国 际 电 信 联 盟

ITU-T Y.2702

国际电信联盟
电信标准化部门

(09/2008)

Y系列：全球信息基础设施、
互联网协议问题和下一代网络

下一代网络 – 安全

下一代网络（NGN）的认证和授权要求第1版

ITU-T Y.2702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

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T Y.2702建议书

下一代网络（NGN）的认证和授权要求第1版

摘要

ITU-T Y.2702建议书规定了下一代网络（NGN）的认证和授权要求。

来源

第13研究组（2005-2008年）根据WTSA第1号决议规定的程序，于2008年9月12日批准了ITU-T Y.2702建议书。

关键词

属性、认证、授权、安全、标识符、身份管理（IdM）、下一代网络（NGN）、特权和安全。

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.2702建议书

下一代网络的认证和授权要求第1版

1 范围

本建议书根据[ITU-T Y.2012]，对下一代网络（NGN）提出了认证和授权要求，其中包括对整个用户到网络接口（UNI）、网络到网络接口（NNI）、应用到网络接口（ANI）以及所有具有可能需要认证与授权的网络的内部实体进行认证与授权的要求。这项协议的范围包括：

1) 用于网络接入的用户认证与授权（如为接入或连接网络而对终端用户设备、归属网络网关或企业网关进行的认证与授权）

2) 业务提供商为接入业务/应用提供的用户认证与授权（即在认证与授权适用于NGN业务/应用接入时，对用户、设备或用户/设备组合进行的认证和授权）

3) 网络用户的认证与授权（即用户对相连的NGN网络或业务提供上的身份进行验证）

4) 用户的对等认证与授权（即对被叫用户（或终接实体）的认证与授权、对始发实体的认证与授权，或对作为网络功能的数据来源认证）

5) 网络的相互认证与授权（如在传输层或业务/应用层的整个NNI接口进行的认证与授权）

6) 对业务/应用提供商的认证与授权

7) 使用第三方的认证与授权服务

8) 对目标（如应用程序、信息内容和数据内容标识符）的认证。

上述项目有可酌情包括对信令、承载商和管理业务的认证。

此外，本建议书还为NGN认证和授权提供了参考模型。

注1 – NGN的认证与授权被视为NGN身份管理（IdM）这一更广泛议题的一部分。具体而言，本建议书介绍的认证与授权功能，应该用于支持NGN IdM的身份管理功能。

注2 – 本建议书所用的“用户”一词不局限于个人。用户可以是个人、团体、公司，也可以是法律实体。

注3 – 实体授权的目的并不说明对个人进行了明确无疑的认证。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.800] ITU-T Recommendation X.800, Security architecture for Open Systems Interconnection

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

[ITU-T X.810] ITU-T recommendation X.810, Information technology – Open System Interconnection – Security framework for open systems: Overview

[ITU-T X.811] ITU-T Recommendation X.811, Information technology – Open System Interconnection – Security frameworks for open system: Authentication framework

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

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 定义

3.1 ［ITU-T X.800］建议书的定义

本建议书采用了［ITU-T X.800］定义的以下术语：

3.1.1 认证信息：用于确认所称身份有效性的信息。

3.1.2 授权：授予权利，包括根据访问权限提供接入权。

3.1.3 资格：为确定一实体自称的身份而传送的数据。

3.1.4 数据源认证：确认收到的数据的来源与所称的来源一致。

3.1.5 对等实体认证：确认联合体中的对等实体的所称身份。

3.2 ［ITU-T X.810］的定义

本建议书采用了［ITU-T X.810］定义的以下术语：

3.2.1 委托：据称实体X只有和仅仅在它相信实体Y会在一系列行动中按一定方式行事时，才会将这些行动委托给实体Y。

3.2.2 受托的第三方：受托采取某些与安全（涉及安全政策）相关的行动的安全机构或其代理。

3.3 ［ITU-T X.811］的定义

本建议书采用了[ITU-T X.811]定义的以下术语：

3.3.1 非对称认证方法：一种两个实体并非共享所有认证信息的认证方法。

3.3.2 经认证的身份：经认证确认的主体的鉴别标识符。

3.3.3 认证：对一实体所称身份的确认。

3.3.4 认证证明：得到认证机关担保并可用于确认一实体身份的安全证明。

3.3.5 认证交换：为认证的目的而进行的一系列一次或多次交换认证信息的转移。

3.3.6 认证信息（AI）：用于认证的信息。

3.3.7 认证发起方：发起认证交换的实体。

3.3.8 申请方：身为或代表一主体从事认证的实体。申请方具有代表主体进行认证交换所需的职能。

3.3.9 申请认证信息（申请AI）：申请方用于生成验证主体所需的交换AI的信息。

3.3.10 交换认证信息（交换AI）：申请方和验证方之间在主体认证过程中交换的信息。

3.3.11 主题：其身份可予认证的实体。

3.3.12 对称认证方法：一种实体双方分享所有认证信息的认证方法。

3.3.13 验证认证信息（验证AI）：验证方通过交换AI用于验证所称身份的信息。

3.3.14 验证方：身为或代表一需要经验证身份的实体的实体。验证方具有从事认证交换所需的功能。

3.4 [ITU-T Y.2701] 的定义

本建议书采用了[ITU-T Y.2701] 定义的以下术语：

3.4.1 边界单元：提供连接不同安全和管理域功能的网元。

3.4.2 公司网络：支持多用户并可能位于多个地点（如企业、校园）的专用网络。

3.4.3 安全域：其内部单元按安全政策进行管理的一组单元、一项安全政策、一个安全机构和一系列与安全相关的活动。安全机构负责管理该政策。一特定的安全域可能横跨多个安全区。

3.4.4 终端设备边界单元：在客户所在地设备和业务提供商网络之间提供安全功能的边界单元。

3.5 本建议书定义的术语

3.5.1 服务等级协议（SLA）：双方或多方谈判达成的正式协议，规定各方的业务特点、职责和工作重点。SLA可能包括公布的有关安全、性能、收费和计费、业务提供和付费等内容。

4 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：

ACL 访问控制表

AI	认证信息
ANI	应用至网络接口
AS	应用服务器
BE	边界单元
BSF	引导程序服务器功能
B-TID	引导程序交易标识符
CSCF	呼叫会话控制功能
DSL	数字用户环路
ENI	ETS国家部署
ETS	应急通信业务
FE	职能部门
GAA	通用认证架构
GBA	通用引导程序架构
GUSS	GBA用户安全设置
HSS	归属用户系统
HTTP	超文本传输协议
HTTPS	超文本传输协议的安全性
IAD	综合接入设备
I-CSCF	询问呼叫会话控制功能
ID-FF	网络身份统一框架
IdM	身份管理
IdP	身份提供商
ID-WSF	统一网络服务框架
IMS	IP多媒体业务
IP	互联网协议
ISDN	综合业务数字网
IWF	互通功能
LUAD	启用Liberty的用户代理或设备
MAC	媒体接入点
MS	媒体服务器
NACF	网络附着控制功能
NAF	网络应用功能
NAP	网络接入点
NGN	下一代网络
NNI	网络到网络接口
OAM&P	运营、管理、维护和配置
OSI	开放系统互连

P-CSCF	代理呼叫会话控制功能
PES	PSTN/ISDN演进业务
PIN	个人识别密码
PKI	公共密钥基础设施
PII	个人可识别信息
PSK	预共享密钥
RACF	资源和许可控制功能
RBAC	基于角色的访问控制
RP	依赖凭证方
RPH	资源优先报头
RSVP	资源预留协议
SAML	安全断言标记语言
SASL	简单认证和安全层
SBC	会话边界控制器
S-CSCF	服务呼叫会话控制功能
SDP	会话描述协议
SIM	用户识别模块
SLA	服务水平协议
SLF	用户定位功能
SOAP	简单对象访问协议
SP	服务提供商
SSOS	单点登录服务
TDR	救灾通信
TE	终端设备
TE-BE	终端设备–边界单元
TLS	传输层安全
UAI	用户认证接口
UE	用户设备
UNI	用户至网络接口
URL	统一资源定位符
WS	网络服务器
XML	可扩展标记语言

5 参考模型

5.1 ITU-T X 811认证框架

本建议书采用了[ITU-T X.811]介绍的认证基本概念，并做了以下归纳。

5.1.1 认证的基本概念

认证可确认一实体所称的身份。认证只有在主体和验证方建立关系的情况下才有意义。有两种情况非常重要：

- 与验证方（实体认证）保持具体联系的申请方是主体的代表；而且
- 主体是验证方所获数据项目的来源（数据源认证）。

实体认证可以验证主体在一通信关系中的身份。该主体经验证的身份只有在采用认证服务时才能得到确认。

注1 – 在采用数据来源认证时，也必须充分确保证数据不被修改。可以通过使用完整性服务达到这一目的，例如：

- 利用数据无法被修改的环境；
- 确认收到的数据与发送的数据具有相同的数字指纹；
- 利用数字签名机制；或者
- 采用对称加密算法。

注2 – 对用于确定实体认证的“通信关系”这一术语可以有广泛的解读，例如它可以指一种OSI连接、程序间通信或用户与终端之间的互动。

5.1.2 标识符

主体是其身份可以认证的实体，并具有与之相关的一个或多个显示特征的标识符。实体利用认证业务验证主体所称的身份。经此验证的主体身份称为经认证的身份，同样，其身份经验证的主体则称为经验证的主体。

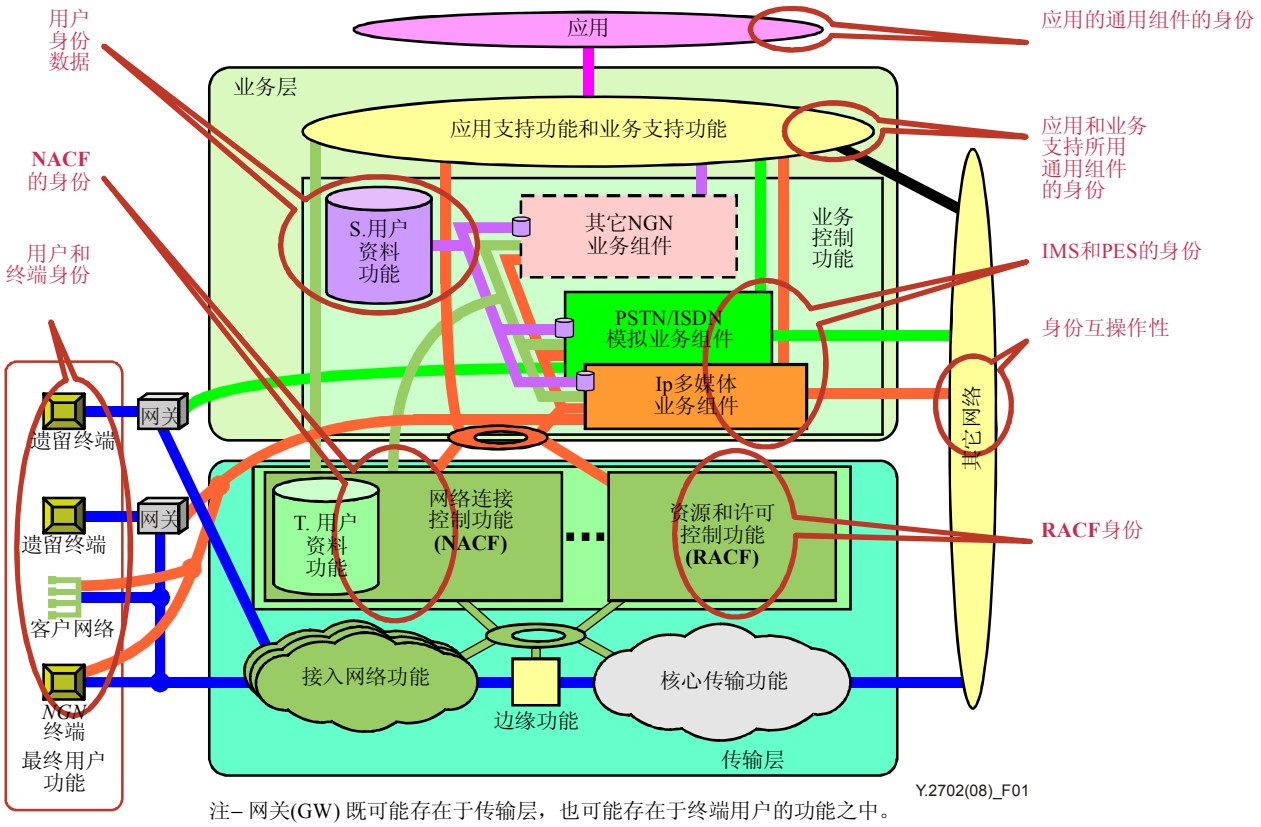
能够确定和认证的主体包括但不限于以下几类：

- 用户；
- NGN提供商；
- 程序；
- 真正的开放系统；
- OSI层实体；
- 企业，和
- 承载、信令和管理业务的流量。

区分标识符被用于查清一特定安全域中的所称身份。区分标识符能够通过以下两种方法之一，将主体与同域的其他方区分开来：

1) 凭借在一实体群组中的成员身份，即认证时对群组的实体一视同仁（此时的整个群组被视为一个主体，并且有一个区分标识符）；或者
2) 仅确定一个实体。

当在两个不同的安全域之间进行认证时，区分标识符可能不足以明确无误地确认一个实体，因为不同安全域的机构可能会使用同一些区分标识符。在这种情况下，区分标识符必须与安全域标识符一同使用，以便为实体提供明确的标识符。



注– 网关(GW) 既可能存在于传输层，也可能存在于终端用户的功能之中。

图 1 – NGN标识符示例

NGN不同分层和层次的组件或功能单元，可用于确定一主体或实体的标识符。图1根据[ITU-T Y.2012]图8（NGN组件）显示了NGN示范性标识符。

常见的区分标识符的实例有：

- 通讯录名称；
- 网址；
- AP标题和AE标题；
- 对象标识符；
- 人名（在域背景中清晰无误）；
- 五元组包括：
  - 源IP地址，
  - 目的地IP地址，
  - 源端口号码，
  - 目的地端口号码，以及
  - 协议号码。

5.1.3 认证实体

“申请方”一词用于说明为认证目的而身为或代表一主体的实体。申请方具有代表一主体从事认证交换所需的功能。

“验证方”一词用于说明身为或代表一需要经认证身份的主体的实体。验证方具有为要求对所称身份进行验证而进行认证交换的功能。

参与相互认证的实体将同时发挥申请方和验证方的作用。

“受托第三方”一词用于说明受其他实体委托开展与安全相关活动的安全主管机构。在本建议书涉及的情况下，受托第三方受申请方和/或验证方委托开展认证工作。

注 – 申请方或验证方可能横跨多个功能组件，也可能处于不同的开放系统之中。

5.1.4 认证信息

本标准中介绍的认证信息类型有：

- 交换认证信息（交换AI）；
- 申请认证信息（申请AI）；
- 验证认证信息（验证AI）。

“认证交换”一词用于说明一系列交换AI的单次或多次转移，以便进行认证工作。

图2显示了申请方、验证方和受托第三方之间的关系，还展示了可以构成认证交换的三类认证信息

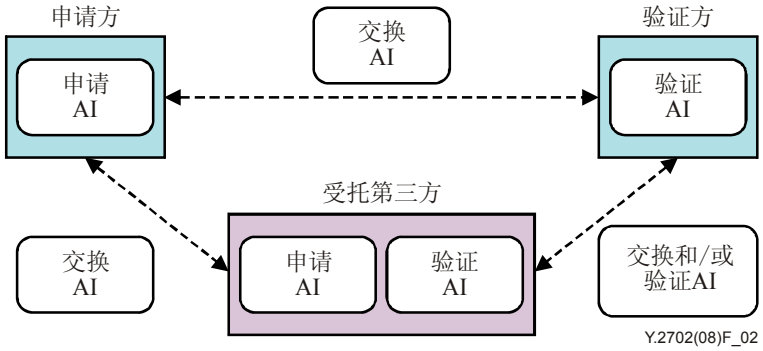


图2 – 申请方、验证方和受托第三方之间的关系

在某些情况下，为了生成交换AI，申请方可能需要与受托第三方开展互动。在这些情况下，受托第三方可以保留与主体相关的验证AI。

受托第三方也可能被用于交换AI的转移。根据交换的情况，第三方可以发挥与验证方相对的申请方的作用。

这些实体也可能需要保留认证信息，供认证受托第三方使用。

5.1.5 多因素认证

多因素认证通过验证多个与主体相关的标识符和属性，确认主体身份的真实性。总而言之，可根据以下认证属性的划分安排多因素认证工作：

1) 你是（如最终用户的实际或行为特征，或可以加以比较的诸如击键模式、声音识别等客户特征或属性）；

2) 你有（如驾照或安全令牌）；

3) 你知（如密码、个人识别码、保安图像）。

密码（你知）是以单一因素认证密钥的最常见实例。有时，密码本身并不能够使人充分信任一个实体的身份，因而需要包括其它认证密钥且形式更为有力的认证，以便使用某些NGN资源、应用和服务。这将取决于未经授权的实体可能获取NGN资源、应用和服务带来的风险。

应当根据需要化解的风险而选择认证因素和密钥。具体而言，必须对未经授权的实体获取NGN资源、应用和服务的影响作出评估，以确定所需的认证方式。示范性电子认证密钥包括：

- 密码，
- 硬件令牌，
- 软件令牌，
- 一次性密码装置令牌。

使用密码进行认证的做法已得到广泛接受。“密码”是申请方熟记在心的秘密，应用于认证其身份。密码通常是一些字符串或图像，用户将它熟记于心，并必须在与其它类似图像一同提供时加以确认。然而，密码系统易受多种攻击。可以通过对通信信道采用附加保护措施保护密码，但这并不能防范所有的攻击。

硬件令牌是保密（通常为加密密钥）和进行加密操作的专用软件装置。认证是通过证明具有该装置和对密钥的控制实现的。加密操作可支持双方认证，并对认证交换所用的通信信道加以保护。

软件令牌主要是对硬件令牌的软件实施，并共享了硬件令牌（如通常存储于磁盘或某些其它媒介的加密密钥）的许多优势。软令牌密钥可以根据从某些激活数据得出的密钥进行加密。通常，激活数据是只为用户所知的密码，因而需要密码激活令牌。认证是通过证明具有密钥并可对它加以控制实现的。与硬件令牌一样，软件令牌可支持双方认证，并对认证交换所用的通信信道加以保护。

一次性密码装置令牌是个人硬件装置，能够生成用于认证的“一次性”密码。一次性密码系统依靠特殊算法生成的一系列密码。这一密码系列中的每一个密码都被称为一次性密码，因为它有别于生成的其它密码，而且只能够使用一次。现有的种类繁多的一次性密码系统，可以提供防范攻击的不同保护。

5.2 对认证的威胁

认证因素和密钥可能受到以下攻击：

1) “你是”– 复制处于比照过程中的客户特点或属性（例如指纹、击键模式）。

2) “你有”– 获取或拷贝客户的物品。

3) “你知”– 研究客户了解的情况。

总之，认证威胁可分为针对认证协议的攻击，以及可能暴露令牌数值或破坏保密信息的其它攻击。

使用多种认证因素可以提高安全性，因为一定会有许多种认证方式受到干扰破坏。使用不易复制的硬件装置（你有）也能缩小攻击范围，因为所有者可望觉察到装置所受损失。基于软件或硬件令牌的认证密钥，可与激活数据（如密码）共同实施双因素认证，使认证不仅依赖于手中的令牌。

客户可能采取先故意向同伙透露单因素认证密钥并随后予以否认的方式，破坏认证系统，以抹杀随后出现的成功的认证结果。采用多种认证因素既可降低这类否认的可信度，也可以吓阻这类攻击。

5.2.1 对认证协议的威胁

认证协议威胁的实例包括：

1) 窃听者：
   - 窃听者监听认证协议信息的交换，以便事后进行分析；
   - 窃听者通常企图获得凭证以冒充申请方。
2) 冒名顶替者：
   - 冒名申请方假冒用户面对验证方，以验证其对令牌的推测或获取有关具体用户的其它信息；
   - 对合法的用户申请方假冒验证方以获得令牌，并利用它假冒用户欺骗合法验证方；
   - 冒名的信赖凭证方假冒信赖凭证系统欺骗验证方，以获取敏感的用户信息。
3) 劫持者：
   - 劫持者通过掌控经认证的会话并冒充用户欺骗凭证信赖方，以获取敏感信息或输入无效信息；
   - 劫持者通过掌控经认证的会话并冒充凭证信赖方欺骗验证方，以获取敏感信息或输入无效信息。

可通过以下方式化解这类攻击：

- 要求每项认证都有新的组成部分，以防攻击的故伎重演。
- 可以利用加密应对窃听者和会议劫持攻击，向用于认证交换（如匿名形式的TLS）的信令信道（信道加密）提供保护。
- 利用与应对窃听者和会议劫持攻击相同的保护方法，可在有限程度上抵御假冒中间人和验证方的攻击。将加密与附加密码技术相结合，可以提高对这些攻击的防御能力（利用基于经认证模式的TLS等加密的相互握手交换，而由客户掌握加密密钥，同时验证方实现“强有力的”相互认证）。
- 加密只能在有限程度上抵御假冒中间人和验证方的攻击，因为交换安全在密码未被破译的情况下也可能受到破坏。例如，用户会因为受到欺骗而接受以为来自但并非来自验证方的认证交换。在客户和验证方之间可以采用基于加密的相互认证技术。

5.2.2 对认证令牌的威胁

倘若攻击者能够控制令牌，他将能够假冒令牌的所有者。对令牌的威胁可以分为以下几个认证密钥攻击类型：

- 攻击者可能会从所有者那里盗窃或克隆其所有。例如，进入所有者电脑的攻击者有可能复制软件令牌。硬件令牌也能被盗窃或复制。
- 你所掌握的知识可能会泄露给攻击者，攻击者可能对密码或PIN进行猜测。当令牌是多方共享的秘密时，攻击者可以从验证方那里获得秘密数值。攻击者可能会为获得这一信息而安装恶意软件（如键盘记录器）。此外，攻击者可能通过对认证尝试生成的网络业务实施离线攻击，测出这一秘密。
- 人的特征可以复制。攻击者可以获得令牌所有者的身份拷贝，并构成复制品。

化解这些威胁的几种战略是：

- 多因素可以提高攻击门槛。如果攻击者需要盗窃加密令牌并猜测密码，工作量因素可能过高。
- 可利用物理安全机制防止被盗令牌受到复制。物理安全机制可提供篡改证据、发现问题并做出反应。
- 复杂密码可降低成功破解密码的可能性。要求使用通用字典未提供的长密码，可能迫使攻击者尝试每一种可能的密码。
- 可利用系统和网络安全控制防止攻击者进入系统或安装恶意软件。

5.2.3 对认证的其它威胁

攻击不仅限于认证协议本身。其它攻击包括：

- 可能破坏认证令牌的恶意密码攻击；
- 通过渗入用户/申请方、认证机构或验证方系统的入侵攻击，获得证书或令牌；
- 可能破坏认证令牌的内线威胁；
- 以其它形式获取令牌的带外攻击，例如通过社会工程或“肩窥”将用户的密码泄露给攻击者；
- 诱骗申请者使用他们自认为安全但其实为不安全的协议，或诱使他们覆写安全协议（例如接受无法认证的服务器证书）；
- 有意破坏其令牌的用户故意予以否认。

对客户的教育和建议是与恶意密码和社会工程攻击作斗争的方法。审计和异常情况检测通常用于应对客户欺诈攻击。使用多重认证密钥能够对客户欺诈攻击形成威慑。人事审核、审计和（酌情）实行职责分离及双重控制可以打击内线攻击。

5.3 认证确认

为保护NGN资源、应用和服务，NGN提供商必须确定需要在多大程度上确认网络接入和应用/服务交易使用的认证。

每个NGN提供商都必须确定和实施认证确认程序。这种程序将包括在认证机制和为认证提供的信息当中进行信任分类（即对于以电子方式向业务提供商提交的身份信息的信任）。

认证确认程序将确定和使用相对和不同等级的确认，以量化认证程序中的信任度。例如，例如，可以采用“n”级的认证确认。0级代表最低的确认级别，而“n”级则代表最高级别。“n”级可用于确定确认级别，即假设认证使用的标识符并非完全平等或必然具有相同的认证数值，认证错误可能造成什么后果（如潜在影响的性质）。

以下举例说明了认证确认方式：

示范认证法

确认级别	相对信任度
0级	不信任所称身份的真实性（如使用接入表控制）
1级	对所称身份的真实性有一定信任
2级	对所称身份的真实性高度信任
–	–
n级	对所称身份的真实性具有最高度的信任

NGN提供商必须评估认证错误带来的潜在风险，或确定实体（如最终用户）身份所需的适当确认级别。可能造成较恶劣后果的认证错误，将需要更高级别的确认。

认证错误的风险是两个因素的函数：

a) 潜在危害或影响；

b) 这种危害或影响的可能性。

危害和影响的类别包括但不限于：

- 不便、困难或对地位或声誉的损害
- 经济损失
- NGN提供商或客户的赔偿责任
- 对NGN提供商的基础设施、资源、应用、业务或公共利益造成破坏
- 对公共和政府利益（如ETS和TDR等重要通信业务）造成损害
- 擅自披露敏感信息
- 对人身安全业务造成损害
- 民事或刑事违法行为

5.4 授权和特权管理

认证本身不足以确定经认证的实体一旦得到接入许可将被授权从事什么工作。认证必须与授权和特权管理机制和方式相结合，以便向NGN业务和资源提供接入控制。例如，确定最终用户/预定用户的作用和特权，以控制对业务和应用以及管理接口的使用，并管理其预订和个人信息。另一个例子是根据接入控制（RBAC）确定作用，以控制OAM&P的使用。

授权或特权可被视为一实体身份的属性。根据安全政策，可以通过认证验证对一实体的授权特权。

5.5 端到端的参考架构模型

此段介绍了本建议书用于构成和划分认证要求的端到端参考模型。参考模型描述了：

1) 用户接入网络的认证和授权（如最终用户设备、家庭网络网关或企业网关为获得网络接入或附着的认证和授权）。
2) 业务提供商为用户使用业务/应用的认证和授权（即在认证和授权适用于NGN业务/应用接入的情况下，对用户、设备或用户/设备组合的认证和授权）。
3) 业务提供商为用户使用具体业务/应用的认证和授权（即针对ETS和TDR的认证和授权[1]）。
4) 用户的网络认证和授权（即用户对连接的NGN网络或业务提供商身份的认证）。
5) 用户的对等认证和授权（如被叫用户（或终接实体）的认证和授权、始发实体的认证和授权，或作为网络函数的数据来源认证）。
6) 相互网络认证和授权（即传输层或业务/应用层NNI接口的认证和授权）。
7) 业务/应用提供商的认证和授权。
8) 使用第三方认证服务。

图3对上述认证参考点做了说明。

本建议书所用的“用户”一词不局限于个人。用户可以是个人、团体、公司，也可以是法律实体。

[1] ETS认证包括的附加要求，可能超出基本要求。

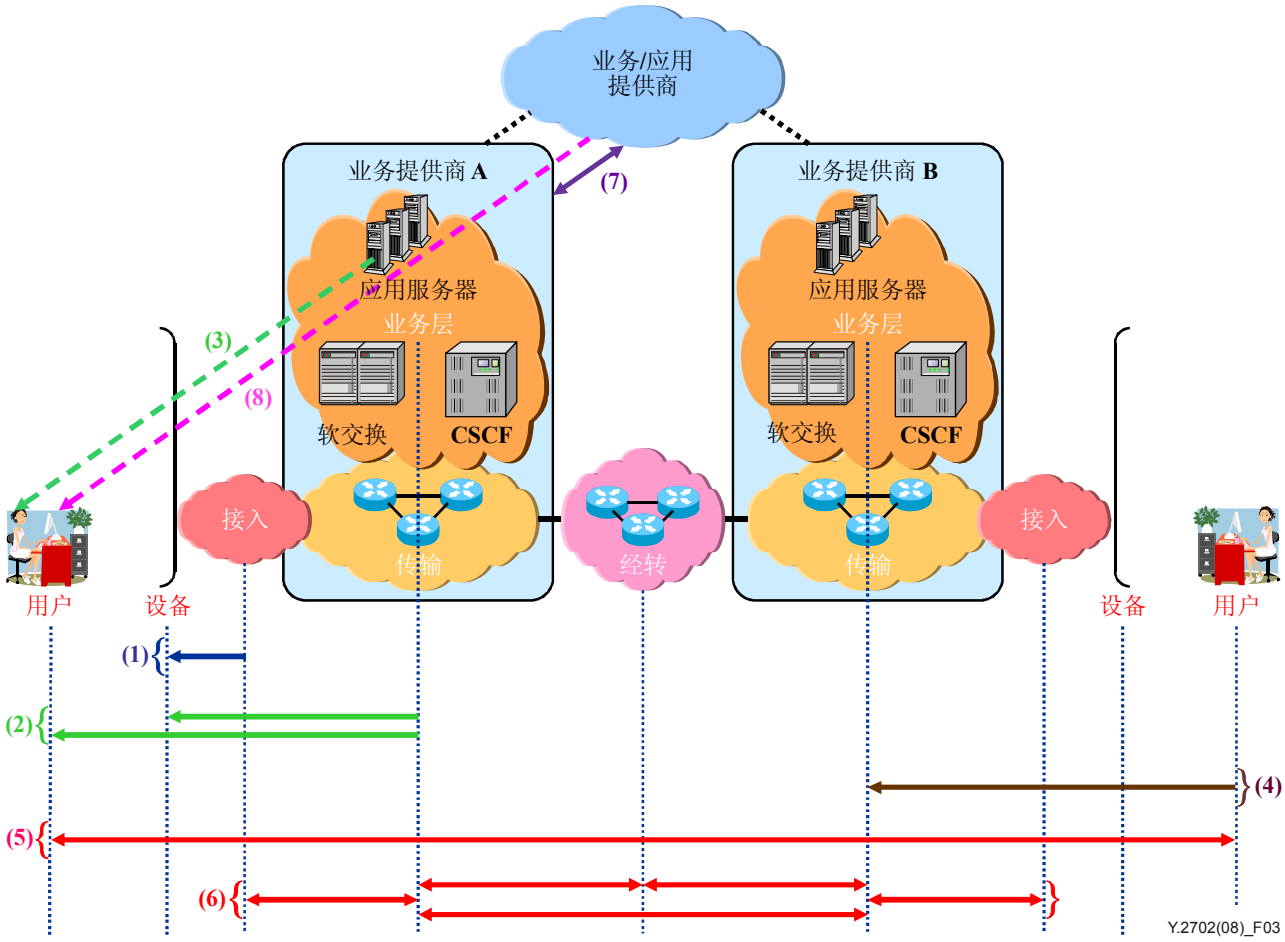


图3 – 端到端的参考架构模型

如图3所示，输层和业务应用层都有认证与授权。此外，还可能出现认证的结合与绑定。这方面的一个例子是，业务提供商为提供更高级别的认证确认，将用户和用户设备的认证加以结合/绑定。在多数情况下，横向认证是逐跳实现的。用户到用户的认证则是一大例外，因为它是端到端的。除用户认证和授权网络的关系之外，其它关系均需要相互认证。

5.6 [ITU-T Y.2012] 详细说明的与NGN架构的关系

本节介绍了本建议书描述的参考模型和[ITU-T Y.2012]涉及的功能架构模型之间的关系。重点谈到：

- [ITU-T Y.2012]图1“NGN架构综述”中的对等认证关系。
- [ITU-T Y.2012]图1中的功能单元旨在履行认证职能。
- [ITU-T Y.2012]图1中的功能单元旨在履行身份管理、对比和整合职能。
- [ITU-T Y.2012]图1中的功能单元旨在根据拒绝认证的规定强化接入控制。

图4利用[ITU-T Y.2012]图1对本建议书5.5款提及的对等认证关系做了说明。对等认证关系以双箭头黑线表示。用户的对等认证和授权（5）未予显示。需要注意的是，即使在NGN提供商向用户提供了应用时（即无ANI），最终用户与应用以及业务层与应用之间依然存在认证关系。

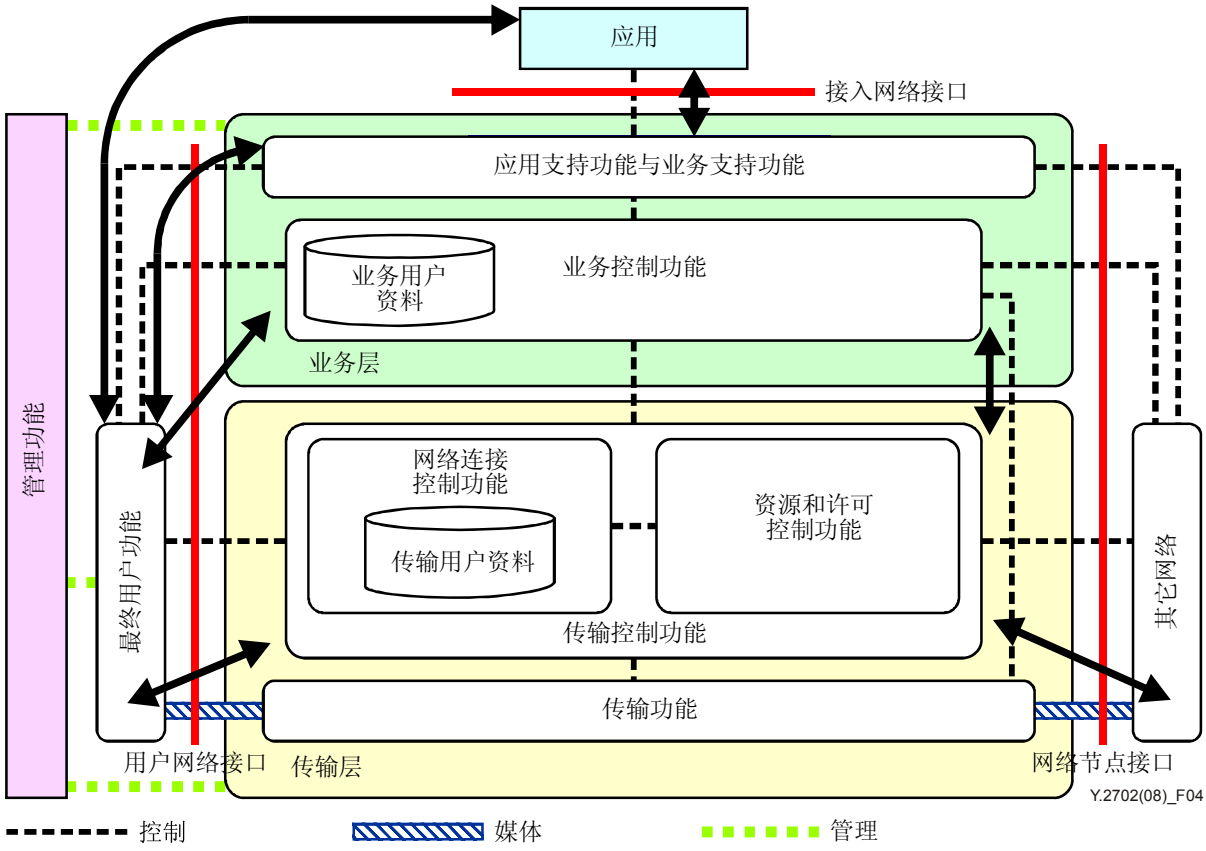


图4 – 认证对等参考

图5重点介绍了[ITU-T Y.2012]参考模型提出的提供或可能提供认证和授权功能的职能实体（FE）。

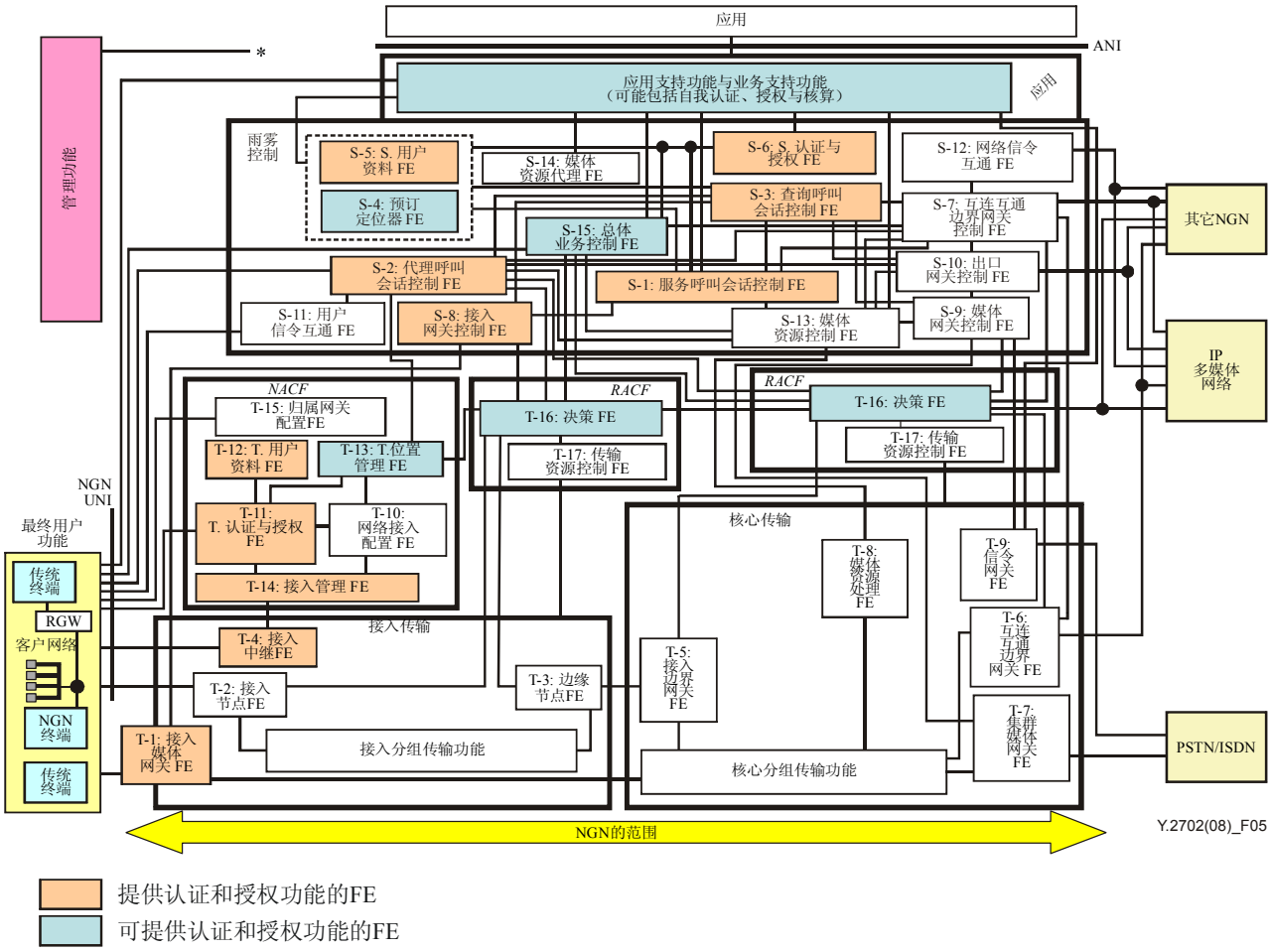


图5 – [ITU-T Y.2012] 的认证和授权功能实体

6 总体要求

本建议书为满足［ITU-T Y.2701］和［ITU-T Y.2201］规定的识别、认证和授权的总体需要，提出了如下要求：

（R-1）– 应满足［ITU-T Y.2701］第7.3.2款（认证）规定的要求。

（R-2）– 应满足［ITU-T Y.2201］第6.12款（识别、认证和授权）规定的要求。

7 对用户的网络接入认证和授权

7.1 说明

有必要利用网络接入认证和授权业务和功能，化解未经授权接入带来的威胁。有必要利用网络接入认证和授权业务验证身份，并确定是否向要求NGN网络连接的最终用户设备（终端设备（TE）和终端设备–边缘元素（TE-BE））提供接入。

一般性假设

a) 最终用户不局限于个人。他可以是个人、团体、公司，也可以是法律实体。

b) 根据[ITU-T Y.2012]，未对可能连接NGN接入网络的多种最终用户接口和最终用户网络作出假设。从单线传统电话到复杂的公司网络，NGN支持所有类型的最终用户设备。最终用户设备既可以是移动的，也可以是固定的。

c) 确定实施接入和认证业务的网元，不在本建议书涉及的范围之内。

d) 网络接入和授权功能，可以作为[ITU-T Y.2012]确定的总体网络连接控制功能（NACF）的一部分加以提供。

7.2 通用参考模型

图6显示了用以下安全域构成的网络接入/附着认证和授权参考模型：

1) 客户域 – 包括用户所拥有和运行的用户设备在内的非信任域，例如：

   a) 传统TE和TE-BE：

      - 传统TE代表经窄带接入（如模拟和ISDN线路）连接的传统用户设备。这些TE通过NGN提供商网关（即接入或媒体网关）接入IP网络。
      - 传统TE-BE代表经窄带接入（如模拟和ISDN线路）连接的作为集合端点（即企业和家庭网络网关）的用户设备。这些TE-BE 通过NGN 提供商网关（即接入或媒体网关）接入IP 网络。

   b) 具有综合接入设备（IAD）的传统TE和TE-BE

      - 配备IAD的传统TE代表经宽带接入（如xDSL或电缆）连接的传统用户设备。这些TE 通过客户域的IAD接入IP网络。
      - 传统TE-BE代表经宽带接入（如xDSL或电缆）连接的作为集合端点（即企业和家庭网络网关）的用户设备。这些用户设备通过客户域的IAD接入IP网络。

   c) NGN TE和TE-BE：

      - NGN TE代表客户域的用户设备，具有支持与IP网络直接连接（如xDSL或电缆）的IP功能。
      - NGN TE-BE代表作为集合端点（即企业和家庭网络网关）的用户设备，具有支持与IP网络直接连接的IP功能。

2) NGN接入提供商域：由NGN提供商（如窄带、xDSL和电缆）托管的接入网络。NGN接入提供商可以选择是否兼任NGN业务提供商。NGN 提供商之间的信任关系受业务水平协议（SLA）的规范。

3) NGN业务提供商域：NGN业务提供商向其用户提供NGN应用服务。NGN提供商之间的信任关系受SLA的规范。

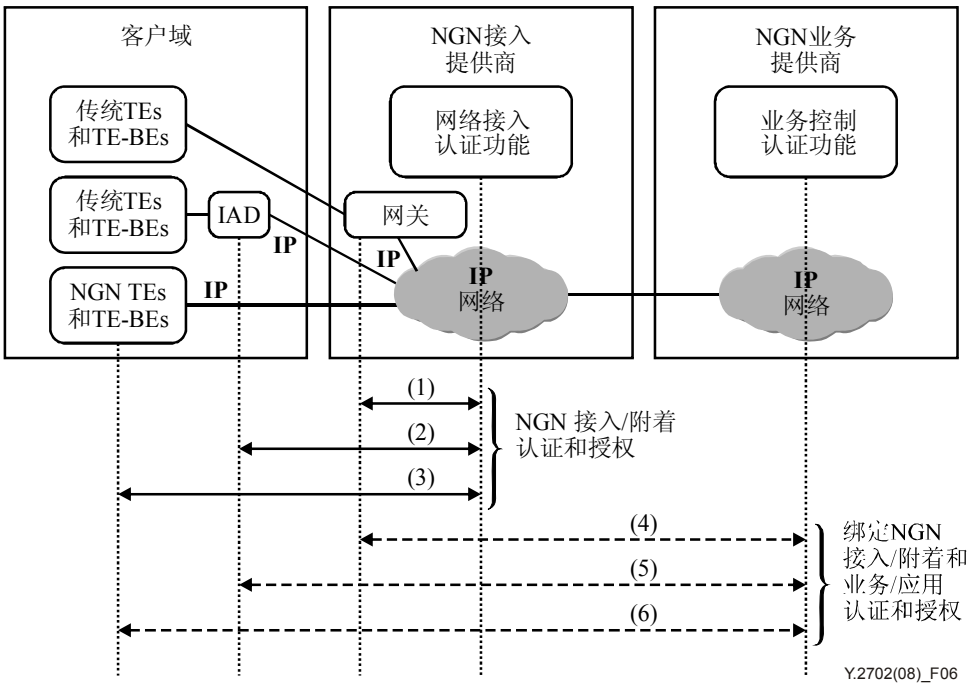


图6 – 网络接入/连接认证和授权参考模型

图6展示了网络接入/附着的识别、认证和授权之间的关系：

a) NGN设备接入/连接的认证和授权–识别、认证和授权用户设备接入或连接IP接入网络的业务和功能。

1) 这一信息流代表识别、认证和授权传统TE和TE-BE接入或连接IP 接入网络的业务和功能。这是在客户域终接传统TE和TE-BE的NGN接入域网关（申请方）和提供NGN接入/附着认证和授权功能的接入域网元（即网络接入点）之间的信息流。NGN接入/附着认证和授权功能（验证工具）可以构成[ITU-T Y.2012]确定的通用NACF的一部分。然而，部署这一功能的位置要视实施情况而定。

2) 这一信息流代表利用客户域的IAD识别、认证和授权传统TE和TE-BE接入或连接IP 接入网络的业务和功能。这是在客户域的IAD（申请方）和提供NGN接入/附着认证和授权功能的NGN接入域网元（即网络接入点）之间的信息流。NGN接入/附着认证和授权功能（验证工具）可以构成[ITU-T Y.2012]确定的通用NACF的一部分。然而，部署这一功能的位置要视实施情况而定。

3) 这一信息流代表利用客户域的IP功能识别、认证和授权NGN TE和TE-BE接入或连接IP接入网络的业务和功能。这是在客户域NGN TE或TE-BE（申请方）和提供NGN接入/附着认证和授权功能的NGN接入域网元（即网络接入点）之间的信息流。NGN接入/附着认证和授权功能（验证工具）可以构成[ITU-T Y.2012]确定的通用NACF 的一部分。然而，部署这一功能的位置要视实施情况而定。

b) 绑定的NGN设备接入/附着的认证和授权–使NGN接入提供商的用户设备认证与NGN业务提供商的用户认证和授权相结合的服务与功能：

4) 这一信息流代表NGN业务提供商隐蓄识别和授权传统TE和TE-BE的业务和功能。这是在接入网络域网关（申请方）和NGN提供商域（验证工具）之间的信息流。

5) 这一信息流代表NGN业务提供商利用IAD隐蓄识别和授权传统TE和TE-BE的业务和功能。这是在客户域IAD（申请方）和NGN业务提供商域（验证工具）之间的信息流。

6) 这一信息流代表NGN业务提供商直接识别、认证和授权客户域传统TE和TE-BE的业务和功能。这是在客户域NGN TE和TE-BE（申请方）和NGN业务提供商域（验证工具）之间的信息流。

游牧性参考模型

图7显示了有关游牧性的参考模型。该模型类似于通用参考模型，只是在这种情景下，需要考虑到受访NGN和归属NGN。

1) 受访NGN域：由受访NGN提供商托管的NGN。可为其他NGN提供商（如归属网络提供商）提供受访网络功能。信任关系受SLA规范。受访网络可以提供NGN业务，并可能拥有自己的用户。

2) 归属NGN域：由归属NGN提供商托管的NGN。归属NGN提供商可为其用户提供NGN业务。信任关系受SLA规范。

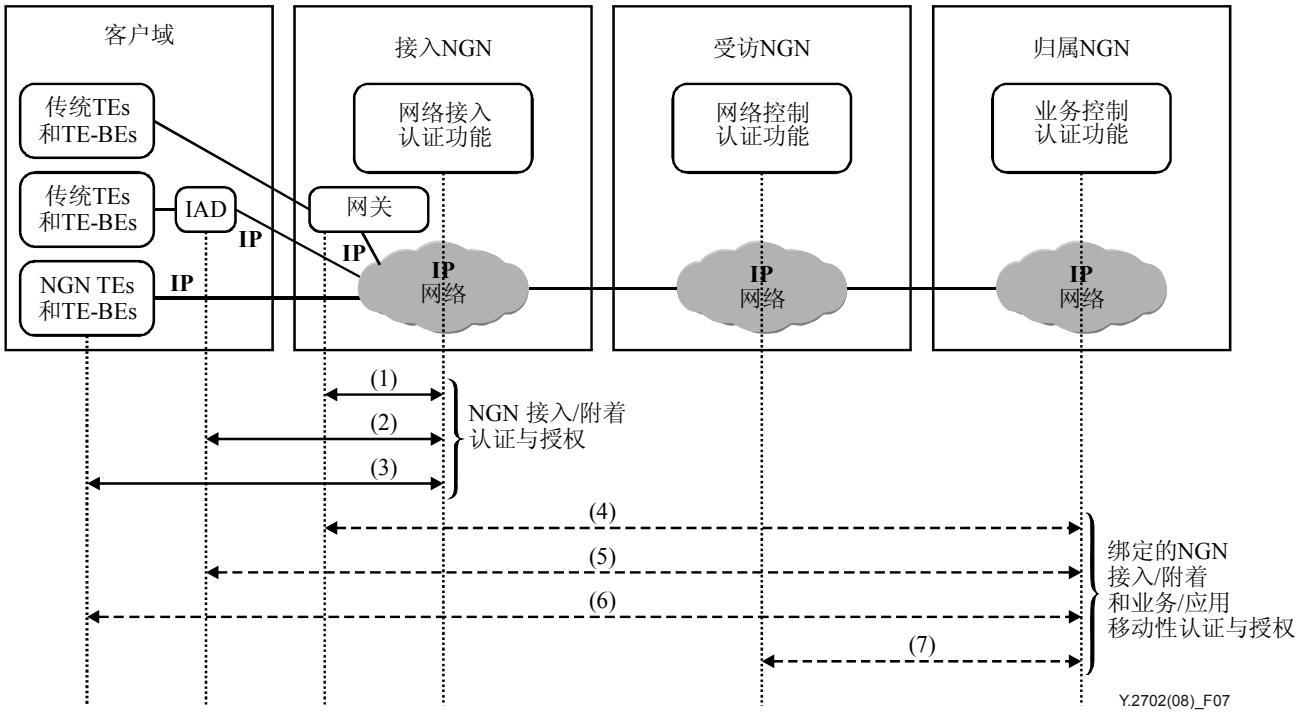


图7 – 游牧性参考模型

参考模型显示了不同域在绑定用户设备认证和授权及用户游牧性认证和授权时的信息流。这一信息流代表将受访NGN提供商的用户设备认证和授权与归属NGN提供商的用户移动性认证和授权相捆绑的服务与功能：

(1) – (6) – 这些信息流正是图7介绍的单一业务提供商状况下的同一些信息流。

(7) – 这一信息流代表受访NGN提供商和归属NGN提供商为支持游牧性而交流识别、认证和授权信息的服务与功能。

7.3 要求

7.3.1 总体要求

以下是有关设备的网络接入/附着识别、认证和授权的总体要求：

(R-3) – NGN必须能够根据NGN提供商的政策，独立识别最终用户/预订用户的设备（如TE和TE-BE）。

(R-4) – NGN必须能够在网络接入点（NAP）对TE和TE-BE的连接进行识别、认证和授权。

(R-5) – 只能向经授权的TE和TE-BE提供网络接入。

(R-6) – 就多网络配置而言，每个管理域（如NGN接入提供商、受访NGN提供商和归属NGN提供商）都必须强化有关TE和TE-BE的网络接入/附着（如使用SLA）识别、认证和授权政策（即信任关系）。

(R-7) – NGN必须支持保护认证和授权信息（如用户资料、服务预订信息、身份模式）免受未经授权的接入、篡改与破坏的功能。

(R-8) – NGN必须支持保护认证和授权所用消息和信息交换的保密性和完整性的功能。

(R-9) – NGN必须向防范认证和授权功能与能力受到攻击（如消息重放和拒绝提供业务的攻击）的功能提供保护。

(R-10) – NGN必须能够发现和记录未经授权的接入企图（如系统可设定一个未经授权接入的门限值，一旦该值被突破，管理系统就会得到由此产生的报警、纪录和报告）。

7.3.2 传统TE和TE-BE

支持传统TE和TE-BE网络接入的NAP，必须支持识别、认证和授权这类接入的功能。

(R-11) – 支持传统TE和TE-BE的网络接入点（NAP）必须支持专门为附着或连通NGN而识别固定线路的功能。二层地址可用于识别固定线路（如MAC或链路层地址）。这项功能可以作为[ITU-T Y.2012]确定的通用NACF的一部分提供。

(R-12) – 支持传统TE和TE-BE的NAP必须支持专门为附着或连通NGN而认证和授权固定线路的功能。访问控制列表（ACL）和传输层预订/用户资料可用于授权固定线路接入NGN。这项功能可以作为[ITU-T Y.2012]确定的通用NACF的一部分提供。

(R-13) – 支持传统TE和TE-BE的NAP必须支持使固定线路与NGN接入连接所用的IP地址相结合的功能。这项功能可以作为[ITU-T Y.2012]确定的通用NACF的一部分提供。

7.3.3 具有IAD的传统TE和TE-BE

支持具有客户域IAD的传统TE和TE-BE网络接入的NAP，必须支持识别、认证和授权这类接入的功能。

(R-14) – 支持具有客户域IAD的传统TE和TE-BE的NAP，必须支持为附着或连通NGN而专门识别固定线路和IAD的功能。二层地址可用于识别固定线路（如MAC或链路层地址）以及为IAD提供的IP地址。这项功能可以作为[ITU-T Y.2012]确定的通用网络NACF的一部分提供。

(R-15) – 支持具有客户域IAD的传统TE和TE-BE的NAP，必须支持为附着或连通NGN而认证和授权IAD的功能。只有经授权的IAD才能获得与NGN的连接或网络连通。访问控制列表（ACL）和传输层预订/用户资料，可用于授权IAD固定线路接入NGN。这项功能可以作为[ITU-T Y.2012]确定的通用网络NACF的一部分提供。

(R-16) – 支持具有客户域IAD的传统TE和TE-BE的NAP，必须支持使固定线路与IAD身份相结合的功能。这项功能可以作为[ITU-T Y.2012]确定的通用NACF的一部分提供。

7.3.4 NGN的TE和TE-BE

支持TE和TE-BE网络接入的NAP，必须支持识别、认证和授权这类接入的功能。

(R-17) – 支持NGN TE和TE-BE（如直接的IP连接）的NAP，必须支持为附着或连通NGN而专门识别其域内用户设备的功能。设备身份和网络地址（如设备身份、SIM卡、安全令牌、IP地址等）可专门确定NGN TE和TE-BE。

(R-18) – 支持NGN TE和TE-BE（如直接的IP连接）的NAP，必须支持为连接或连通NGN而认证和授权其域内用户设备的功能。认证和授权可以传输层预订/用户资料为依据。只有经授权的NGN TE和TE-BE才能获得与NGN的附着或网络连通。这项功能可以作为[ITU-T Y.2012]确定的通用NACF的一部分提供。

7.3.5 对绑定的用户和用户设备的认证和授权

根据对风险的评估, 可能需要对用户及用户设备组合进行认证和授权，以提供更高等级的身份确认。NGN可支持将NGN接入/附着与基于传输层（即用户设备和网络信息）和业务层（即预订/用户资料）信息的业务/应用接入的认证功能相结合的能力。

(R-19) – 有必要根据NGN提供商的策略，支持专门识别和整合用户和用户设备组合的功能。

(R-20) – 有必要根据NGN提供商的策略，支持用户和用户设备组合的功能。只有经授权的用户和用户设备才能获得附着/网络及业务/应用接入。

7.3.6 对绑定用户和用户设备的游牧性的认证和授权

可能向用户及用户设备组合的认证和授权提供支持，以提供更高等级的游牧性身份确认。在不同管理域（如NGN接入提供商、受访NGN提供商和归属NGN提供商）间交换和共享识别、认证和授权信息（如用户文档信息）的功能，也会得到支持（见第8.2.2款）。

(R-21) – 有必要根据NGN提供商的策略，支持专门确认用户和用户设备组合游牧性的功能。

(R-22) – 有必要根据NGN提供商的策略，支持认证和授权用户和用户设备组合游牧性的功能。在业务独立于用户设备的情况下，对固定线路、位置或接入地址等接入信息的认证，可与对用户的认证相结合，以提供更高等级的确认。

8 NGN业务提供商对用户业务/应用接入的认证和授权

8.1 说明

有必要掌握缓解未经授权接入NGN提供商提供的业务和特性带来的威胁的能力。有必要利用业务与功能的认证和授权功能，确定用户是否有权接受服务，或获准根据其特权采取行动。业务/应用的认证与授权被视为NGN提供商对用户的认证，也是对用户接受服务或根据其特权采取行动的授权。业务/应用的认证与授权可能包括以下的身份验证和特权授权：

- 用户
- 用户设备
- 用户和设备的组合

根据[ITU-T Y.2012]确定的NGN结构，将在业务层利用预订和用户资料支持业务/应用的认证和授权功能。

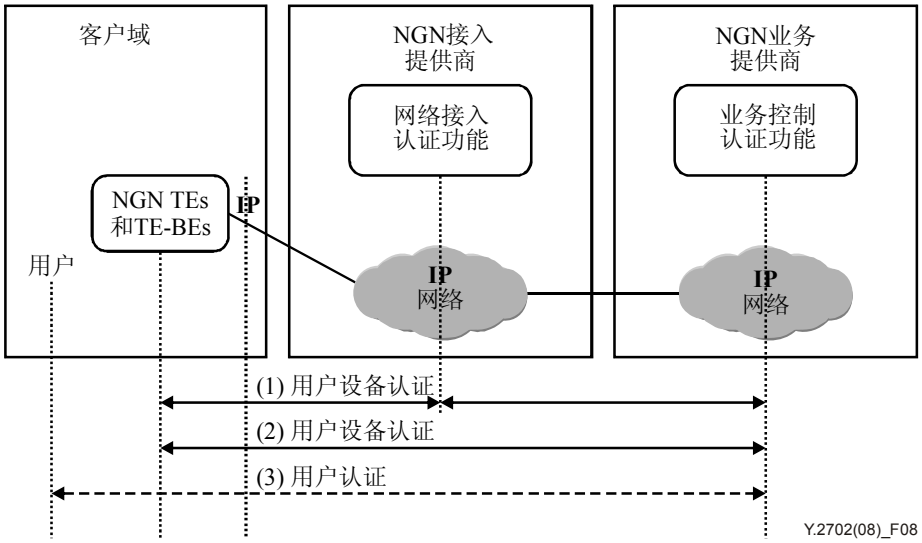


图8 – 业务/应用认证与授权的参考模型

图8介绍了业务/应用认证与授权在多网络提供商情况下的典型关系：

(1) 这一信息流代表NGN业务提供商依靠NGN接入提供商，通过信任关系认证用户设备。

(2) 这一信息流代表NGN业务提供商对用户设备的认证和授权。这种情况需要用户具有特殊的认证能力（如SIM）。

(3) 这一信息流代表NGN业务提供商对用户的认证（如用户登录并提供密码或PIN）。

8.2 要求

8.2.1 总体要求

以下是有关网络提供商对用户认证和授权的总体要求：

(R-23) – NGN必须能够支持根据预订和用户资料识别用户、用户设备以及用户和设备组合的能力。

(R-24) – NGN必须能够支持根据预订和用户资料认证和授权用户、用户设备以及用户和设备组合的能力。

(R-25) – 根据要求，NGN业务只能提供给经授权的用户、用户设备以及用户和设备组合。

(R-26) – NGN必须能够支持验证和授权用户特权的能力（如只允许其作用或特权得到授权的用户采取某些行动）。

(R-27) – 就多网络配置而言，每个管理域（如NGN接入提供商、受访NGN提供商和归属NGN提供商）都必须强化对用户、用户设备以及用户和设备组合的识别、认证和授权政策（即SLA）。

(R-28) – NGN必须支持保护认证和授权用户、用户设备以及用户和设备组合所用消息和信息交换的保密性和完整性的功能。

(R-29) – NGN必须支持保护业务认证和授权信息（如用户资料、服务预订信息）免受未经授权的接入、篡改与破坏的功能。

(R-30) – NGN必须向防范业务认证和授权功能与能力受到攻击（如消息重放和拒绝提供业务的攻击）的功能提供保护。

(R-31) – NGN必须根据NGN提供商的策略，支持将针对用户设备的接入网络技术与用户认证相结合的能力。

(R-32) – NGN必须能够发现和记录未经授权的接入NGN业务和资源的企图（如系统可设定一个未经授权接入的门限值，一旦该值被突破，管理系统就会得到由此产生的报警、纪录和报告）。

(R-33) – NGN必须能够发现和记录未经授权的特权使用企图（即未经授权的用户行为）。

8.2.2 IdM认证结果的共享

NGN提供商可能需要在其网络内部的不同业务和/或应用以及外部的其它NGN提供商之间交换认证结果，以便向身份管理（IdM）提供支持。这可能包括（但不限于）身份声明及与IdM相关的其它信息：

a) 信任策略；

b) 认证方法和认证所需的信息（如认证密钥）；

c) 确认等级；

d) 特权管理信息（如特权的分配或验证）。

认证结果（如身份声明）和其它上述信息的安全交换能力，将使NGN提供商能够利用有效和用户友好的认证和授权特性，设计业务/应用平台。例如，认证结果信息可在支持不同业务和/或应用的系统（如应用服务器）之间共享，使NGN提供商能够提供方便用户的“单点登录”特性与功能。以下要求适用于NGN提供商网络内部认证结果的交换与共享：

(R-34) – NGN必须能够稳妥地根据针对NGN提供商的业务/应用的设计和安全策略，向支持不同业务和/或应用交换及共享认证结果的信息（如身份声明、特权管理信息、信任策略和确认等级）提供支持。

(R-35) – 必须保护交换和共享认证结果的不同系统或网元（如应用服务器）免受未经授权的接入、监视、篡改与破坏（如使保密性和完整性受到保护）。这包括对所有存储信息的保护。

在多网络配置环境中，NGN提供商可能需要根据SLA相互安全地交换和共享认证结果。以下要求适用于不同NGN提供商之间的认证结果交换和共享：

(R-36) – 有必要支持使NGN提供商能够根据NGN提供商之间的信任关系、策略和SLA，安全地（如跨NNI和ANI）交换和共享认证结果的能力。

(R-37) – 必须保护NGN提供商之间交换和共享IdM认证结果的通信（如跨NNI和ANI）免受未经授权的接入、监视、篡改与破坏（即使保密性和完整性受到保护）。这包括对所有存储信息的保护。具体的安全机制和安全作法将基于NGN提供商之间的信任关系、策略和SLA。

(R-38) – 有必要支持可证明认证方法的能力，并向依赖凭证方通报以下有关认证实体所用方法的信息：

- 用户身份验证方法；
- 认证方法（使用数字证书、签名、安全令牌、生物辨识数据、SIM等）；
- 信任策略；
- 认证确认等级。

认证信息和结果的共享，须遵守保护个人可识别信息（PII）的国家和区域规则和立法等相关政策。

(R-39) – NGN提供商须确保保护个人可识别信息（PII）的国家和区域规则和立法等相关政策得到遵守。这包括根据以下基本数据保护原则制定的政策：

- 为具体目的整合数据；
- 目的不同的应用之间不共享数据；
- 将数据限制在达到一具体目的所需的最低限度；

- 个人对其PII具有支配权。

8.2.3 NGN业务提供商对用户接入具体业务/应用的认证和授权

NGN提供商有必要对以下用户的接入特权（包括用户采取行动的身份和特权）进行管理：

- 语音业务
- 流媒体业务
- 数据和短信业务
- 应急通信业务（ETS）和救灾通信（TDR）

每项业务都可能有各自的确认等级要求，可根据可能出现未经授权的实体获得业务资源的风险，验证用户、用户设备以及用户和设备组合的特权。应根据NGN的安全策略，对具体业务确定和实施认证和验证用户、用户设备以及用户和设备组合特权所需等级的确认。这包括支持和使用各种基本的认证方法，既有采用密码和个人身份号码（PIN）的基本认证方法，也有以下更为严格的方法：

a) 数字证书（如 X.509 PKI）

b) 安全令牌（硬件和软件令牌）和智能卡

c) 行为特征数据（如击键分析）

d) 生物特征辨识数据（如语音识别、指纹、虹膜或视网膜识别）

注 – 对实体进行认证的目的不在于说明某人的认证合格。

在认证和授权过程中还要考虑到用户的易用性，对于ETS和TDR等某些类型的业务尤其如此。认证程序最好做到用户友好。有关ETS认证和授权的实例，见附录II提供的信息。

在考虑使用针对业务的认证和授权时，可采用8.2.1和8.2.2款以外的以下附加要求：

(R-40) – 有必要根据NGN提供商的策略支持对证书的认证方法。根据NGN提供商的身份和特权确认策略，有必要酌情支持和使用多因素认证方法。

(R-41) – 必须能够根据NGN提供商的策略，专门确定所有与预订一应用服务相关的用户。这包括确定集合最终用户，但其身份不一定提供给NGN提供商。[2]

(R-42) – 必须能够根据NGN提供商的策略，将一定数量的用户与同一预订相捆绑。

(R-43) – 为通信目的，每位与一应用业务预订相关的用户/预订者，都必须具有可单独确认的地址。

---

2 集合端点将具有两个或更多与之相关的集合用户。可能只有集合端点了解这些用户的身份，而NGN提供商并不知情。

(R-44) – 根据NGN提供商的策略，必须能够使最终用户多次和/或从多种设备同时接入业务。

(R-45) – 必须能够支持个体最终用户的多个预订资料，而这些资料必须具有单独的可识别性。

根据NGN提供商的策略，可能需要进行定期认证，以提供高度的保障与安全。

(R-46) – 根据NGN提供商的策略，必须能够在已建立的通信会话或交易期间，定期对用户（如最终用户、网员或对象）进行再认证。

9 用户对NGN提供商的认证与授权

本款提出的要求涉及用户对网络的认证和授权（即用户对连接的NGN网络或业务提供商的身份进行认证）。

9.1 说明

NGN的架构使最终用户能够从多个NGN提供商获得业务。此外，NGN传输提供商（如NGN接入提供商）可能并不同时又是NGN业务提供商。因此，最终用户可能需要验证NGN提供商的身份（如接入、传输还是业务提供商）。具体而言，需要向以下几个方面提供支持：

- 使最终用户能够识别、认证和授权进行网络连接（即网络接入）的NGN接入提供商
- 使最终用户能够识别、认证和授权NGN业务提供商

9.2 目标和要求

9.2.1 NGN提供商网络附着的用户认证

支持NGN TE和TE-BE网络接入的网络接入点应能够支持用户确定、认证和授权网络附着的功能。

(R-47) – 支持NGN TE和TE-BE的网络接入点（NPA）（即直接IP连接）应能够根据安全政策的需要，支持最终用户确定独特的NGN提供商网络附着和连接功能。

(R-48) – 支持NGN TE和TE-BE的网络接入点（NPA）（即直接IP连接）应能够根据安全政策的需要，支持用户对NGN提供商网络附着和连接进行认证和授权的功能。可以按照[ITU-T Y.2012]的定义，将这些功能作为网络总体附着控制功能（NACF）的一部分加以提供。

(R-49) – 在多网络安排中，每一个行政域（即网络接入提供商、受访NGN提供商和归属NGN提供商）都需要（通过使用SLA等）执行有关网络附着确认、认证和授权的政策（如信任关系）。

9.2.2 用户为获得服务而进行的NGN提供商认证

可以为最终用户提供对NGN提供商进行认证和授权、以获得NGN服务的功能。

(R-50) – NGN应根据安全政策的需要，具有支持最终用户确定独特的提供一种服务或一套服务的NGN提供商的功能。

(R-51) – NGN应根据安全政策的需要，具有支持最终用户对提供一种或一套服务的NGN提供商进行认证和授权的功能。

10 NGN提供商支持的用户对等认证和授权

本节内容旨在使全文内容更加完整并提供参考信息。

由于流量只通过NGN网络提供商的传输层，因此对等通信对NGN提供商而言是透明的。应当指出，NGN提供商可以在这种通信情况下发挥IdP作用，提供IdM服务（如对等认证功能）。

11 人工网络认证和授权

11.1 描述

为减少未经授权的网络接入的威胁，有必要进行人工网络认证和授权。需要通过网络接入认证和授权服务来确认身份并决定是否给予网络传输接入、和/或提供服务和功能。网络接入可在NNI或ANI上进行。

图9具体说明包含下列安全域的人工网络认证和授权参考模型：

1) 接入网域：由接入网提供商托管的接入网（如窄带、xDSL和有线网络）。接入网提供商可以是或不是同一个NGN提供商。接入网提供商和NGN提供商之间的信任关系受服务水平协议（SLA）的约束。

2) 受访NGN域：由受访网络提供商托管的NGN，为其它NGN网络提供商（即归属网络提供商）提供受访网络功能。信任关系受服务水平协议（SLA）的约束。受访网络可以提供NGN服务并可以拥有自己的订购服务用户。此外，受访网络还可以与第3方应用服务提供商达成协议，并通过经转网与归属网进行连接，其信任关系受SLA约束。

3) 归属网域：由归属网提供商托管的NGN，归属网向其订购服务用户提供NGN服务。此外，归属网可以与通过ANI提供应用服务的第3方提供商达成协议。受访和归属网提供商（包括第3方提供商）之间的信任关系受服务水平协议（SLA）约束，同时，归属网可以通过经转网与受访网或其它网络进行连接，其信任关系受SLA约束。

4) 经转网域：NGN只提供经转服务，传输和相邻网（包括第3方提供商）之间的信任关系受服务水平协议（SLA）约束。

5) 其它网域：NGN或非NGN提供商。信任关系受服务水平协议（SLA）约束。

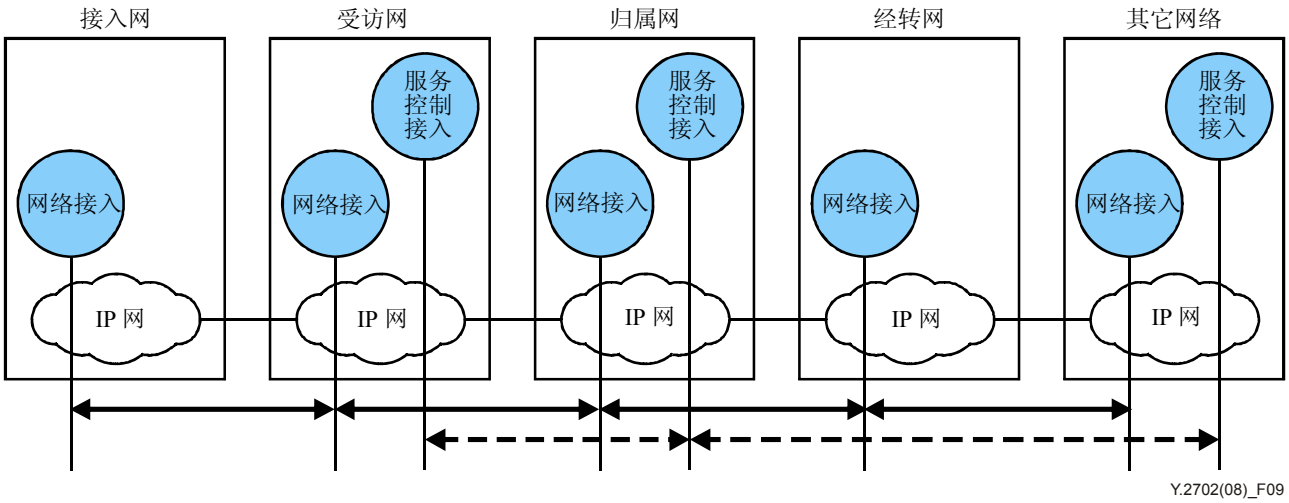


图9 – 人工网络认证

11.1.1 传输层认证

如图9所示，传输层认证逐段（hop-by-hop）进行，认证总是在传输层面与相邻网进行，这就意味着，归属网并非需要与图中所示的其它网络达成SLA协议，而是在归属网和经转网之间在传输层面建立关系，然后在经转网和其它网络之间建立关系。

11.1.2 服务/应用层认证

如图9所示，服务/应用层认证是受访、归属和其它网络在对等服务/应用层面的服务控制层的直接认证。该对等关系是一种逻辑而非物理关系。从一个网络的服务控制到网络接入之间的物理路径为纵向路径，然后直接或通过经转网进行传输，最后在对等服务/应用网络中从网络到服务控制接入进行纵向传输。

11.2 人工网络认证要求

(R-52) – 要求NGN在传输层提供支持独特确认相邻网络的功能。

(R-53) – 要求NGN在传输层提供支持对相邻网络的接入进行认证和授权的功能。

(R-54) – 要求NGN在服务层提供支持独特确认相邻网络的功能。

(R-55) – 要求NGN在服务层提供支持对相邻网络的接入进行认证和授权的功能。

(R-56) – 要求每一个NGN提供商均执行有关人工网络确认、认证和授权的政策（如使用SLA和信任关系）

(R-57) – 在网间通信方面，要求能够通过网元识别符与相关互连的NGN提供商识别符之间的相互关系独特确认所涉及到的网元。

(R-58) – 要求NGN具有支持防止非授权接入、操纵和破坏人工网络认证和授权信息的功能。

(R-59) – 要求NGN具有支持防止对人工认证和授权功能及能力进行攻击（如重播消息和拒绝服务攻击）的功能。

(R-60) – 要求NGN能够发现并记录其它网络试图进行的非授权接入（如，可以在系统上设定非授权接入企图的次数门限值，超过该限值时则发出告警、进行记录并向管理系统做出报告）。

为保证网络更加安全，根据NGN提供商的政策，可能有必要定期对相邻NGN提供商进行认证。

(R-61) – 根据NGN提供商的政策，在已建立的通信会话或交易过程中，要求能够定期对互连的NGN提供商重新进行认证。

12 NGN提供商对第3方服务/应用提供商的认证和授权

12.1 描述

在有些情况下，应用或服务提供商并非NGN提供商（即他们是第3方服务/应用提供商），在这种情况下，NGN提供商需要按照图11对第3方服务/应用提供商进行认证和授权。

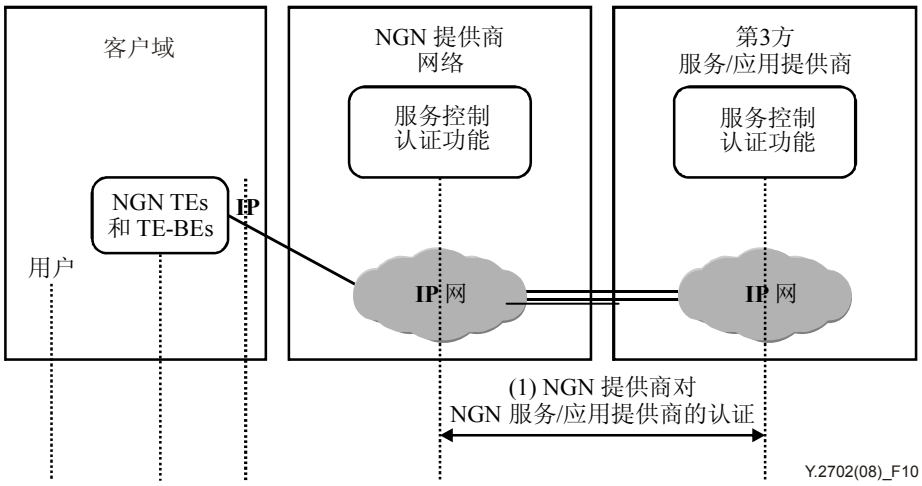


图10 – 第3方服务/应用提供商的认证和授权

应当指出，图10和下述案文未涵盖前几节所述的用户和网络认证。

12.2 要求

(R-62) – 要求第3方服务/应用提供商支持向NGN服务提供商确认自己身份的功能。

(R-63) – 要求第3方服务/应用提供商支持向用户确认自己身份的功能。

(R-64) – 要求NGN支持独特确认第3方服务/应用提供商的功能。

(R-65) – 要求NGN支持对第3方服务/应用提供商进行认证和授权的功能。

(R-66) – 要求NGN提供商和第3方服务/应用提供商执行有关确认、认证和授权的政策（如使用SLA和信任关系）。

(R-67) – 要求NGN和第3方服务/应用提供商支持防止非授权接入、操纵和破坏认证和授权信息的功能。

(R-68) – 要求NGN和第3方服务/应用提供商支持防止对认证和授权功能和能力进行攻击（如消息重播和拒绝服务攻击）的功能。

(R-69) – 要求NGN能够发现和记录第3方服务/应用提供商试图进行的非授权接入（如，可以在系统上设定非授权接入企图的次数门限值，超过该限值时则发出告警、进行记录并向管理系统做出报告）。

为保证网络更加安全，根据NGN提供商的政策，可能有必要定期对第3方服务/应用提供商进行认证。

(R-70) – 根据NGN提供商的政策，在已建立的通信会话或交易过程中，要求能够定期对第3方服务/应用提供商重新进行认证。

13 第3方认证和授权服务的使用

13.1 描述

第3方认证和授权服务提供商可以提供：

- 用户到服务提供商的认证；
- 服务提供商到用户的认证；
- 服务提供商之间的认证；
- 由用户或服务提供商进行的服务/应用提供商认证。

在此方面，如果使用第3方认证服务提供商，则至少涉及三个实体。除第3方认证服务提供商应要求履行其认证服务职能外，还要求其对要求提出方和被要求方进行自身认证。

13.2 要求

适用第12.2段所述的要求。

14 对象的认证和授权

14.1 描述

除对用户、用户装置和服务提供商进行认证和授权外，还需要对对象进行总体认证，其中包括物理对象（如网元或系统）及以下虚拟对象：

- 应用；
- 应用程序；
- 软件程序；

- 信令、管理和承载消息及数据内容。

14.2 要求

(R-71) – 根据NGN提供商的政策，要求NGN提供支持独特确认对象的功能。

(R-72) – 根据NGN提供商的政策，要求NGN提供支持对对象进行认证和授权的功能。

(R-73) – 要求NGN提供支持对对象特权进行验证和授权的功能（例如，只有当对象的作用或特权得到授权时才允许其采取行动或履行程序）。

(R-74) – 要求NGN提供商执行有关对象确认、认证和授权的政策。

(R-75) – 要求NGN支持有关保护消息和信息交流（用于对象认证和授权）保密性和完整性的功能。

(R-76) – 要求NGN支持有关保护对象认证和授权信息免受非授权接入、操纵和破坏的功能。

(R-77) – 要求NGN支持有关保护对象认证和授权功能和能力免受攻击（如消息重播和拒绝服务攻击）的功能。

(R-78) – 要求NGN能够发现和记录对象试图进行的非授权接入（如，可以在系统上设定非授权接入企图的次数门限值，超过该限值时则发出告警、进行记录并向管理系统做出报告）。

(R-79) – 要求NGN能够发现和记录有关获得非授权特权的企图（如未经授权的用户行动）。

为保证网络更加安全，根据NGN提供商的政策，可能有必要定期对相邻NGN提供商进行认证。

(R-80) – 根据NGN提供商的政策，在已建立的相关通信会话或交易过程中，要求能够定期对关联对象重新进行认证。

附录 I

安全断定标识语言使用案例

（本附录不构成本建议书的组成部分）

I.1 ［B-ITU-T X.1141］安全断定标识语言（SAML 2.0）的使用

本附件以使用示例说明在支持服务/应用认证中单独使用SAML的同时，如何对认证结果进行传送。

I.2 服务/应用认证程序

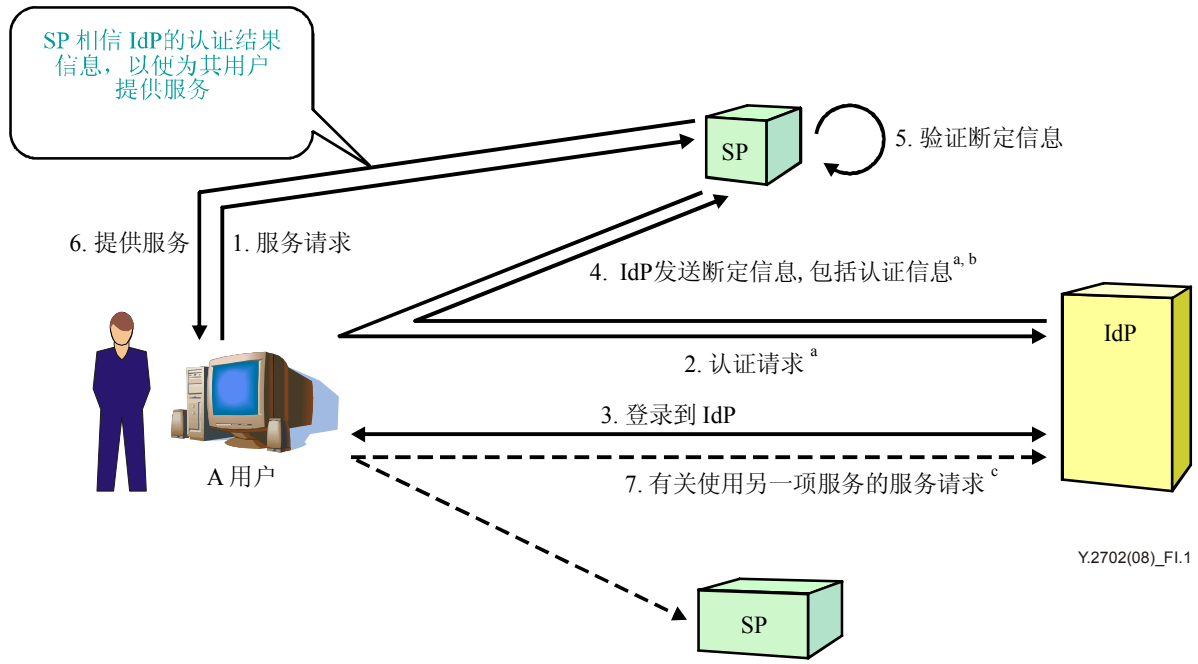
当需要在相互信任的服务和/或应用（可能是第3方提供商的服务/应用）之间交换认证结果时，可以使用安全断定标识语言（SAML 2.0）。SAML 2.0是推进结构化信息标准发展组织（OASIS）制定的开放性规范，可具体用于下列情况：

– 单点登录：为方便用户，不同的服务和应用在无须交换所有用户信息的情况下，允许用户进行单点登录。

– 账户联合：不同服务和应用将同一用户的账户联合一体。

I.3 服务/应用认证 – 呼叫流程示例

图I.1以典型示例说明使用SAML 2.0的、账户联合单点登录。



a) 2 和 4 是通过用户代理(如万维网浏览器)的、已经完成的通信（如HTTP重发)。

b) 必要时，断定信息可包括属性信息和授权决定。

c) 同1至6,不包括到IdP的登录。（换言之，用户只需登录一次IdP即可得到认证）。

图I.1 – 使用SAML 2.0的SSO呼叫流程示例

[b-ITU-T X.1141]-对图I.1所示的术语定义如下：

- 身份提供商（IdP）

  在联合体中为主要方面（principal）创建、维护和管理身份信息、并为其它服务提供商提供主认证的服务提供商（如采用万维网浏览器资料）。

- 服务提供商

  系统实体为主要方面或其它系统实体提供服务时发挥的作用。

- 断定。

  SAML机构就主体（subject）、有关主体属性信息的认证行为、或适用于主体的就特定资源的授权数据产生的相关数据。

I.4 服务/应用认证程序和机制的安全性

为保护安全和隐私，SAML2.0本身具有匿名联合和化名等功能特性。匿名联合为服务提供商提供瞬间的名称ID，化名则方便用户在单点登录时向服务提供商表明身份，即，使用成对的化名来保护隐私，同时有助于与用户保持长久的关系。SAML 2.0还能够实现对属性声明、名称标识符或整体断定信息的加密，该功能特性确保在必要时实现这些元素的、端到端地保密性。

附录 II

ETS认证和授权

（本附录不构成本建议书的组成部分）

II.1 概述

各国已经或正在开发应急通信服务（ETS）。从定义上而言，落实ETS是一国的国内事务，然而，灾害/紧急情况往往跨越地理国界，因此，相关国家/主管部门可能需要通过双边和/或多边协议来将各自的ETS系统连接一起。[b-ITU-T E.107]提供的指导意见将有助于一国落实的ETS（ENI）与其它ENI进行通信。

要求NGN提供商只允许经授权的ETS用户进行接入，必须避免未经授权的用户（如假冒经授权的用户的入侵者）的接入，因此，按照相关政策[3]和具体服务（如话音、数据、视频）的安全保障水平提供对ETS用户、装置或用户及装置进行接入认证和授权的机制和功能，对于ETS的安全极为重要。

在实现ETS国内落实的互连中，NGN提供商必须相互依赖，通过服务水平协议对ETS用户进行认证和授权。在此方面可以采用多种方式方法，本附录以具体示例说明ETS的认证和授权方式，其中包括一些呼叫流程示例。

II.2 ETS用户的认证和授权

如何对ETS用户进行认证和授权是一国的国内事务。通常而言，NGN提供商根据登记/注册方法以及服务启动形式，对用户的ETS呼叫/会话请求进行认证和授权。认证可以按每个呼叫/会话进行，也可以按照ETS用户目前的接入地位进行一次性（一定时间的）认证，或在订购使用基础上进行认证。NGN提供商应在呼叫/会话建立过程的初期对得到授权的应急通信用户尽快进行认证。须按照适用的政策（如个人身份识别码（PIN）的使用、用户和订购资料）采用具体的认证和授权机制及方法。一旦按照适用的政策对用户、用户装置或用户及装置进行了认证和授权，则ETS呼叫/会话得到相应标识和说明，并向前传向随后的网络，同时标出ETS用户的优先等级（可选功能）。此外，一旦完成认证和授权，ETS呼叫/会话、信令/控制、承载流量以及任何适用的管理等各方面均获得优先地位。

有关ETS认证和授权的方式方法示例包括：

a) 使用个人身份识别码（PIN）：该方法利用PIN对用户进行认证和授权。我们利用该方法确认用户，不确认装置，因此，通常用于用户可从任何装置启动ETS服务的情况。

b) 使用订购/服务资料：此方法提供说明ETS订购使用的用户终端服务资料，它对用户终端进行认证并将用户服务资料确定为NGN提供商（即ETS提供商）普通注册程序的一个组成部分。当用户提出请求时，按照用户的服务资料进行查验，以确定是否已授权该用户使用ETS。如果证实用户终端对ETS的订购使用有效，则授予其使用ETS的权利。

---

[3] 注 – 政策在此包括所有适用的政策，如NGN提供商、监管和政府法规和规则。

c) 合并使用PIN和服务资料：可合并使用PIN和服务资料这种方法来对用户以及用户装置进行认证，以提高安全保障水平。

d) 使用特殊的安全令牌和生物特征：除上述方法以外，还可以使用更为复杂的、采用特殊安全令牌和生物特征等功能的方法来对ETS用户进行认证和授权，以提高身份的安全保障水平。

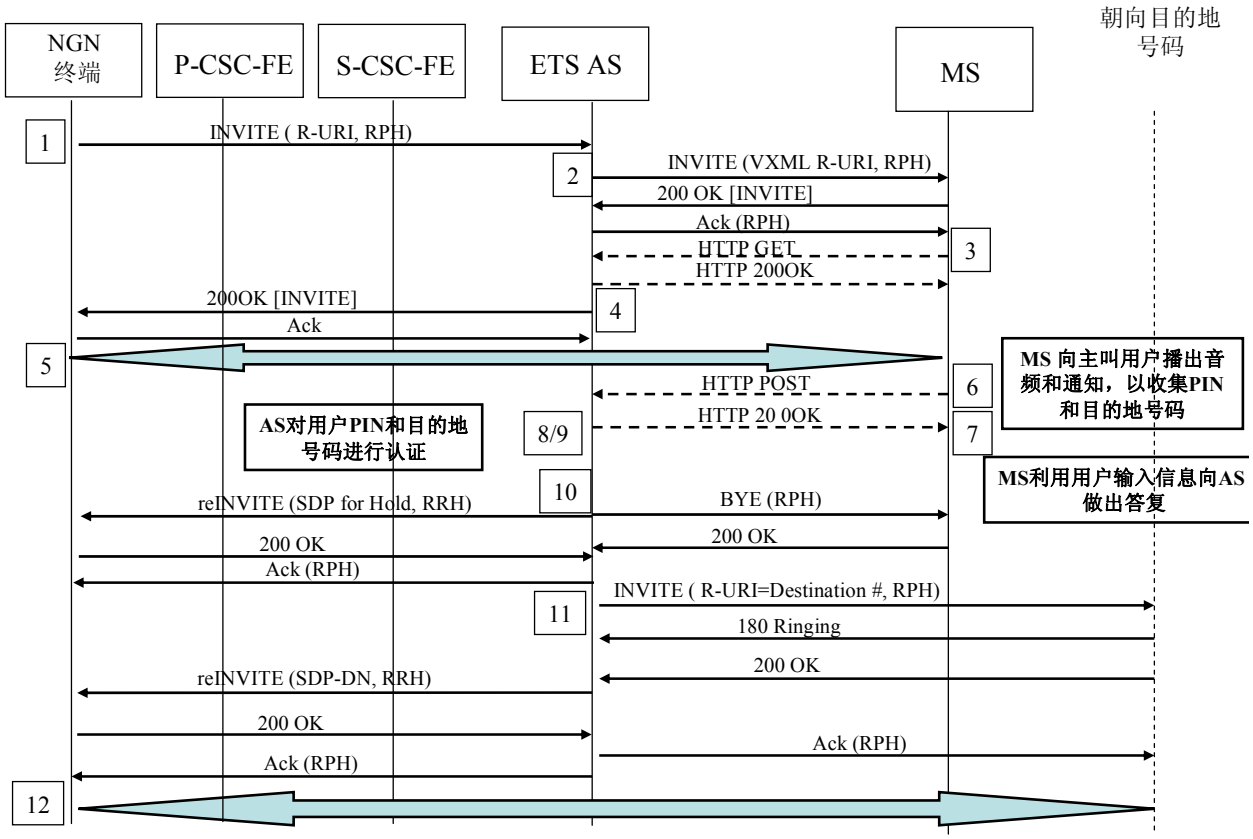
II.3 对NGN提供商使用ETS进行认证和授权

由于在现实环境中存在多家提供商，且服务控制和传输相互分离，因此必须考虑对NGN提供商之间ETS流量的切换和接收进行认证和授权，同时，按照SLA和适用的政策，对NGN提供商的ETS呼叫/会话和流量的切换和接收进行认证和授权，这对于ETS的安全性亦十分重要。

II.4 ETS认证和授权使用示例

II.4.1 以基本PIN为基础的认证和授权使用示例

图II.1以具体示例说明采用个人身份识别码（PIN）的、基本ETS认证和授权。



图II.1 – PIN认证和授权

该示例假设ETS用户向ETS号码提出呼叫/会话请求来请求/发起ETS呼叫/会话。此外，所有SIP请求均包括资源优先字头（RPH）[b-IETF RFC 4412]，说明需要进行优先处理。

1) 呼叫/会话被路由到发起用户认证程序的ETS应用服务器（AS）。

2) ETS AS向选定的媒介服务器（MS）发送INVITE消息，并附带与主叫相关的SDP要约。INVITE消息包括存储于ETS AS中的话音XML脚本的URL。脚本旨在说明MS如何与主叫进行互动（播出何种通知，如何收集数字（digit），收集多少数字以及数字间的定时符等）。

3) MS一旦收到INVITE消息，则可以：

- 向ETS AS发送一个100尝试（100Trying）；
- 利用HTTP和INVITE消息中的URL，直接从ETS AS检索话音XML脚本（MS向AS发送HTTP GET，然后话音XML脚本在HTTP 200 OK中由ETS AS返回）；
- 证实脚本；
- 制定并向ETS AS发送包含其自身SDP的200 OK消息。

4) ETS AS向主叫方（NGN终端）发送200 OK，其中包括收自MS的会话信息。

5) 此时已实现MS与主叫方之间的媒介连接。

6) MS一旦收到HTTP 200 OK中的ACK和VXML脚本，则开始执行话音XML脚本。MS播放音频并收集主叫方输入的数字（PIN）。

7) 之后MS采用HTTP POST消息直接向ETS AS发送收集到的数字。

8) ETS AS一经收到所收集的数字，则开始验证所收到的数字（PIN）是否有效。

- 如果收到的数字无效（收到的数字的数量不符或号码错误），则ETS AS确定需要与主叫进一步进行互动。ETS AS通过新的话音XML脚本向MS返回一条HTTP 200 OK消息，ETS AS将就最终的处理方法做出指示。
- 如果收到的数字有效，则ETS AS指示MS播出收集数字（目的地号码）的通知。

9) ETS AS确定主叫方输入的目的地号码有效。

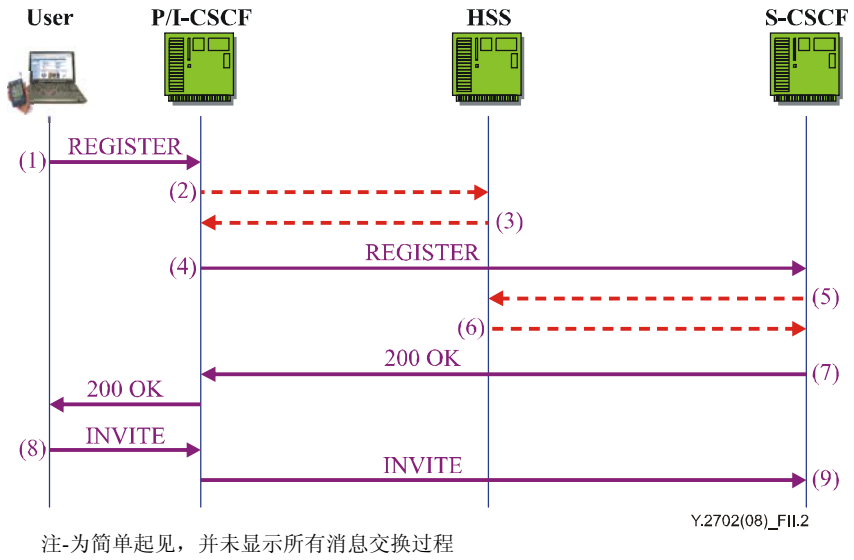
10) ETS AS通过SIP BYE将MS从呼叫/会话中解除出来，并向主叫方发送reINVITE，同时利用SDP保持媒介的连接状态。

11) ETS AS向目的地方发送INVITE，ETS AS一旦收到200 OK（应答），则向主叫方发送带有与目的地相关的SDP的reINVITE。

12) 主叫方和目的地号码之间建立起媒介路径，呼叫控制路径中含有认证ETS AS。

II.4.2 订购使用/服务资料认证和授权示例

图II.2以具体示例说明采用订购使用/服务资料进行ETS认证和授权的情况。



注-为简单起见，并未显示所有消息交换过程

图II.2 – 基于订购使用的示例

该示例依靠与用户装置相关联的订购使用/服务资料。通常由网络进行用户装置的注册和认证。当用户发起ETS呼叫/会话时，对服务/订购使用资料进行检查，以确定是否已授权

用户装置进行ETS呼叫/会话。呼叫流程如下：

1) 注册发起

2) P/I-CSCF向HSS进行查询

3) HSS验证用户的订购使用情况并提供S-CSCF的身份

4) P/I-CSCF向S-CSCF发送注册消息

5) S-CSCF向HSS进行查询

6) HSS提供用户服务资料信息（可能需要与AS进行互动）

7) S-CSCF发送200 OK

8) 用户发起ETS会话

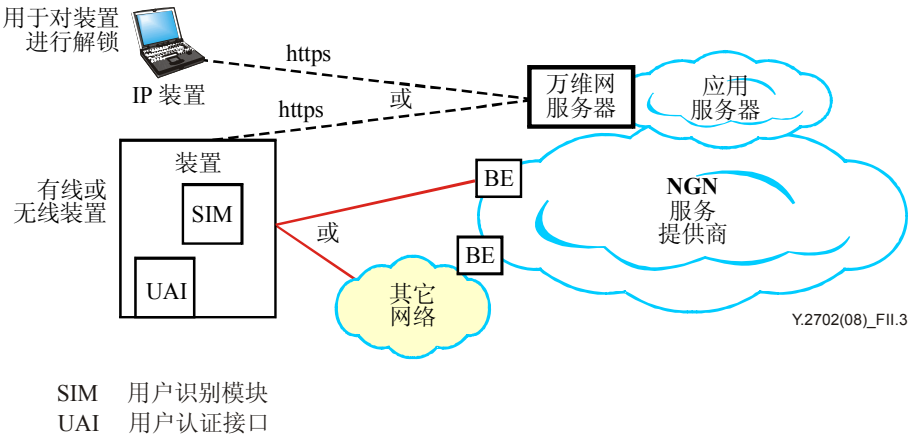
9) S-CSCF检查服务资料，以确定是否对ETS会话进行授权。

II.4.3 用户及装置认证和授权示例

图II.3的具体示例涉及附着于网络的、带有SIM卡的用户装置（采用标准的3GPP通用引导（bootstrap）认证（GBA））。

在该示例中，装置带有用户认证接口（UAI），方便用户在服务提供商网络的应用层中通过装置提供认证信息。最简单的UAI可以是键盘，最复杂的UAI可以采用生物特征。

在此假设信令和媒介之间存在安全通信。



图II.3 – ETS用户认证和授权

呼叫/会话流程：

1) 打开用户装置。

2) 装置使用3GPP GBA紧紧附着于网络。

3) ETS用户利用装置上的SIM通过UAI发起局部认证。UAI可以是键盘（通过该键盘输入PIN），抑或是某种生物特征。

   a) SIM对ETS用户进行认证并提供成功指示符。SIM通知ETS应用服务器已对ETS用户进行认证。

   b) 反过来，可以将信息安全传递至服务提供商网络的应用层。

4) 此时，“正常”用户和装置获得网络的认证。发挥ETS用户作用的用户已由ETS AS认证。

如果用户经过x次试验后无法得到局部认证，则该用户被锁定在装置之外。为装置解锁的一种方式是用户通过AS/WS接口接入GUI，并输入需进行验证的PIN。如果用户身份得到验证，则AS/WS可向装置发出消息，指示装置进行解锁。

II.4.4 在企业所在地进行使用的示例

ETS呼叫可以起始或终接于政府企业所在地，典型部署如下：

- 政府所在地和服务提供商之间具有专门设施。
- 用户在企业所在地而非与服务提供商进行注册。
- 企业所在地与路由器工具（wildcard）进行注册，或服务提供商网络边缘的IWF（如SBC）代表企业进行代理注册。

因此，如果需要基于PIN的认证以外的认证，则需要完成附加功能，其中包括但不局限于：

- 企业向服务提供商公布用户的存在，该数据将提高认证的安全保障。
- 由企业向服务提供商传递安全令牌，并在2/3层将此确定为潜在的ETS呼叫/会话（如RSVP中的安全令牌扩展）。

根据用户情况，可能需要确保对来自多种途径的数据进行认证。

附录 III

3GPP通用引导架构

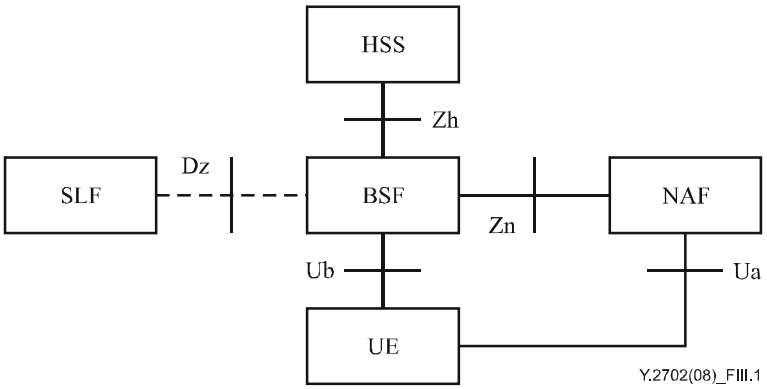
（本附录不构成本建议书的组成部分）

通用引导架构（GBA）具体规定与接入无关的引导程序。该程序提供最终用户和网络应用功能（NAF）之间的相互认证框架。

GBA是由三个部分组成的认证系统：

- 利用用户设备（UE）试图获得网络服务的最终用户
- 应用服务器（被叫网络应用功能或NAF）
- 参与其它两个实体认证和密钥交换的的受信任实体（被叫引导服务器功能或BSF）。

下述参考模型及内容具体说明GBA认证程序的基本原理。



图III.1 – [b-ETSI TS 133 220]所述的引导架构简单网络模型

GBA程序的基本步骤如下：

1) NAF在Ua参考点上请求认证并商谈GBA的使用。

2) 在UE上运行的BSF客户机在Ub参考点上发起引导程序。BSF通过Zh从HSS获取认证信息和GBA用户安全设置信息。UE和BSF使用HTTP Digest AKA进行相互认证。通过这一程序，UE接收来自BSF的引导交易识别符（B-TID），并在UE和BSF之间建立共享密钥（Ks）。

3) UE从Ks衍生出Ks_NAF，并向NAF发送B-TID（以及针对应用的数据）。

4) NAF通过Zn参考点向BSF发送B-TID。

5) 基于B-TID的BSF确定应使用的Ks，并从Ks衍生出Ks_NAF，然后将其发送至NAF。

6) 最后，UE和NAF可使用共享密钥Ks_NAF进行相互认证。确切的认证程序取决于UE和NAF之间的协议。例如，GBA规定，基于HTTP的应用可以使用HTTP Digest认证[b-IETF RFC2617] 或TLS预共享密钥加密套件[b-IETF RFC4279]。

注 – BSF 通过 Dz 参考点向 SLF 进行询问，以获得包含具体订购用户数据的 HSS 的名称。当 BSF 被配置为使用预定义 HSS 时，则不需要 SLF。

将 GBA 实体映射到[ITU-T Y.2012] 规定的 NGN 实体中。

- NAF – 对应［ITU-T Y.2012］图3中的应用实体。
- BSF – 可以包括在T-11认证和授权FE中，也就是说可以通过BSF服务器的功能提高和启动T-11。
- HSS对应S-5服务用户资料FE
- SLF对应S-4订购使用定位FE
- UE对应最终用户功能

附录 IV

身份管理（IdM）呼叫流程示例

（本附录不构成本建议书的组成部分）

IV.1 概述

本附录的实例流程来自[b-TR 33.980] 。

流程详细说明安全断定标识语言v2.0（SAML v2.0）（或自由联盟身份联合框架-ID-FF）、身份万维网服务框架（ID-WSF）、安全断定标识语言（SAML）与GAA中被称作通用引导架构（GBA）部分的互通方法。本附录旨在提供信息，且只适用于ID-WSF与GBA或SAMLv2.0与GBA合并使用的情况。

IV.2 呼叫流程示例

这些流程只适用于自由联盟与GBA或SAML v2.0与GBA合并使用的情况。

IV.2.1 SSO情景：带有<lib:AuthnResponse>传送的ID-FF

IV.2.1.1 采用传统TLS的HTTP

在这种情形中，UE对LAP毫无意识，所有协议元素均源于ID联合框架[b-ID-FF]并得到[b-TS 33.222]中针对具体GAA的细节的补充。首先概要说明根据[b-TS 33.222]第5.3段采用HTTP部署传统TLS[b-IETF RFC 2246] 所需的步骤：

1) UE 发送 HTTP 请求，与 SP 取得联系，希望获得 SP 提供的服务。该请求包含基于 GBA 的认证支持指示（参见步骤 3），因为根据步骤 3 重发请求时需要这一信息。

2) SP 在收到 UE 发出的 HTTP 请求时，即获得了身份提供商的地址，并向 UE 发出带有 <lib:AuthnRequest>的重发 HTTP 答复。获得身份提供商地址的手段取决于实施情况并由服务提供商决定。

3) UE 按照地点字头字段中给出的 URL 与 IdP 进行联系，且必须通过带有 <lib:AuthnRequest>信息[b-ID-FF 绑定]的 HTTP 请求访问 NAF/IdP URL。

   UE 在“用户代理”HTTP 字头上增加恒定串（作为[b-IETF RFC 2616]规定的产品标识），向 NAF/IdP 说明支持基于 GBA 的认证。应根据[b-TS 33.222]的步骤 2 第 5.3 段，设定上述恒定串。

   如果 UE 和 IdP 之间存在引导安全关联性，则 UE 和 IdP/NAF 共享密钥，以保护 Ua 参考点，且 UE 具有所有的按照此前消息进行 HTTP Digest 认证的数据。在这种情况下，步骤 3 与步骤 5 中的请求合并，并省略步骤 4。

4) 由于 IdP 与 NAF 共置一地，因此应按照[b-TS 33.222]进行 HTTP Digest 认证，并向 UE 发送带有非授权状态和 WWW-认证字头字段的 HTTP 答复。[b-TS 33.222]具体规定了该方法以及上述认证细节，但[b-ID-FF]中没有这些内容。

   如果 UE 未包括有效的引导会话，或 IdP 认为其密钥资料不够新鲜，则 UE 将与 BSF 执行一项新的引导程序，且该程序对 SP 是透明的。

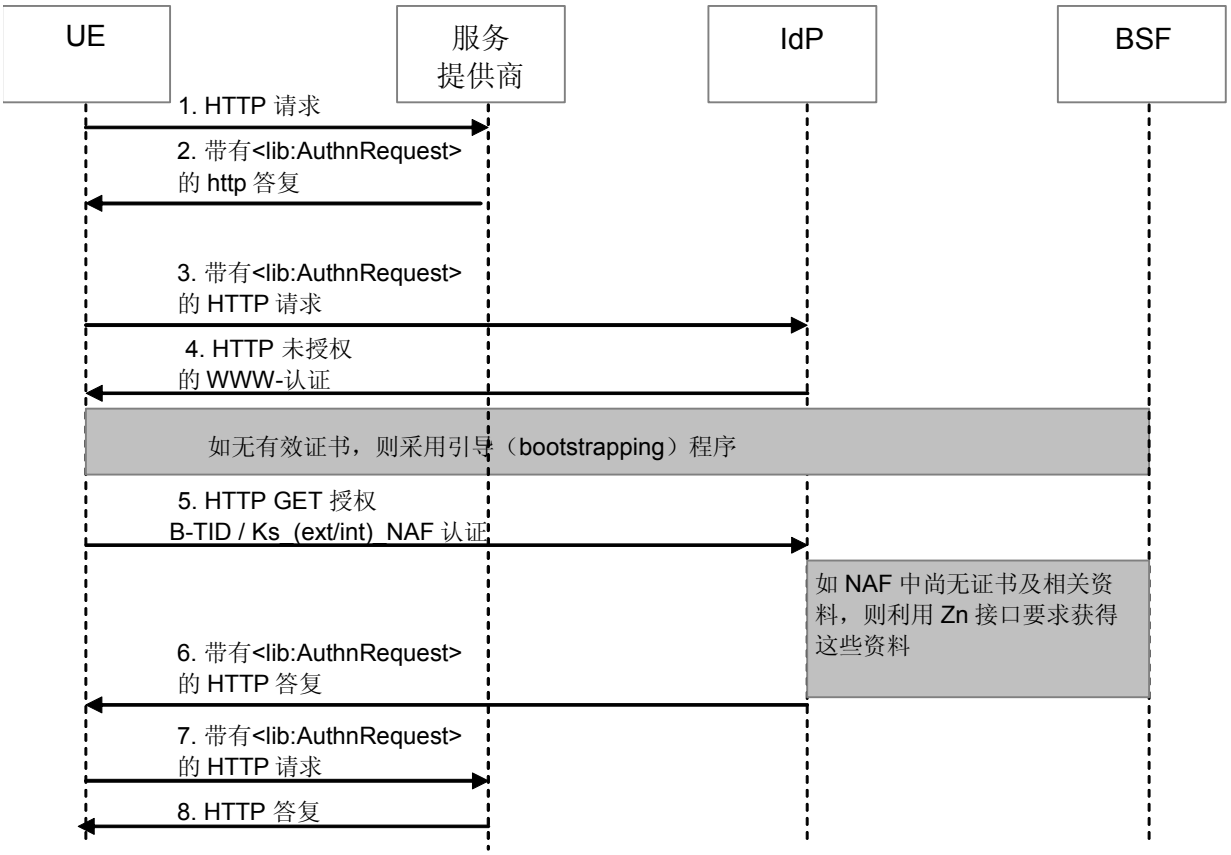
5) UE 利用 B-TID 这一用户名和 Ks_（ext/int）_NAF 这一密码向 IdP 返回授权数据，UE 可以包含更多的与 LAP 有关的用户数据。

如果 IdP 与 NAF 共置一地，则情形为[b-TS 33.222]说明的情形。USS 可以包含具体针对自由（Liberty）的信息。

6) <lib:AuthnRequest>得到处理。IdP 在 HTTP 答复重发 URL[b-ID-FF 绑定]中通过 <lib:AuthnResponse>做出答复，IdP 可以包含更多的与 LAP 有关的数据。

7) UE 利用这一 URL 和带有<lib:AuthnResponse>的 HTTP 请求再次与 SP 联系。

8) SP 通过 HTTP 答复做出应答。



图IV.1 – 带有<lib:AuthnResponse>的SSO和带有GBA的传统TLS消息流程

注 1– 由于 IdP 与 NAF 共置一地，即按照 TS [b-TS 33.222]选择 Ua 进行认证，因此每一个经过 Ua 的请求均进行自我认证，因为每一项请求均包含完整授权字头。第一次请求和随后的请求之间不存在差别。

注 2– LAP ID-FF 规范[b-ID-FF]除定义了带有询问串的、基于 GET 的请求外，还定义了 UE 与 IdP 之间的、基于 POST 的通信，这符合[b-TS 33.222]，因为只有一项得到具体规定的 HTTP 请求不包括明确说明的方法。

注 3– SP 可以利用步骤 1 中收到的、基于 GBA 的认证支持指示来选择适当的身份提供商地址。

IV.2.1.2 带有PSK TLS的HTTP

当按照[b-TS 33.222]第5.4段使用带有预共享密钥TLS的HTTP时，则步骤如下：

1) UE 发送 HTTP 请求，与 SP 取得联系，希望获得 SP 提供的服务。该请求包含基于 GBA 的认证支持指示（参见第 IV.2.1.1 段步骤 3），因为即使 UE 主动提出使用 PSK TLS，IdP/NAF 仍可能迫使其使用传统的 TLS。

2) SP 在收到 UE 发出的 HTTP 请求时，即获得了身份提供商的地址，并在 URL 中向 UE 发出带有<lib:AuthnRequest>的重发 HTTP 答复。获得身份提供商地址的手段取决于实施情况并由服务提供商决定。

3) UE 按照[b-TS 33.222]第 5.4 段开始建立通向 IdP/NAF 的 PSK TLS 隧道，为向 IdP/NAF 发送重发请求做出准备（参见步骤 4）。UE 在建立 TLS 隧道过程中说明可以使用 PSK TLS，因此 IdP/NAF 可以选择带有 GBA 的 PSK TLS。

   如果 IdP/NAF 使用 PSK TLS，则 UE 从前者选择的 TLS 加密套件中认识到这一点。

   如果 UE 和 IdP/NAF 之间存在引导安全关联性，则 UE 和 IdP/NAF 共享密钥，以保护 Ua 参考点，因此 UE 具有所有的按照[b-TS 33.222]建立 PSK TLS 隧道所需的的数据，且可以在不执行引导程序的情况下立即开始下一步骤。

   如果 UE 和 IdP/NAF 之间不存在引导安全关联性，但 UE 确实包含有效的引导密钥 Ks，则 UE 根据相关的 Ks_(ext)_NAF 建立通向 IdP/NAF 的 PSK TLS 隧道。

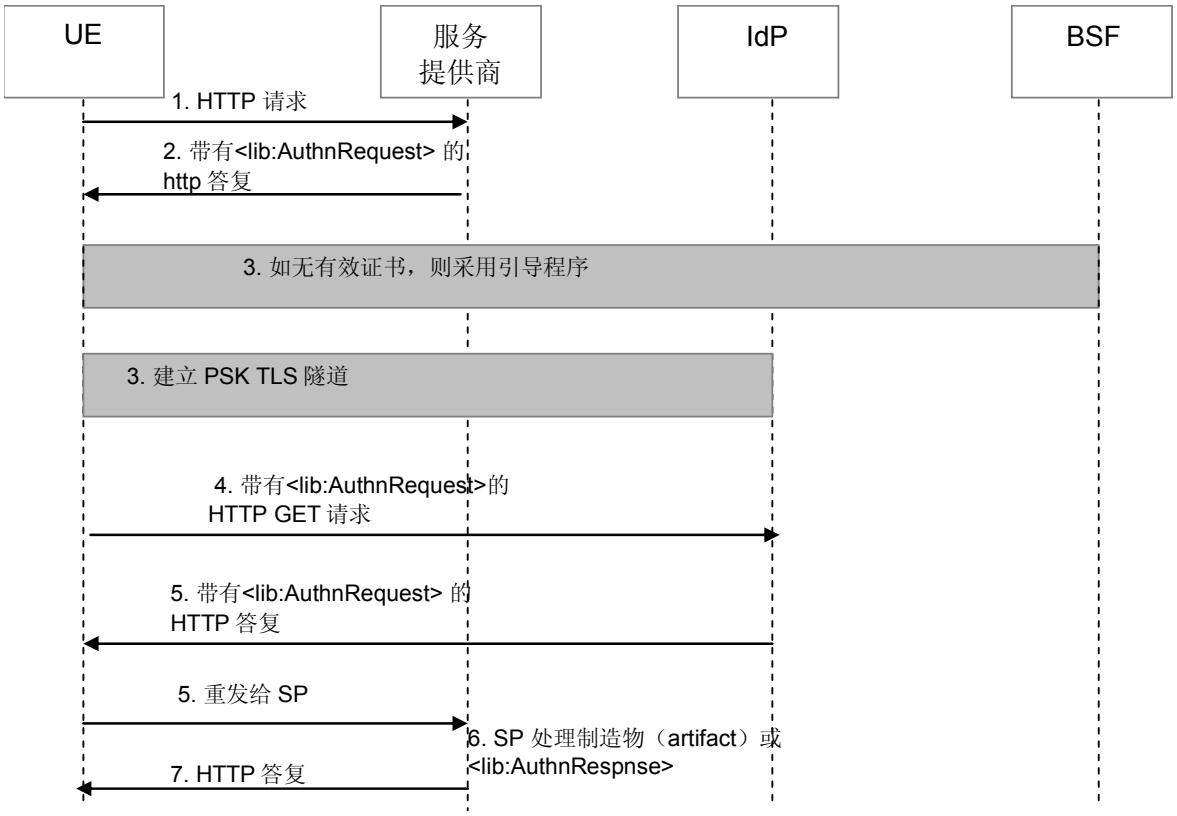
   如果 UE 未包括有效的引导会话，或 IdP 认为其密钥资料不够新鲜，则 UE 将与 BSF 执行一项新的引导程序，且该程序对 SP 是透明的。

4) UE 在业已建立起的 PSK TLS 隧道内通过带有<lib:AuthnRequest>信息[b-ID-FF 绑定]的 HTTP GET 请求访问 IdP/NAF URL。

5) IdP 提取<lib:AuthnRequest>，对其加以处理，使用 PSK TLS 隧道建立过程中进行的 UF 认证，并向 UE 发送重发 HTTP 答复，从而将 UE 重新发回给 SP。URL 可以包含一个 SAML 制造物（artefact）或<lib:AuthnResponse>。

6) SP 提取 SAML 制造物或<lib:AuthnResponse>，对其加以处理，并利用 HTTP 答复做出应答。

7) SP 利用 HTTP 答复做出应答。



图IV.2 – 有<lib:AuthnResponse>的SSO及使用带有GBA的PSK TLS的消息流程

注 – IV.2.1.1 段中的注释也适用于本段落定义的 PSK TLS 的使用情况。

IV.2.2 SSO情形：带有制造物传送的ID-FF

该情形与第IV.2.1段所述的情形相似，只是增加了服务提供商可以直接与IdP进行联系的功能。

注 – 制造物和<lib:AuthnResponse>使用的基本消息流程相同，因此第 IV.2.1 段所述的传统 TLS 与 PSK TLS 使用之间的差别也适用于本段。本段所述的消息流程涉及传统 TLS，但也可以类比使用 PSK TLS。

SP必须支持附加的与SP连接的接口才能够检索认证断定信息。由于认证信息可能包含与GBA有关的信息（如用户身份、化名以及源于GUSS的更多信息和基于GBA的限制等），因此上述接口并非与GBA完全分离。

1) UE发送HTTP请求，与SP取得联系，希望获得SP提供的服务。该请求包含基于GBA的认证支持指示（参见步骤3），因为根据步骤3重发请求时需要这一信息。

2) SP在收到UE发出的HTTP请求时，即获得了身份提供商的地址，并向UE发出带有<lib:AuthnResponse>的重发HTTP答复。获得身份提供商地址的手段取决于实施情况并由服务提供商决定。

3) UE按照地点字头字段中给出的URL与IdP进行联系，且必须通过带有<lib:AuthnResponse>信息[b-ID-FF绑定]的HTTP请求访问NAF/IdP URL。

   UE在“用户代理”HTTP字头上增加恒定串（作为［b-IETF RFC 2616]规定的产品标识），向NAF/IdP说明支持基于GBA的认证。应根据[b-TS 33.222]的步骤2第5.3段落，设定上述恒定串。

如果UE和IdP之间存在引导安全关联性，则UE和IdP/NAF共享密钥，以保护Ua参考点，且UE具有所有的按照此前消息进行HTTP Digest认证的数据。在这种情况下，步骤3与步骤5中的请求合并，并省略步骤4。

4) 如果UE尚未与IdP进行认证，则应按照[b-TS 33.222]在此进行认证。自由联盟[b-ID-FF]未定义具体规定该认证的方法和细节。IdP按照[b-TS 33.222]向UE发送带有非授权状态HTTP答复。

如果NAF未包括有效的针对NAF的密钥资料，或NAF或IdP认为其密钥资料不尽如人意，则必须按照[b-TS 33.220]执行引导程序，且该程序对SP是透明的。

5) UE利用包含B-TID这一用户名和Ks_（ext/int）_NAF这一密码的、带有授权字头字段的HTTP GET做出应答，UE可以包含更多的与LAP有关的用户数据。

如果IdP/NAF尚未存储相关证书和资料，则可以请求得到这些信息。收到的USS可以包含更多的具体针对自由（Liberty）的信息。

6) IdP在HTTP答复重发URL[b-ID-FF绑定]中利用SAML制造物做出答复，IdP可以包含更多的与LAP有关的数据。

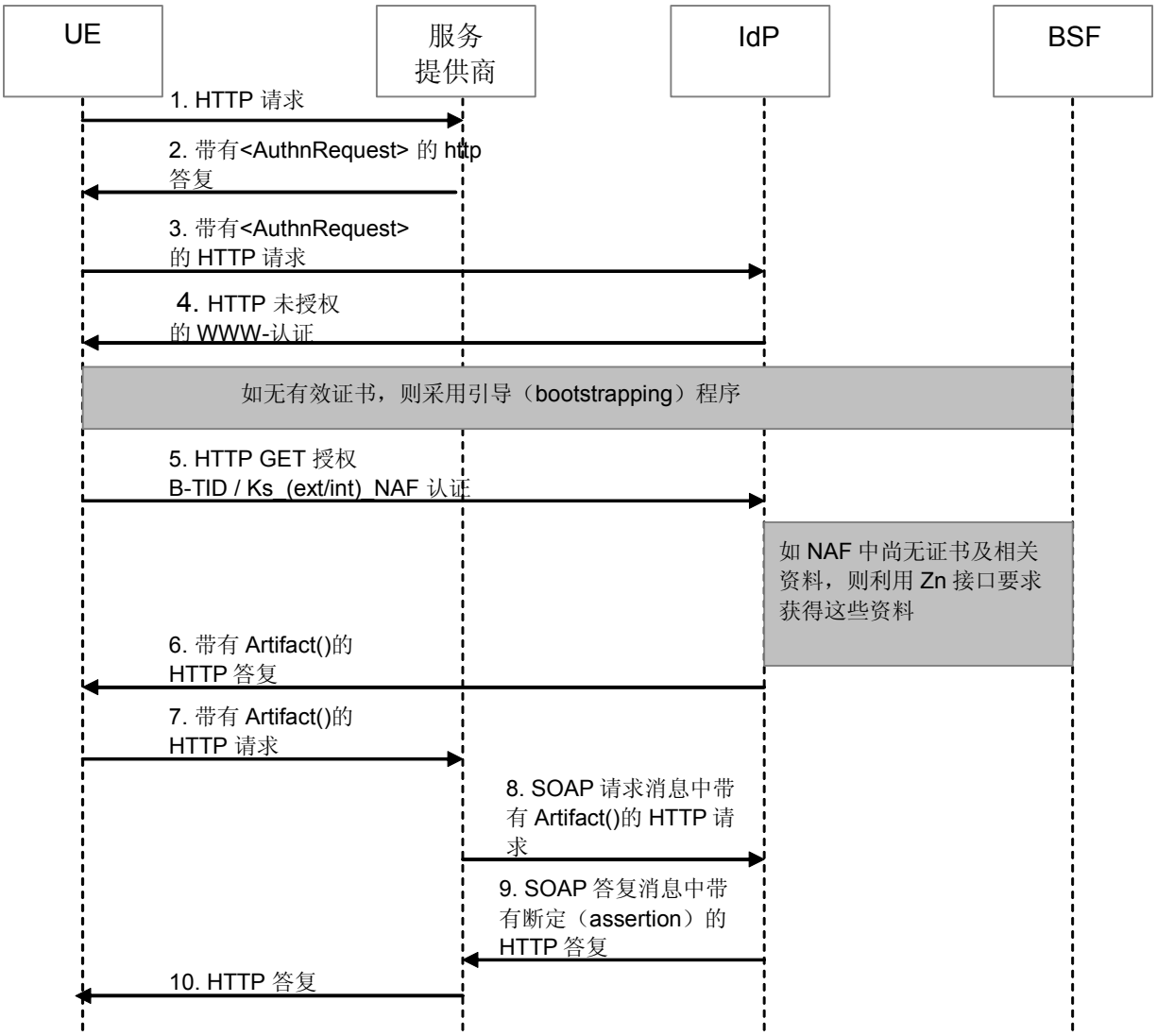
7) UE利用该URL和带有SAML制造物的HTTP请求再次与SP进行联系。

8) SP向IdP发送带有SAML制造物的HTTP请求，该请求包含<samlp:Request>SOAP请求消息，以确认提供商的SOAP端点，并按照[b-ID-FF绑定]通过提供<samlp:AssertionArtefact>元素中的SAML断定制造物该请求断定。

9) 由此IdP可以建立或找出请求得到的断定，并按照[b-OASIS]通过带有请求得到的<saml:Assertion>的<samlp:Response>SOAP答复消息或状态码做出答复。IdP发送与制造物相对应的认证断定。

10) SP通过利用<samlp:Response>返回的<saml:Assertion>处理SOAP消息，验证<saml:Assertion>上的签名，按照[b-ID-FF绑定]处理消息，并通过HTTTP答复做出应答。

SAML认证断定的寿命应与B-TID相同，或低于后者。



图IV.3 – 带有制造物传送并使用GBA的SSO的消息流程

IV.2.3 SSO情形：ID-WSF认证服务

在该情形中，UE由LAP启动，也就是说，由LUAD（自由启动用户代理或装置规范[b-ID-WSF概况]定义的自由ID-WSF资料中的自由启动用户代理或装置）启动。所用的协议元素源于ID-WSF认证服务[b-ID-WSF业务]，且UE与IdP的互动包括两次连续的协议运行。工作中的LUAD在接入SP提供的服务之前首先与NAF/IdP联系。

1) UE与IdP的认证服务（AS）进行认证，并检索使UE有权启动某些服务的安全令牌（security token）。

2) UE利用安全令牌启动IdP的单点登录服务，在此过程中，UE收到将在SP使用的认证断定（认证和授权信息）。

3) UE作为万维网服务接入的WSP向SP提交认证断定。

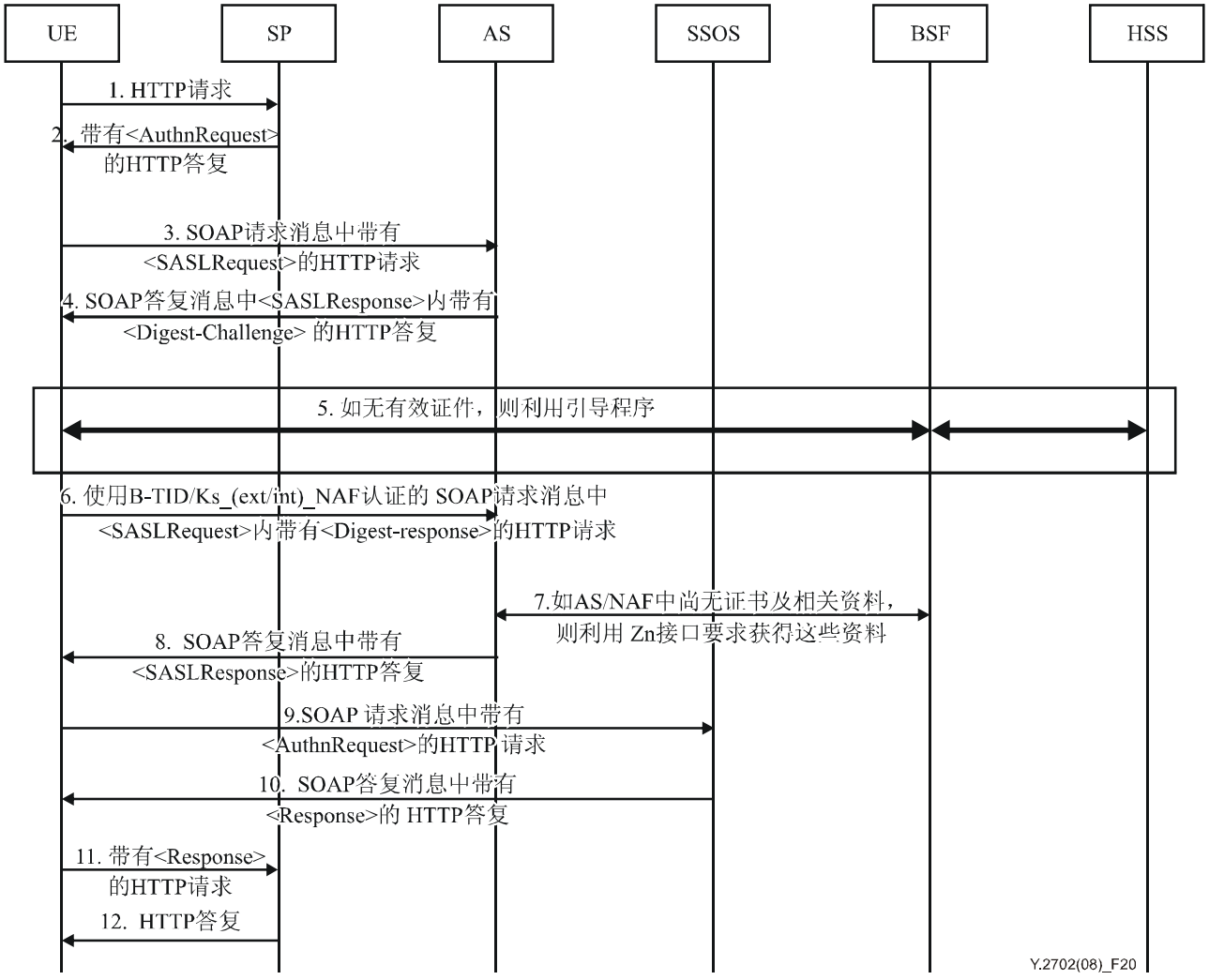
如果WSP向构成IdP运营商组成部分的用户提供万维网服务，则LUAD客户机可以利用安全令牌直接与WSP联系，在这种情况下可以省去与SSOS的联系。

将这三个步骤映射到GBA的方法如下：

– 按照 LAP[b-ID-WSF 业务]将步骤一映射到用户（LUAD）与 AS 之间的通信，认证协议已嵌入 SASL 协议之中。必要时必须由 UE 运行 Ub，这并非是基于 LAP[b-ID-WSF 安全]、[b-ID-FF]或[b-ID-WSF 业务]协议之上的，而是基于 GAB[b-TS 33.220]协议之上的。

– 步骤二和三完全按照 LAP 的定义进行（不与 GBA 连接）。对 GBA 的唯一依赖是 SAML 认证断定内容方面的依赖（在某种程度上取决于 GBA 的结果（协议参数，如执行时间和具体针对用户的参数，如源于 USS 的参数））。

以下为带有答复转移的、ID-WSF认证服务SSO情形的消息流程，它也适用于SSOS提供ID-WSF认证服务的情况（在此情况下，SSOS与AS共置一地）。



图IV.4 – 带有答复转移并采用GBA的ID-WSF AS和SSO的消息流程

1) UE 发送 HTTP 请求，与 SP 取得联系，希望获得 SP 提供的服务。

2) SP 在收到 UE 发出的 HTTP 请求时，即获得了 AS 的地址，并向 UE 发出重发 HTTP 答复。根据应用或部署模式，HTTP 答复可以包含或不包含<lib:AuthnRequest>。获得 AS 地址的手段取决于实施情况。

3) UE（LUAD-WSC）向 AS 发送 HTTP 请求，其中包括 soap 方向的<SASLRequest>字头，该字头中的“机制”参数中应填写一个或多个客户机支持的 SASL 机制名称清单。

UE 在“用户代理”HTTP 字头上增加恒定串（作为[b-IETF RFC 2616]规定的产品标识），向 NAF/IdP 说明支持基于 GBA 的认证。应根据[b-TS 33.222]的步骤 2 第 5.3 段，设定上述恒定串。

如果 UE 和 NAF/AS 之间存在引导安全关联性，则 UE 和 NAF/AS 共享密钥，以保护 Ua 参考点，且 UE 在 SASL 资料允许的情况下进行随后的认证程序。在这种情况下，步骤 3 与步骤 6 中的请求合并，并省略步骤 4 和步骤 5。

4) AS 向 UE 发送 HTTP 答复，其中包括 soap 方向的<SASLResponse>）字头，该字头中的“服务器机制”参数应填写从客户机支持的 SASL 机制清单中选出的 SASL 机制名称（即 DIGEST 认证），在这种情况下，<SASLResponse>字头也包含<digest-challenge>参数。该参数的方法和细节应符合[b-IETF RFC2831]。

5) 如果 UE 未包括有效的引导会话，或 AS 认为其密钥资料不够新鲜，则 UE 将与 BSF 执行一项新的引导程序，并获得共享密钥 Ks_（ext/int）_NAF。该程序对 SP 是透明的。

6) UE 向 AS 重新发送 HTTP 请求，其中包括 soap 方向的<SASLRequest>字头，该字头“机制”参数中应填写步骤 4 返回的 SASL 机制，在这种情况下，<SASLRequest>字头也包含<digest-response>参数，其授权数据通过使用 B-TID 用户名和 Ks_（ext/int）_NAF 密码得到计算。该参数的方法和细节应符合[b-IETF RFC2831]。UE 也可以包含更多的与 LAP 有关的用户数据。

7) 如果 AS 与 NAF 共置一地，则 AS 还需要通过使用 Zn 请求 BSF 提供 Ks_（ext/int）_NAF 和其它资料（如果尚未提供的话）。

8) AS 处理<SASLRequest>字头中的<digest-response>参数，之后 AS 利用 HTTP 答复中的、soap 方向的<SASLResponse>字头做出答复。<SASLResponse>字头包含涉及 SSOS 情形的 ID-WSF EPR（端点参考）参数，同时按照[b-ID-WSF 业务]设定服务类型 URL，以确定 ID-WSF SSOS。<SASLResponse>字头还包括 UE 启动 SSOS 所需的某些证书。AS 可以包含更多的与 LAP 有关的数据。

9) UE 向 SSOS 发送 HTTP 请求，其中包括 soap 方向的<samlp2:AuthnRequest>字头，该字头中的 Protocolbuilding 属性按照[b-ID-WSF 业务]设定，以确定将使用的 SAML 协议绑定。该请求还包含包括步骤 8 返回的资格在内的<wsse:security>字头。根据相关应用或部署模式，如果 UE 未在步骤 2 收到<samlp2:AuthnRequest>字头，则必须自己创建该字头。

10) <samlp2:AuthnRequest>得到处理。SSOS 在 HTTP 答复重发 URL[b-ID-FF 绑定]中利用<samlp2: Response>字头做出答复。<samlp2: Response>字头包含<saml2:Assertion>参数。SSOS 可以包含更多的与 LAP 有关的数据。

11) UE 利用该 URL 和带有<samlp2: Response >的 HTTP 请求再次与 SP 联系。

12) SP 通过 HTTP 答复做出应答。

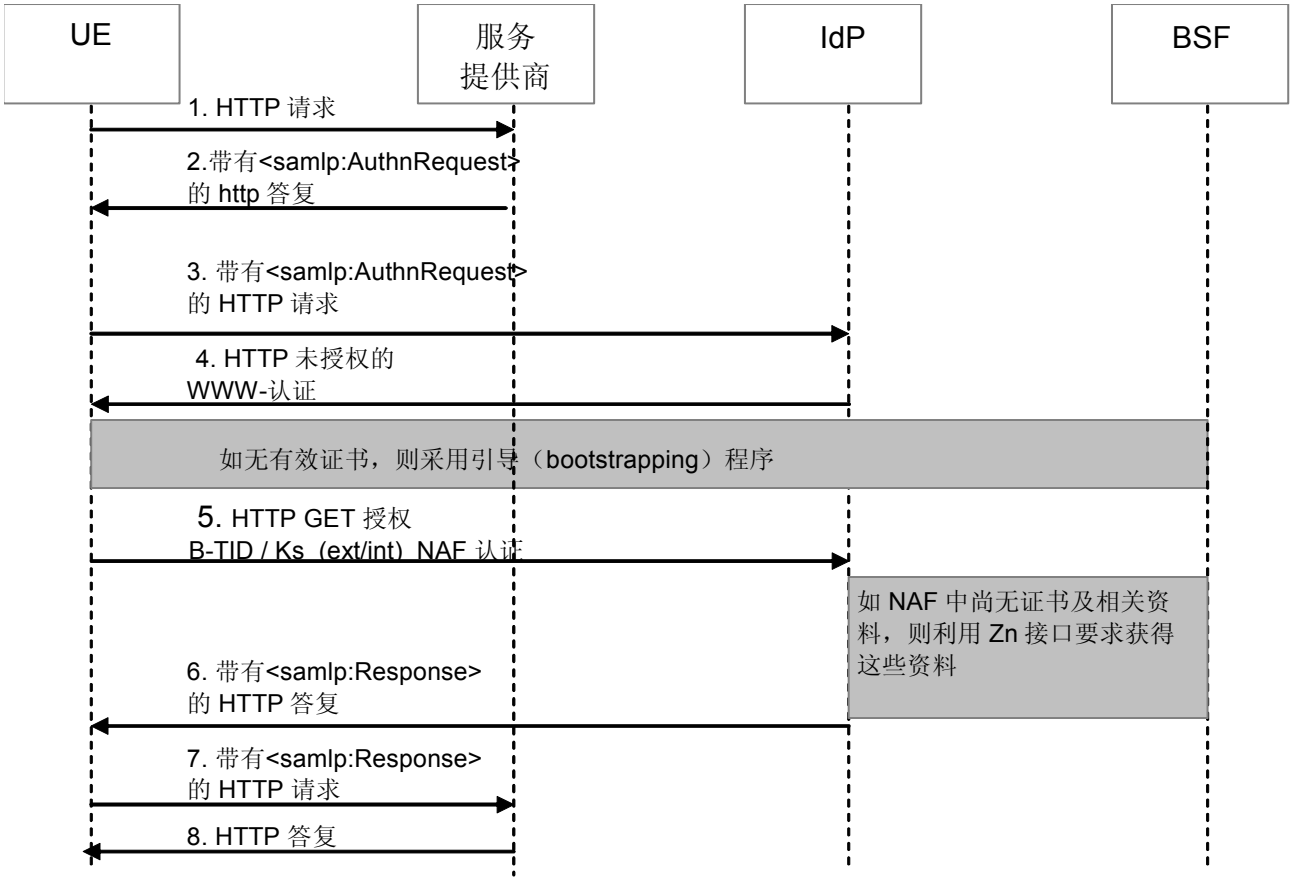
注 – 如果 IdP 与 BSF 共同托管，则进一步可以映射到 GBA[b-TS 24.109]的 Ub 参考点，第二步可以映射到 GBA 的 Ua 接口。

尽管这两个协议领域之间存在协议的两次连续运行的相象之处，但似乎无法实现简单的映射。GBA 和 LAP 之间传送的信息元素的语法和语义大为不同。

IV.2.4 SSO情形：带有<samlp:Response>转移的SAML v2.0

IV.2.4.1 带有TLS的HTTP

该情形是第IV.2.1.1段所述情形的一种形式，唯一的区别是所有的协议元素均源自按照[b-OASIS]实施万维网浏览器SSP资料的[b-SAML v2.0]内部，因此上述段落描述的各种步骤也适用于本段所述情形，只是需要用<samlp:AuthnRequest>替代<lib:AuthnRequest>，并用<samlp:Response>替代<lib:AuthnResponse>。在此仅给出经过调整的图IV.1，不再重复各相关步骤。

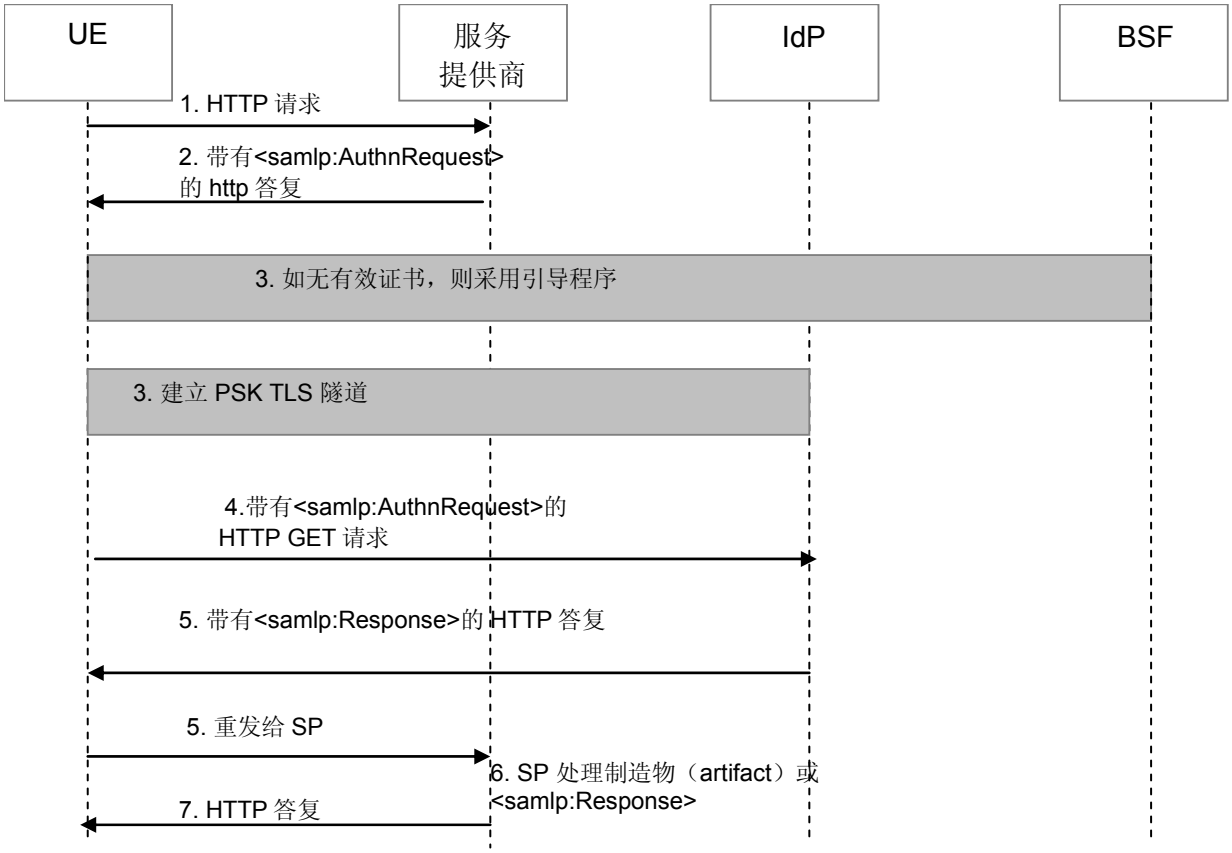


图IV.5 – 带有<samlp:Response>的SSO和带有GBA的TLS的消息流程

IV.2.4.2 带有PSK TLS的HTTP

该情形是第IV.2.1.2段所述情形的一种形式，唯一的区别是所有的协议元素均源自按照[b-13]实施万维网浏览器SSO资料的[b-SAML v2.0]内部，因此上述段落描述的各种步骤也适用于本段所述情形，只是需要用<samlp:AuthnRequest>替代<lib:AuthnRequest>，并用

<samlp:Response>替代<lib:AuthnResponse>。在此仅给出经过调整的图IV.2，不再重复各相关步骤。



图IV.6 – 带有<samlp:Response>的SSO和带有GBA的PSK TLS使用的消息流程

IV.2.5 SSO情形：带有制造物转移（分辨率）的SAML v2.0

该情形是第IV.2.2段所述情形的一种形式，唯一的区别是所有的协议元素均源自按照[b-OASIS]实施万维网浏览器SSP资料的[b-SAML v2.0]内部，因此上述段落描述的各种步骤也适用于本段所述情形，只是需要用<samlp:AuthnRequest>替代<lib:AuthnRequest>。在此仅给出经过调整的图IV.3，不再重复各相关步骤。

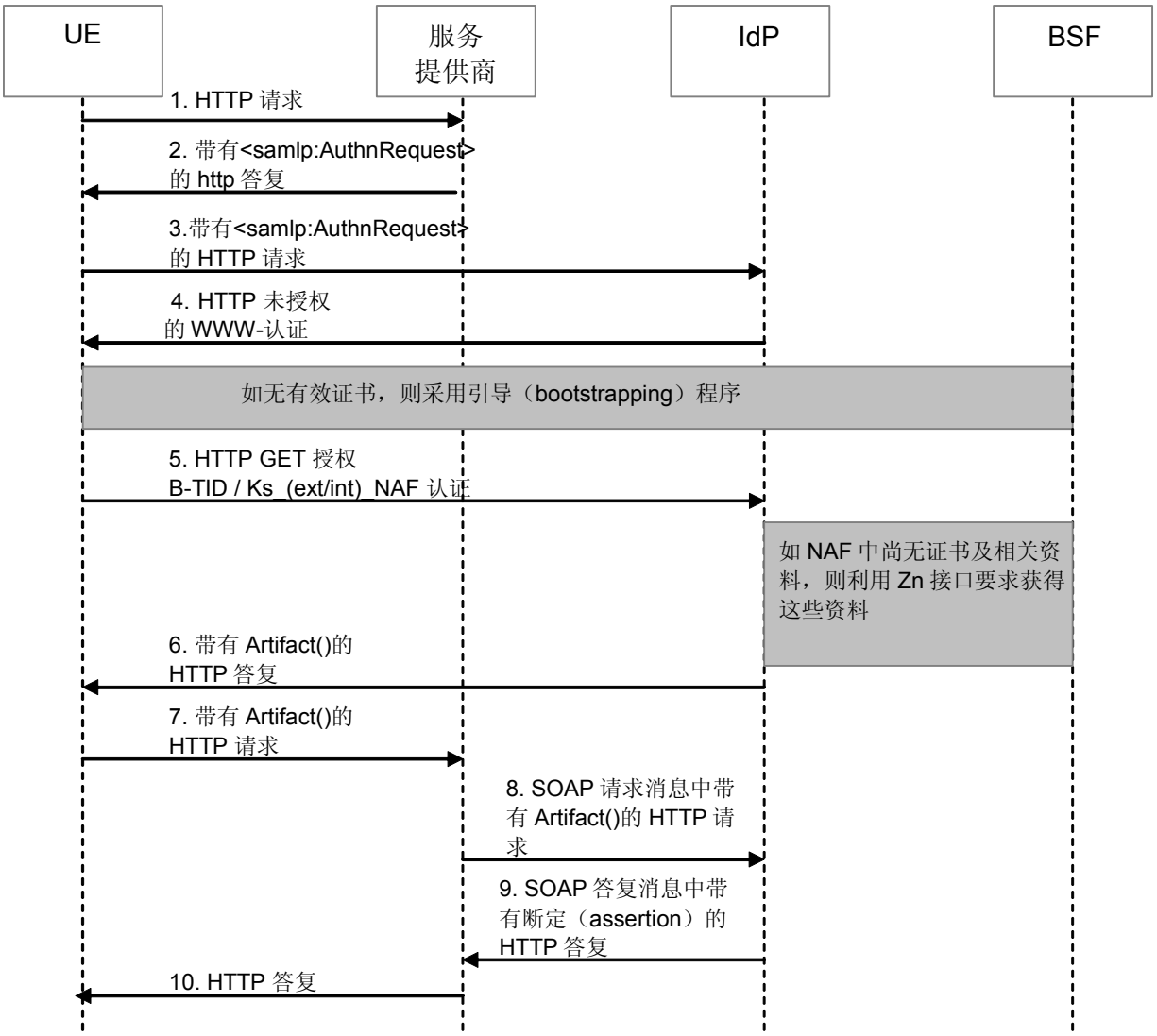


图 IV.7 – 带有制造物分辨率（SAML v2.0）和使用 GBA 的 SSO 消息流程

参考文献

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

[b-ITU-T X.509] Recommendation ITU-T X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-Alliance] Liberty Alliance Project, ID-SIS: *Liberty Alliance ID-SIS 1.0 Specifications*.
<http://www.projectliberty.org/liberty/specifications__1>

[b-ID-FF] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Architecture Overview*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF bindings] Liberty Alliance Project, *ID-FF v1.2: Liberty ID-FF Bindings and Profiles Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF protocols] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Protocols and Schema Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-WSF binding] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF SOAP Binding Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID WSF discovery] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Discovery Service Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF profiles] Liberty Alliance Project, ID-WSF: *Profiles for Liberty enabled User Agents and Devices*.
<http://projectliberty.org/liberty/content/download/3447/22967/file/liberty-idwsf-client-profiles-v2.0-original.pdf>

[b-ID-WSF security] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Security Mechanisms*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF service] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Authentication Service Specification and Single Sign-On Service*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF v1.2] Liberty Alliance Project, ID-WSF v1.2: *Security Mechanisms*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications>

[b-LAP] Liberty Alliance Project Support Documents: *Authentication Context Specification v2.0*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-M-04-04] M-04-04: *E-Authentication Guidance for Federal Agencies*. <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf >

[b-NIST 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf >

[b-OASIS] OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

[b-OASIS auth] OASIS, *Authentication Contexts for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

[b-Reverse] Liberty Alliance Project Support Documents: *Liberty Reverse HTTP Binding for SOAP Specification v1.1*. <http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-SAML assertions] OASIS, SAML v2 Core, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[b-SAML v2.0] OASIS, SAML v2 Core, *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*. <http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

[b-TR 21.905] 3GPP TR 21.905 (in force), *Vocabulary for 3GPP Specifications*. <http://www.3gpp.org/ftp/Specs/html-info/21905.htm>

[b-TR 33.980] 3GPP TR 33.980 (in force), *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) (Release 7)*. <http://www.3gpp.org/ftp/Specs/html-info/33980.htm>

[b-TS 24.109] 3GPP TS 24.109 (in force), *Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details*. <http://www.3gpp.org/ftp/Specs/html-info/24109.htm>

[b-TS 29.109] 3GPP TS 29.109 (in force), *Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*. <http://www.3gpp.org/ftp/Specs/html-info/29109.htm>

[b-TS 33.220] 3GPP TS 33.220 (in force), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*. <http://www.3gpp.org/ftp/Specs/html-info/33220.htm>

[b-TS 33.221] 3GPP TS 33.221 (in force), *Generic Authentication Architecture (GAA); Support for subscriber certificates*.
<http://www.3gpp.org/ftp/Specs/html-info/33221.htm>

[b-TS 33.222] 3GPP TS 33.222 (in force), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*.
<http://www.3gpp.org/ftp/Specs/html-info/33222.htm>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*.
<http://www.ietf.org/rfc/rfc2222.txt?number=2222>

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.
<http://www.ietf.org/rfc/rfc2246.txt?number=2246>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol-HTTP/1.1*.
<http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
<http://www.ietf.org/rfc/rfc2617.txt?number=2617>

[b-IETF RFC 2831] IETF RFC 2831 (2000), *Using Digest Authentication as a SASL Mechanism*.
<http://www.ietf.org/rfc/rfc2831.txt?number=2831>

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.
<http://www.ietf.org/rfc/rfc3546.txt?number=3546>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.
<http://www.ietf.org/rfc/rfc4279.txt?number=4279>

[b-IETF RFC 4412] IETF RFC 4412 (2006), *Communication Resource Priority for the Session Initiation Protocol*.
<http://www.ietf.org/rfc/rfc4412.txt?number=4412>

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	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	**全球信息基础设施、互联网协议问题和下一代网络**
Z系列	电信系统使用的语言和一般性软件情况

瑞士印刷
2009年，日内瓦