可以表示当前。
- *(P', Q)*是接入节点FE已经接收到的一个数据包。

最终用户功能试图发送一个数据包*P*给接入节点FE时，它首先计算一个量*H(F, t+i, K)*，这是*F*、*t+i*和*K*级联的散列函数，然后把这个量添加到数据包*P*。因此，由最终用户功能发送给接入节点FE的整个数据包是*[P, H(F, t+i, K)]*。当接入节点FE收到数据包*(P', Q)* 时，它会计算*H(F, t+i, K)*。如果使用时间戳，接入节点FE会针对最终用户功能和接入节点FE时间差在约定范围内的所有数值*t*计算散列值(只需要在会话开始时计算一次)。在这种情况下，接入节点FE会在*Q*与任何一个计算得到的散列值之间寻找匹配的数值。如果找到了匹配的数值，则数据包通过认证，相应的t值将会用于数据流中的数据包。

如果使用当前，则接入节点FE只检查计算得到的散列值是否等于*Q*。如果相等，则数据包通过认证。

在可能发生数据包丢失的环境中，数据包到数据包仅仅增加*i*可能是不够的，在这种情况下，接入节点FE可能会从*i*搜索到*i* + *d*(这里d是一个较小的数)以便重新同步*i*。

这种认证机制的使用有助于抵御欺骗性攻击，如欺骗或RTP介入。

这种机制还可在不泄露用户身份的情况下实现用户生成业务的认证。

为了实现这种机制，建议最终用户功能与接入节点FE就以下内容达成一致：标识符*F*的格式、共享秘密*K*、散列函数*H*、距离开始时间戳*t*的准确同步时间、散列值加入到数据包*P*的位置和方式、*d*的值以及什么时候开始重新同步*i*。

这种机制的应用是网络运营商安全策略的一个课题，还有其他的机制能够用于数据流的认证，如IPsec。这种机制与IPsec相比的好处是IPsec需要对整个IP数据包(在隧道模式下)或有效载荷(在传输模式下)进行加密，而这种机制只需要计算散列值*H(F, t+i, K)*，能够更快地完成并且使用更少的计算资源。

9 信令和OAMP的传输安全

传输安全用于在NGN基础设施中提供信令数据和OAMP信息的机密性和完整性保护。本节简要介绍了被NGN基础设施网元作为两种重要安全机制使用的TLS和IPsec，机制列表不是全部，可以依据NGN提供商的策略采取其他实现方式。

在可信区和可信但脆弱的区内，需要VPN隧道(例如IPsec或TLS)保护OAMP信息。第9.1节给出了TLS应用案例的简介，第9.2节给出了相应的IPsec应用案例的简介。在TE-BE和OAMP-NBE之间(即在不可信区和可信但脆弱的区之间)，IPsec用于建立一个VPN隧道。第9.3节给出了IPsec的适当简介。

虽然在NGN基础设施内不要求媒体安全，但一些边界元素实现了对特定端点服务的媒体安全，对于这些元素，第10节包含了媒体安全协议的简介。

9.1 TLS

在NGN基础设施中，TLS通常用来保护可信区内网元之间各种类型的信令业务(例如SIP、COPS、TRIP、HTTP)，在可能收到客户端点的加密信令的边界元素中也支持TLS，加密信令经过TE-BE传递给NBE，[ITU-T Y.2701]给出了对各种网元的具体要求。

TLS协议的定义见[b-IETF RFC 5246]，它提供了在一个可靠传输层协议如TCP或SCTP上的私密性和数据完整性。

本节中除非另有说明，最好是需要TLS的NGN基础设施网元都符合[b-IETF RFC 5246]TLS规范和[b-IETF RFC 3261]中明确的与TLS在SIP中的应用有关的所有要求。虽然TLS支持压缩方式的协商和使用，但由于性能下降，可能不会在NGN基础设施中使用压缩。

9.1.1 密码组件

密码组件包括在TLS握手中使用的、经过认证的密钥协商方法，以及用于保护记录层的加密和认证密码。TLS客户在客户呼叫信息中提出所支持的系列密码组件，服务器以服务器呼叫信息中选定的密码组件作为响应，从而协商得到密码组件。

影响加密算法选择的因素有很多，下面是一些影响加密算法的常见因素的例子：

1) 必需的安全
   - 数据的价值(对于组织和/或其他实体而言 — 数据价值越高，需要的加密越强)。
   - 数据的时间价值(如果数据有价值但只是在一个较短的时期 [例如相对于年的天]内有价值，则可以使用较弱的加密算法)。
   - 对数据的威胁(威胁级别越高，需要的加密越强)。
   - 适当的其他保护措施，可能会减少对高强度加密的需求 — 例如，采用通信保护手段，如相对于公共互联网的专用电路。
2) 必需的性能(较高的性能要求可能需要获取额外的系统资源，如硬件加密加速器或可能被迫采用较弱的加密)。

3) 系统资源(较少的资源(例如进程、存储器)可能迫使采用较弱的加密)。

4) 输入、输出或使用限制。

5) 网元支持的加密体制。

6) 用户设备支持的加密体制。

表3所示的是适用于NGN的候选密码组件列表，但是本表不是全部。

表3 – 用于NGN的候选密码组件

密码组件名称	出处	密钥交换	密码	散列
TLS_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	RSA	采用CBC模式的AES-128	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	采用RSA签名的Diffie-Hellman Ephemeral 模式	采用CBC模式的AES-128	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 2246]	RSA	采用CBC模式的3DES	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 5246]	采用RSA签名的Diffie-Hellman Ephemeral 模式	采用CBC模式的3DES	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132]	RSA	采用CBC模式的Camellia-128	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	采用RSA签名的Diffie-Hellman Ephemeral 模式	采用CBC模式的Camellia-128	SHA-1

来自[b-IETF RFC 5246]、[b-IETF RFC 4132]和[b-IETF RFC 4492]，在表4中描述的密码组件也能够可选地被任何NE使用。

表4 – 用于NGN的候选密码序列(可选的)

密码组件名称	出处	密钥交换	密码	散列
TLS_DH_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	采用DSS签名的Diffie-Hellman	采用CBC模式的AES-128	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	采用RSA签名的Diffie-Hellman	采用CBC模式的AES-128	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	采用DSS 签名的Diffie-Hellman Ephemeral 模式	采用CBC模式的AES-128	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 5246]	采用RSA 签名的Diffie-Hellman Ephemeral模式	采用CBC模式的AES-128	SHA-1

表4 – 用于NGN的候选密码序列(可选的)

密码组件名称	出处	密钥交换	密码	散列
TLS_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	RSA	采用CBC模式的AES-256	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	采用DSS签名的Diffie-Hellman	采用CBC模式的AES-256	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	采用RSA 签名的Diffie-Hellman	采用CBC模式的AES-256	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	[b-IETF RFC 5246]	采用DSS 签名的Diffie-Hellman Ephemeral模式	采用CBC模式的AES-256	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4132]	采用RSA 签名的Diffie-Hellman Ephemeral模式	采用CBC模式的AES-256	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	采用DSS 签名的Diffie-Hellman	采用CBC模式的Camellia-128	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	采用RSA 签名的Diffie-Hellman	采用CBC模式的Camellia-128	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	[b-IETF RFC 4132]	采用DSS 签名的Diffie-Hellman Ephemeral模式	采用CBC模式的Camellia-128	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	RSA	采用CBC模式的Camellia-256	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	采用DSS 签名的Diffie-Hellman	采用CBC模式的Camellia-256	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	采用RSA 签名的Diffie-Hellman	采用CBC模式的Camellia-256	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	采用DSS 签名的Diffie-Hellman Ephemeral 模式	采用CBC模式的Camellia-256	SHA-1

表4 – 用于NGN的候选密码序列(可选的)

密码组件名称	出处	密钥交换	密码	散列
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	[b-IETF RFC 4132]	采用RSA 签名的 Diffie-Hellman Ephemeral 模式	采用CBC 模式的 Camellia-256	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman	采用CBC 模式的 3DES	SHA-1
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman	采用CBC 模式的 AES-128	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman	采用CBC 模式的 AES-256	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman Ephemeral模式	采用CBC 模式的 3DES	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman Ephemeral 模式	采用CBC 模式的 AES-128	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	采用ECDSA签名的EC-Diffie-Hellman Ephemeral模式	采用CBC 模式的 AES-256	SHA-1
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的 EC-Diffie-Hellman	采用CBC 模式的 3DES	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的 EC-Diffie-Hellman	采用CBC 模式的 AES-128	SHA-1
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的 EC-Diffie-Hellman	采用CBC 模式的 AES-256	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的 EC-Diffie-Hellman Ephemeral 模式	采用CBC 模式的 3DES	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的 EC-Diffie-Hellman Ephemeral模式	采用CBC 模式的 AES-128	SHA-1

表4 – 用于NGN的候选密码序列(可选的)

密码组件名称	出处	密钥交换	密码	散列
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	[b-IETF RFC 4492]	采用RSA签名的EC-Diffie-Hellman Ephemeral模式	采用CBC模式的AES-256	SHA-1

注1 — RC-4是一个流行的并被普遍使用的密码。然而，它没有被包含在上面的列表中，原因是它不是一个开放的标准。

注2 — 椭圆曲线密码(ECC)是一个公开密钥密码系统，可能能够满足NGN中某些应用的需要。特别地，由于ECC在效率上的优势，ECC对于某些应用是有吸引力的。与其他流行的密码系统如RSA相比，ECC能够以短得多的密钥长度提供相当的安全性。此外，ECC在实现相同级别的保护时具有优于其他公开密钥技术的计算效率和优势。

9.1.2 TLS使用证书

TLS是一个基于客户机-服务器的协议，具有可选的客户认证。然而，在NGN基础设施的可信区内，在可信区和可信但脆弱的区之间，可以使用TLS实现相互认证。在这种情况下，TLS服务器会发送一个证书请求给客户端，如果可信区或可信但脆弱的区内的客户不能提供一个客户证书，则连接请求可能会被服务器拒绝。TLS客户证书和服务器证书都应该符合在第8.3节给出的NGN基础设施证书规范，都可以按第8.3节的规定对证书进行验证。在继续一个TLS连接之前，TLS服务器或客户端可以验证远程系统是否与它的证书匹配。

在可信但脆弱的区和不可信区之间，TLS服务器可能发送一个证书请求到客户端，如果客户端没有证书，它会以一个空白的客户端证书信息作为响应，以一个匿名客户端继续进行会话。

当NBE根据NGN最终用户证书接受与一个端点的经过认证的连接时(见第8.5.2节)，则NBE可能在连接上实现两个定时器。第一个定时器T1在连接建立时开始计时，第二个计时器T2在连接建立时开始计时，每当NBE通过该连接收到一个请求时复位到零。只要定时器到达它的极限值(这个数值可能取决于证书中包含的数值)，该连接就会被NBE复位，将由端点重新建立连接以便更新NGN最终用户证书。

9.1.3 会话密钥管理

NGN基础设施网元之间的TLS会话应该长时间保持，因此，周期性地更换会话密钥十分重要，可以在可配置的一段时间后更换TLS会话的会话密钥。

9.2 可信区和可信但脆弱的区内的IPsec

在NGN的基础设施中，IPsec可以用于保护可信区内网元之间各种类型的业务(例如SNMP、RADIUS)，[ITU-T Y.2701]给出了对各种网元的具体要求。

按[b-IETF RFC 4301]的一般描述，IPsec由多个不同的部分组成。这些部分能够用于提供机密性、完整性和重放保护。这些部分中有一些能够手工进行配置，但是通常会采用密钥管理部件。另外，使用IPsec的决定一般受策略数据库的控制。本节描述了IPsec部件的强制执行子集。

在使用IPsec的网元中，建议要确保受TLS保护的连接不是运行IPsec之上。

注 — 使用IPsec的网元应确保采用SRTP或RC-4保护的媒体流不是运行在IPsec之上，这是为了确保不进行双重加密，双重加密将会浪费NGN资源。还应注意到可能出现来自最终用户的加密隧道。

9.2.1 AH和ESP

[IETF RFC 4302]和[b-IETF RFC 4835]中描述的认证报头(AH)和[IETF RFC 4303]中描述的封装安全协议(ESP)是经过线路安全协议的两种选择。两者都可选地提供重放保护。ESP一般用于提供业务的机密性、完整性和认证，ESP也能提供在没有机密性情况下的完整性和认证。ESP还能用于只提供机密性。AH保护以前的IP报头部分，包括源地址和目的地址，AH还能保护那些需要让中间路由器看到、但是发送到接收系统时要求完整可信的IP部分，尽管这些IP部分极少使用。

NGN基础设施网元可能支持封装安全协议(ESP)，见[IETF RFC 4303]的定义。加密分组链接模式可能支持ESP_DES(40比特和56比特)、ESP_3DES、ESP_AES[b-IETF RFC 3602]和ESP_CAMELLIA[b-IETF RFC 4312]。支持ESP_NULL的网元在与其他NGN基础设施网元进行通信时，可能不使用ESP_NULL。在ESP中使用的实际加密算法是在密钥管理期间通过协商得到的。

[b-IETF RFC 4301]要求完全地实现ESP以便支持安全关联(SA)的概念，并且[b-IETF RFC 4301]提供了一个处理与SA有关的IP业务的通用模式。尽管特殊的IPsec实现不必遵循这种通用模式的细节，但任何IPsec实现的外部特性可能与通用模式的外部特性相匹配，这确保了各部件不会接受来自未知地址的业务，也不会发送或接受没有安全性的业务(当要求安全性时)。实现IPsec的NGN基础设施网元可能提供与[b-IETF RFC 4301]描述的通用模式相匹配的特性。

9.2.2 传输模式和隧道模式

AH和ESP都可以用于传输模式或隧道模式。在隧道模式下，IPsec报头后面会跟着一个内部IP报头，这是虚拟专用网络(VPN)的通常用法，当IPsec保护路径的任何一个端点不是最终目的地如在防火墙或路由器中实现IPsec时，这通常是必需的。传输模式更适用于点对点通信。

NGN基础设施网元可能支持传输模式的IPsec。

9.2.3 重放保护

NGN基础设施网元可能使用IPsec可选的重放保护服务(抗重放服务)。在NGN基础设施网元内，IPsec抗重放服务可以一直开启，在当前抗重放窗口之外的IPsec序列号被标记为重放，该数据包被拒绝。当抗重放服务开启时，IPsec序列号不能溢出，不能回转到0。在这种情况下发生之前，应该按[IETF RFC 4303]的说明建立一个新的安全关联。

9.2.4 密钥管理

所有的密码系统都需要密钥管理，虽然IPsec提供了手工和自动密钥管理体制，但是手工体制所占的比例不如自动体制，也不提供重放保护。所有密钥管理体制都提供认证。NGN基础设施网元应实现本节中描述的一种自动密钥管理体制。

当IKE不被用于密钥管理时，为了创建/更新/删除Ipsec安全关联，备选的密钥管理协议需要一个与IPsec层的接口。可以根据需要自动创建或重新建立IPsec安全关联，这意味着当需要建立一个新的安全关联时(例如，旧的SA将要到期，或在一个特定接口上没有SA)，IPsec层也需要一种方法告知密钥管理应用。另外，可能要求某些边界元素运行多种密钥管理协议(例如，IKE用于OAMP的安全连接，PKINIT用于安全连接)。在这些情况下，建议使用PF_KEY[b-IETF RFC 2367]接口。

9.2.4.1 变换标识符

IPsec变换标识符被密钥管理程序用于协商一个被IPsec中ESP使用的加密算法。变换标识符还被IKE用于保护其第1阶段和第2阶段的信息。[b-IETF RFC 5282]给出了可用的IPsec变换标识符列表。在NGN基础设施中，可能支持变换ID ESP_3DES(数值为0x03，密钥长度为192比特，CBC模式)和ESP_CAMELLIA(数值为0x16，密钥长度为128比特，CBC模式)[b-IETF RFC 4312]，建议支持变换ID ESP_AES(数值为0x0C，密钥长度为128比特，CBC模式)。IKE允许对密钥长度进行协商，这样如果将来需要为上述的某一种算法增加密钥长度时，IKE将使用这种固有的功能。

对于所有这些变换，CBC初始向量(IV)能在各个ESP数据包有效载荷[b-IETF RFC 2451]内顺畅地传送。[b-NIST FIPS 197]和[b-IETF RFC 3602]定义的AES-128可以采取CBC模式，分组大小为128比特，使用随机生成的初始向量。AES-128要求进行10轮加密运算[b-IETF RFC 3602]。[b-IETF RFC 3713]和[b-IETF RFC 4312]定义的Camellia-128可以采取CBC模式，分组大小为128比特，使用随机生成的初始向量，它要求进行18轮加密运算[b-IETF RFC 3713]。

9.2.4.2 认证算法

IPsec认证算法被密钥管理程序用于协商一个要使用的数据包认证算法。[b-IETF RFC 5282]给出了可用的IPsec认证算法列表。在NGN基础设施内，可能支持认证算法HMAC-MD5-96(数值为0x01，密钥长度为128比特，在[b-IETF RFC 2403]中定义)和HMAC-SHA-1-96(数值为0x02，密钥长度为160比特，在[b-IETF RFC 4835]中定义)。

9.2.4.3 互联网密钥交换(IKE)

[b-IETF RFC 2409]描述了一种自动密钥交换机制，被称做IKE。IKE密钥管理与数据信息完全异步，在通信建立期间不会带来任何时延，唯一的例外将是出现一些没有预料到的错误，其中一个端点意外地失去了安全关联的情况。

IKE是一个对等的密钥管理协议，它包括两个阶段。在第一个阶段，通过Diffie-Hellman密钥交换协商出一个共享秘密，然后该秘密被用于认证第二个IKE阶段，第二个阶段协商出另一个秘密，用于导出IPsec ESP协议的密钥。

9.2.4.3.1 第一个IKE阶段

在第一个IKE阶段定义了三种不同的认证模式。采用公开密钥加密的IKE认证不会在NGN基础设施中使用，因为它需要发起者事先知道响应者的公开密钥，NGN基础设施可能会支持采用签名的IKE认证和采用预先共享密钥的IKE认证。

IKE定义了可以用于第一个阶段IKE交换的特定Diffie-Hellman参数集(即素数和发生器)。NGN基础设施网元可能支持第一组参数，建议也支持剩余的参数组。

如果使用具有签名的IKE认证，则客户端和服务器都可以交换X.509证书(见第8.3.2节)。可以按第8.3节的说明验证证书。

当网络边界元素根据NGN最终用户证书接受一个与端点的经过认证的连接时，NBE可能在该连接上实现两个定时器。第一个定时器T1当连接建立时开始计时，第二个定时器T2当连接建立时开始计时，每当NBE通过该连接收到一个请求时复位到0。只要定时器到达它的极限值(这个数值可能取决于证书中包含的数值)，该连接就会被NBE复位，将由端点重新建立连接以便更新NGN最终用户证书。

如果使用采用共享密钥的认证，则来源于某些带外(如手工)机制的密钥会被用于认证交换。实现方案可能允许拥有长度至少为128字节的预先共享密钥，在网元中，对预先共享密钥的要求进行验证不是必需的。实现方案可能支持[b-IETF RFC 2409]第5.4节中定义的主动模式，使用密钥名称做为发起者/响应者的身份。已知与预共享密钥结合使用的IKE v1主动模式[b-IETF RFC 2409]是不安全的。采用这种模式，秘密的一个散列值通过网络用明文发送；如果IP业务遭到攻击者的截击，则可以通过离线的强力计算来检索密钥。建议采用长度至少为128比特的PSK，以防根据其散列值对PSK进行强力计算。

当使用预先共享的密钥时，系统的强度取决于共享秘密的长度，目标是不让共享秘密成为安全链条的薄弱环节。这意味着共享秘密需要含有与使用的密码同样多的熵(随机性)。换句话说，建议共享秘密至少要有128-160比特的熵。

9.2.4.3.2 第二个IKE阶段

在第二个IKE阶段，建立一个IPsec ESP安全关联，包括ESP密钥和密码组件。首先，建立一个共享的第二阶段秘密，然后采用[b-IETF RFC 2409]中规定的单向函数由该秘密导出全部的IPsec密钥体。第二个阶段秘密来自双方交换的、加密过的随机数。除了加密过的随机数以外，[b-IETF RFC 2409]提供了另外一种Diffie-Hellman交换，但是可能不会在NGN基础设施网元中使用，这是为了避免相关的性能损失。

9.3 不可信区和可信但脆弱的区之间的密钥管理协议

为IMS网络规定的认证和密钥协商(AKA)协议也可能是适用的。通用移动通信系统(UMTS)认证和密钥协商(AKA)协议支持移动台(MS)与网络之间的相互认证。UMTS AKA是一种询问-应答协议，它使用在通用订户身份模块(USIM)与认证中心(AuC)之间共享的一个长期密钥*K*。这些实体分别位于移动台的通用集成电路卡(UICC)中和移动台的归属网中。AKA协议在题为“安全体制结构”的[b-3GPP TS 33.102]中规定。

虽然AKA机制一般用于装备了智能卡(例如UICC)的无线设备的认证，然而AKA规范中没有任何内容妨碍将这种机制用于能够运行USIM应用的固定设备的认证。

9.4 不可信区和可信但脆弱的区之间的IPsec

TE-BE是位于不可信区内的NGN网元，然而，它仍然由NGN运营商管理，并且需要接入位于可信区内的OAMP系统，因此，存在着一个位于可信但脆弱的区内但作为OAMP信息中继点的OAMP-SE。

TE-BE可以确保受TLS保护的连接不会运行在IPsec VPN隧道上，TE-BE可以确保受SRTP媒体保护的媒体流不会运行在IPsec VPN隧道上。

IPsec VPN隧道可以使用隧道模式[b-IETF RFC 4301]下的IPsec ESP [IETF RFC 4303]。

IPsec的抗重放服务可以一直开启。

IPsec VPN隧道可能支持变换标识符ESP_3DES(密钥长度为192比特，采用CBC模式)和ESP_CAMELLIA(密钥长度为128比特，采用CBC模式)[b-IETF RFC 4312]。建议IPsec VPN隧道支持变换标识符ESP_AES(密钥长度为128比特，采用CBC模式)。

IPsec VPN隧道可能支持认证算法HMAC-MD5-96(密钥长度为128比特)和HMAC-SHA-1-96(密钥长度为160比特)。

通过IKE[b-IETF RFC 2409]、使用具有数字签名的IKE认证或具有预先共享密钥的IKE认证，可以实现适用于IPsec VPN隧道的密钥生成和管理。如果使用具有数字签名的IKE认证，客户端和服务器都可以交换X.509证书，也可以验证证书。

10 媒体安全

在NGN基础设施内，媒体安全不是必需的，但是为了支持希望利用媒体安全的客户，可能会要求媒体安全。这种支持可能包括支持媒体加密协议SRTP [b-IETF RFC 3711]。在本节其余部分中，假设由网络边界元素(即网络供货商领域的边界)完成加密/解密，尽管NBE之间共用的独立平台也可能完成同样的功能。在两种情况下，都要求加密和解密与其他媒体处理能力如双音多频(DTMF)检测和转换一同配置。

由于需要连接要求其接入链路实施媒体加密的订户或那些要求其接入链路不实施媒体加密(或不支持媒体加密)的订户，有五种独立的情况需要考虑，如图4所示。

第一种并且是最简单的情况是两个端点都不要求加密。媒体将从源头流向目的地，经过边界元素，所有链路都不加密。网络边界元素(NBE)#1(作为发起者)和网络边界元素(NBE)#2(作为目的地)两者都不进行加密或解密。

出现第二种情况是指，如果发起者要求一个加密的媒体流，但是目的地要求不加密，NBE #1作为加密/解密中继点。NBE #1收到来自发起者经过加密的数据流，未加密并且通过NGN基础设施把它传送给NBE#2，NBE#2把它(仍然是未加密的)传送到目的地。在相反方向，NBE#1通过NGN基础设施收到未加密的媒体流，在把它发送给发起者对它进行加密。因此，流经路径#1(从发起者到NBE#1)的媒体是加密过的，流经路径#2(NBE#1和NBE#2之间)的媒体则没有加密，流经路径#3(NBE#2和目的地之间)的媒体也没有加密。

出现第三种情况是指，如果目的地要求一个加密的媒体流，但发起者要求不加密，NBE#2作为加密/解密中继点。NBE#1收到来自发起者未经加密过的媒体流，通过NGN基础设施把它传送给NBE#2，NBE#2加密并把它传送到目的地。在相反方向，NBE#2收到来自目的地端点的经过加密的媒体流，在通过NGN基础设施转发之前解密。NBE#1将未加密的媒体流传送给发起者。因此，流经路径#1和#2的媒体是未加密的，而流经路径#3的媒体是加过密的。

出现第四种情况是指，如果发起者和目的地两者都要求加密的媒体流，但是他们不支持相互兼容的加密体制，或NGN基础设施提供了一些增强型服务(如用于电话卡应用的双音多频(DTMF)检测)。NBE#1和NBE#2都作为加密/解密中继点。NBE#1收到来自发起者的经过加密的媒体流，解密并且通过NGN基础设施把它传送给NBE#2，NBE#2加密并把它传送到目的地。在相反方向，NBE#2收到来自目的地端点的经过加密的媒体流，在通过NGN基础设施转发前解密，NBE#1收到未加密的媒体流，在将它发送到发起者之前加密。因此，流经路径#1和#3的媒体流是加密的，流经NGN基础设施(路径#2)的媒体是未加密的。

出现第五种情况是指，如果发起者和目的地两者都要求加密的媒体流，支持相互兼容的加密体制，并且NGN基础设施没有提供增强型服务。NBE#1收到来自发起者的加密媒体流，不做改变通过NGN基础设施发送给NBE#2，NBE#2不做改变将其发送到目的地。在相反方向，NBE#2收到来自目的地的加密媒体流，不做改变通过NGN基础设施发送给NBE#1，NBE#1不做改变将其发送给发起者。因此，流经所有三条路径的媒体都是加密的，实现这种情况所需要的信令超出了本建议书的范畴。

本节描述的媒体加密提供了认证、机密性和信息完整性。

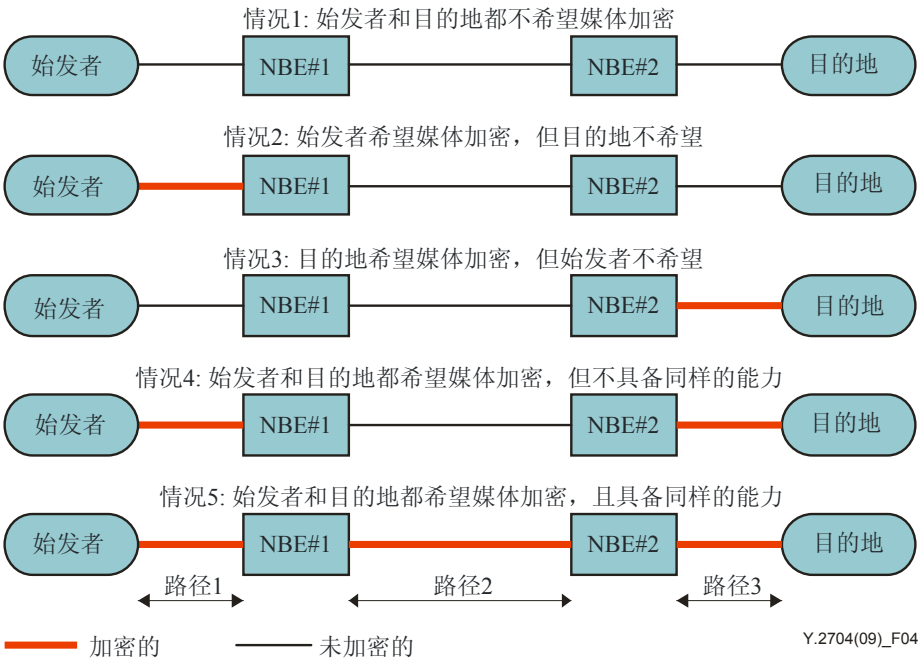


图4－媒体加密、BE的能力和发起者/目的地的需求之间的关系

10.1 SRTP

安全RTP的描述见[b-IETF RFC 3711]，它被定义成一个简化的RTP[b-IETF RFC 3550]，拟在RTP应用和协议栈的传输层之间实现–发送端拦截一个RTP数据包，转发一个等效的SRTP数据包，接收端拦截SRTP数据包，传送一个在堆栈上方的等效的RTP数据包，基本上是在发送端对RTP数据包的有效载荷进行加密，并在数据包的结尾添加一个认证标签，接收端验证认证标签并解密有效载荷。

10.1.1 加密和认证算法

支持SRTP的NBE可能支持计数器模式[b-IETF RFC 3711]的AES，更多信息也可参见[b-NIST FIPS SP 800-38a]，NBE可能支持用于信息完整性检验生成、标签长度为80比特的HMAC-SHA1。

10.1.2 密码组件协商和密钥生成

SRTP密钥生成有几种方式：

1) 预先提供(通过TE提供元素)；

2) 采用由端点设备生成的且包含在INVITE(邀请)请求的会话描述协议(SDP)[b-IETF RFC 4566]中的密钥体；

3) 利用独立的密钥管理协议交换并且采用SDP附带运输的密钥体。

对于每一个订户，NBE可以从SAA/TAA-FE获得SRTP主密钥，并从这个主密钥中导出预备的加密和认证会话密钥。NBE可能支持长度为128比特的SRTP主密钥，可能支持[b-IETF RFC 3711]中描述的密钥导出算法，预备加密密钥长度可能为128比特，预备会话salt密钥长度可能为112比特，而预备加密密钥长度可能为160比特。当给订户分发一个新的SRTP主密钥时，NBE可以立即使用该主密钥。

如果邀请请求中包含的SDP以“RTP/SAVP”作为“m=”行中媒体协议数值、“k=”行中无密钥数据、无“a=crypto”属性，则NBE可以使用由提供系统生成的预备密钥作为实际的会话密钥。在这种情况下，密码组件不是通过协商得到的。

如果邀请请求中包含的SDP以“RTP/SAVP”作为“m=”行中媒体协议数值、无“a=crypto”属性、“k=”行中有一个密钥数据，则NBE可以使用包含在“k=”行中的密钥作为SRTP主密钥，并从该密钥中产生会话密钥和认证密钥。在这种情况下，密码组件不是通过协商得到的。

如果邀请请求中包含的SDP以“RTP/SAVP”作为“m=”行中媒体协议数值、有“a=crypto”属性，则NBE可以按照[b-IETF RFC 4568]的要求产生会话密钥和认证密钥。例如，SDP条目“a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline: PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4”表示密码组件是AES_CM_128_HMAC_SHA1_80，key_param由以“inline:”开始的文本定义。在key_param内，第一个字段是串接的主密钥附加主要的随机字节，然后是base64编码。[b-IETF RFC 4568]第5.2节给出了有效的密码组件列表，可以从中选择一个作为SDP提供/响应交换的一部分。

如果邀请请求中包含的SDP以“RTP/SAVP”作为“m=”行中媒体协议数值、有“a= key-mgmt”属性，则NBE可以按照[b-IETF RFC 4567]的要求产生密钥和安全参数。例如，“a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAAA...”表示密钥管理协议是mikey [b-IETF RFC 3830]，其余文本是采用base64 [b-IETF RFC 4648]编码的密钥管理数据。

10.1.3 NGN网元和安全令牌服务器之间的认证接口

NGN网元可能实现SASL[b-RFC4422]保护其OAMP功能。SASL层可能包含基于安全令牌的认证检验，安全令牌的定义见[b-IETF RFC 2808]，被标识为SASL密钥“安全令牌”。需要OAMP访问的用户提供：

1) 一个授权身份(允许系统管理员以不同的用户身份登录；如果为空，则缺省地为认证身份)；
2) 一个认证身份(其口令将被使用的一个身份)；
3) 安全令牌中用户的个人身份号码数值和6位数字口令。

NGN网元可能实现一个SAA/TAA-FE兼容客户端，作为安全令牌的SASL处理的一部分，NGN网元收集已存在的用户凭证，然后将其发送到安全令牌服务器。收集的字段包括用户名、PIN码和当前显示的安全令牌数值。网元接收返回一个接受/拒绝/重试状态信息。如果成功，则SASL根据与该用户名相关的访问级别，允许用户访问OAMP功能。

11 OAMP

应该对所有的OAMP访问尝试(无论成功还是失败)、所有的OAMP变更和所有的OAMP中止都进行审计跟踪。另外，要记录NGN供货商策略着重考虑的事件。

本节中描述了一些关于重要特性的机制。这些机制并非详尽，可能依据NGN供货商的策略采取其他的实现方案。

注 — 事件日志安全是必需的，更多信息见 [ITU-T Y.2701]和[b-ITU-T M.3016.0]。

11.1 网元与登录系统的接口

建议网元将他们的登录信息发送到一个远端的日志主机。利用系统日志协议[b-IETF RFC 5424]获得该功能的这些元素可以遵循本节的要求。

利用系统日志协议的网元可能包括一个以通过SNTP/NTP从可信时间源收到的时间为基础的时间戳，并且可能在UTC中提供该时间戳，元素可能包含他们的主机名(如果已经提供了)或在系统日志信息报头中他们的IP地址。

11.2 网元使用SNMP

NGN网元能接受一个远端平台的管理是有必要的，SNMP是实现这一功能的工业标准。随着SNMPv3[b-IETF RFC 3413]、[b-IETF RFC 3414]和[b-IETF RFC 3415]解决了SNMPv2中存在的一些安全缺陷，它正日益得到广泛地应用。

建议网元将其登录信息发送到一个远端日志主机，这些网元可以利用SNMP协议实现这种功能，同时顾及本建议书中关于SNMPv3的其他注意事项。

SNMP是按照总体体系结构[b-IETF RFC 3411]，主体和事件的命名机制(MIB[b-IETF RFC 1155]、[b-IETF RFC 1212]、[b-IETF RFC 1215]、[b-IETF RFC 2578]、[b-IETF RFC 2579]和[b-IETF RFC 2580]，以及协议运行[b-IETF RFC 3416]和[b-IETF RFC 3417]来规定的。关于描述目前互联网标准管理框架的文档，[b-IETF RFC 3410]的第7节中有更为详细的综述。

每一个NGN网元都可能实现一个SNMP客户端。如果使用SNMP v1或v2，并且如果NGN供货商的安全策略需要SNMPv1或v2，则要求他们使用IPSec上的UDP作为传输协议。可以采用ASN.1[b-ITU-T X.690]基本编码规则将各个消息实例编码成一个UDP数据报。客户可以在端口161上监听命令响应者应用，也可以在端口162上监听通知接收者应用。

要求NGN网元实现所有必要的、用于报告安全事件和审计跟踪的MIB。

11.3 安全补丁管理

在NGN网元和服务器上定期地安装维护和安全补丁，会使他们针对攻击和无意故障的脆弱性最小。需要配置一个全面的补丁管理策略，包括安装、验证过程和平台。

11.4 版本管理

网元的配置和变更必须进行备份，系统备份的主要目的是在硬件或软件发生故障导致软件加载和/或相关系统数据损坏的情况下，实现系统恢复。下列类型的信息可能包含在一个系统备份加载中：

- 客户数据和逻辑。
- 网络业务连接性，例如设施和中继线。
- NGN运营商和供货商提供的应用软件。
- 操作系统。
- 硬件配置。

需要保留一个不断更新的设备配置工作记录，以便获得备份映像之后发生的设备配置行动能对网元(NE)进行更新。

提供平台可能提供以下性能：

- 各个直接供给网元的提供活动的日志。
- 对各个NE相当于至少一个星期的提供活动。

提供平台可以允许用户手工地回顾所存储的对各个NE的提供行为。提供给用户的活动描述必须在一个给定的时间间隔内总结事务的规模、数量和类型。

提供平台可以提供一个实用程序，允许通过把数据重新输入到一个特定的NE再次提供一个指定的NE。该实用程序应允许为将要被再次提供的数据选择开始和结束日期/时间。根据特定的开始和结束日期/时间，提供平台应能自动地把全部中间数据重新输入到特定的NE中。

11.5 TE-BE的审计跟踪、捕获和记录

关于NGN网元的所有审计跟踪、捕获和记录要求均适用于TE-BE。

TE-BE通过一个VPN隧道连接到OAMP系统，因此它通过这个VPN发送它的登录信息，接收SNMP请求并发送SNMP响应。建议TE-BE不要接受任何其他接口上的任何OAMP请求。

第9.4节中给出了对VPN隧道的要求。

12 不可信区内设备供应

由TE提供元素配置所有的客户驻地设备，TE提供元素位于可信区内，可能通过网络边界元素(NBE)只与TE进行通信，如图2所示。TE或TE-BE可能在它能够从TE设置元素获得配置文件之前，认证和建立一个与NNBE的安全关联。NNBE可能支持用TLS和IPsec建立与TE(包括TE-BE)的SA。更多细节参见第9.1节和第9.2节。

在本上下文中，由提供商控制的设备能被当做NBE的一部分来对待。

TE提供元素在下载到已认证设备的配置数据中包含了NBE的地址，TE提供元素还可能包含一个证书，该证书用于与NNBE一起认证订户，见第8.4节的描述。

TE设备将从NGN设备提供商请求提供，NBE将收到该请求，与SAA/TAA-FE一起认证TE。当设备通过认证时，边界元素将转发提供请求到TE提供元素，然后TE提供元素下载配置和/或固件到TE。如果TE不能通过认证，则记录失败。

附录一

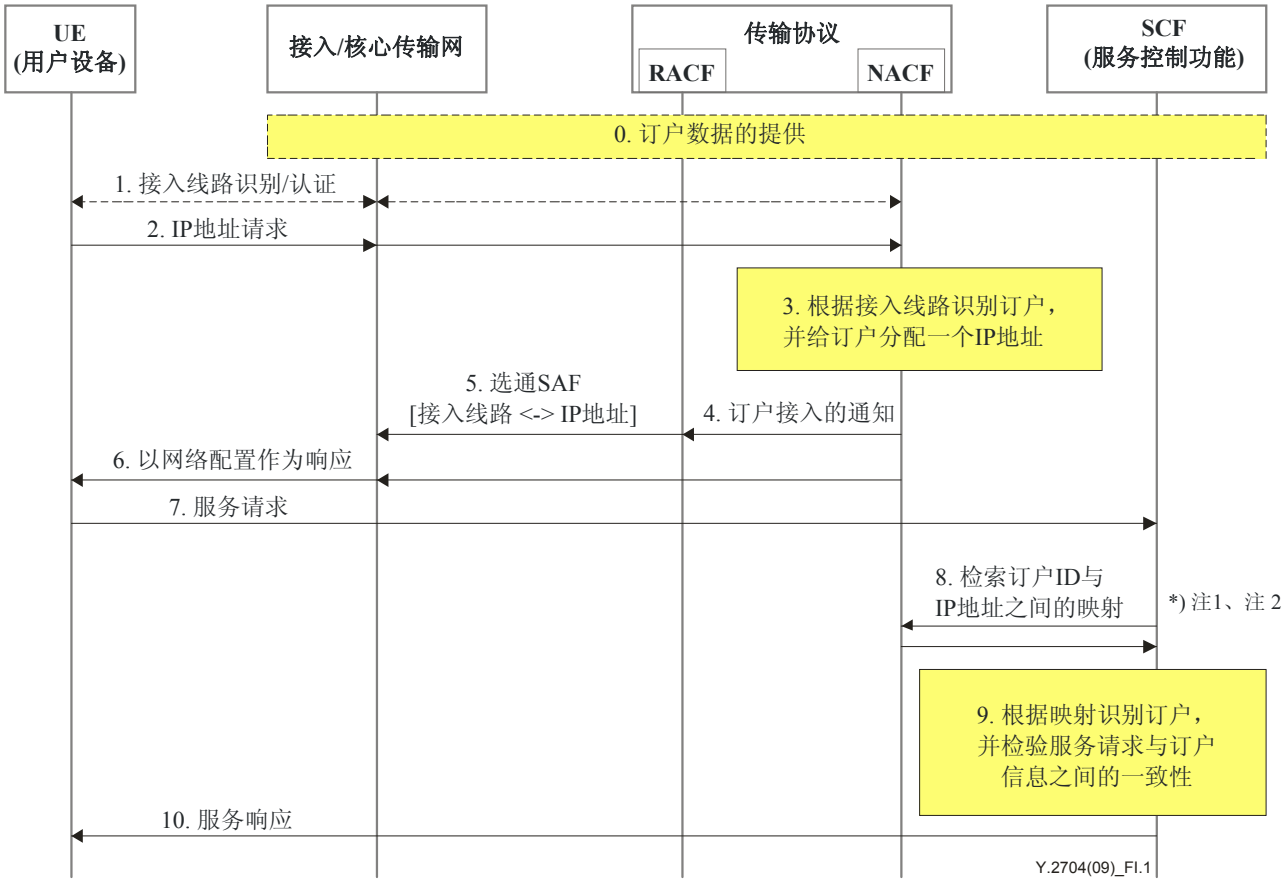
源地址保证及其在订户识别和认证机制中的应用举例

(本附录不是本建议书的组成部分)

本附录提供了源地址保证机制以及通过第8.4.2节描述的网络源地址它在订户识别和认证方面应用的具体例子。

I.1 与接入线路认证相关联的订户识别和认证

本节提供了订户识别和认证的一个例子，在这个例子中接入线路认证之后会分配一个IP地址。在本例子中，各个订户固定不变地与他/她的接入线路相关联。因此，本例子中描述的机制只适合于非漫游(即固定)服务。



注1 — NACF可能在分配地址的时候向SCF提供IP地址和订户ID之间的映射信息。

注2 — NACF可能提供IP地址和位置信息(例如线路标识符)之间的映射取代IP地址和订户ID之间的映射。在这种情况下，SCF必须维护订户ID和位置之间的映射，并且从NACF发送的位置信息中得到订户ID。

图I.1－例1的高级信息流

说明

0. 订户信息被重新分配给NACF或SCF中相应的FE(例如TUP-FE，SUP-FE)。

   在这种情况下最重要的设置问题是：

   1) NACF(一般为TUP-FE)维护订户ID(订户账户标识符)和逻辑/物理接入线路ID(如VLAN ID或访问端口)之间的映射。

   2) SCF(一般为SUP-FE)维护订户ID和相应订户的属性或信息(例如，在基于SIP服务的情况下“来源”报头的数值)之间的映射。在SCF中订户ID的名称空间不同于NACF中订户ID的名称空间的情况下，建议SCF也应该维护这些ID之间的映射。

      或者，NACF可以不必维护订户ID和接入线路ID之间的映射，在这种情况下，建议由SCF维护订户ID和接入线路ID之间的映射，这样SCF能够由接入线路ID检索相应的订户ID。

      在接入/核心传输的网关上，订户接入线路的所有通路最初都配置成关闭，这样除了UE连接网络所必需的数据包(例如发送的地址请求或认证请求)以外，任何输入的IP数据包都被丢弃。

1. UE通过其接入线路连接到接入网，以便获得到NGN的IP连通性。这个例子假设NACF的接入认证是隐含的，在第3步执行。然而，作为选择，NACF可能使用一个明确的接入认证方式(例如IEEE 802.1X)。在这种情况下，网络接入认证在本阶段进行，即在IP地址分配之前。

2. UE请求分配一个IP地址，这一般通过发送DHCP发现和请求来实现，这些信息由网关转发到NACF。

3. 在这个例子中，接入网认证接入线路，向NACF提供经过认证的接入线路ID(例如VLAN ID或访问端口)。因此，NACF能够根据接入线路ID识别订户ID，通过该订户ID发送IP地址请求。然后，NACF给请求UE分配一个IP地址并保存订户ID和分配IP地址之间的映射。

   这种映射关系可以由NACF推送到SCF，并保存在SCF中。在这情况下，可以跳过下面的第8步。

4. NACF通知RACF订户已经连接上了。这个通知包含订户ID、接入线路ID(物理的/逻辑的)、分配的IP地址和QoS信息。

5. RACF对分配给订户的网络资源做出策略性决定，命令网关按数据包过滤规则打开接入线路通路，数据包过滤规则定义为接受并转发源地址为分配给订户的IP地址的输入IP数据包，丢弃其他输入的数据包。

   实施源IP地址过滤要与NACF的接入线路认证协调工作，接入线路认证的描述见上面，确保IP地址只能由分配了该IP地址的订户使用。

6. NACF给UE返回分配的IP地址以及其他网络配置参数(例如DNS服务器和P-CSC-FE的地址)。这通常通过发送DHCP提供和响应信息来实现。

7. UE在获得了IP连通性以后，会向SCF发送一个服务请求(例如在基于SIP服务情况下的登录信息)，只有请求的源地址是NACF分配的地址时，网关(防火墙具有源地址过滤功能)才将该服务请求传递给SCF。

8. SCF从NACF中检索与服务请求的源地址相对应的映射信息(即订户ID和分配给它的IP地址)。

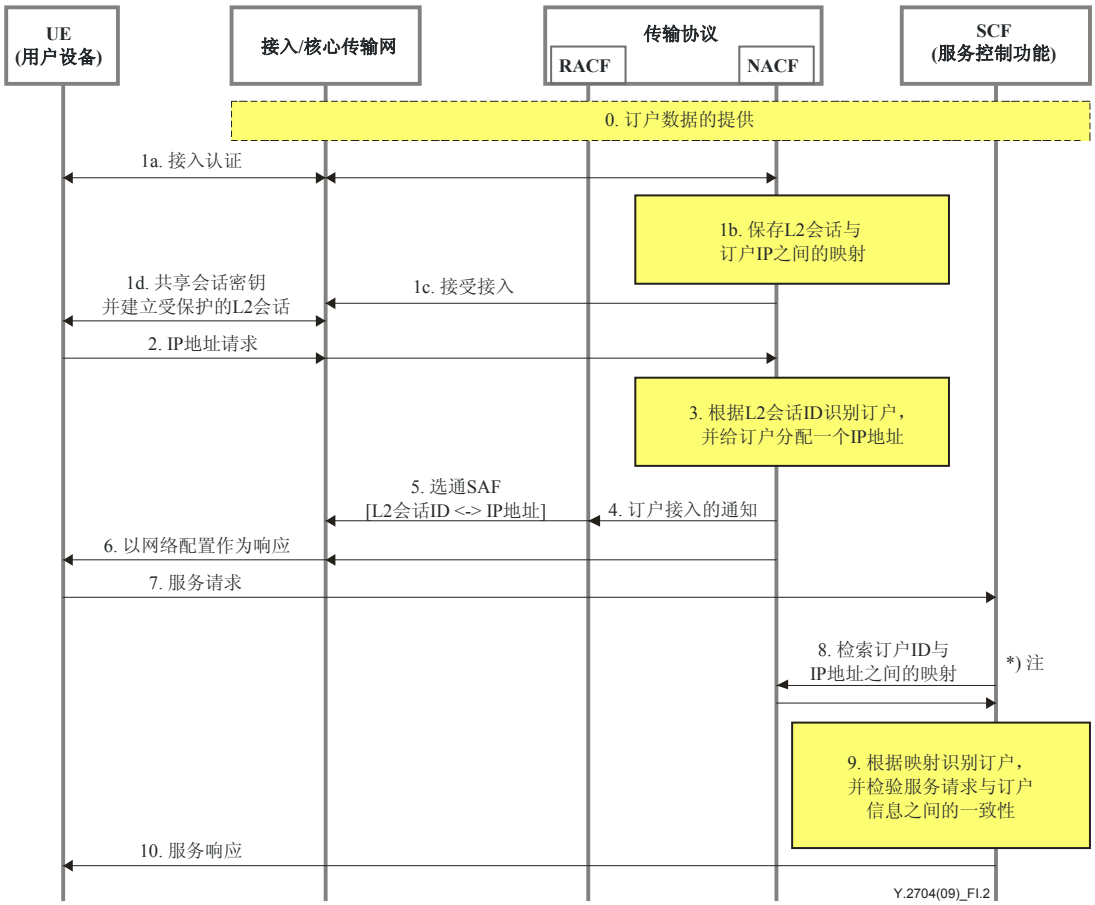
9. SCF认为服务请求源自于分配了在检索的映射信息中所包含订户ID的订户。在SCF中订户ID的名称空间不同于NACF中订户空间的名称空间的情况下，检索得到的订户ID必须由SCF根据这些ID之间的映射转换成相同名称空间内的订户ID。

   SCF从服务请求中提取与订户身份(例如在基于SIP服务情况下“来源”报头中的数值)相关的属性值，检验那些数值和相应订户信息之间的一致性。

10. 如果认证和授权成功，则SCF返回正常的应答以提供所请求的服务(例如在基于SIP服务情况下的“200 OK”)。

I.2 在IP连通性建立期间与明确接入认证相关的订户识别和认证

本节提供了订户识别和认证的一个例子，在这个例子中IP连通性建立期间明确的接入认证之后会分配一个IP地址。在本例子中，各个订户动态地与在接入认证期间建立的L2会话相关联。因此，本例子中描述的机制适用于漫游和非漫游服务。



注 — NACF可能在分配地址的时候向SCF提供IP地址和订户ID之间的映射信息。

图I.2－例2的高级信息流

说明

0. 订户信息被重新分配给NACF或SCF中相应的FE(例如TUP-FE，SUP-FE)。与前面的例子相比，NACF不需要维护订户ID和接入线路ID之间的映射。

   在接入/核心传输的网关上，与UE的L2会话的所有通路最初都配置成关闭，这样除了UE连接网络所必需的数据包(例如发送的地址请求或认证请求)以外，所有输入的IP数据包都被丢弃。

1a. 当UE请求到NGN的连通性时，接入网动态地建立一个和UE的L2会话，根据订户凭证(一般采用一个明确的认证方式，如IEEE 802.1X和RADIUS/Diameter)执行UE和NACF之间的接入认证程序。由网关转发用于认证的信令消息。

1b. 在认证程序期间，分配给UE的L2会话的标识符(例如VLAN-ID，UE的L2地址等)被发送到NACF。当认证成功时，NACF采用通过认证的订户ID保存这个L2会话标识符。

1c. NACF通知接入网UE已经成功地通过认证，访问网络已经得到授权(例如采用RADIUS协议情况下的访问接受信息)。

1d. 当收到NACF的成功认证订户的通知时，接入网建立一个和UE的安全关联(SA)，以便保护L2会话的完整性和机密性。通常这通过IEEE 802.1X中定义的会话密钥导出机制和为各项L2技术定义的保护程序来实现(例如IEEE 802.11i中为802.11无线局域网定义的TKIP/CCMP) 。

上面描述的安全机制保护L2会话不被其他订户使用，并提供必要的防止IP地址欺骗的基础。

2. UE请求分配一个IP地址，这通常通过发送DHCP发现和请求来实现，这些信息被网关转发到NACF。

3. NACF依据L2会话的标识符来识别订户ID，通过该订户ID发送请求。然后，NACF给请求UE分配一个IP地址，并保存订户ID和分配的IP地址之间的映射。

这种映射信息可以由NACF推送到SCF，并保护在SCF中，在这种情况下，可以跳过下面的第8步。

4. NACF通知RACF订户已经连接上了，该通知包含订户ID、L2会话ID(物理的/逻辑的)、分配的IP地址和QoS信息。

5. RACF对分配给订户的网络资源做出策略性决定，命令网关按数据包过滤规则打开L2会话的通路，数据包过滤规则定义为接受并转发源地址为分配给订户的IP地址的输入IP数据包，丢弃其他输入的数据包。

实施源IP地址过滤要与NACF的接入认证协调工作，接入线路认证的描述见上面，确保IP地址只能由分配了该IP地址的订户使用。

第6-第10步与第I.1节描述的前一个例子中的那些说明完全相同。

附录二

应急电信服务(ETS)的互连安全

(本附录不是本建议书的组成部分)

II.1 背景

应急电信服务(ETS)是一种国家服务，在灾难和应急情况发生时能给经过授权的ETS用户提供优先级服务。ETS的实施是国家事务。然而，灾难/应急情况能够超越地理界线，因此，国家/主管部门有可能加入一个双边/多边协议，以连接他们各自的ETS系统。这将实现ETS保护下的优先级通信服务(例如话音、信息、视频和数据)，灾难和应急情况发生时具有双边和/或多边协议的不同国家网络之间将支持ETS。ETS通信的可靠性和可用性将取决于与端对端通信有关的各个国家网络的安全性能和采取的措施。

II.2 范围/目的

本附录提供了指导，对跨不同国家网络(即国家/主管部门)实现ETS通信的网络提供安全给予支持。

使用特定最终用户设备安全功能的最终用户对等安全功能不在本附录的范畴之内。本附录的范围限于在逐跳基础上跨多个网络ETS通信的网络提供安全，然而，建议NGN能够透明地支持这种对等功能。

本附录不是要给ETS国家实现方案强加条件，它的主要目的是实现跨不同国家网络(即国家/主管部门)ETS通信(即优先级话音、视频、数据和消息通信)的网络提供安全。

II.3 ETS安全目标和ETS互连准则

关于ETS的安全目标和互连准则见[ITU-T Y.2701]的附录一。

II.4 认证和授权

建议国家网络根据有权使用特定服务(例如话音、数据和视频)所需的保证等级和适当策略，支持并实现机制和能力来对ETS用户、设备或用户和设备的组合进行认证、授权。

建议适当利用本建议书正文中描述的用户和用户设备识别和认证的安全机制，来支持国家网络中ETS实现方案：

- IPsec/TLS关联。
- SIP询问/应答和X.509证书。
- 通用引导体系结构。

此外，建议应实现监测访问ETS资源的安全措施来检测和防止拒绝服务类型的攻击。

同样，关于ETS认证和授权方法例子的信息，见[ITU-T Y.2702]附录一。

II.5 信令和OAMP的传输安全

建议适当利用在本建议书正文中描述的安全机制、IPsec和TLS，来保护国家网络中的ETS信令和OAMP业务。

II.6 媒体业务

建议适当利用在本建议书正文中描述的识别和保护媒体业务的安全机制，来保护国家网络中的ETS媒体业务。

II.7 支持主叫号码ID和主叫名称ID限制特性

主叫号码ID和主叫名称ID是从PSTN继承下来的两个特性，允许用户知道谁是主叫。ETS呼叫可能服务于不同国家团体用户，这些用户对于把这样的信息向被叫方公开有不同的敏感性。因此，建议支持适当的机制强制实施显示或公开ETS用户信息的策略。

II.8 不可追溯性

对于某些ETS通信，各方都不能得到与主叫方和被叫方有关的位置信息，这一点对于实现最大程度的灵活性很重要。特别地，建议禁止发布任何与位置有关的信息，或如果有必要，基于适当的策略，用适当的无意义的信息取代。位置相关信息包含但不限于：

1) 主叫方和被叫方NPA-NXX或URI。
2) 主叫方和被叫方地理地址。
3) 主叫方和被叫方x-y坐标。
4) 可能在蜂窝下方的狭窄位置中使用的主叫方和被叫方蜂窝信息。
5) 主叫方和被叫方IP地址。
6) 主叫方和被叫方端局或其他能够确定主叫方地理邻近位置的设备信息。

II.9 端对端对等加密

选定的用户可能需要用户设备(UE)对ETS呼叫/会话进行加密，对于这些呼叫/会话，将实行正常的呼叫/会话建立程序，由UE为到终端UE的承载信息(例如话音)提供端对端的加密处理。这个加密处理对于NGN是透明的，然而，建议NGN能够透明地支持这种对等功能。

附录三

安全最佳做法

(本附录不是本建议书的组成部分)

III.1 引言

为了满足[ITU-T Y.2701]提出的要求，可能需要超出本建议书规定的那些安全机制之外的附加的安全机制。可以采用最佳做法安全机制如使用防火墙、操作系统加固、脆弱性扫描和侵入检测系统(IDS)来保护NGN基础设施。关于侵入检测和预防系统(IDPS)的指南参见[b-NIST SP 800-94]，有关恶意事件预防和处理的指导参见[b-NIST SP 800-83]。

本附录提供了应该采用的一些示范性最佳做法安全机制的概述。

III.2 防火墙

防火墙是提供不同网段或不同网络之间边界网络隔离的基本安全构件。防火墙根据所配置的特定业务过滤规则实施隔离。防火墙可以与其他安全机制一起使用，提供一个附加的安全层。增加防火墙有助于提供“纵深防卫”安全，由此叠加多种安全机制从而获得更加牢固的安全。

防火墙对进出防火墙的业务都进行检查，防火墙应配置成除非防火墙规则明确允许，否则拒绝所有业务。防火墙还可以在检测到未经授权的数据包时提供业务日志并触发报警。防火墙可以在物理上是一个独立的设备，也可以是主机上的软件。各种类型的防火墙包括静态包过滤、应用层、状态感知包过滤防火墙，防火墙的选用取决于具体的用户需求和偏爱。

静态包过滤防火墙检查输入和输出的数据包，引用一组规则来决定允许数据包通过防火墙还是丢弃数据包。这个决定一般依据数据包的源和目的地IP地址、协议类型以及TCP源和目的地端口。根据数据包和规则，防火墙将丢弃或转发数据包，可能会建立一条日志记录和/或发出警告。一些静态包过滤防火墙还可以提供更深入的数据包检查，可能会到应用层。

应用层防火墙代表网络中他们正在保护的设备来运行应用程序，通常被称做“代理”防火墙。当运行应用程序时，应用层防火墙将检测所有的异常行为，如果发现异常，应用层防火墙不会把数据传递给他们正在保护的设备。必须要给应用层防火墙提供所有必需的应用程序，应用层防火墙必须代表所有被保护的设备来运行这些应用程序。因为这一点，应用层防火墙对网络性能的影响很大。

状态感知防火墙执行与静态包过滤防火墙相似的数据包过滤功能，另外维护关于业务连接状态的信息。状态信息能够使防火墙对允许或拒绝特殊的业务做出更好的判决。例如，状态感知防火墙可能配置成只允许来自网络一侧设备的业务发起通信，这在专用网络连接到公共网络的情况下特别有用。

当防火墙被用做一种附加的信息和控制平台安全时，防火墙应配置成只允许一组设备之间期望的信令和控制通信，网络上不是期望通信的其他业务都应被拒绝，从而为这些设备提供一层保护。

注意到如果防火墙可能会有系统工程和产品的影响，一些应用程序可能必须做成让防火墙知晓的程序。还应注意到防火墙不能防止受到所有的安全攻击，如攻击者骗取合法的信令数据包信息。

III.3 操作系统加固

用于信令和控制层面功能的服务器和网元容易受到多种攻击，包括：

- 后门程序。
- 嗅探程序。
- 口令截获器和破解工具。
- 利用操作系统服务的缺点。
- 拒绝服务(DoS)。

这些攻击中有很多是基于公开的技术，利用脚本和其他可以获得的工具，知识不怎么渊博的黑客有可能非法利用系统。一旦系统被损害，侵入者能够做许多事情，包括：

- 修改或破坏信息。
- 泄露敏感信息。
- 安装恶意代码来收集信息。
- 用受害服务器攻击其他系统。

操作系统加固程序可以用于提高操作系统对于攻击的抵抗能力。操作系统加固程序是在操作系统安装和配置期间遵循的、必需的明智做法。虽然没有系统是绝对安全的，但下列操作系统加固程序将使得系统更难以被攻击者损害。

操作系统加固程序基本上包括限制服务、端口以及对应用程序和文件的访问，操作系统加固还包括只运行来自受限访问权限账户的应用程序，只运行绝对必要的端口和服务。应咨询操作系统厂商获取最新的操作系统加固程序和安全补丁。

III.4 脆弱性评估

对网元进行脆弱性评估的目的是发现安全脆弱性、弱点和风险区域。脆弱性测试是通过中断服务、绕过设计的安全控制、捕获机密数据、获得对系统的非授权访问、窃取或拒绝服务，有意尝试并使得系统停止运行。为了确保更牢固的安全性，可能会包含对NGN元素的脆弱性评估。

对网元的脆弱性评估可以在产品检验阶段进行，然后作为网络维护的一部分来开展，在产品检验阶段包含安全脆弱性测试是有利的，因为已经有预先设定的程序来记录和提交请求的变化。开展例行脆弱性评估对于识别新的威胁、脆弱性是有用的，能够开展行动来减缓确定的问题。

III.5 侵入检测系统

侵入检测系统能够用于提供针对侵入和非授权行动的保护。例如，侵入检测系统可以用于警告网络管理员可能发生的安全事件，例如，SIP服务器泄密或拒绝服务攻击。

根据下列准则，侵入检测系统(IDS)可以大致分为：

- 实时或离线事件检测：实时IDS系统是在事件发生时分析网络业务和日志，离线IDS系统是在事件已经发生了之后以批处理方式分析侵入行为。
- 基于网络或基于主机安装：基于网络的IDS一般包含安装在网络瓶颈处的多个监听器，在这里两点间的所有业务都能被监听，基于主机的IDS需要将软件直接安装在要保护的服务器上，监听那些服务器上的网络连接和用户活动。
- 反应式或被动式：反应式IDS通过修改防火墙规则或路由器过滤器或采取其他措施主动介入阻止攻击，被动式IDS系统只是将问题通知管理员或其他网络系统。

大多数商业IDS产品提供综合的基于网络和基于主机的监听能力，有一个中央管理设备接收来自各个监听器的报告，并向网络管理员发出警告。

参考资料

[b-ITU-T E.107] ITU-T E.107建议书 (2007)，《应急电信服务(ETS)和ETS国家级实施方案(ENI)的互连框架》。

[b-ITU-T M.3016.0] ITU-T M.3016.0建议书 (2005)，《管理平面的安全：概述》。

[b-ITU-T X.690] ITU-T X.690建议书(2008) | ISO/IEC 8825-1:2008，《信息技术 — ASN.1编码规则：基本编码规则(BER)、规范编码规则(CER)和特异编码规则(DER)的规范》。

[b-ITU-T X.810] ITU-T X.810建议书 (1995) | ISO/IEC 10181-1:1996，《信息技术 — 开放系统互连 — 开放系统的安全框架：概述》。

[b-ITU-T Y.2091] ITU-T Y.2091建议书(2008)，《下一代网络(NGN)的术语和定义》。

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture*.

[b-3GPP TS 33.328] 3GPP TS 33.328, *IP Multimedia System (IMS) media plane security*.

[b-ETSI TS 133 220] ETSI TS 133 220 V9.2.0 (2010), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture.*

[b-IETF RFC 1155] IETF RFC 1155 (1990), *Structure and Identification of Management Information for TCP/IP-based Internets.*

[b-IETF RFC 1212] IETF RFC 1212 (1991), *Concise MIB definitions.*

[b-IETF RFC 1215] IETF RFC 1215 (1991), *A Convention for Defining Traps for use with the SNMP.*

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

[b-IETF RFC 2367] IETF RFC 2367 (1998), *PF_KEY Key Management API, Version 2.*

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

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE).*

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

[b-IETF RFC 2578] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2).*

[b-IETF RFC 2579] IETF RFC 2579 (1999), *Textual Conventions for SMIv2.*

[b-IETF RFC 2580] IETF RFC 2580 (1999), *Conformance Statements for SMIv2.*

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication.*

[b-IETF RFC 2808] IETF RFC 2808 (2000), *The SecurID® SASL Mechanism.*

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).*

[b-IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework.*

[b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.*

[b-IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications.*

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).*

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).*

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).*

[b-IETF RFC 3417] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP).*

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol.*

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

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

[b-IETF RFC 3713] IETF RFC 3713 (2004), *A Description of the Camellia Encryption Algorithm.*

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing.*

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

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS).*

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

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

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

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL).*

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).*

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[b-IETF RFC 4567] IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP).*

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams.*

[b-IETF RFC 4590] IETF RFC 4590 (2006), *RADIUS Extension for Digest Authentication.*

[b-IETF RFC 4648] IETF RFC 4648 (2006), *The Base16, Base32, and Base64 Data Encodings.*

[b-IETF RFC 4740] IETF RFC 4740 (2006), *Diameter Session Initiation Protocol (SIP) Application.*

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[b-IETF RFC 5077] IETF RFC 5077 (2008), *Transport Layer Security (TLS) Session Resumption without Server-Side State.*

[b-IETF RFC 5090] IETF RFC 5090 (2008), *Radius Extension for Digest Authentication.*

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2.*

[b-IETF RFC 5282] IETF RFC 5282 (2008), *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol.*

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol.*

[b-ISO/IEC 15946-1] ISO/IEC 15946-1:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General.*

[b-ISO/IEC 15946-2] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures.*

[b-ISO/IEC 15946-3] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.*

[b-ISO/IEC 15946-4] ISO/IEC 15946-4:2004: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery.*

[b-ISO/IEC 15946-5] ISO/IEC 15946-5:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation.*

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*

[b-NIST FIPS 197] NIST Federal Information Processing Standards (FIPS) 197 (2001): *Advanced Encryption Standard.*

[b-NIST FIPS 198-1] NIST Federal Information Processing Standards (FIPS) 198-1 (2008), *The Keyed-Hash Message Authentication Code (HMAC).*

[b-NIST FIPS SP 800-38a] NIST Federal Information Processing Standards (FIPS), *Special Publication 800-38: Recommendation for Block Cipher Modes of Operations. Methods and Techniques, December 2001.*

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers.*

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation on Key Management – Part 1: General (Revised).*

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling.*

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS).*

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

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、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、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	终端和主观与客观评估方法
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
2010年，日内瓦