国　际　电　信　联　盟

ITU-T

国际电信联盟
电信标准化部门

Y.2703

（01/2009）

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）中认证、授权和结算（AAA）业务的应用

ITU-T Y.2703 建议书

ITU 国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

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

如果需要进一步了解细目，请查阅ITU-T建议书清单。

ITU-T Y.2703建议书

下一代网络（NGN）中认证、授权和结算（AAA）业务的应用

摘要

ITU-T Y.2703建议书提出了下一代网络（NGN）第一阶段的认证、授权和结算（AAA）业务的一项应用。

来源

ITU-T 第13研究组（2009-2012年）按照WTSA第1号决议规定的程序，于2009年1月23日批准了ITU-T Y.2703建议书。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工委员会（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

ITU-T Y.2703建议书

下一代网络（NGN）中认证、授权和结算（AAA）业务的应用

1 范围

本建议书阐述下一代网络（NGN）中认证、授权和结算（AAA）的一项应用，其基础是[b-ITU-T Y.2201]：NGN第一阶段的要求、[b-ITU-T Y.2012]：NGN第一阶段的功能要求和体系结构（FRA）、[b-ITU-T Y.2701]：NGN第一阶段的安全要求和[b-ITU-T Y.2702]：NGN的认证。本建议书适用于采用AAA客户机和AAA服务器接入NGN的认证、授权和结算进程。具体而言，本建议书仅从结算功能对安全结算的影响的角度阐述结算功能。

本建议书的范围包括：

1) 注册进程。
2) 认证功能和程序。
3) 授权功能和程序。
4) 安全结算功能和程序。

2 参考文献

无。

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 authentication 认证[b-ITU-T X.811]：为某一实体自称的身份提供保证。

3.1.2 authentication certificate 认证证书[b-ITU-T X.811]：由认证机构担保的且可用于确保实体身份的安全证书。

3.1.3 authentication information 认证信息[b-ITU-T X.811]：用于进行认证的信息。

3.1.4 authorization 授权[b-ITU-T X.800]：赋予权利，包括按照接入权赋予接入的权利。

3.1.5 claimant 权利主张者[b-ITU-T X.811]：授权的主体或代表授权的主体。权利主张者包括代表主体进行授权交换所需的功能。

3.1.6 security audit trail 安全审计跟踪 [b-ITU-T X.800]：得到收集且可能用于促进安全审计的数据。

3.2 本建议书规定的术语

本建议书规定下列术语：

3.2.1 security accounting 安全结算：在安全审计功能中可以作为资源被纳入的与安全有关的行动或事件的跟踪作用。

4 缩写词和首字母缩略语

本建议书采用下列缩写：

AAA 认证、授权和结算
AM-FE 接入管理功能实体
ANI 网络接口应用
EAP 可扩展认证协议
ID 身份 – 由被访问的网络、业务或实体规定
NAS 网络接入服务器
NGN 下一代网络
NNI 网络网络接口
NP 网络提供商
OAMP 运营、管理、维护和提供
RACF 资源和接纳控制功能
SCTP 流控制传输协议
SR 业务资源
TAA-FE 传输认证和授权功能实体
TE 终端设备
TUP-FE 传输用户信息功能实体
UNI 用户网络接口

5 约定

无。

6 AAA业务的一般性概念

本节阐述AAA的基本概念。

6.1 概述

认证、授权和结算业务提供对用户身份进行验证（认证）和准予用户访问业务（授权）的各项功能，并提供一种衡量资源消耗（结算）的手段。

6.2 AAA进程

AAA框架中的各进程如下：

认证是在最终用户被允许接入网络之前对其身份进行验证。最终用户提供一套凭证，如用户名/密码组合、安全密钥、证书或生物特征识别数据（例如指纹）。这些凭证通常在注册过程中得到认可。验证凭证后即开始授权进程。

授权旨在一经给予最终用户网络接入权则定义其应享有的特权和服务，可能包括提供一个IP地址或启动过滤功能，以便确定支持哪些应用或协议。在AAA管理环境中，认证和授权同时进行。

结算旨在提供收集最终用户有关资源消耗方面的信息的方法，通过这些信息的处理可以对最终用户进行计费、审计和容量规划。某些结算数据还可用于制定安全审计跟踪。

上述三个进程集中于一套功能之中，并共同提供接入控制。

6.3 AAA程序

AAA业务系统由一个AAA服务器和一个AAA客户机组成。

AAA服务器可以接入用户资料和配置数据数据，它与置于网元（如NAS（网络接入服务器））上的AAA客户机和路由器进行通信，以提供分布式AAA业务。

有关AAA的业务情形概述如下：

- 最终用户与进入点设备连接并请求接入网络。
- AAA客户机将最终用户身份/认证凭证前转至AAA服务器。
- AAA服务器根据凭证对用户进行认证。如果认证成功，则服务器确定将对哪些业务进行授权并向AAA客户机发回接受或拒绝答复以及其他相关数据。
- AAA客户机通知最终用户有关接入具体资源的要求是被接受还是被拒绝。

在连接建立和终止过程中，AAA客户机向AAA服务器发送结算信息，以便进行记录的收集和存储。

7 NGN中的认证和授权应用模型

本建议书的基础是有关NGN安全要求的[b-ITU-T Y.2701]和有关NGN认证参考模型的[b-ITU-T Y.2702]。NGN认证参考模型（图7-1）具体描述八个认证参考点，本建议书考虑/顾及其中三个认证参考点。

这些参考点为：

(1) 用户接入网络；

(2) 网户接入由网络提供的业务；

(4) 业务提供商接入接收用户。

参考点(1)和(4)系指用户流量的传输且根据传输控制层的“横向”接入控制情况可被看到，而参考点(2)和(8)则根据传输和业务控制层的控制数据情况可被看到，因此是“纵向”的。图7-2具体说明这一关系。

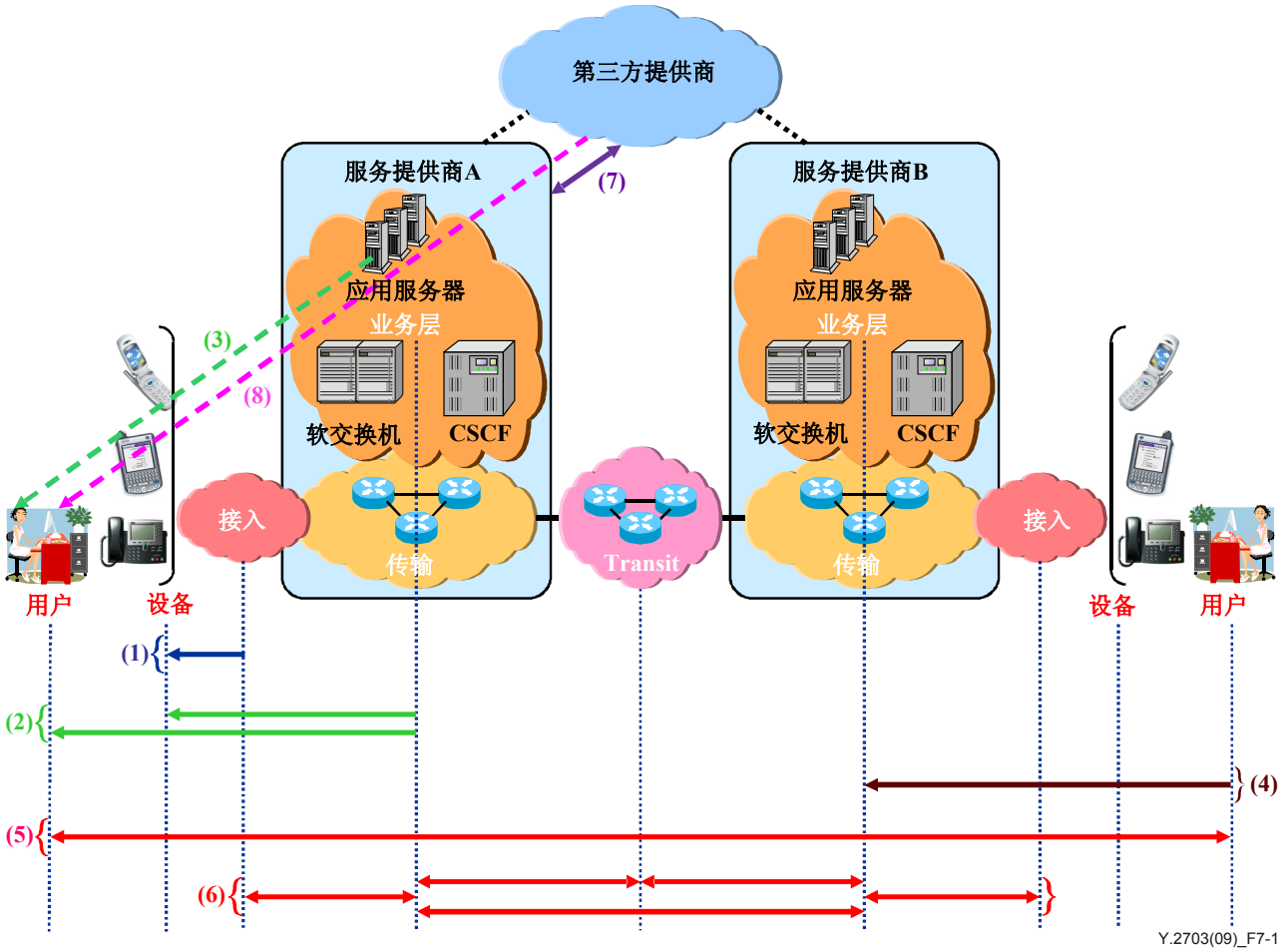


图7-1 – 端对端参考架构模型（Y.2702 NGN认证）

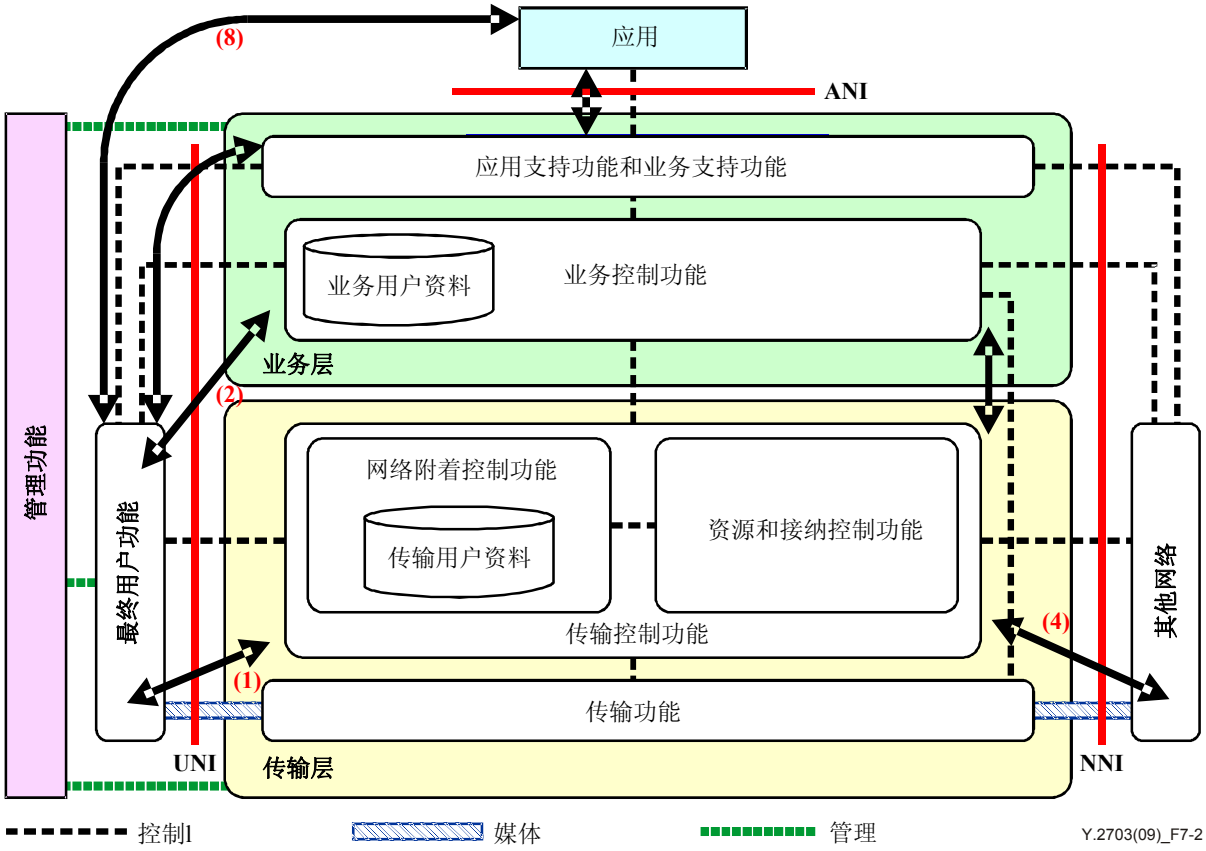


图7-2 – NGN架构和与AAA相关的域（Y.2702 NGN认证）

8 NGN中的AAA架构

本节阐述[b-ITU-T Y.2012]所述的AAA参考模型与功能架构模型之间的关系。

8.1 用户接入网络

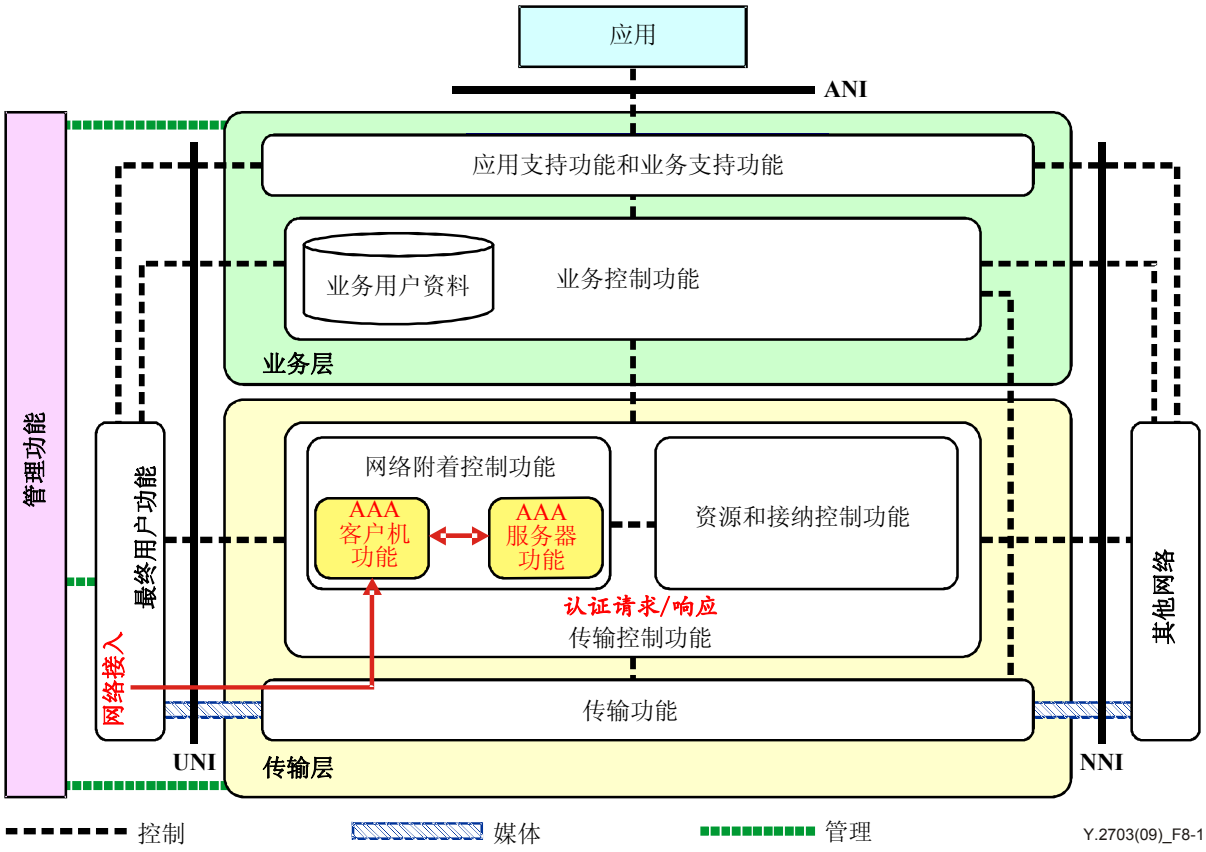
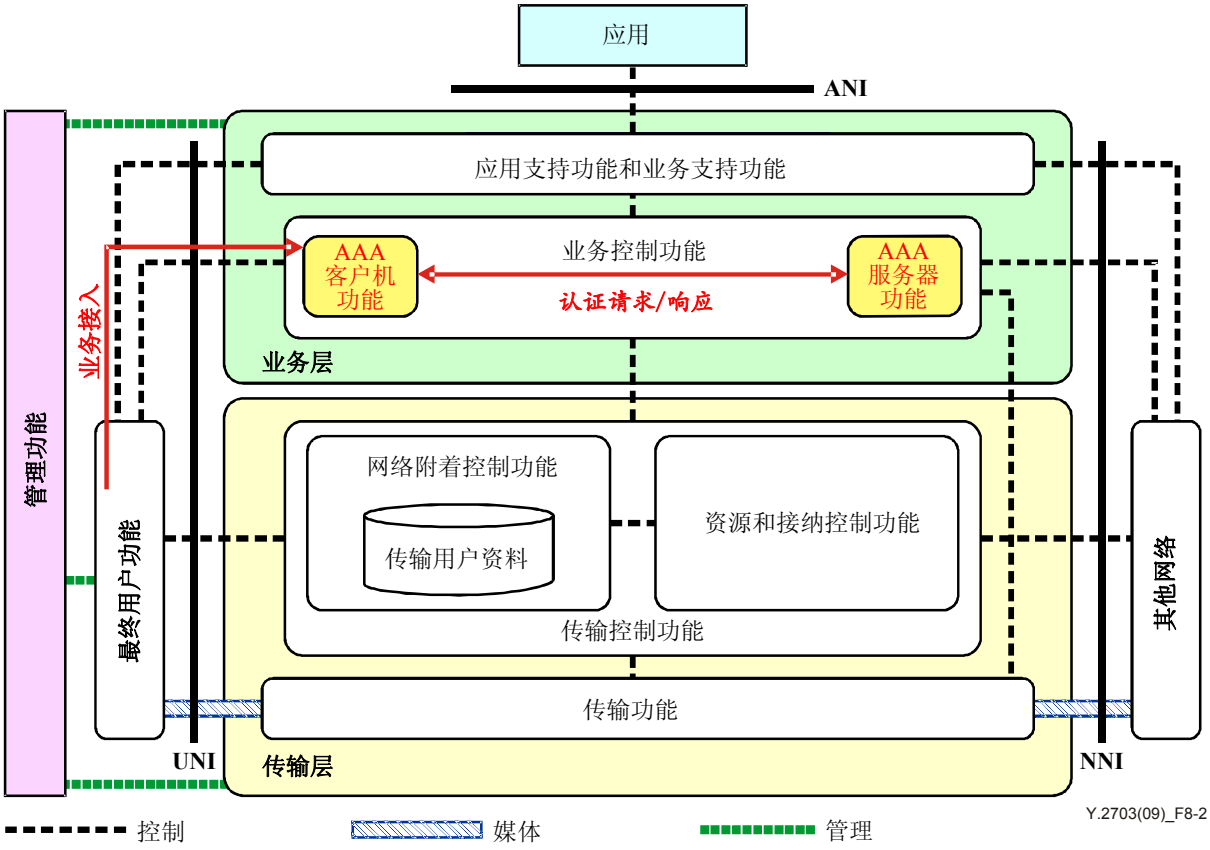


图8-1 – 用户接入网络的认证和授权

图8-1所示为用户接入网络时的AAA的应用（即上述图7.1中的1类应用）。

一旦传输控制功能中的实体（通常为T-14 AM-FE）发现用户终端提出连接请求，则开始作为AAA客户机进行行事。它要求在传输控制功能中发挥AAA服务器作用的实体（如T-11 TAA-FE和T-12 TUP-FE）对用户进行认证并授权对NGN资源的使用。可以在这一请求和答复程序中使用诸如RADIUS或Diameter的协议。根据AAA客户机的请求情况，AAA服务器根据明示（如EAP）或暗示（如接入线认证）程序对用户进行认证。在根据用户资料（通常由TUP-FE管理）成功对用户进行授权后，AAA服务器要求RACF为该用户预留并分配NGN资源。一旦进行授权，AAA服务器则通知AAA客户机允许它连接该用户设备。

8.2 用户使用网络业务附着



8-2 – 用户业务接入的认证和授权

图8-2 显示用户接入业务时的AAA的应用（即上述图7-1中的2类应用）。

同图8-1所示的情况相似，业务控制功能中的AAA客户机（通常为S-1 S-CES-FE）发现用户终端提出的连接请求，并要求AAA服务器（如S-5 SUP-FE或S-6 SAA-FE）对所请求业务进行认证和授权。基于业务请求的业务根据认证和授权情况被予以提供或拒绝。

一旦将用户与网络和业务连接，则每一个AAA客户机均通知其AAA服务器有关用户对NGN资源的耗费信息，以帮助AAA服务器收集与该用户有关的结算信息。

8.3 用户接入第三方业务的认证和授权

NGN第一阶段未说明通过ANI接入第三方业务的情况，因此，用户接入第三方业务的认证和授权不属于本建议书的范围。本建议书对第三方业务参考模型不做描述。但在附录三中给出了具体说明第三方业务认证和授权的用例。

9 注册

AAA的前提条件之一是识别将得到认证的实体，如用户或设备。识别用户/设备独特身份的注册（enrolment）进程能够建立识别实体所需的凭证。这些凭证被用于寻求业务接入时的认证进程。注册进程可以包括接受相关条款和条件以及财务安排。虽然身份的最初验证和资格被称做注册，随后进行的业务接入和资格检查则被称做登记（registration）。有关注册的确切安排取决于提供商的政策、业务性质等。

10 认证

本建议书采用[b-ITU-T X.811]中有关认证的基本概念。需要提供网络和业务接入认证服务和功能以减少企图进行的、未经授权的接入所带来的风险威胁。附录第II节提供有关数字证书的更多信息。

10.1 认证实体

“权利主张者”一词用于描述提出认证请求的实体。权利主张者包括进行认证交换所需的功能。

AAA客户机提供权利主张者与验证实体之间接入路径组成部分的专门功能（在每一个接入请求上），并执行验证者做出的决定。

在AAA管理环境中，AAA服务器为进行验证的实体并在成功认证之后向权利主张者发出认证证书。

10.2 认证程序

在AAA管理环境中，AAA服务器为用户提供认证服务，该服务器充分识别请求接入的实体，以确定可以授权接入哪些业务并对其进行收费。AAA服务器可以发出认证证书。

10.2.1 成功认证

下列步骤以及图10-1以示例说明成功认证的信息进程。

步骤1： 实体向AAA客户机提出接入请求。

步骤2： AAA客户机请求AAA服务器对实体进行认证。

步骤3： AAA服务器请求AAA客户机提供实体的凭证，以开始认证程序。

步骤4： AAA客户机请求实体提供认证所需的凭证。

步骤5： 现已成为权利主张者的实体向AAA客户机发送所要求的凭证。

步骤6： AAA客户机向AAA服务器前转所要求的凭证，以进行认证。

步骤7： AAA服务器根据权利主张者的用户资料对所收到的凭证进行验证。

步骤8： 如果凭证可以得到验证，则AAA服务器在无须通知AAA客户机或权利主张者的情况下开始进行授权。

步骤9： 授权程序完成之后，AAA服务器向AAA客户机发出允许接入的信息。

步骤10： AAA客户机向权利主张者前转允许接入的信息。

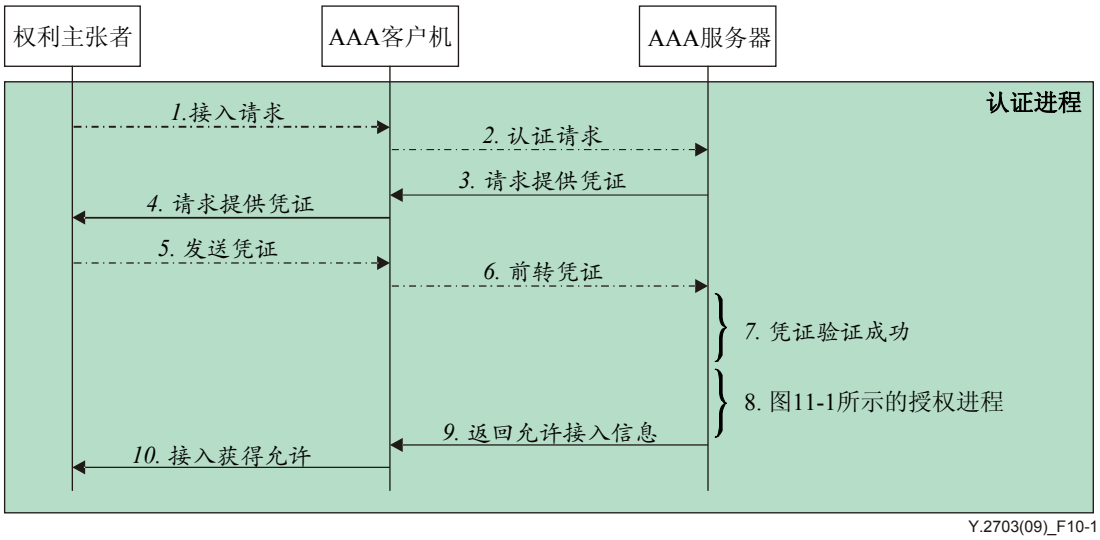


图10-1 – 成功认证的信息流

10.2.2 不成功的认证

下列步骤及图10-2以示例说明不成功的认证的信息流。

步骤1： 实体向AAA客户机发出接入请求。

步骤2： AAA客户机请求AAA服务器对实体进行认证。

步骤3： AAA服务器请求AAA客户机提供实体的凭证，以便开始认证。

步骤4： AAA客户机请求实体提供所要求的认证所需的凭证。

步骤5： 现已成为权利主张者的实体向AAA客户机发送所要求的凭证。

步骤6： AAA客户机向AAA服务器前转所要求的凭证，以进行认证。

步骤7： AAA服务器按照权利主张者的用户资料对所收到的凭证进行验证。

步骤8： 如果无法验证凭证，则AAA服务器向AAA客户机发送拒绝接入信息。

步骤9： AAA客户机将拒绝接入信息前转权利主张者。

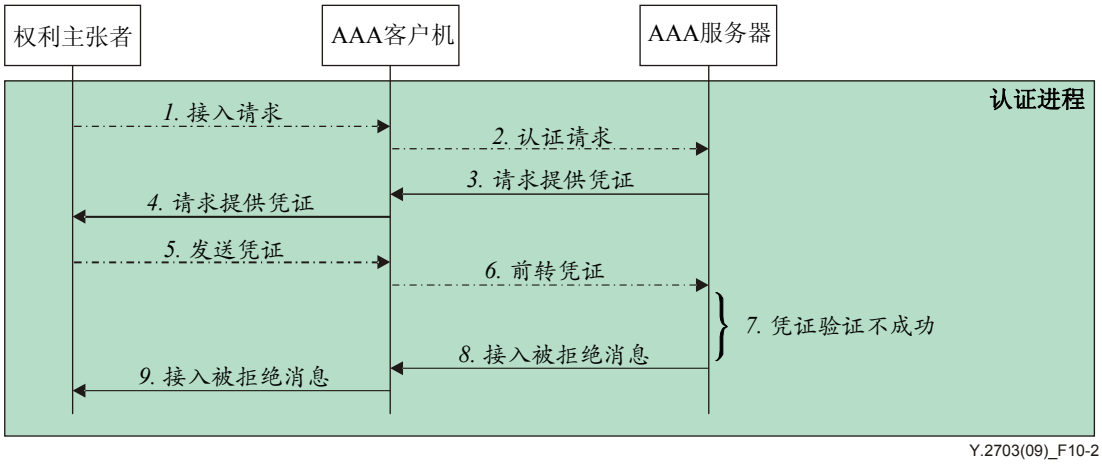


图10-2 – 不成功的认证的信息流

11 授权

授权的定义为确定是否向具体凭证提交方授予某一特权的行为。特权可以是业务资源(SR)的接入权，可以包括根据政策来进行的资源的读取、写入或修改。授权程序是认证之后进行的程序，旨在根据此前进行的认证步骤的结果和政策来批准或拒绝接入NGN业务。

11.1 NGN的授权问题

授权旨在为经认证的用户提供并控制有关经授权业务的接入。在NGN中，AAA服务器与包含被注册实体接入特权信息的网元进行通信。

本建议书将认证和授权作为相关程序进行处理，通常则在每次提出接入请求时对被注册实体顺序进行认证和授权。然而，提供商的政策也可以允许实体不经过重新认证或注册而直接提出接入/使用权。本建议书未涉及这一情况。

AAA服务器通过沟通并接收相关网元的授权信息完成用户对业务使用的授权。AAA服务器完成授权程序之后，向提出业务使用要求的用户前转确认信息。

收到确认信息则表示成功完成了一整套认证和授权程序，进行接入的实体被视为已与网络或得到授权的SR进行连接。

11.2 授权实体

AAA服务器在认证之后无需接入实体的参与即自动进行授权。AAA服务器提供通过使用接入控制政策规则而做出授权决定的专门功能。

11.3 授权程序

下述图11-1描述授权程序。

步骤A： 对实体成功认证之后，AAA服务器确认可提供给权利主张者并由其接入的业务和资源。

步骤B： 完成步骤A之后，AAA服务器通知传输和业务控制功能指配/分配经授权的业务和资源，供权利主张者使用。

步骤C： AAA服务器向AAA客户机发送允许接入信息。

步骤D： AAA客户机向权利主张者前转允许接入信息。

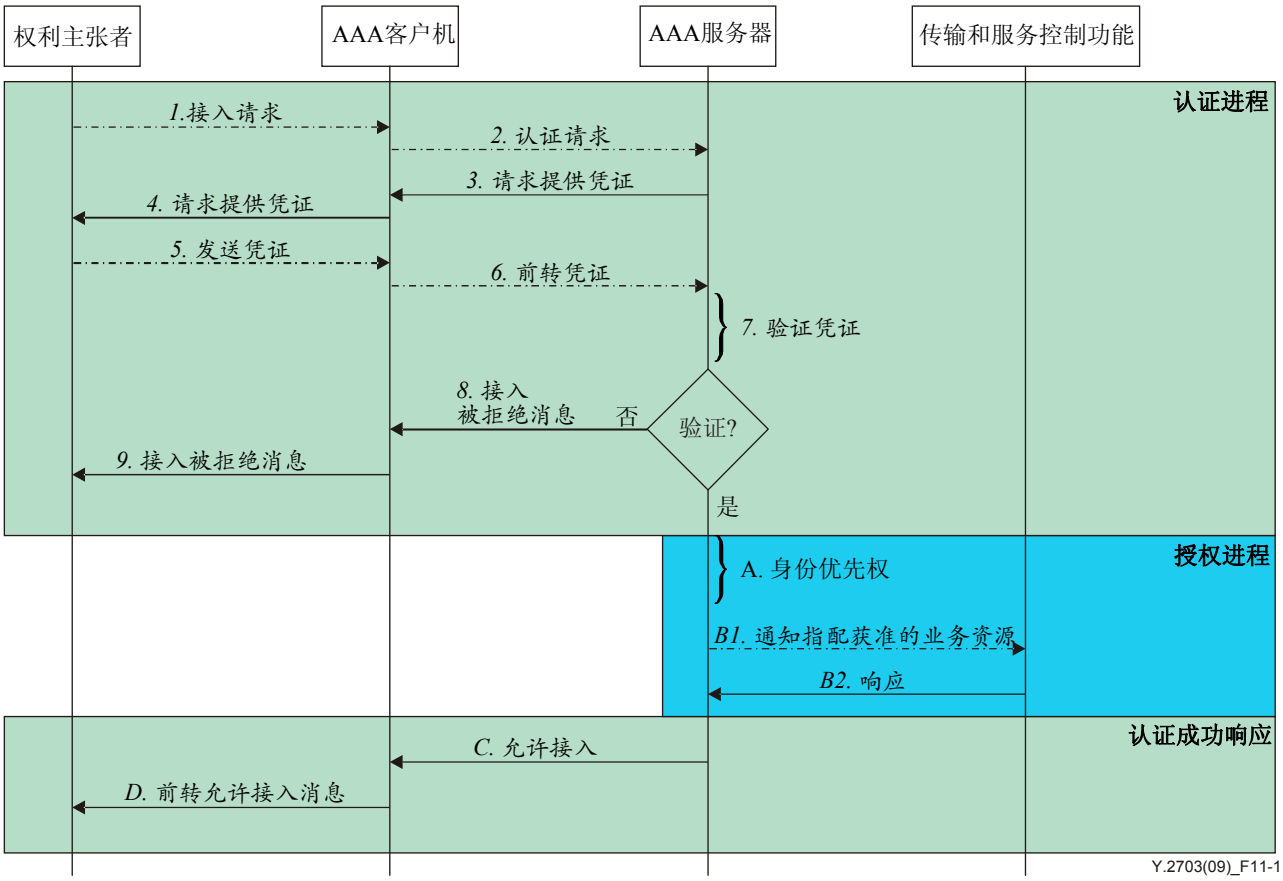


图11-1 – 授权程序信息流

12 结算

“AAA”中的最后一个“A”表示结算。AAA背景下的结算包括可与其他安全事件数据一道使用、以支持结算功能的安全元素。

12.1 安全结算

安全事件结算使用提供结算数据的结算子功能，结算数据此后被用于制定安全审计跟踪（由安全审计功能使用）。安全审计跟踪程度取决于NGN提供商为具体环境确定的安全审计需求和政策，如网络或业务接入的成功和不成功起始和终止时间、所接入的业务、接入实体的身份信息（用于成功认证）。真正的审计功能不属于本建议书的范围。图12-1所示为安全结算程序。

12.2 安全结算功能

安全结算是发挥下列功能的业务区：

1) 捕获：负责从事件中获取可发现的数据并提供与安全环境相关的信息。将捕获的数据可以包括：
   - 认证结果；
   - 与吊销认证和/或证书相关的信息；
   - 有关认证保障的信息；
   - 与认证程序有关的其他信息。

2) 存储：保存捕获功能所产生的表述。

3) 回顾：通过下列工作准确描述事件：验证所捕获数据的准确性、通过检查已捕获的数据明确事实。

4) 报告：将通过回顾功能得到的信息提交审计功能。

5) 审计：验证安全结算报告的正确性或验证其是否符合使用政策和安全导则。审计功能可以包括立即发出报警的功能。

应注意，只有捕获功能为AAA功能之一，存储、回顾、报告和审计均为管理功能。后者不属于本建议书的范围。

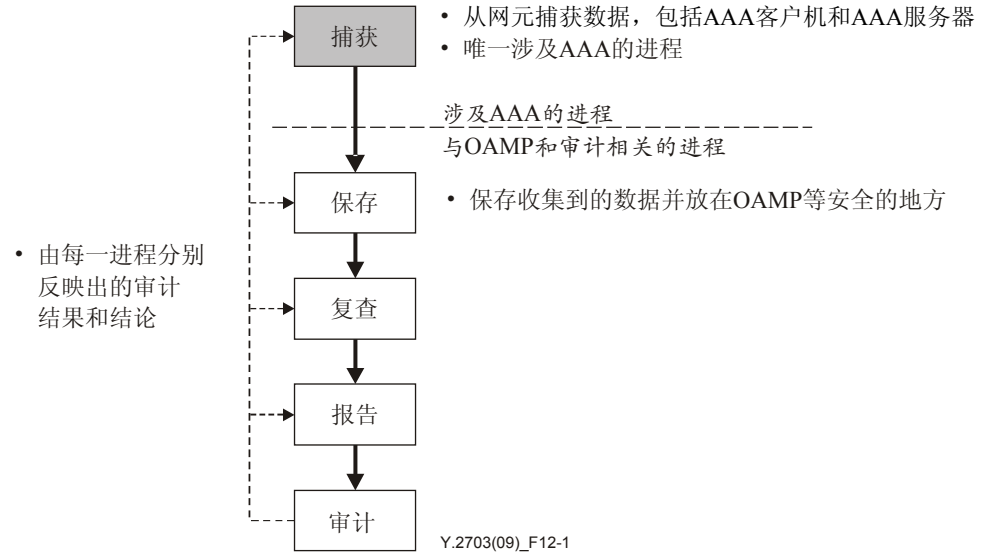


图12-1 – 安全结算进程示例

附录一

NGN中AAA的认证协议

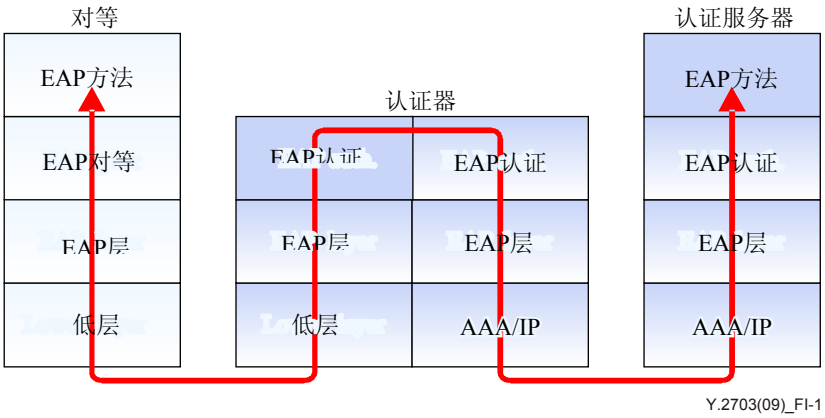
（本附录不是本建议书的组成部分）

本节描述经数据链路层传输的EAP协议和在各应用上提供AAA框架的AAA协议。

I.1 NGN中AAA业务的EAP协议

EAP协议定义支持各种认证方法的认证框架。EAP通过认证器在对等和认证服务器上运行。EAP直接在诸如IEEE 802和PPP（点对点协议）的数据链路层上传输。

然而，由于EAP协议具有依赖链路的特点，因此要求存在更低层，如EAPoL、IEEE 802.1X和IEEE 802.11i。图I-1说明EAP多路复用模型。EAP方法层包括认证算法。EAP对等和认证器分别具有认证客户机和认证器的功能性。EAP层的作用是交付EAP信息。更低层则传输或接收对等和认证器之间的EAP帧。由于链路层包括各种链路协议，因此EAP要求每一链路协议均存在不同的下层。



图I.1 – EAP前转模型

EAP需要有下层的存在来可靠地交付信息、差错检测并对信息排序，具体如下：

- 由于EAP不知道对等方从认证器接收信息，因此要求在对等和认证器之间提供可靠的信道。
- EAP不能确保在无误码的情况下将EAP信息交付目的地，因此EAP需要下层提供纠错功能。
- 可以出于任何原因对EAP信息进行重新排序或复制，因此，EAP要求有复制发现和排序功能，以确保操作正确。
- 下层并不知道上层是否包括认证协议，因此EAP要求指明认证协议。

I.2 AAA协议

诸如RADIUS的AAA协议最初用于提供拨号PPP和终端服务器接入。随着互联网的发展和新接入技术的应用，制定了Diameter协议。表I-1对AAA协议做出比较。

表I.1 – AAA协议比较

	RADIUS	DIAMETER
网络规模	小	大
传输	UDP	SCTP/TCP
加密	只需密码	整个数据包
认证/授权	组合	组合
标准	IETF	IETF
协议体系结构	C/S	P2P
可扩展性	低	高

在RADIUS协议方面，为大量用户管理分散的串行线路和调制解调器池可能会需要得到大量的行政支持。由于调制解调器池从定义上而言是与外界连接的链路，因此需要对其安全、授权和结算给予格外关注，最佳方法是管理单一的用户“数据库”，以便于认证（验证用户名和密码）并了解详细说明将向用户交付的业务类型的配置信息。

基本Diameter协议本身可用于结算应用，但当用于认证和授权时，总是针对具体应用得到扩展。

附录二

作为凭证的X.509数字证书

（本附录不是本建议书的组成部分）

提供认证保障的常用方法是使用[b-ITU-T X.509]和[b-ITU-T X.811]所述的数字证书。得到广泛使用的[b-ITU-T X.509]定义的证书包括下列数据类别：

– ***version***（**版本**）为经过编码的证书的版本。如果在证书中出现extensions部件，那么版本应为v3。如果出现issuerUniqueIdentifier 或 subjectUniqueIdentifier部件，那么版本应为v2或v3。

– ***serialNumber***（**序列号**）是CA为每个证书分配的一个整数。对某个特定CA发放的每个证书，serialNumber的值应是唯一的（即利用发放者姓名和序列号可以确定一个唯一的证书）。

– ***signature***（**签名**）包含签署证书过程中所用的算法和散列函数的算法标识符（例如，md5WithRSAEncryption、sha-1WithRSAEncryption、id-dsa-with-sha1等）。

– ***issuer***（**核发者**）用于确定签署和发放证书的实体。

– ***validity***（**验证**）是一个时间间隔，在其期间CA保证，它将对证书状态信息进行维护。

– ***subject***（**主体**）用于确定与在对象公开密钥字段中找到的公开密钥相关的实体。

– ***subjectPublicKeyInfo***（**主体公开密钥信息**）用于传达正在经受认证的公开密钥，并用于确定该公开密钥为其一个实例的算法（例如，rsaEncryption、dhpublicnumber、id-dsa等）。

– ***issuerUniqueIdentifier***（**核发者唯一标识符**）用于名称重用情况下唯一确定一个发放者。

– ***subjectUniqueIdentifier***（**主体唯一标识符**）用于名称重用情况下唯一确定一个对象。

– **extensions**（**扩展**）字段允许向结构增加新的字段。

附录三

认证和授权用例

（本附录不是本建议书的组成部分）

本附录所述的采用AAA业务的用例以[b-ITU-T Y.2702]提供的参考模型为基础。

III.1 用户接入网络的认证和授权

需要网络接入认证和授权业务来验证身份，并确定是否授予最终用户设备接入权。

III.1.1 设备接入/附着到NGN的认证和授权

在这种情况下，有3类NGN的设备接入/附着(附属设备)、认证和授权。这些业务和能力对用户设备接入到/附着到IP接入网进行识别、认证和授权：

– 对原有TE和TE-BE接入到/附着到IP接入网进行识别、认证和授权(图III.1的(1))；

– 对客户域中采用IAD的原有TE和TE-BE接入到/附着到IP接入网进行识别、认证和授权（图III.1的(2)）；

– 对客户域中采用IAD的NGN的TE和TE-BE接入到/附着到IP接入网进行识别、认证和授权（图III.1的(3)）。

AAA客户机为设备和网络提供商提供认证服务：它在必要时自动允许设备接入网络提供商。

图III.1的(1)描述的识别程序如下：

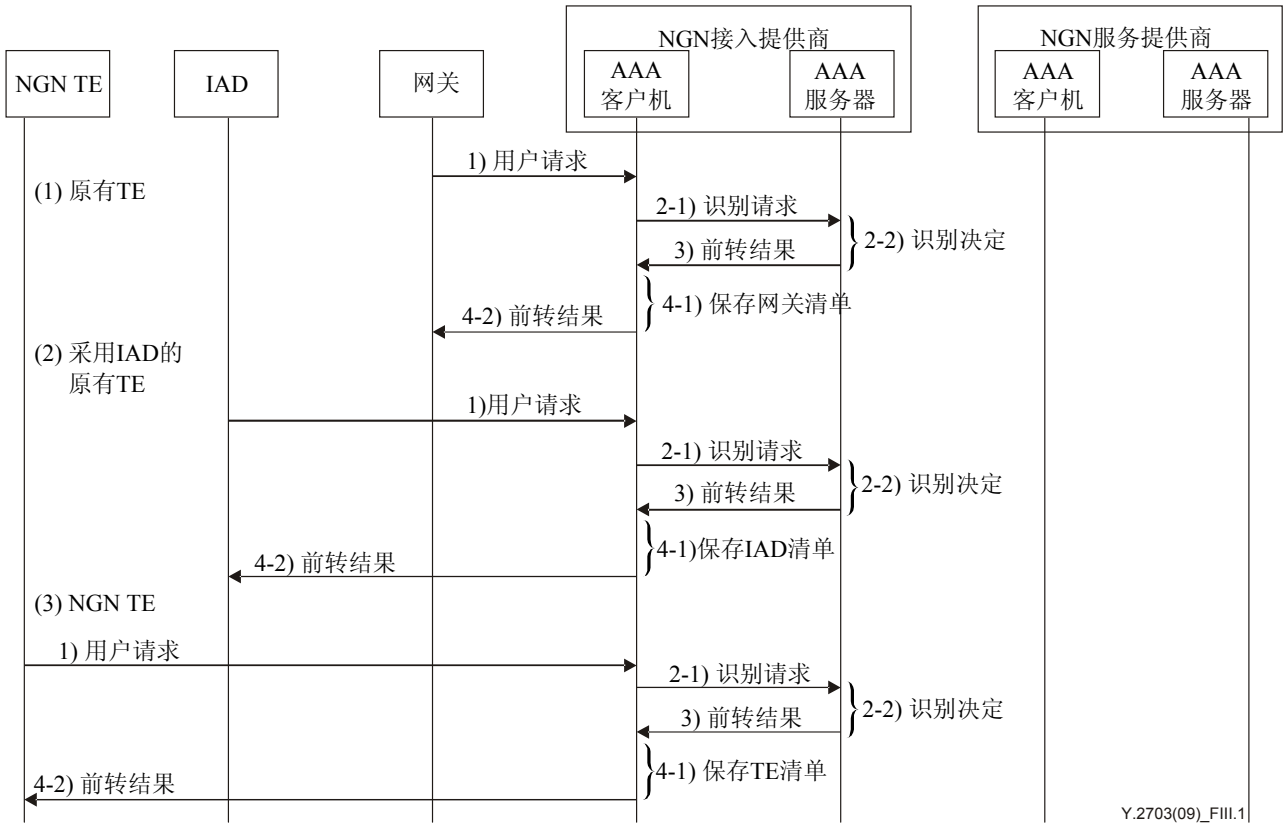
步骤1：网关（权利主张者）向AAA客户机提出网络接入/附着请求。

步骤2：AAA客户机要求AAA服务器（验证者）对网关进行识别，此时AAA服务器识别网关。

步骤3：AAA服务器将识别结果发送AAA客户机。

步骤4：AAA客户机向网关前转结果，此时AAA客户机存储网关接入清单。

在(2)和(3)中，IAD和NGN TE分别为权利主张者。其余的进程与程序(1)相同。



图III.1 – 接入NGN网络的设备识别程序

III.1.2 设备接入到/附着到NGN及业务/应用的捆绑式认证和授权

在本情况中，有3类设备接入到/附着到NGN的认证和授权。这些业务和能力将用户设备的NGN接入提供商认证与NGN服务提供商的业务和能力捆绑在一起：

– 业务NGN提供商以暗含方式识别和授权原有TE和TE-BE的业务和功能（图III-2的(1)）；

– 业务NGN提供商以暗含方式识别和授权采用IAD的原有TE和TE-BE的业务和功能（图III-2的(2)）；

– 业务NGN提供商在客户域直接识别、认证和授权NGN TE和TE-BE的业务和功能（图III-2的(3)）。

AAA客户机为设备和业务/应用提供商提供认证服务：它视需要自动允许设备接入业务/应用提供商。

图 III-2 的(1)描述的识别程序如下：

步骤1：网关（权利主张者）向AAA客户机提出使用业务/应用的请求。

步骤2：AAA客户机要求接入网域的AAA服务器（验证者）识别网关，此时AAA服务器识别网关。

步骤3：AAA服务器同时向AAA客户机和业务NGN提供商域的AAA服务器发送识别结果。

步骤4：AAA客户机向网关前转结果，此时AAA客户机存储网关接入清单。

图III-2的(2)描述的识别程序如下：

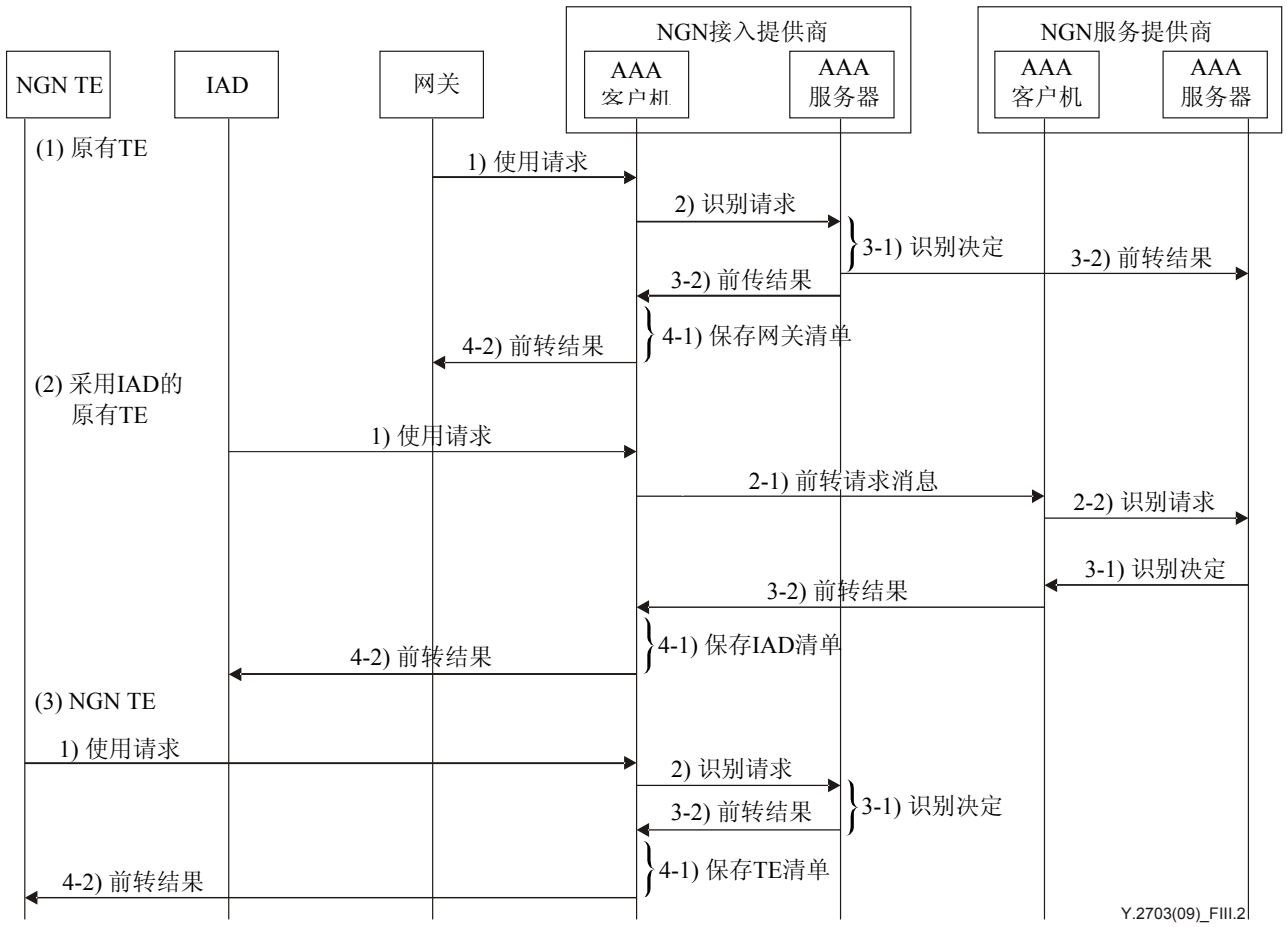
步骤1：IAD（权利主张者）向AAA客户机提出使用业务/应用的请求。

步骤2：AAA客户机要求业务NGN提供商域中的AAA客户机识别IAD，此时业务NGN提供商域中的AAA服务器（验证者）识别IAD。

步骤3：AAA服务器向AAA客户机发送识别结果。

步骤4：AAA客户机向IAD前转结果，此时AAA客户机存储IAD接入清单。

在(3)中，NGN TE是权利主张者，其余程序与程序(2)相同。



图III.2 – 使用业务/应用的设备识别程序

III.2 业务NGN提供商对用户接入业务/应用的认证和授权

在此情况中，在多网络提供商情况下存在3类业务/应用认证和授权：

– 业务NGN提供商通过与接入NGN提供商的信任关系间接对用户设备进行认证（图III-3的(1)）；

– 业务NGN提供商直接对用户设备进行认证和授权（图III-3的(2)）；

– 业务NGN提供商直接对用户进行认证（图III-3的(3)）。

AAA客户机为用户和业务/应用提供商提供认证服务：它视需要自动允许用户接入业务/应用提供商。

图III-3的(1)描述的识别程序如下：

步骤1：TE（权利主张者）向AAA客户机提出使用业务/应用的请求。

步骤2：AAA客户机要求接入网域中的AAA服务器（验证者）识别设备，此时AAA服务器识别设备。

步骤3：AAA服务器向AAA客户机和在业务NGN提供商域中的AAA服务器同时发送识别结果。

步骤4：AAA客户机向网关前转结果，此时AAA客户机存储设备接入清单。

图III-3的(2)的识别程序如下：

步骤1：TE（权利主张者）向业务NGN提供商域中的AAA客户机提出使用业务/应用的请求。

步骤2：AAA客户机要求业务NGN提供商域中的AAA服务器（验证者）识别设备，此时AAA服务器识别设备。

步骤3：AAA服务器向AAA客户机发送识别结果。

步骤4：AAA客户机向设备前转结果，此时AAA客户机存储设备接入清单。

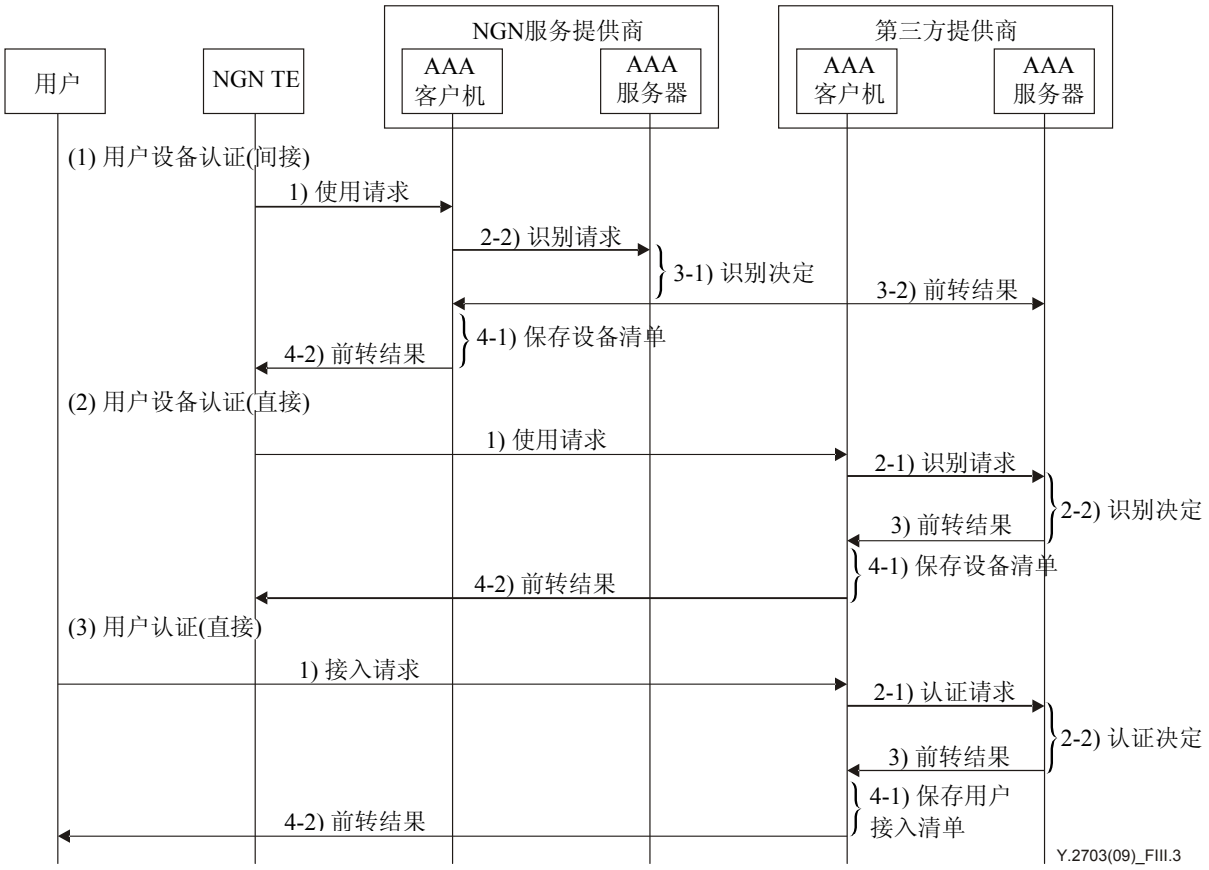
图III-3的(3)描述的认证程序如下：

步骤1：用户（权利主张者）向业务NGN提供商域中的AAA客户机提出使用业务/应用的请求。

步骤2：AAA客户机要求业务NGN提供商域中的AAA服务器（验证者）认证用户。

步骤3：AAA服务器向AAA客户机发送认证结果。

步骤4：AAA客户机向用户前转结果，此时AAA客户机存储用户接入清单。



图III.3 – 业务NGN提供商对用户进行认证和授权的程序

III.3 NGN提供商的用户认证和授权

在这种情况中，存在2类网络用户的认证和授权：

– NGN提供商对网络附着进行用户认证（图III-4的(1)）；

– NGN提供商对需获得业务的用户进行用户认证（图III-4的(2)）。

AAA客户机为网络用户的认证和授权提供认证服务：它视需要自动允许用户接入网络提供商。

图III-4的(1)描述的识别程序如下：

步骤1： 用户（权利主张者）向第三方验证者提出NAP（网络接入点）认证请求。

步骤2： 第三方验证者向NAP前转AI（认证信息）。

步骤3： 第三方验证者与NAP之间交换AI。

步骤4： 第三方验证者向用户前转结果，此时第三方验证者进行验证。

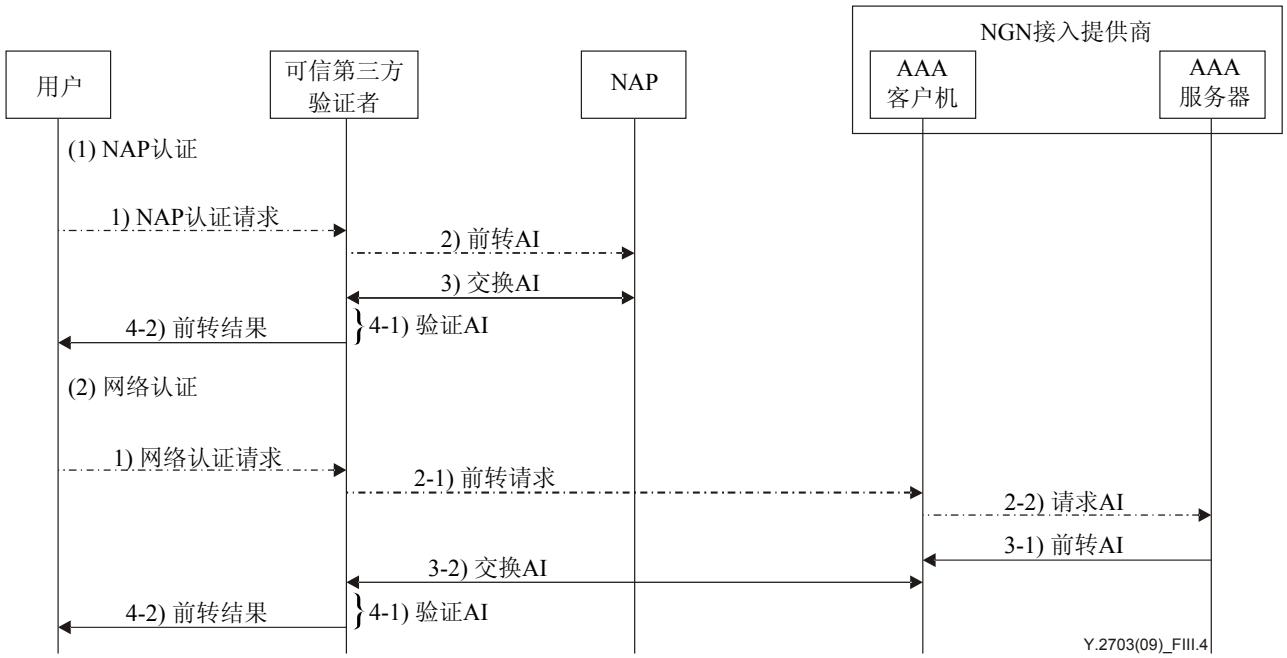
图III-4的(2)描述的识别程序如下：

步骤1： 用户（权利主张者）向第三方验证者提出网络认证请求。

步骤2： 第三方验证者向AAA客户机前转用户请求，此时AAA客户机向AAA服务器提出AI请求。

步骤3： AAA服务器向AAA客户机发送AI并在第三方验证者和AAA客户机之间交换AI。

步骤4： 第三方验证者向用户前转结果，此时第三方验证者在此进行验证。



图III.4 – NGN提供商的用户认证和授权程序

III.4 NGN提供商对第三方业务/应用提供商的认证和授权

在某些情况下，应用或业务提供商可能不同于NGN提供商（即第三方业务/应用提供商）。NGN提供商此时需要对第三方业务/应用提供商进行认证和授权。

AAA客户机为对第三方业务/应用提供方进行认证和授权的NGN提供商提供认证服务。

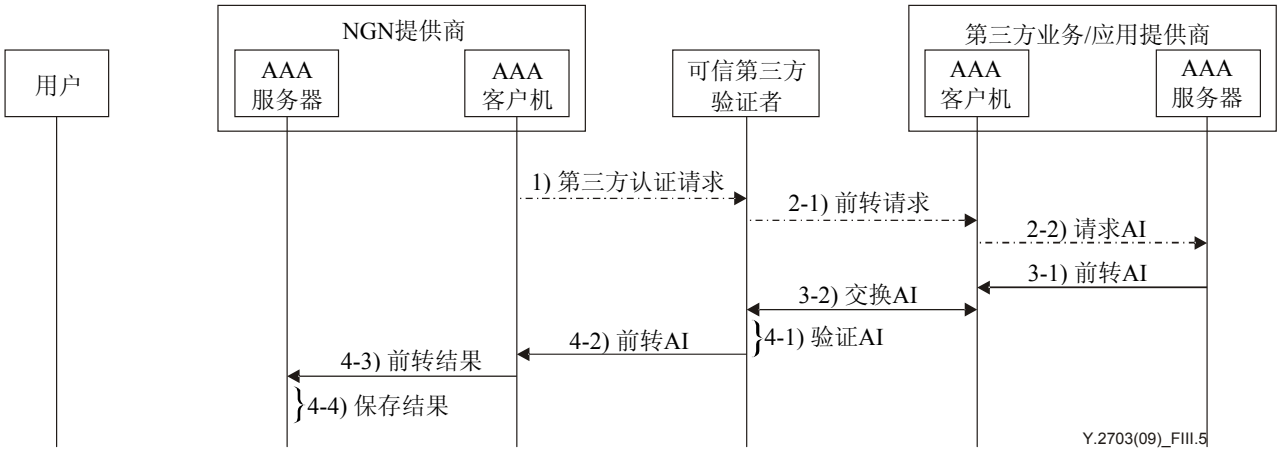
图III-5描述的识别程序如下：

步骤1： NGN提供商中的AAA客户机（权利主张者）向第三方验证者提出对第三方业务/应用提供商进行认证的请求。

步骤2： 第三方验证者向第三方业务/应用提供商中的AAA客户机前转用户请求，且AAA客户机要求AAA服务器提供AI。

步骤3： AAA服务器向AAA客户机前转AI，并在第三方验证者和AAA客户机之间交换AI。

步骤4： 第三方验证者向NGN提供商中的AAA客户机前转结果，此时第三方验证者进行验证，且AAA服务器存储结果。



图III.5 – NGN提供商对第三方业务/应用提供商的认证和授权程序

III.5 第三方认证和授权业务的使用

第三方的认证和授权业务提供商可提供这一业务。在这种情况下，存在2类第三方认证和授权业务的使用：

– 对使用业务提供商的用户进行认证（图III-6的(1)）；

– 对与用户连接的业务提供商进行认证（图III-6的(2)）。

III.5.1 使用业务提供商业务用户的认证

AAA客户机提供用户使用业务提供商业务的认证和授权服务：它视需要自动允许用户接入第三方业务/应用提供商。

图III-6描述的识别程序如下：

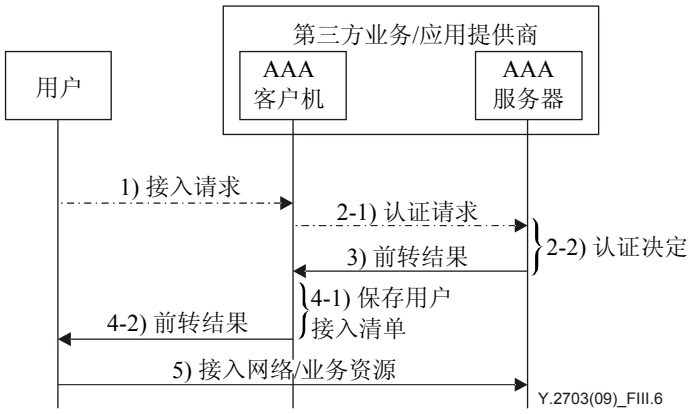
步骤1： 用户（权利主张者）向AAA客户机提出网络接入请求。

步骤2： AAA客户机要求第三方业务/应用提供商中的AAA服务器对用户资格进行审查，此时AAA服务器（验证者）认证用户。

步骤3： AAA服务器向AAA客户机发送认证结果。

步骤4： AAA客户机向用户前转结果，此时AAA客户机存储用户接入清单。

步骤5： 如果得到授权，则用户可以接入规定的网络资源。



图III.6 – 第三方认证和授权业务的使用程序

III.5.2 对与用户连接的业务提供商进行认证

AAA客户机为与用户连接的业务提供商提供认证服务，图III-7描述的识别程序如下：

步骤1： 客户域中的用户（权利主张者）向第三方验证者提出第三方业务/应用提供商认证请求。

步骤2： 第三方验证者向第三方业务/应用提供商中的AAA客户机前转用户请求，AAA客户机要求AAA服务器提供AI。

步骤3： AAA服务器向AAA客户机前转AI，并在第三方验证者和AAA客户机之间交换AI。

步骤4： 第三方验证者向NGN提供商中的AAA客户机前转结果，此时第三方验证者进行验证并存储结果。

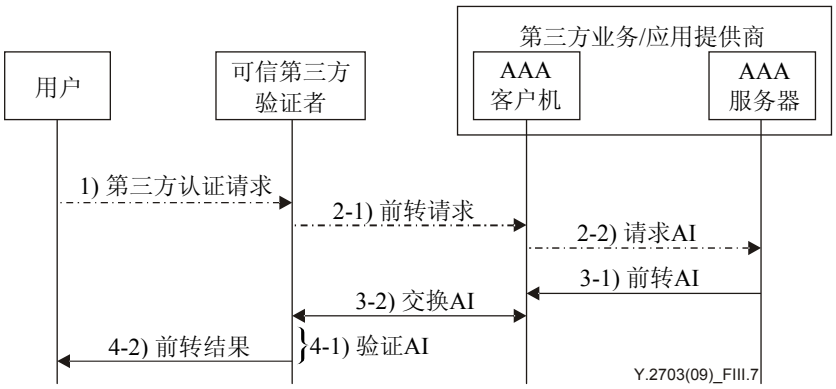


图 III.7 – 第三方认证和授权业务的使用程序

参考资料

[b-ITU-T M.3410] ITU-T M.3410建议书 (2008)，《支持电信管理的安全管理系统的指导原则和要求》。

[b-ITU-T Q.3201] ITU-T Q.3201 (2007) 建议书，《用于网络附着的基于EAP的安全信令协议体系框架》。

[b-ITU-T Q.3202.1] ITU-T Q.3202.1建议书 (2008)，《用于下一代网络(NGN)中3GPP、WiMax和WLAN互通的基于EAP-AKA的认证协议》。

[b-ITU-T X.509] ITU-T X.509建议书 (2005) | ISO/IEC 9594-8:2005，《信息技术 – 开放系统互连 – 号码簿：公开密钥和属性证书框架》。

[b-ITU-T X.800] ITU-T X.800建议书 (1991)，《CCITT应用的开放系统互连的安全体系结构》。

[b-ITU-T X.805] ITU-T X.805建议书 (2003)，《提供端对端通信的系统的安全体系结构》。

[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 – 开放系统安全框架：概述》。

[b-ITU-T X.811] ITU-T X.811建议书 (1995) | ISO/IEC 10181-2:1996，《信息技术 – 开放系统互连 – 开放系统安全框架：认证框架》。

[b-ITU-T X.812] ITU-T X.812建议书 (1995) | ISO/IEC 10181-3:1996，《信息技术 – 开放系统互连 – 开放系统安全框架：访问控制框架》。

[b-ITU-T X.816] ITU-T X.816建议书 (1995) | ISO/IEC 10181-7:1996，《信息技术 – 开放系统互连 – 开放系统安全框架：安全审计和告警框架》。

[b-ITU-T Y.2001] ITU-T Y.2001建议书 (2004)，《下一代网络(NGN)综述》。

[b-ITU-T Y.2011] ITU-T Y.2011建议书 (2004)，《下一代网络(NGN)的一般原则和一般参考模型》。

[b-ITU-T Y.2012] ITU-T Y.2012建议书 (2006)，《下一代网络(NGN)第一阶段的功能要求和体系结构》。

[b-ITU-T Y.2201] ITU-T Y.2201建议书(2007)，《下一代网络(NGN)第一阶段的要求》。

[b-ITU-T Y.2233] ITU-T Y.2233建议书(2008)，《在下一代网络(NGN)中提供结算和计费能力的要求和框架》。

[b-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》。

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

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	电话传输质量、电话设施、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网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