国 际 电 信 联 盟

ITU-T

Y.2721

(09/2010)

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)的身份管理要求和使用案例

ITU-T Y.2721 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
运行于NGN的IPTV	Y.1900–Y.1999
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
智能泛在网络	Y.2600–Y.2699
安全	**Y.2700–Y.2799**
通用移动性	Y.2800–Y.2899
电信级开放环境	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.2721 建议书

下一代网络（NGN）的身份管理要求和使用案例

摘要

本建议书阐述下一代网络（NGN）的身份管理（IdM）使用案例示例和要求及其接口。IdM的功能和能力旨在增加身份信息的信任。同时支持并改善业务和安全应该（包括基于身份的服务）。

本建议书阐述的要求适用于ITU-T Y.2001建议书定义的下一代网络（NGN）（即，受管理的分组网络）。

本建议书提出的目标和要求以ITU-T Y.2720建议书规定的IdM框架为基础，同时对NGN的使用案例示例进行了分析。使用案例旨在提供信息，并在本建议书的附录中记录成文。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T Y.2721	2010-09-16	13

关键词

联合身份、身份管理、下一代网络、安全。

前言

国际电信联盟（国际电联）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）是国际电联的常设机构，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

ITU-T Y.2721 建议书

下一代网络（NGN）的身份管理要求和使用案例

1 范围

本建议书提供下一代网络（NGN）的身份管理（IdM）目标、要求、导则和使用案例示例及其接口。IdM的功能和能力旨在增加身份信息的信任；增加身份信息的信任，同时支持并改善业务和安全应用（包括基于身份的服务）。

本建议书的范围包括目标、要求、导则和使用案例示例，旨在：

- 增加NGN实体（如用户、团体、用户装置、服务提供商、企业、联合、网元和对象）身份信息的信任及其一个或多个身份。
- 根据用户的具体和知情同意，保证对身份信息寿命周期的管理（如注册、证实、吊销）。
- 通过IdM推动业务（如多个应用服务的单点登录和退出）和安全应用（如接入控制），包括基于身份的服务（如认证、断言和联合身份）。
- 根据用户的具体和知情同意，确保发现和交换与NGN实体的一个或多个身份有关的信息，其中包括可能置于NGN内或跨越不同管理域或联合的信息。
- NGN提供商域内（即网内）IdM系统和能力的互通/互操作。
- 根据用户的具体和知情同意，不同提供商域或联合（如NGN提供商、网络服务提供商和内容提供商之间）之间的IdM系统和能力的互通/互操作。
- 执行与实体身份或身份信息相关的适用政策（如保护个人可识别信息）。
- IdM系统、功能、能力、数据和通信的安全。

本建议书阐述的目标和要求适用于[ITU-T Y.2001] – 下一代网络（NGN）概述 – 定义的NGN（即，受管理的分组网络）。

本建议书提出的目标和要求以[ITU-T Y.2720]建议书规定的IdM框架为基础，并在各附录中对使用案例示例分析予以记录。

注1 – 本建议书中使用的与IdM有关的“身份”这一术语不表示本身的含义，尤其不能构成通常意义的对个人身份的证实。

注2 – 本建议书中使用的“用户”可以是个人、团体、公司或法律实体，或任何使用NGN服务日其他实体。

注3 – 本建议书中“NGN/IdSP（身份服务提供商）”术语的使用旨在表示可以是NGN提供商或是提供IdM服务的第三方。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T E.107] ITU-T E.107建议书（2007）– 应急通信服务（ETS）以及国家实施ETS的互连框架

[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

[ITU-T X.1252] ITU-T X.1252建议书（2010）– 身份管理基准术语定义

[ITU-T Y.2001] ITU-T Y.2001建议书（2004）– 下一代网络（NGN）概述

[ITU-T Y.2012] ITU-T Y.2012建议书（2010）– 下一代网络（NGN）的功能要求和架构

[ITU-T Y.2201] ITU-T Y.2201建议书（2009）– ITU-T NGN的要求和功能

[ITU-T Y.2205] ITU-T Y.2205建议书（2008）– 下一代网络 – 应急通信 – 技术考虑

[ITU-T Y.2702] ITU-T Y.2702建议书（2008）– 下一代网络（NGN）的认证和授权要求第1版本

[ITU-T Y.2720] ITU-T Y.2720建议书（2009）– 下一代网络（NGN）身份管理框架

3 定义

3.1 国际电联其它建议书定义的术语

本建议书使用了其它文件定义的下列术语。

3.1.1 匿名性[ITU-T X.1252]：在一组用户实体中不能确定一个实体的情况。

注 — 匿名性防止跟踪实体或其行为，如用户的位置、服务使用频率等。

3.1.2 断言[ITU-T X.1252]：（一个实体）在没有有效性凭证的情况下做出的声明。

3.1.3 属性 [ITU-T X.1252]：绑定到一个实体的信息，规定了一个实体的特征。

3.1.4 认证 [ITU-T X.1252]：为在实体和所表示的身份之间的约束力达到足够的信任所使用的程序。

注 — 在身份管理（IdM）情况下采用期限认证意味着实体认证。

3.1.5 认证保证[ITU-T X.1252]：在认证过程中所达到的信任度，通信伙伴是其声称是或预计是的实体。

注 — 信任是基于通信实体与其表示的身份之间的约束力的信任程度。

3.1.6 授权[ITU-T的X.1252]：授予权利，并根据这些权利准许访问。

3.1.7 绑定[ITU-T X.1252]：明确形成的相关性、捆绑关系或纽带。

3.1.8 声称[ITU-T X.1252]：声明情况如此，无法提供证据。

3.1.9 要求者[ITU-T X.1252]：要求认证的实体或该实体的代表。要求者包括代表实体进行认证交换所需的功能。

注 — 要求者包括代表委托人从事认证交换所必须的功能。

3.1.10 语境[ITU-T X.1252]：确定实体存在和互动的边界条件的环境。

3.1.11 证书[ITU-T X.1252]：作为被声称的身份和/或权利的证明的一组数据。

3.1.12 分派[ITU-T X.1252]：向另一对象分配权力、责任或功（职）能的行动。

3.1.13 发现[ITU-T Y.2720]：一种定位机器可处理网络资源描述的行动，这种行动以前可能是未知的，它满足一定功能标准。它涉及将一系列功能和其它标准与一系列资源描述相匹配。发现的目的是寻找适当的服务资源。

3.1.14 实体[ITU-T X.1252]：任何可单独识别的独立生存的事物。可在一定范围内识别。

注 — 一个实体可以是自然人、动物、法人、组织、主动或被动的事情、设备、软件应用、服务等或这些实体的组合。在电信方面，实体的例子包括接入点、签约用户、用户、网元、网络、软件应用、服务和设备、接口等。

3.1.15 应急通信（ET）[ITU-T Y.2205]：应急通信指任何相对于其它业务而言需要NGN特别处理的与应急相关的服务。它包括政府授权的应急服务和公共安全服务。

3.1.16 应急通信服务（ETS）[ITU-T E.107]：一项国家级服务，它在灾难和应急情况下为ETS授权用户提供优先通信服务。

3.1.17 联合[ITU-T X.1252]：用户、服务提供商和身份服务提供商构成的联合体。

3.1.18 联合身份[ITU-T Y.2720]：用来接入通过政策和联合条件捆绑一起的一组服务或应用的身份。

3.1.19 识别码[ITU-T X.1252]：用来确定语境中的一个实体一个或多个属性。

注 — 在[b-ITU-T Y.2091]中定义的NGN语境中，识别码是用来识别签约用户、用户、网络元素、功能、提供服务和应用的网络实体或其它实体（如物理或逻辑对象）的一系列数字、字符、符号或其它任何形式的数据。

3.1.20 身份[ITU-T X.1252]：以一个或多个属性表示一实体，使实体足以在语境内得到区分。在IdM中，身份这一术语被理解为语境下的身份（属性子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）框架。

注 – 各实体通过一个综合身份表示，它包括所有描述该实体特点的可能信息元素。然而，这种综合身份是一个理论问题，不包括任何描述和实用情况，因为可能的属性数量是无限的。

3.1.21 身份保证[ITU-T X.1252]：用来确定获得证书的一实体身份的身份证实和核实过程中的信任程度，以及对有关使用该证书的实体就是证书被颁发或分配的实体的信任程度。

3.1.22 身份管理[ITU-T Y.2720]：用于以下目的的一套功能和能力（如，行政管理、管理和维护、发现、通信交流、关联和捆绑、政策执行、认证和断言）：

- 身份信息（如，识别码、证书、属性）保证；
- 实体（如，签约用户/用户、团体、用户装置、机构、网络和服务提供商、网元和对象及虚拟对象）身份的保证；
- 实现业务和安全应用。

3.1.23 身份模式[ITU-T X.1252]：对实体属性的结构表示（如实体行为），可用于一些识别过程。

3.1.24 身份提供方：见身份服务提供方（IdSP）。

注 — 术语“身份提供方（IdSP）”在ITU-T Y.2720]和其他组织的规范中使用。然而，为了避免误解，它可以被解释为表示提供身份的实体，而不是管理身份的实体，期限身份服务提供方(IdSP) 在本建议书中使用。

3.1.25 身份服务提供方（IdSP）[ITU-T X.1252]：认证、维护、管理并可能创建和分配其他实体身份信息的实体。

3.1.26 下一代网络（NGN）[ITU-T Y.2001]：能够利用宽带和具有服务质量（QoS）机制的传输技术的、提供电信业务的分组网络。该网络中提供的与业务相关的功能独立于底层与传输相关的技术。该网络允许用户不受限地接入网络，并自由选择服务提供商和/或服务。该网络支持通用移动性，使得网络可以随时随地向用户提供统一一致的业务。

3.1.27 个人可识别信息（PII）[ITU-T X.1252]：a) 识别或可用于识别、联系或找到信息与之相关的个人的信息；b) 可由之推出识别或联系信息的信息；c) 与自然人或可与自然人直接或间接联系一起的信息。

3.1.28 现状[ITU-T Y.2720]：一套说明一实体现状的属性。

3.1.29 主体[ITU-T X.811]：身份可被认证的实体。

3.1.30 隐私[ITU-T X.1252]：个人的控制或影响权，涉及与其个人相关的哪些信息可能被收集、管理、保留、访问、使用或分发。

3.1.31 依赖方（RP）[ITU-T X.1252]：在要求的语境下，依赖于身份表述或请求/断言实体的声称的实体。

3.1.32 安全域[ITU-T X.1252]：一套元素、一项安全政策、一个安全权力机构和其中元素须按照安全政策进行管理的安全相关活动。

3.1.33 信任[ITU-T X.1252]：在一定语境内，对信息可靠性和真实度或对实体适当行事能力的高度信任。

3.1.34 用户[ITU-T X.1252]：使用如系统、设备、终端、流程、应用或公司网络等资源的实体。

注 — 在NGN的语境中，根据[b-ITU-T Y.2091]，它包括最终用户、个人、签约用户、系统、设备、终端（例如，传真、PC）、（功能）实体、过程、应用、供应商或公司网络。

3.1.35 核实方[ITU-T X.1252]：核实和验证身份信息实体。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书采用下列缩写：

3G 第3代（3rd Generation）
AKA 认证和密钥协议（Authentication and Key Agreement）
ANI 应用到网络接口（Application-to-Network Interface）
API 应用程序界面（Application Programming Interface）
BSS 业务支持系统（Business Support System）
CSP 通信服务提供商（Communications Service Provider）
DDoS 分步式拒绝服务（Distributed Denial of Service）
DeviceID 装置身份（Device Identity）
DoS 拒绝服务（Denial of Service）
EAG 外部应用网关（External Application Gateway）
EDS 企业目录服务（Enterprise Directory Service）
ET 应急通信（Emergency Telecommunications）
ETS 应急通信服务（Emergency Telecommunications Service）
EV-DO 优化演进数据（Evolution Data Optimized）
FE 功能实体（Functional Entity）
FTTX 光纤到X（Fiber-To-The-X）
GBA 一般性自举架（Generic Bootstrapping 架构）
HSS 归属签约用户服务器（Home Subscriber Server）
IBGC-FE 互连边界网关控制功能实体（Interconnection Border Gateway Control Functional Entity）
IdM 身份管理（Identity Management）
IdMCC-FE IdM协调和控制功能实体（IdM Coordination and Control Functional Entity）
IdSP 身份服务提供商（Identity Service Provider）
IDPS 入侵发现和预防系统（Intrusion Detection and Prevention Systems）

ID-WSF	身份网络服务框架（Identity Web Services Framework）
IMS	IP多媒体子系统（IP Multimedia Subsystem）
IP	互联网协议（Internet Protocol）
IPTV	IP电视（IP Television）
ISC	IMS服务控制（IMS Service Control）
IT	信息技术（Information Technology）
KDC	密钥分配中心（Key Distribution Center）
LS	位置服务器（Location Server）
LTE	长期演进（Long Term Evolution）
MNO	移动网络运营商（Mobile Network Operator）
MSISDN	移动签约用户综合业务导向号码（Mobile Subscriber Integrated Service Director Number）
NACF	网络附着控制功能（Network Attachment Control Functions
NGN	下一代网络（Next Generation Network）
NNI	网络到网络接口（Network-to-Network Interface）
OAM&P	操作、管理、维护和调配（Operation, Administration, Maintenance and Provisioning）
OSS	操作支持系统（Operations Support System）
PC	个人计算机（Personal Computer）
P-CSC-FE	代理呼叫会话控制功能实体（Proxy Call Session Control Functional Entity）
PDA	个人数字助理（Personal Digital Assistant）
PII	个人可识别信息（Personally Identifiable information）
POTS	普通老式电话系统（Plain Old Telephone System）
PS	现状服务器（Presence Server）
PSTN	公众交换电话网（Public Switched Telephone Network）
QoS	服务质量（Quality of Service）
RACF	资源和接纳控制功能（Resource and Admission Control Functions）
RFID	射频识别（Radio-Frequency Identification）
RP	依赖方（Relying Party）
SAA-FE	服务认证和授权功能实体（Service Authentication and Authorization Functional Entity）
SAML	安全断言标记语言（Security Assertion Markup Language）
S-CSC-FE	呼出呼叫会话控制功能实体（Serving Call Session Control Functional Entity）
SIM	用户身份模块（签约用户 Identity Module）
SIP	会话起始协议（Session Initiation Protocol）
SLA	服务水平协议（Service Level Agreement）
SN	服务节点（Service Node）
SNI	服务器到网络接口（Server-to-Network Interface）
SP	服务提供商（Service Provider）

SUP-FE 业务用户资料功能实体（Service User Profile Functional Entity）
TGS 票据授权服务器（Ticket Granting Server）
UE 用户设备（User Equipment）
UICC 通用集成电路卡（Universal Integrated Circuit Card）
UNI 用户到网络接口（User-to-Network Interface）
URI 统一资源标识符（Uniform Resource Identifier）
UserID 用户身份（User Identity）
VoD 视频点播（Video on Demand）
VoIP 互联网协议电话（IP电视）（Voice over Internet Protocol）
WiFi 无线保真（Wireless Fidelity）
WiMAX 微波接入全球互操作性（Worldwide Interoperability for Microwave Access）
WLAN 无线局域网（Wireless Local Area Network）
WS 网络服务器（Web Server）
WSG 网络服务网关（Web Service Gateway）
xDSL x数字用户线（x Digital Subscriber Loop）

5 惯例

本建议书中：

关键词“**要求**”表示必须得到遵守的要求，且如果声称遵守本文件，则不得与该要求有任何偏差。

关键词“**建议**”表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键词“**禁止**”表示必须得到遵守的要求，且如果声称遵守本文件，则不得与之有任何偏差。

关键词“**作为选择可以**”表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。也就是说，厂商可以作为选择提供这一功能，同时仍然声称遵守本文件提出的规范。

在本文件正文和附件中使用了*必须*、*不得*、*应*和*可能*等术语，应分别将这些理解为*要求*、*禁止*、*建议*和*作为选择可以*。附录或其它明确标为*资料性*材料中出现的此类短句或关键词应被理解为不含有任何规范性意图。

6 IdM概述

6.1 综述

[ITU-T Y.2720]建议书提供了 IdM 的框架。IdM 的功能和能力旨在增加身份信息的信任、保证实体的身份并支持业务和安全应用（如接入控制和授权），包括基于身份的服务。实体是单独和独特存在的、可被进行独一无二识别的任何事物（个人）。在 IdM 语境中，实体示例包括签约用户、用户、网元、网络、软件应用、服务和装置。

NGN 将支持最终用户/签约用户、政府和商业企业所用的广泛应用服务。为保障应用服务的完整性并确保其安全性，建议同，NGN 支持必要的功能和能力以保证具体语境中与实体相关的身份和身份数据所不可或缺的。有关 IdM 的定义见[ITU-T Y.2720]建议书。

下列附件记录的使用案例示例在确定 IdM 要求时得到了考虑：

- 附录一 — 一般性IdM使用案例
- 附录二 — NGN应用的IdM使用案例
- 附录三 — 与应急通信服务（ETS）相关的IdM使用案例
- 附录四 — 与移动相关的使用案例。

此外，在确定 IdM 要求时还考虑到了 NGN 环境中与最终用户身份相关的下列因素：

- 日益增多的、最终用户使用多种身份的现象
- 身份可能与不同语境和服务特权相关
- 身份可能只能部分地识别最终用户
- 假名可作为身份
- 身份可能被随时随地由任何装置加以使用
- NGN提供商之间的身份可能无法互操作。

6.2 IdM关系

图1概要提供按照[ITU-T Y.2720]确定的框架理出的IdM关系。

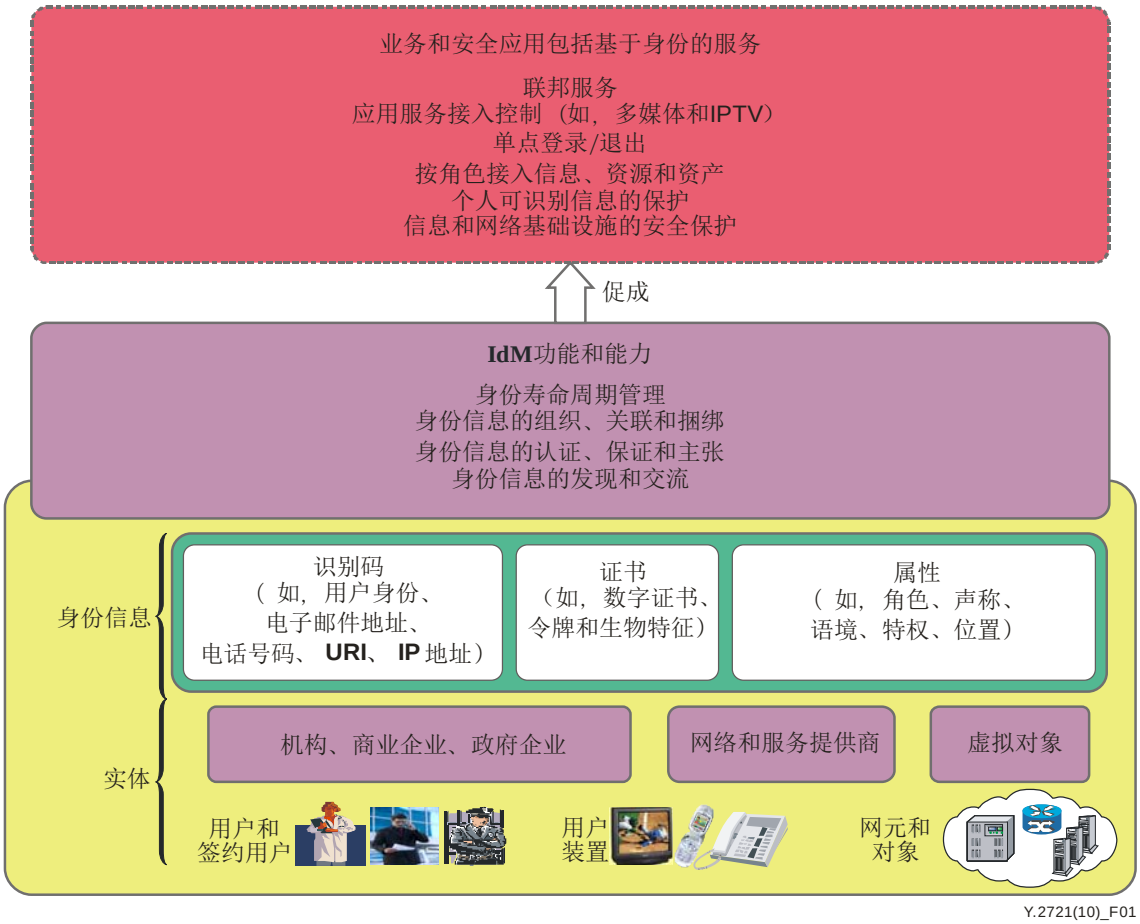


图1 – IdM 关系

这些实体包括个人用户和各类繁多的机构，如企业和虚拟对象（如电子应用）。与实体相关的身份信息既包括敏感信息，也包括相对公开的信息，如在公共号码簿中所列出的电话号码，同时还涵盖高度敏感的身份数据，如密码、数字证书和其它进行私人认证的信息。

一个实体可以有一个或多个身份。这些身份可以表示多种角色（如公民、配偶、父母、客户和病人）并涵盖从商业到社会活动的具体交易过程。根据图 1 所示的不同语境，一个个人可能与多种数字身份相关。此外，通过数字身份行事的个人可能通过在公众或社会上被设想或表现为一个或多个人，或通过某种权力机构分配的角色（如应急响应者）而被其它人所熟悉。

图 1 显示了下列内容：

a) 实体

在服务是基于语境和角色、且随时随地可由任何装置访问的 NGN 环境中，与实体相关的身份信息可能呈多种形式。此外，实体可能根据语境拥有一个或多个身份。实体示例包括：

- 用户和签约用户
- 用户装置、网元和对象
- 机构、团体、商业企业和政府企业

- 网络和服务提供商
- 虚拟对象。

b) 身份信息

与实体相关的身份信息可组合如下：

- 识别码（如，签约用户、网络元素地址、服务提供商识别码）
- 属性（例如、电子邮件地址、电话号码、URI、IP地址、角色、声称、特权、认证方法、模式和位置）。
- 证书（如，数字证书、令牌）

c) IdM功能和能力

IdM 功能和能力用来增加身份信息的信任，保证实体的一个或多个身份，并支持或改善业务和安全应用，包括基于身份的服务。IdM 功能和能力示例包括：

- 身份寿命周期管理
- 身份信息的组织、相互关联和捆绑
- 认证、认证保证和断言
- 身份信息的发现和交流
- 桥接不同IdM系统以促进互操作的功能和能力

d) 业务和安全应用

旨在支持并改善业务和安全应用，包括基于身份的服务的 IdM 功能和能力。

业务应用示例包括：

- 联合服务（如，跨越不同联合或NGN提供商接入服务）
- 单点登录和退出（如，无需向各应用或服务平台重新提交认证证书的情况下接入多项应用和服务）

安全应用示例包括：

- 接入控制
- 授权和特权管理
- 个人可识别信息（PII）的保护

基于身份的服务示例包括：

- 识别码、认证证书和属性服务
- 桥接服务（在异质环境中的身份信息的映射和互通）
- 模式信息服务

IdM 包括寿命周期从始至终的管理过程，以及发现和获得权威身份来源（用以核实身份及有效性）的功能和能力。IdM 服务和能力有利于实体对其身份信息的使用和传播方式进行控制。IdM 为实体（如依赖方）提供必要信息，使其做出有关身份保证的决定，并对相关的交易和通信怀有信任。IdM 还有利于联合成员分享和使用联合身份信息（如不同 NGN 提供商、商业企业或政府企业），以支持联合服务。例如，联合身份服务有助于得到授权的联合成员用户根据联合规则和政策获得基于其角色和特权的资源，同时无需针对每一个联合成员进行注册和认证。

6.3 驱动因素和动机

由于诸多NGN服务和能力涉及基于签约用户身份和喜好、并可由任何装置随时随地接入的个性化服务，因此IdM解决方案必须实时对日益复杂的互动（如客户在不同装置间的移动）、接入技术、支付方式甚至身份做出响应。此外，最终用户还要求功能特性简便和易于使用。更加重要的是，最终用户要求的能力要有利于用户控制其隐私性和个人可识别信息（PII）。

IdM的驱动因素和动机源于最终用户（如应用和服务签约用户）、NGN提供商、商业和政府企业，所有各方都要求通过实施IdM保护其利益并满足其需求。在确定NGN的IdM要求时考虑到了下列因素：

- 最终用户/签约用户需要控制和保护其在线个人身份信息，希望以灵活和统一的方式获取资源，并在享受社交网络益处和暴露个人信息之间达成平衡。
- NGN提供商（网络和服务提供商）需要保护其网络基础设施资源、服务和应用，推行联合服务，普及基于签约的服务并满足最终用户有关保护隐私和个人可识别信息（PII）的需求。
- 保护网络基础设施不受网络攻击并保护私人数据。
- 政府企业需保护其网络基础设施免受网络攻击影响，保护其公民的私人数据，并支持电子政府服务、公共安全服务、早期预警服务、应急通信服务（ETS）和其它国家性服务。

6.4 多服务提供商和联合环境

IdM服务和能力在多服务提供商和联合环境中可被用于发现和交流相关信息以便建立对实体身份的信任。例如，可由被视为依赖方信任的身份服务提供商核实与身份相关的识别码、证书和属性，并通过断言向依赖方（如用户、服务提供商）通报这些信息，从而支持作为接入控制基础的认证、业务决定和适用政策（如保护隐私和个人可识别信息）的执行。

此外，一些不同和独立的IdM解决方案可能要求在不同服务提供商之间实现互操作性。

6.5 身份服务提供商（IdSP）

本建议书不强行规定有关谁应提供身份服务（IdSP）的限制。

IdSP是创建、维护和管理其它实体（如用户/签约用户、机构和装置）受信赖的身份信息的实体，并根据信任、业务和其它类型关系提供基于身份的服务。

在多服务提供商环境中，NGN提供商有可能是一个IdSP，同时还可能向其它提供商提供身份管理服务（如基于身份的服务）。

在本建议书中，“NGN/IdSP”这一术语表示NGN提供商，或提供IdM服务的第三方。

6.6 NGN架构语境中的IdM和参考模型

6.6.1 与NGN功能架构的关系

在[ITU-T Y.2012]中规定，在NGN参考架构模型语境中，与IdM有关的功能可能存在于分布式架构中的不同平面（如用户、控制和管理平面）和层（如业务层和传输层）中。从落实和实施的角度而言，支持IdM服务和能力可能涉及到NGN中现有网元和补充网元（如专业应用服务器）的使用。

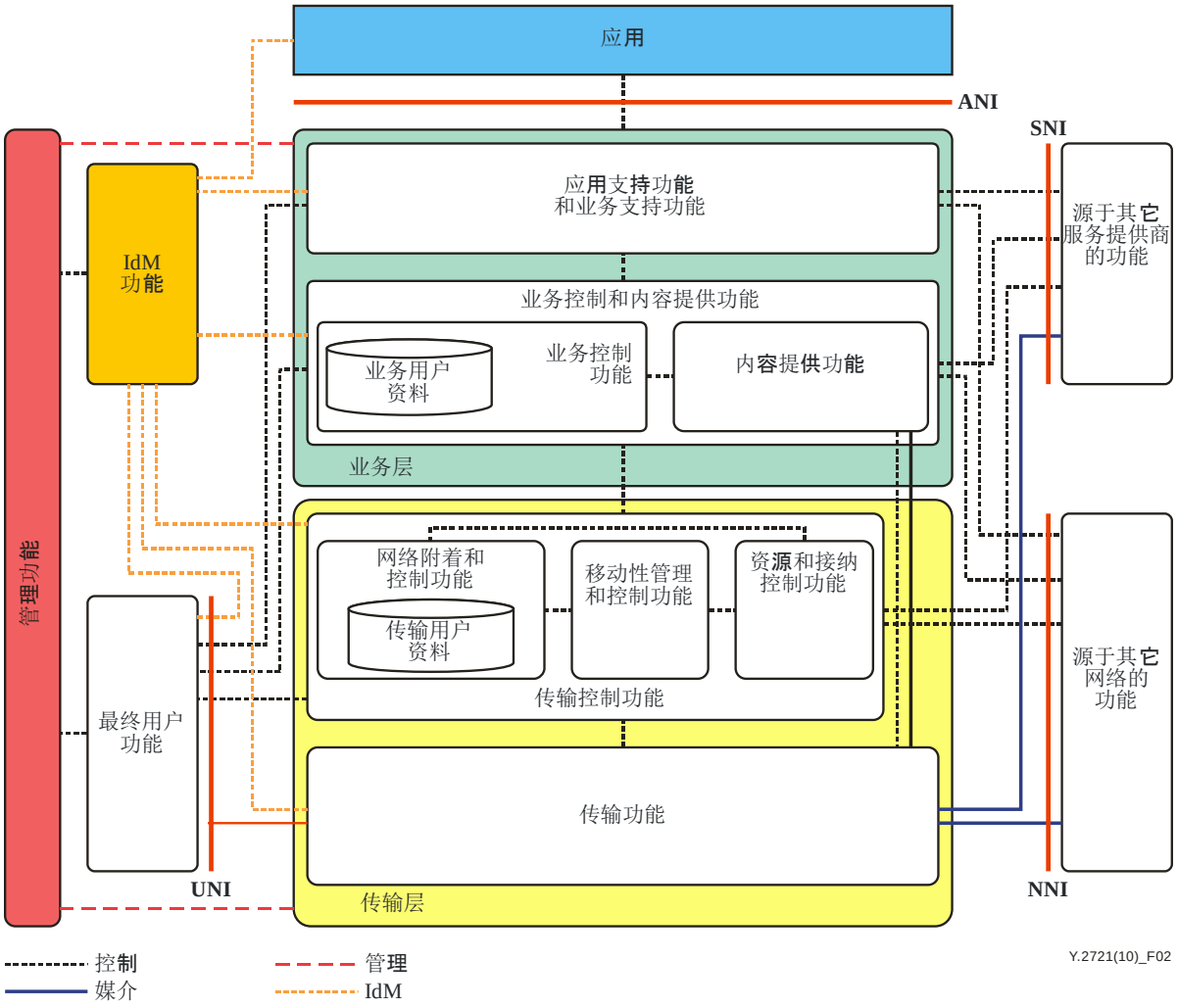


图 2 – NGN 架构概述

[ITU-T Y.2012]中图7-1包含的功能块代表NGN功能架构中的IdM功能。[ITU-T Y.2012]的图7-1说明这样的总体概念，即支持IdM服务和能力可能需要与特定功能实体（FE）进行互动，以实现和支持包括身份服务在内的服务。根据所支持的具体IdM服务或能力以及实施设计，其中可能包括与下列功能块中的FE的互动：

– 应用；

– 业务层：应用支持功能和业务支持功能、业务控制功能和内容提供功能；

– 传输层：传输控制功能和传输功能；

– 最终用户功能；

– 管理功能。

在NGN功能架构中，IdM功能可能存在于分布式架构中的不同平面（如用户、控制和管理平面）和不同层（如业务层和传输层）中。虽然上图所示的IdM功能为自成一体的一套功能，但其目的并非在于为IdM的实施设计强行提出要求或限制。实施身份管理功能应遵守相关政策，如保护身份数据（例如，PII）的国家和地区的法规和立法。具体来说，实施和使用的IDM功能必须确保遵守基本数据保护原则的相关政策：

• 数据与一个特定的目的结合；

• 不同用途的应用程序之间不数据共享；

• 数据限制为特定目的的最低所需要；

• 人有控制其PII的权利。

注 — 对于某些特定国家的法规，这可能意味着 IdM功能在不同的NGN层面分开实施。

6.6.2 外部接口和IdM通信

[ITU-T Y.FRA REV2]确定的标准接口用于在不同管理域和联合之间交流身份数据，其中酌情包括下列接口：

• 用户到网络接口（UNI）

• 网络到网络接口（NNI）

• 应用到网络接口（ANI）

• 服务器到网络接口（SNI）

接口解决方案取决于下列因素：具体应用和服务需求（如实时与近实时）、协议解决方案（如SAML、diameter、远程用户拨号认证系统（radius）、SIP）和相关机制和方式。

有关实现IdM的情形示例见附录五，该示例具体说明如何应用NGN的外部接口。

6.6.3 交易模型

[b-ITU-T X.1250]具体阐述涉及多方（如用户、身份服务提供商和依赖方）的交易模型示例。有关对[b-ITU-T X.1250]描述的交易模型的总结见附录五。

7 IdM的目标

IdM的总体目标如下：

1) 促进实体之间的信任决定。

2) NGN支持的IdM解决方案应在最大程度上降低对用户/签约用户的影响。

3) 涉及新能力的解决方案应提供适当的过渡解决方案。

4) 在NGN提供商域中支持互操作的IdM解决方案。例如，支持多应用服务（如VoIP、IPTV、视频和数据）的不同厂商产品之间的互操作性。

5) 根据适用的业务安排和关系并根据PII的保护法规和政策的应用。支持不同NGN提供商和业务提供商域和联合之间的、可互操作的IdM解决方案。

6) 根据适用的业务安排和关系并根据PII的保护法规和政策的应用。支持异质IdM系统和联合的桥接。例如，提供便于NGN提供商的IdM系统和其它类型IdM系统（如网络服务、内容和第3方提供商的IdM系统）之间实现桥接的能力。

7) 最终用户/签约用户能够方便自如地实现互动并使用应用服务，同时在其整个寿命周期保持对自己的个人数据的控制。这其中包括何时、由何人以及以何种方式使用信息。

8) 最终用户/签约用户根据适用的政策在建立相互信任的关系和开展交易时，仅需要透露必不可少的信息。

9) 最终用户/签约用户能够检查提出身份数据要求和PII的实体的真实性。在此的一个的目标是最终用户/签约用户能够根据语境使用多个识别码。

10) 最终用户/签约用户根据应用语境和适用政策，能够匿名、以假名或以实名进行操作。

8 对IdM的要求

本节根据[ITU-T Y.2201]中有关对NGN的概括要求，阐述适用于NGN的对IdM的要求。

8.1 总体要求

以下为针对身份管理的总体要求：

R-1 要求NGN/IdSP支持由NGN支持的各种不同类型实体的身份管理功能和能力：

a) 用户/团体

b) 机构/联合/企业/服务提供商

c) 装置/网元/系统

d) 对象（如应用程序、内容、数据）。

R-2 要求NGN/IdSP支持：

a) 寿命周期的安全管理（如从实体的注册到吊销）

b) 与实体一个或多个身份有关的身份信息的安全发现和交流，其中包括可能位于NGN内和跨不同管理域的身份信息的发现和交流。

R-3 要求NGN/IdSP支持执行与实体身份或身份信息相关的适用政策。

R-4 要求NGN/IdSP支持实时（如VoIP和IPTV）和近实时应用（如基于网络的数据交易）的IdM功能和能力。

R-5 要求NGN/IdSP支持根据适用政策方便匿名断言身份信息（如身份和属性）的IdM功能和能力。

R-6 要求NGN/IdSP支持IdM在NGN提供商域内不同网元（即网内）和不同提供商域（如其它NGN提供商、网络服务提供商）之间的安全互通。

R-7 要求NGN/IdSP支持便于最终用户使用的业务和功能特性，如：

a) 多种应用服务的单点登录/退出

b) 融合业务（如固定和移动融合）

c) 控制和保护个人可识别信息（PII）。

R-8 根据应用的安全要求，适用时，要求NGN/IdSP支持应用服务的单点登录，使用与签约用户设备相关的证书（例如，UICC证书），或与用户/签约用户相关的证书 (例如，SIP摘要证书)。具体为：

- 应可使用签约用户证书 (如，SIP摘要证书) 通过移动设备访问的应用程序，支持单点登录。
- 应可使用签约用户证书 (如，SIP摘要证书) 通过固定设备访问的应用程序，支持单点登录。

8.2 有关身份寿命周期的管理要求

身份寿命周期管理涉及与实体身份相关的身份及信息（如识别码、证书和属性）的吸纳和颁发的过程和程序。

R-9 要求NGN/IdSP制定并执行有关身份寿命周期管理的适用政策，其中包括证明、吸纳、颁发和吊销身份信息的过程、程序和政策。

8.2.1 注册和发布

实体（如签约用户、装置、机构、NGN提供商或对象）注册到语境中的开始是身份或证书的证明和注册。注册是实体进入语境的过程，包括实体身份的记录，以及可能对特定属性（例如，标识符）或证书或角色）的分配。在最终用户为签约用户的情况下，该程序为申请人申请成为IdSP或NGN提供商的签约用户。

证明包括核实并验证属性和可能相关的证书。

R-10 要求NGN/IdSP在注册和颁发身份时应按照语境的要求证明和核实实体。对于具体语境，实体身份的记录和标识符、证书和属性的分配和属性服从适用的标准和政策的成功确认。

证明过程和政策须基于获得和使用身份的、未经授权的实体的身份和与之相关的风险所允许的资源价值（如服务、交易、信息和特权）。具体而言，需采取确保下列方面的措施：

- 具有声称属性的实体（如个人、机构或法律实体）确实存在，且这些属性足以对该实体进行独一无二的识别；
- 其身份已记录的申请人事实上是享有该身份的实体；
- 对于已使用记录的身份和证书的实体，以后否定注册/登记并争端认证是很困难的。

成功完成注册和证明过程后即可记录身份，可包括分配的属性和/或给予实体在未来将得到认证的证书。

R-11 要求只有在成功进行过实体身份证明之后才颁发身份及相关的身份信息（识别码、证书和属性）。

在某些情况下，这可能涉及到与身份捆绑的数字证书（如电子证书）和令牌的注册和颁发或对身份做出声称（即属性）。根据所用的令牌类型，NGN/IdSP或创建新的令牌，并将之提供给签约用户，或要求签约用户就申请人已拥有或新创建的令牌进行注册。

R-12 在上述任何一种情况下，均要求令牌始发点到另一方之间的传送机制是安全的，以确保维护新创建令牌的秘密性和完整性。

8.2.2 维护和更新

在包括身份信息（识别码、证书和属性）在内的身份得到注册和颁发之后，NGN/IdSP和签约用户均在操作和使用阶段有责任保护其安全。

R-13 要求NGN/IdSP安全地管理和维护与身份相关的数据和数据状况（如识别码、证书、属性）。

R-14 要求NGN/IdSP安全地管理和记录身份的更新和变化。

R-15 要求NGN/IdSP定期证实身份的状况。

R-16 要求NGN/IdSP支持相关程序，以通知需要了解身份更新和变化的系统及网元有关身份的更新或变化。

R-17 要求NGN/IdSP 提供告知用户有关其身份的数据、更改或删除的功能。

签约用户亦有责任按照与NGN/IdSP签订的业务和政策协议，确保得到分配的证书的安全。例如，签约用户有责任管理其电子证书（如令牌）并保证其安全。

R-18 要求NGN/IdSP根据业务和合同协议采取措施，确保一个实体（例如，签约用户或其他NGN/IdSP）按照适用的身份相关的法规和政策，安全管理和发布的证书（如数字证书或令牌）。

8.2.3 吊销

吊销身份是撤回身份及相关证书的过程。颁发身份或证书的一方或系统（如NGN/IdSP）负责终止或撤除身份。要求吊销程序做到防止已失效或安全受到破坏的身份或证书继续得到使用。

R-19 要求NGN/IdSP建立和执行有关吊销身份的适用政策。具体而言，需支持这样的能力，即当身份已失效或其安全受到破坏时终止或销毁与身份相关的证书（如数字证书或令牌）。

R-20 要求NGN/IdSP支持相关程序，以便向需要了解情况的实体和系统和网元通知有关身份或与身份相关的数据的吊销或终止情况（即通知所有需要利用身份接入的系统和程序有关身份已失效的情况）。

8.3 身份管理的OAM&P功能

8.3.1 数据模型和略图（schema）

每一个NGN提供商、联合或企业均可拥有其自身的旨在表述和共享有关身份的数据和信息的格式、略图、定义或语义。[ITU-T Y.2720]第8.2.1段说明有必要实现使用不同数据模型、结构和略图的异质IdM系统间的互操作性。

R-21 要求NGN/IdSP支持有利于实现使用不同数据模型、结构和略图的异质IdM系统之间互操作性的功能和能力。

8.3.2 身份数据管理

[ITU-T Y.2720]第8.2节说明有必要对身份数据进行管理（如管理识别码、证书和属性）。有关身份数据管理的详细要求不在本建议书的范围之内。

在NGN中，可通过不同的管理系统和操作程序（如操作支持系统（OSS）/业务支持系统（BSS））管理不同身份数据（如电子邮件地址、电话号码、URI和IP地址等识别码）。下列一般性要求适用于为支持IdM服务和能力而在不同管理系统和客户关照系统之间实现互动而采用结构化和协调方式的环境。

R-22 要求NGN/IdSP支持标准接口（如客户门户），以方便最终用户/签约用户与支持最终用户/签约用户身份数据管理交易（如更改和更新）的相关NGN管理系统和程序实现互动，服从适用的数据保护法规和政策。

R-23 要求NGN/IdSP支持必要接口、功能和能力，以酌情推动与身份数据管理相关的不同管理系统和程序之间一致的交易和工作流程（如需通过不同OSS/BSS、客户关照系统和应用服务平台）的更改和更新，服从适用的数据保护法规和政策。

R-24 要求NGN/IdSP支持登录和存储（如备份数据）与身份数据管理相关的交易记录的功能和能力，服从适用的数据保护法规和政策。

R-25 要求NGN/IdSP支持将不同管理系统和程序之间身份数据的更改和更新统一一致的功能和能力，服从适用的数据保护法规和政策。

R-26 要求NGN/IdSP支持在与实体（如签约用户）相关的身份数据和合同服务（如接入、话音、数据、视频）之间联系进行核实的功能和能力，服从适用的数据保护法规和政策。

8.4 信令和控制功能

8.4.1 发现身份信息

在分布式NGN环境中，身份信息可能存在于不同网元内（如用户数据库、地点数据库、现状数据库、归属用户数据库等）。一个应用在使用身份信息时需要了解该信息确实存在，且需知道上何处去找到该信息。

R-27 要求NGN/IdSP支持在NGN/IdSP域内发现身份信息源的功能和能力。例如，身份管理服务器具有发现在其它网元中存在身份信息的功能和能力，如地点、现状或用户服务器，同时应用/服务需具有能力发现身份管理或其它托管身份数据的服务器。

R-28 要求NGN/IdSP支持使用标准接口和协议的功能和能力，以发现各不同NGN/IdSP域内的身份信息源。例如，根据适用的网间协议，使用标准接口和协议发现其它NGN/IdSP域内的身份信息源。

R-29 要求NGN/IdSP支持有关保护发现能力和机制的能力。

8.4.2 身份信息的接入控制

身份信息应只能由得到授权可接入该信息的实体接入。

R-30 要求按照适用的规则和政策仅由得到授权的实体接入身份信息。具体而言：

- 要求NGN/IdSP对提出身份数据要求的实体（如依赖方）进行认证，或进行相互认证。
- 要求NGN/IdSP在提供信息接入之前或在交换所要求的身份数据之前，对提出身份数据要求的实体（如依赖方或申请方）的授权进行证实。

8.4.3 IdM通信

网络系统和网元需要建立通信会话来交流位于不同网络系统（如身份管理服务器、用户服务器、地点服务器、现状服务器等）之间的、能够相互关联和得到核实（即，由提供认证和关联功能的IdM应用服务器进行）的身份信息（如识别码、证书和属性），以提供身份保证能力。

NGN/IdSP可向依赖方通报有关身份及其相关属性（如声称和特权）的断言，以便后者做出接入控制决定。这将有助于不同应用服务（即不同厂商平台）使用共同的IdM基础设施，而非使用独立的各自为政的解决方案。应考虑的通信关系包括：

- 网内：与NGN提供商域（如网元之间）的通信
- 网间：不同NGN提供商之间的通信
- 联合：联合中不同成员之间的通信

8.4.3.1 实时和近实时通信

用于发现和交流身份信息的解决方案必须考虑是否要求实现实时或近实时通信，这将取决于得到支持的具体应用。某些应用（如VoIP和IPTV）可能需要证实提出要求的用户/签约用户的身份并对应用服务进行授权。其它应用（如数据和消息处理业务）可能只需要近实时通信会话来证实提出申请的用户/签约用户的身份并对应用服务进行授权。

R-31 要求NGN/IdSP根据具体应用服务要求支持建立通信的能力，以便以实时或近实时方式交流身份信息，其中包括在NGN提供商域内建立交流身份信息的通信会话，以及在不同NGN提供商和联合不同成员之间的身份信息的交流。

属性信息包括但不限于成员状况、附属功能（计费、操作）、由其它业务使用的属性（如目录服务或认证服务）。这有利于依赖方根据用户属性为用户提供量身定制的信息和内容。

R-32 NGN/IdSP与依赖方之间须能够交流与实体身份有关的断言，包括属性的断言。

8.4.4 相互关联和捆绑

可通过将身份信息（如识别码、证书和属性）相互关联来建立捆绑，从而保证实体的身份。例如，可以将与签约用户（如用户ID）、签约用户装置（如装置ID）和其它相关信息（如地点和模式数据）相关的身份信息进行相互关联来建立起捆绑关系，从而在更高级别上保证签约用户的身份（即对身份的有效性具有信任）。

R-33 要求NGN/IdSP支持将与身份相关的多份数据（如地点和模式）相关联的能力，从而建立起与实体身份恰当的捆绑关系。服从适用的数据保护法规和政策。使用这些功能需要用户的具体和知情同意。

注 — 一些国家的数据保护法规和政策可能会限制支持这一要求。

8.4.5 认证要求

在实体和身份的绑定中，认证是对实体身份建立信任的过程。实现认证保证的手段之一是说明量化实体身份或声称身份风险的目标和导则，其中包括在识别过程中确立哪些实体识别码比其它识别码更为重要，以及为何认证中使用的某些识别码不应具有同样的认证价值。

有关NGN的认证要求见[ITU-T Y.2702]。

以下为IdM认证的安全要求：

R-34 实体（例如用户、NGN/IdSP、依赖方）之间的相互认证应是可能的。

R-35 依赖方须可以向IdSP/NGN提出进行实体（如用户/签约用户）认证的请求。

R-36 IdSP/NGN须可以对实体（如用户/签约用户）进行认证并向依赖方提供结果。

R-37 依赖方需能够要求对于用户进行再认证，同时提出现有的或备选的再认证方法。

8.4.6 认证保证

认证保证系指对使用证书的实体即为身份已得到核实的实体的信任程度或水平（已为该实体颁发或分配了证书）。根据语境，应用服务可能需要有不同认证保证。有些情况下，需要根据认证保证的敏感度以及信息和交易的价值提供接入不同资源的不同认证强度。在此类情况下，NGN/IdSP及依赖方需要多于通常的更多细节（如认证方法、认证因素数量、认证环境等）来满足所期待的认证保证，其中涉及错误认证带来的潜在风险，或在实体（如最终用户）身份上确定适当的保证水平。带来潜在的更糟后果的错误认证要求有更高的保证水平。

R-38 要求NGN/IdSP根据所需的保证水平支持适当的认证方法。

R-39 依赖方须可以向IdSP/NGN说明其对实体认证所需的保证水平。

R-40 须可以在IdSP/NGN、依赖方和正在得到认证的实体（如最终用户或签约用户）之间商谈保证水平。

8.4.6.1 用户装置身份的保证和完整性

NGN将支持繁复多样的用户装置（如固定电话、无线手机、个人计算机、PDA、IP电视机顶盒）。附着于NGN的装置的软硬件元器件从简单到复杂，如果被窃或遭到破坏，则可被用来进行一些列的攻击活动。NGN 也需要支持设备（如“哑”终端或POTS设备），它无法提供所需的保护程度，这是公认的。

R-41 NGN/IdSP须可以支持这样的最终用户装置，即，硬件部分具有抗破坏的安全能力，从而以加密形式保存身份管理数据（如密码、数字密钥和证书），并利用该信息独特的识别最终用户装置。

R-42 NGN/IdSP须可以通过标准接口与最终用户装置中抗破坏硬件的安全能力进行通信，以支持将专门防篡改硬件部分作为信任条件而唯一标识并确保最终用户装置身份的安全应用服务。

在签约用户装置上执行、以便于用户与服务和本地装置功能特性进行互动的应用可能会潜在地使装置完整性受到破坏。广受欢迎的互联网应用，如网络浏览和电子邮件，可能会带来改变签约用户装置完整性的薄弱环节。软件和文件下载，特别是从并非得到信任的渠道进行此类下载，可能会使签约用户装置受到恶意代码、蠕虫、病毒和特洛伊木马病毒的侵害。可以在最终用户装置上设计和实施专门的抗破坏硬件部分，从而核实装置的完整性。例如，专门的抗破坏硬件部分可以包含厂商的特定算法和功能，以查验完整性是否受到了破坏。专门硬件部分可以包含一个参考模型，其中列出一整套人们熟知的、有效完整性衡量标准，以具体识别装置的正确代码并提供其参考数值。人们熟知的有效完整性衡量标准可用来将实际报告的数值与配置进行比较，并确定装置是否在吻合范围内。

R-43 NGN/IdSP须可以支持具有专门抗破坏硬件部分的最终用户装置，以对装置完整性进行检查并确认装置完整性与应用和服务相吻合。

R-44 NGN/IdSP须可以通过标准接口与最终用户装置中抗破坏硬件部分的安全能力进行通信，以支持依赖装置完整性检查和确认装置完整性吻合的安全应用服务。

带有PII及其它敏感数据的装置的丢失和被窃可能对个人、企业和政府企业带来严重后果。旨在独一无二地识别和确认受到信任的装置的完整性的专门硬件部分还可潜在地支持在最终用户装置上对PII和其它敏感数据进行加密和保护的能力。

R-45 NGN/IdSP须可以支持带有专门抗破坏硬件部分的最终用户装置，以便对最终用户装置上的PII和其它敏感数据进行加密和保护。

8.4.7 支持要求优先得到处理的业务

NGN的IdM系统和能力须支持要求得到比其它业务更优先处理的应用服务和通信会话。[ITU-T Y.2205]描述要求得到NGN特殊处理的应急通信（ET），其中一个具体示例是[ITU-T E.107]定义的应急通信服务（ETS）。ETS充分利用用于普通服务的IdM能力（如身份保证和受信赖的身份的发现），因此，IdM系统必须支持必要的功能和能力，以便根据适用的国家规则和政策，在建立和维护ETS呼叫/会话时认识并提供优先处理。有关要求得到优先处理的业务和能力的信息见[ITU-T E.107]和[ITU-T Y.2205]。

R-46 要求NGN/IdSP IdM系统支持必要的功能和能力，以便根据适用的国家规则和政策，在建立和维护ETS呼叫/会话时，认识和提供优先处理。

R-47 要求用于支持ETS呼叫/会话的IdM网元和数据库根据适用的国家规则和政策提供优先处理，这包括但不限于：

- 网内IdM通信（如NGN提供商IdM系统内的互动）
- 网间IdM通信（如根据双边协议和政策的两个NGN提供商系统之间的互动）
- 联合式IdM通信（根据适用的联合身份规则和政策的联合成员之间的互动）

有关与ETS相关的使用案例示例见附录三。

8.5 身份管理的联合身份功能

联合涉及两个或两个以上实体之间建立关系，或建立包括服务提供商和身份服务提供商任何成员在内的协会。联合的总体概念是方便每一个联合成员在促进具体身份信息交流（以方便联合服务）的同时保持独立性。例如，根据联合政策和条件以及数据保护规则和政策，用户/签约用户的某些身份信息（如签约用户资料的子集）可实现联合（即，向联合成员提供）。联合身份有助于各安全域之间身份信息的便携和传输，如若不然，根据联合政策和条件以及适用的规则、法规和政策，这些安全域为自治安全域。联合身份有利于一个域的用户安全地接入另一个域的数据和系统，同时无需进行完全属于多余的用户管理。

R-48 须可以根据适用的规则、法规和政策，在联合成员之间发现和交流联合身份信息。

R-49 要求NGN/IdSP支持有助于签约用户提供必要授权、以实现其身份联合化的能力。

R-50 要求NGN/IdSP支持签约用户具有选择来终止参加所有或特定联合身份服务和应用并终止其联合身份的能力。

R-51 要求NGN/IdSP支持签约用户能够针对其联合身份信息确定许可和禁止的能力。签约用户须可以控制其哪些个人数据可由哪些人使用以及用于何种目的。

注 — 第8.6节所述的有关PII保护的要求也适用于联合身份。

总体而言，每一个NGN提供商、企业或联合成员均可采用自身的表述和共享与身份相关的数据和信息的格式、略图、定义或语义。例如，诸如出生日期等同样的信息可由两个不同系统做出不同表述。此外，用于表述、请求和交流与身份相关的信息的语义、略图、技术和机制也可能不同，从而带来互操作性问题。因此，有必要具备有助于受信赖的联合之间进行桥接和互通的能力。

R-52 须可以在使用不同IdM系统、语义、略图、机制和技术的受信赖的联合之间完成桥接和互操作。例如，不同域（如NGN域和网络服务/互联网）的依赖方须可以使用不同IdM能力和技术来进行互通和互操作。具体而言，须保证联合身份信息的安全传输。

8.6 用户/签约用户的功能及对PII的保护

需要向最终用户/签约用户提供适当的直观界面和能力，以保护其PII并在充分掌握信息的基础上就其个人数据做出决定和同意。最终用户/签约用户应能够表达其隐私策略和偏好，并且与NGN/IdSP就数据披露条件展开谈判。

应根据适当的政策（如，用户/签约用户的同意、政府的监管规则）仅向被授权实体做出个人数据披露。此外，应尽可能减少对PII的收集、存储和使用，并遵守适用的政策。

R-53 NGN/IdSP必须根据适用的法规、政策和规定对PII予以保密。

R-54 最终用户/签约用户须可根据适当的法规、政策（如，个人同意声明书、提供商的政策或监管规定）就其个人数据偏好（如，设置隐私偏好）与NGN/IdSP进行沟通。

R-55 在提供所要求的信息前，最终用户/签约用户须可审查请求获得PII的实体的真实性。

R-56 在根据适用的法规、政策和规定实现了数据采集和保留的具体目的时，NGN/IdSP必须删除PII。

R-57 最终用户/签约用户须可根据应用的具体情况及适用的法规、政策和规定以匿名或假名方式操作。

8.7 安全

身份信息和数据极为敏感，是入侵者觊觎的目标。同时，由于IdM业务和能力将被用来进行企业、政策和社交网应用的访问控制，这些网元和系统（如，支持IdM功能和能力的网元和数据库）将成为安全攻击和入侵的目标。因此，必须采用适当的安全措施，为提供IdM功能、服务和能力的网元及系统提供安全保障和保护。

8.7.1 系统和数据的访问控制

系统访问控制涉及采取安全措施，以防范对网元和系统以及相关接入点的非授权访问。由于对支持IdM功能、能力和数据的网元和系统的非授权访问会造成威胁，因此，必须制定并实施适当的访问控制措施，以防止非授权访问。

R-58 NGN/IdSP必须支持并实施系统访问控制措施，以防范对支持IdM功能和能力的网元和系统的非授权访问。NGN/IdSP不应允许某一实体访问支持IdM功能和能力的网元和数据库，除非该实体的身份被确认，并获得认证和授权。这适用于所有实体（如，个人、流程和远程系统）。

数据访问控制涉及采取安全措施，以防范对储存或调配的数据以及传输中数据的非授权访问。由于对支持IdM功能、能力和数据的网元和系统的非授权访问会造成威胁，因此，必须制定并实施适当的访问控制措施，以防止非授权访问。

R-59 NGN/IdSP必须支持并实施访问控制措施，以防范对IdM数据的非授权访问。这包括IdM数据库、应用服务器、归属签约用户服务器（HSS）或任何其它网元中存储或调配的任何身份数据。NGN/IdSP不应允许某一实体访问IdM数据，除非该实体的身份被确认，并获得认证和授权。这适用于所有实体（如，个人、流程和远程系统）。

8.7.2 系统和数据的完整性

必须保护支持IdM业务和能力的网元、系统和功能的完整性。这包括IdM数据库和应用服务器。

R-60 NGN/IdSP必须保护支持IdM业务和能力的所有网元、系统和功能的完整性。

必须为储存的身份数据和信息提供完整性保护，防范对数据的破坏或操纵，以免影响到数据的完整性。

R-61 NGN/IdSP必须为IdM调配数据提供完整性保护。

R-62 NGN/IdSP必须为任何数据分配、通信、更新或修改以及任何与IdM有关的离线数据提供完整性保护。

8.7.3 数据的保密

R-63 NGN/IdSP必须支持并实施必要的措施，以防止非授权实体（如，非授权的内部人士）观测到调配的IdM数据。

R-64 NGN/IdSP必须支持并实施必要的措施，以防止非授权实体（如，非授权的内部人士）观测到IdM数据的分配、通信、更新或更改以及任何离线IdM数据。

8.7.4 IdM通信的安全防范

必须防止IdM通信（信令和媒体）受到任何非授权访问、破坏、操纵和截取（如，截听）。

R-65 NGN/IdSP必须保护内部网和网间IdM通信的完整性和保密性。必须为跨网络到网络接口（NNI）、应用到网络接口（NANI）或网域之间服务器到网络接口（SNI）的所有与IdM相关的信令和媒体流量提供完整性保护。

8.7.5 管理的安全性

必须保证对NGN网元和调配数据管理访问的安全，并防止非授权访问和控制。

R-66 NGN/IdSP须防止对管理界面的非授权访问及对支持IdM的网元和功能实体的控制。

必须保证管理流量的安全，防止受到破坏、操纵和非授权观测。

R-67 NGN/IdSP必须为与支持IdM相关的管理流量提供完整性和保密性保护。

8.7.6 安全和审计日志

记录事件，支持对具体活动将进行的事后调查，有必要保持安全和审计日志。

R-68 为保持事件记录，帮助对与支持IdM相关的具体活动进行事后调查（如，登入、对关键系统资源和数据的修改、管理层访问调配的NGN参数和资源），NGN/IdSP必须创建安全日志。

8.7.7 防范拒绝服务（DoS）攻击和分布式拒绝服务（DDoS）攻击

IdM业务和能力必须具备高度的可用性，因而必须防范可能会影响其可用性的DoS和DDoS威胁。

R-69 NGN/IdSP必须防范可能影响IdM业务和能力可用性的DoS、DDoS和其它类型的攻击。这包括支持和使用适当的能力和工具，发现、隔离并尽可能减少DDoS及其它类型的攻击。

8.7.8 监控及入侵发现

R-70 NGN/IdSP必须 酌情支持并利用各类安全监测和入侵发现工具，以发现对IdM网元和系统的欺诈、滥用及入侵。

附录 I

IdM一般使用案例

（本附录不构成本建议书的组成部分）

I.1 引言

本附录提供了政府、企业和最终用户/签约用户三个方面的IdM一般使用案例。

I.2 政府

政府可利用IdM能力增强并保障政府企业与公民之间、政府机构（联合政府服务）和部门之间以及不同政府之间（如，政府之间的联合服务）的应用和交易。政府使用案例示例包括：

- 确保公民身份识别：政府可通过IdM来验证公民的身份，以获得电子政务服务，同时提高对PII的保护。以卫生保健为例，卫生相关信息的敏感性突出表明了数字缩小的重要性，并且在更大的范围内，表明有必要保持身份信息的安全性和私密性。
- 针对联合政府服务确保政府雇员身份识别：政府企业可利用IdM能力为政府雇员开发安全可靠的通用身份识别解决方案，这些解决方案可提供更高的安全性、效率，减少身份欺诈，并保护个人隐私。
- 增进并支持政府之间的联合服务：可将IdM用于增强并保障不同政府之间的联合服务。如，政府可为在各国之间旅行的公民协同开发增强型IdM解决方案，强调安全性、隐私及用户体验。

I.3 企业

企业机构可将IdM用于加强并支持新的和现有业务，同时改进安全性、隐私和PII保护。企业使用案例示例包括：

- 联合身份服务：可利用IdM支持对多业务合作伙伴（包括NGN、网络服务、内容和第三方提供商）的单点登录和退出服务。
- 通信服务：NGN提供商可利用IdM，在不同平台（如，托管IP网络、互联网和移动平台）向最终用户/签约用户提供应用服务，并允许用户以适合其偏好的独特方式在多个平台获取所选择的应用。
- 电子财务交易和应用：可将IdM用于增强并支持电子商务交易中的电子支付应用。

I.4 最终用户/签约用户

对于最终用户/签约用户而言，可利用IdM增强体验并控制PII。最终用户/签约用户的使用案例包括：

- 用户对PII的控制：可利用IdM增强用户体验并控制PII。个人可使用多个假名参与不同的活动，如，查看新闻报导、发表博客帖、管理社交网，以及交换照片或音乐。IdM可有助于向个人提供更多的选择——关于如何参加不同的社区，以及希望不同的身份内容被链接的程度（如，对其PII的控制）。
- 社交网：通过提供必要的工具，以便提高用户对PII的有效控制并增加可核查性，IdM可被用于增强并支持社交网应用。

附录 II

有关NGN应用的IdM使用案例

（本附录不构成本建议书的组成部分）

II.1 引言

本附录提供了有关NGN的身份管理（IdM）使用案例。这些使用案例将作为制定有关NGN的IdM要求的依据。

II.2 基本使用案例示例

图II.1显示了一个基本的使用案例示例，其中涉及到三个基本要素。这个基本例子以外还可能出现其他的情况。请参阅附录V关于其他可能出现的情况的说明（例如，用户中心情况）。

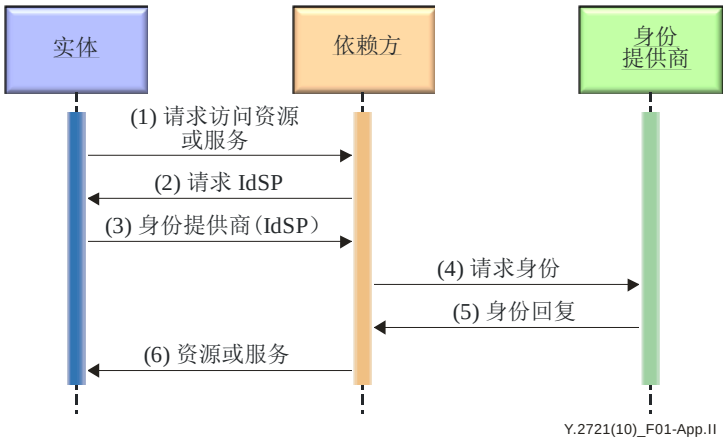


图 II.1 – 基本使用案例示例

三个要素包括一个寻求从依赖方（即RP，可能是一个网络或一项应用程序）获得服务的实体（一个断言方或主体），该实体从一个身份服务提供商（IdSP）基于信任和安全政策获得相关身份断言，包括匿名或假名断言。

图II.1显示了下述高水平的IdM信息流程。

1) 实体向依赖方（资源或服务提供商）提供了一个所声称的身份，并请求从依赖方获得资源或服务。

2) 在提供所请求的资源或服务之前，依赖方（网络或应用）需要对实体进行认证。依赖方需要从适当的身份服务提供商那里获得必要的信息，因此必须确定并联络适当的身份服务提供商。依赖方向实体回复一个“请求IdSP信息”，要求实体提供适当的IdSP名称。

3) 通过确定适当的IdSP，实体向依赖方回复该“请求IdSP信息”。实体可确定多个IdSP。

4) 依赖方随后对适当的IdSP进行查询，根据需要验证该实体所声称的身份能否达到足够的信任水平（保证水平）。

5) IdSP通过认证，确认实体所声称的身份。IdSP的职能可包括委托（指IdSP可通过向其它IdSP中转身份断言，将认证过程的某些部分或全部委托给其它IdSP）。如需更高

保证程度的认证，或需要其它具体实施方面的能力，依赖方可向IdSP提出后续请求。

6) 在收到IdSP对实体声称身份的验证后，依赖方提供所请求的资源或服务。

这三种要素（实体、依赖方和身份服务提供商）有可能产生不同的组合。这与其中涉及的基本媒体无关。唯一的要求是，如果这些通信机制具有使用这些机制的必要许可，应通过涉及各方所熟悉或可能获得的句法和描述形成“紧凑的结构”。应酌情采用可信赖的、具全球互操作性的标准机制。

此外，其它高水平的IdM信息流程也是可能的。例如：

1) RP可直接要求实体提供认证证书。

2) 实体可将其认证证书提供给可信赖的IdSP。

3) 身份服务提供商可对实体提供的证书进行验证，然后为实体生成新的证书，以便满足RP的认证请求。

4) 实体（或其代表）可从身份服务提供商那里获得所生成的证书，然后将其提供给RP。

5) 实体向RP发送的生成证书可包含以下两者之一：1)身份服务提供商所生成的身份声明副本，或2)对该副本的引证。

此外，实体可决定是否向RP提供IdSP所生成的认证证书。

也有可能存在不同层级的身份服务提供商或依赖方。实体也可拥有一名以上的代表。

II.3 在一个服务提供商网络内使用通用IdM系统支持多项应用服务（如，语音、数据、IP电视）

II.3.1 概述

网络/服务提供商（如，NGN提供商）可能会支持并管理多项应用和业务。NGN环境分布式的性质产生了这种可能性，即不同的应用服务可能被托管于不同的网元和厂商各自特有的平台（如，VoIP、数据IP电视）。每项业务均有其互不兼容的、基于特定厂商或特定技术的访问控制方法，因此，不得不分别加以配置、管理并单独使用。

采取一种利用共同IdM基础设施的方法推动多项应用/业务可产生成本和业务效益。也将提供一种标准的方法，使应用程序开发商能够利用IdM的通用功能，而不是让各项应用/业务支持特定的IdM功能（如，厂商专有的特定访问控制能力和机制），并形成一种有效的设计、实施和提供应用服务的流程。此外，需要一种共同的方法，对每项应用服务以及整个网络基础设施的安全风险加以全面管理。

针对NGN的 IdM方法将包括网络内解决方案（如，NGN提供商域内解决方案）以及网络间解决方案（如，不同NGN之间的解决方案，包括第三方提供商）。对于网络内的情境，可采取允许不同的网元之间或NGN提供商域内的各个组成部分之间进行IdM互动（如，申请人、依赖方系统和身份系统）这一方法。对于网络间的情境，可允许不同NGN域的网元实体之间进行跨域IdM互动（如，申请人、依赖方和身份服务提供商）。

注 — NGN提供商也可以是一个IdSP。

II.3.2 使用案例描述

本使用案例示例说明了多项应用服务（如，VoIP、数据和IP电视）如何使用共同的身份管理基础设施进行访问控制，并对应用服务提供安全保护。本使用案例涉及下述实体之间的互动：

- 最终用户（如，最终用户和/或最终用户装置）
- 依赖方系统（如，应用服务或网络系统）
- IdM系统（如，提供IdM业务的网络系统，如注册、认证和授权、签约用户简介信息）。

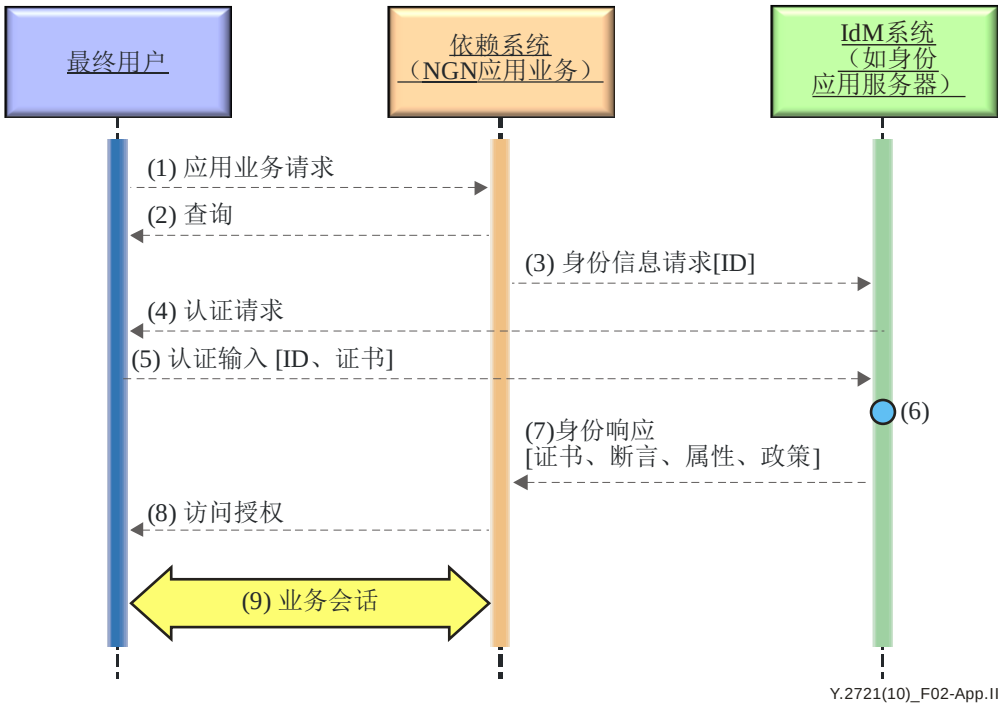


图 II.2 – 基本使用案例示例

图II.2介绍了一个基本示例，其中一项应用服务使用了应用服务外部的或独立于该应用服务的IdM系统的服务，进行访问控制和特权管理。该呼叫流程示例如下：

1) 应用服务请求。该信息流程表示最终用户请求调用该应用服务。
2) 查询。该应用服务发送一个回复，对用户访问提出查询。
3) 身份信息请求[用户身份]。应用服务向IdM系统发送一项请求，以断言用户身份并提供与该用户身份有关的属性。其中可包括这类信息：如，业务描述、特权、偏好以及政策。例如，任何与身份有关的政策或限制条件。
4) 认证请求。IdM系统向用户发送要求认证的请求。
5) 认证输入[证书]。用户提供认证信息（如，用户身份和密码，或个人识别码）。
6) 认证。IdM系统执行认证并获得其它必要的信息。这一过程可能涉及从其它网络系统（如，HSS）获得信息。
7) 身份信息回复[证书断言、属性、政策]。IdM系统提供断言证书的信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

8) 访问授权。应用服务向用户发出指示，表示对该业务的访问已被批准。

9) 应用服务会话。该信息流程表示用户与该应用服务的会话取得成功。

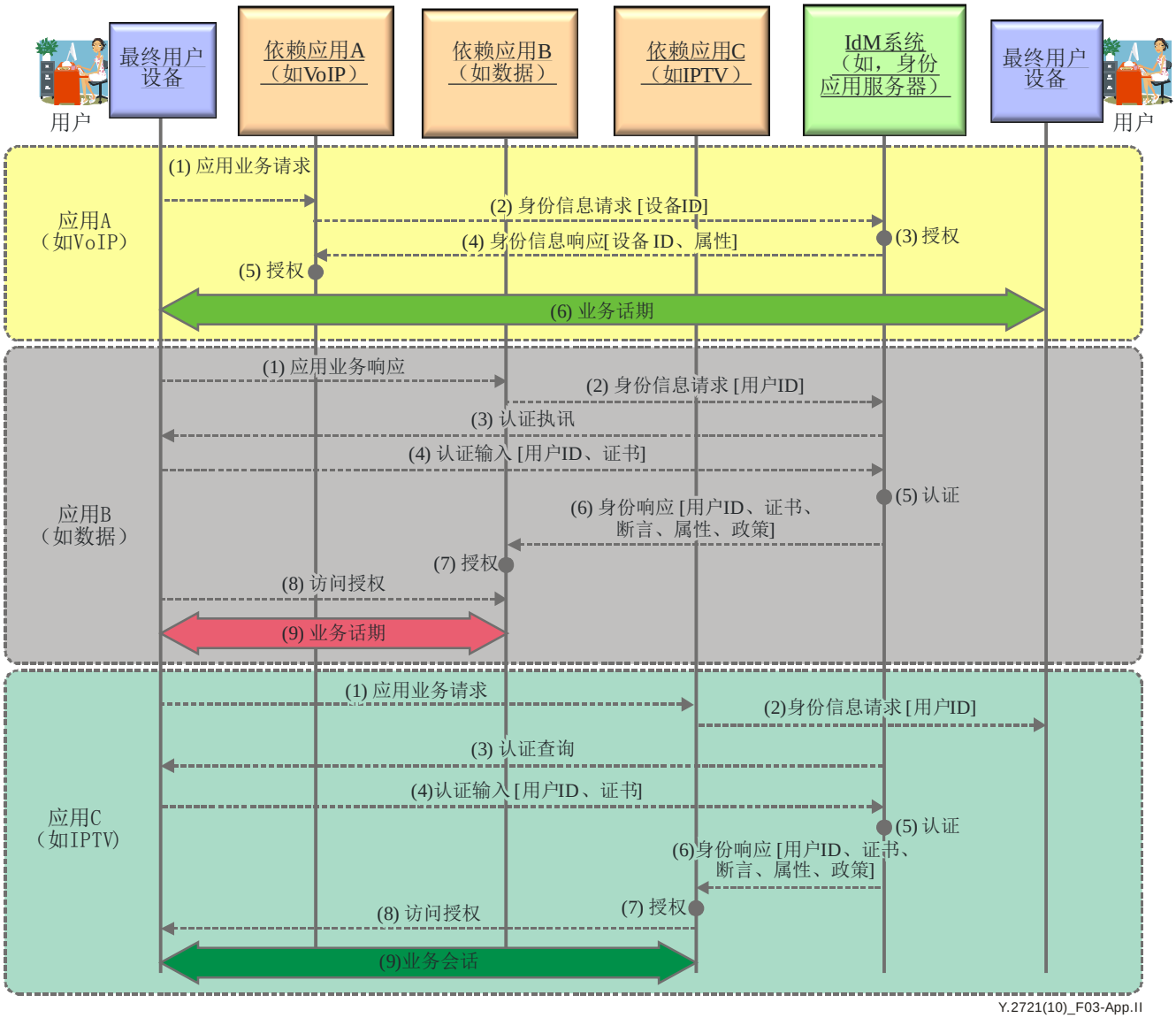


图 II.3 – 多项应用服务使用共同的IdM基础设施

图II.3介绍了一个使用案例，其中多项应用服务（如，VoIP、数据和IP电视）使用了一个该应用服务外部的并独立于该应用服务的共同的IdM系统。本示例假定最终用户装置通过正常程序注册，并连接到业务提供商。

应用程序A（VoIP）的示范呼叫流程如下：

1) 应用服务请求：该信息流程表示最终用户正在调用一个呼叫。

2) 身份信息请求[装置身份]：应用服务向IdM系统发送一项请求，以核实最终用户装置是否获得了使用VoIP业务的授权。本示例假定VoIP业务基于用户装置的签约用户描述或线路（如，x数字用户线）。

3) 授权：IdM系统确定最终用户是否获得了使用VoIP业务的授权。

注1 – 假定这一过程将涉及检索该最终用户装置或线路（如，x数字用户线）的签约用户描述信息。此外，还假定对于VoIP，不需要进行最终用户认证。

4) 身份信息回复[装置身份、属性] ：IdM系统提供与装置身份相关的属性（如，该装置是否获得了使用VoIP业务的授权）。这一过程将包括签约用户描述的相关信息（如，特权和偏好）。

5) 访问授权：应用服务向用户发出指示，表示对该业务的访问已被批准。

6) 应用服务会话：该信息流程表示用户与该应用服务的会话取得成功。

应用B（数据）的示范呼叫流程如下：

1) 应用服务请求：该信息流程表示该最终用户请求调用应用服务。

2) 身份信息请求[用户身份] ：该应用服务向IdM系统发送一项请求，以断言用户身份并提供与用户身份相关的属性。其中可包括这类信息：如，业务描述、特权、偏好以及政策。如，任何与身份有关的政策或限制条件。

3) 认证查询：IdM系统向用户发出一项查询，要求进行认证。

4) 认证输入[证书] ：用户提供有关认证信息（如，用户身份和密码或个人识别码）。

5) 认证：IdM系统进行认证并获得其它必要信息。这一过程可涉及从其它网络系统获得信息（如，HSS或其它签约用户数据库）。

6) 身份信息回复[证书断言、属性、政策] ：IdM系统提供证书断言信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

7) 授权：该应用服务处理信息，确定该用户获得使用该项业务的授权。

8) 访问授权：应用服务向用户发出指示，表示对该业务的访问已被批准。

9) 应用服务会话：该信息流程表示用户与该应用服务的会话取得成功。

应用C（IP电视）示范呼叫流如下：

1) 应用服务请求：该信息流程表示最终用户请求调用应用服务。

2) 身份信息请求[用户身份] ：应用服务向IdM系统发送一项请求，以断言用户身份并提供与用户身份相关的属性。其中可包括这类信息：如，业务描述、特权、偏好以及政策。如，任何与身份有关的政策或限制条件。

3) 认证查询：IdM系统向用户发出一项查询，要求进行认证。

4) 认证输入[证书] ：用户提供有关认证信息（如，用户身份和密码或个人识别码）。

5) 认证。IdM系统进行认证并获得其它必要的信息。这可涉及从其它网络系统获得信息（如，HSS或其它签约用户数据库）。

6) 身份信息回复[证书断言、属性、政策] ：IdM系统提供断言证书的信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

7) 授权：应用服务处理信息，确定用户获得了使用该项业务的授权。

8) 访问授权：应用服务向用户发出指示，表示对该项业务的访问已被批准。

9) 应用服务会话：该信息流程表示用户与该应用服务的会话取得成功。

注 2 — 为提供相互认证（即认证应用程序或服务提供商），必需更多的功能和流量。但是，这并没有在图II.3中显示。

II.3.3 隐含要求

本使用案例隐含了以下要求：

- NGN可以拥有一个通用的IdM解决方案，用于独立于应用平台或特定厂商解决方案的多项应用和业务
- 如果违背数据收集限制、数据最小化、数据分离、目的规范和使用限制的原则，不得使用共同IDM功能。
- NGN须支持一种标准和结构化方法，允许各项应用服务以安全的方式发现IdM系统并交换身份数据。

II.4 在一个业务提供商网络内单点登录/单点退出多项应用服务（如，语音、数据和IP电视）

II.4.1 概述

用户通常被迫登录托管应用服务的多个系统（如，VoIP、数据和IP电视），从而不得不进行相同数量的登录对话，其中每次对话均可能涉及不同的用户名和认证信息。系统管理员必须对每个系统中的用户账户进行管理，以便通过协调的方式访问这些账户，从而保证执行安全政策的一致性。

最终用户/签约用户要求简化诸如“单点登录/退出”这类使用特性。“单点登录”的前提条件是最终用户、装置或最终用户和装置的组合在下一代网络（NGN）中可以一次性登录某一业务（如，提供证书输入以便进行认证和授权），从而能够在同一NGN中就一项或一项以上的额外业务进行认证（如，最终用户不必针对每项业务反复进行认证）。这里所使用的“登录”一词与“注册”、“登入”或“签入”同义，即最终用户/装置“注册”、“签入”或“签入”至一项业务。与此类似，“单点登录”为用户提供了一种特性，可避免在一个特定的会话中被迫“退出”每一项应用服务。

单点登录/退出业务的益处包括：

- 减少了用户登录操作中进入每个域所花费的时间，包括降低了这类登录操作失败的可能性
- 用户不必再处理及记忆多套认证信息，从而提高了安全性。

- 减少了系统管理员为添加或取消某一系统用户或修改其访问权限而花费的时间，提高了响应速度。
- 通过提高系统管理员维护用户账户配置一致性的能力（包括以协调一致的方式阻止或取消某个用户访问所有系统资源），提高了安全性。

II.4.2 使用案例描述

本使用案例介绍了在一个NGN提供商域内使用IdM系统支持对多项应用服务（如VoIP、数据和IP电视）的“单点登录/退出”。本使用案例涉及以下实体间的互动：

- 最终用户（如，最终用户和/或最终用户装置）
- 依赖系统（如，应用服务或网络系统）
- IdM系统（如，提供注册、认证和授权及签约用户描述这类信息的IdM业务网络系统）。

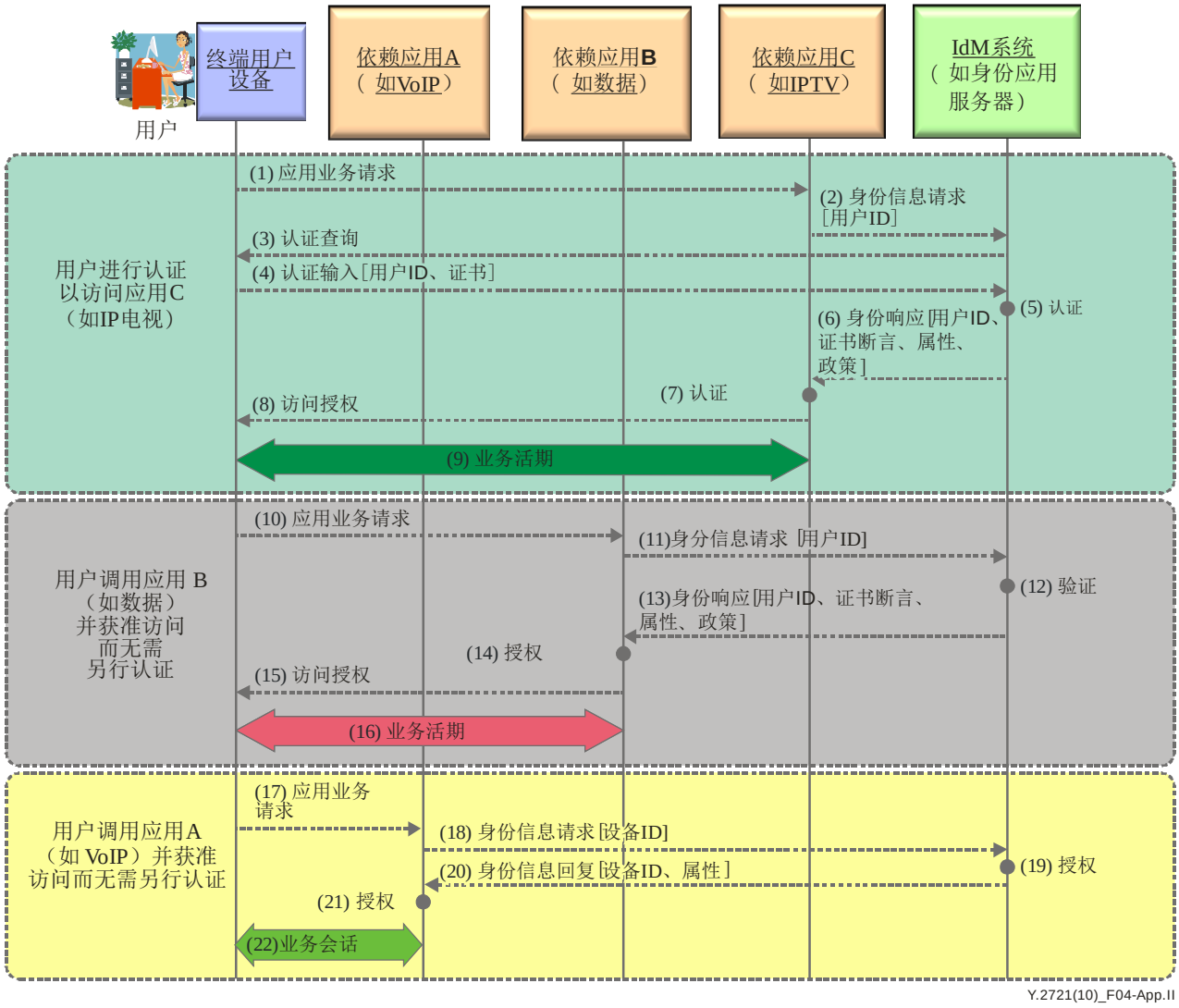


图 II.4 – 单点登录业务

图II.4介绍了一个最终用户/签约用户使用单点登录服务访问多项应用服务的情况（如，VoIP、数据和IP电视）。本示例假定该最终用户装置通过正常程序注册并连接到NGN。

呼叫流程示例如下：

1) 应用服务请求：该信息流程表示该最终用户请求调用应用服务C（IP电视）。

2) 身份信息请求[用户身份] ：应用服务C（IP电视）向IdM系统发送一项请求，以断言用户身份并提供与用户身份相关的属性。其中可包括这类信息：如，业务描述、特权、偏好以及政策。如，任何与身份有关的政策或限制条件。

3) 认证查询：IdM系统向用户发出一项查询，要求进行认证。

4) 认证输入[证书] ：用户提供有关认证信息（如，用户身份和密码或个人识别码）。

5) 认证：IdM系统进行认证并获得其它必要的信息。这可涉及从其它网络系统获得信息（如，HSS或其它签约用户数据库）。

6) 身份信息回复[证书断言、属性、政策] ：IdM系统提供断言证书的信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

7) 授权：应用服务C（IP电视）处理信息，确定用户获得了使用该项业务的授权。

8) 访问授权：应用服务向用户发出指示，表示对该项业务的访问已被批准。

9) 应用服务会话：该信息流程表示用户与该应用服务C（IP电视）的会话取得成功。

10) 应用服务请求：该信息流程表示该最终用户请求调用应用服务 B（数据）。

11) 身份信息请求[用户身份] ：应用服务B（数据）向IdM系统发送一项请求，以断言用户身份并提供与用户身份相关的属性。其中可包括这类信息：如，业务描述、特权、偏好以及政策。如，任何与身份有关的政策或限制条件。

12) 核实：IdM处理该请求，确定适用单点登录，核实用户认证仍然有效。

13) 身份信息回复[证书断言、属性、政策] ：IdM系统提供断言证书的信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

14) 授权：应用服务B（数据）处理信息，确定用户获得了使用该项业务的授权。

15) 访问授权：应用服务B（数据）向用户发出指示，表示对该项业务的访问已被批准

16) 应用服务会话：该信息流程表示用户与该应用服务B（数据）的会话取得成功。

17) 应用服务请求：该信息流程表示该最终用户请求调用应用服务A（VoIP）。

18) 身份信息请求[用户身份]：应用服务A（VoIP）向IdM系统发送一项请求，以断言用户身份并提供与用户身份相关的属性。

19) 核实：IdM处理该请求，确定适用单点登录，核实用户认证仍然有效。

20) 身份信息回复[证书断言、属性、政策]：IdM系统提供断言证书的信息。可纳入的其它信息为与用户身份相关的属性（如，特权和偏好）以及与身份信息相关的政策（如，任何使用、显示和传播方面的限制）。

21) 授权：应用服务A（VoIP）处理信息，确定用户获得了使用该项业务的授权。

22) 应用服务会话：该信息流程表示用户与该应用服务A（VoIP）的会话取得成功。

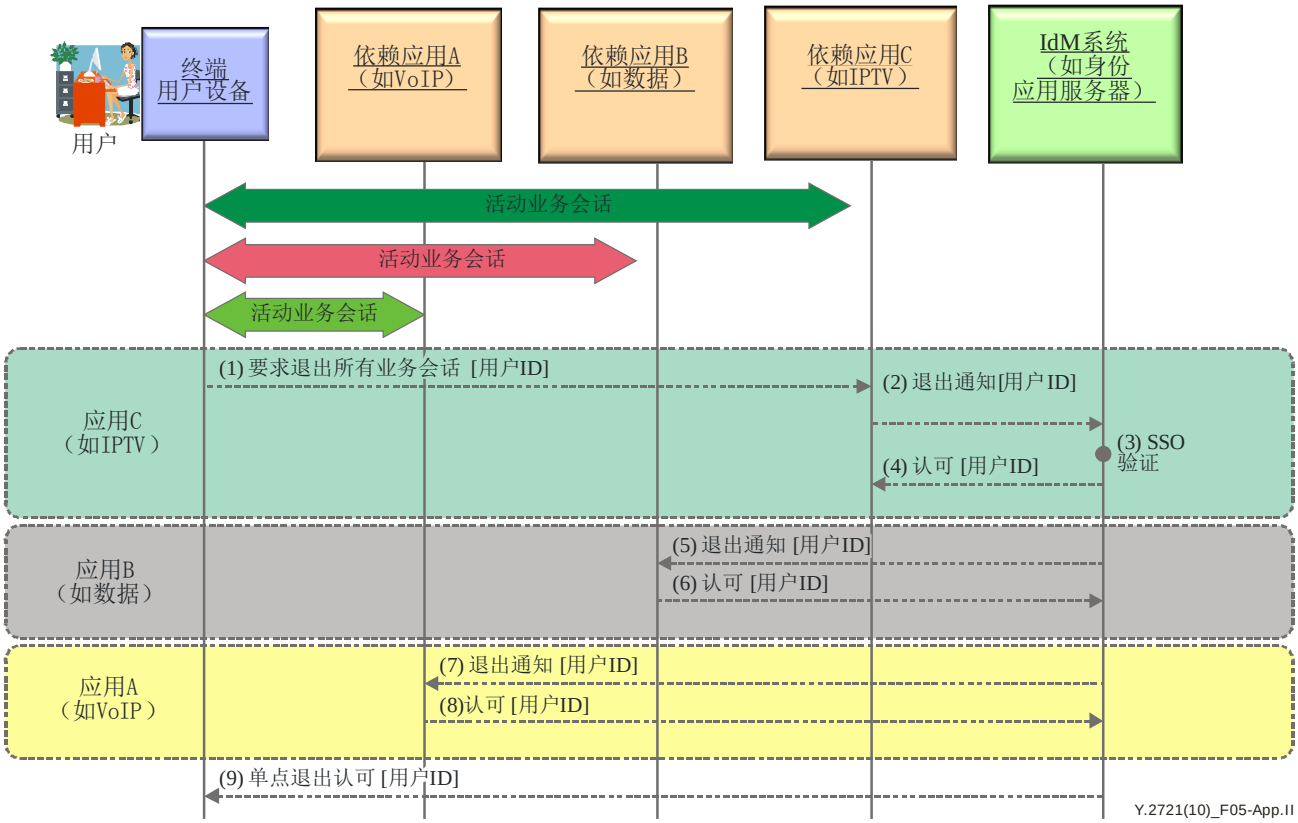


图 II.5 – 单点退出业务

图II.5介绍了“单点退出业务”，即用户可自动退出多项应用服务（VoIP、数据和IP电视），而不必分别退出会话中的各项应用服务。本使用案例假定该用户正在与处于活动状态的应用服务A（VoIP）、B（Data）和C（IP电视）进行业务会话。

该呼叫流程如下：

1) 业务退出[用户身份]：该呼叫流表示用户要求终止所有的业务会话。

2) 退出通知[用户身份]：应用服务C（IP电视）通知IdM系统用户的退出请求。

3) SSO核实：IdM系统确定可适用单点退出，并核实应用服务处于活动状态。

4) 确认[用户身份]：IdM系统向应用服务C（IP电视）发送有关终止业务会话的确认。

5) 退出通知[用户身份]：IdM系统通知应用服务B（数据）退出。

6) 确认[用户身份]：应用服务B（数据）确认退出。

7) 退出通知[装置身份]：IdM系统通知应用服务A（VoIP）退出。

8) 确认[装置身份]：应用服务A（VoIP）确认退出。

9) 单点退出确认[用户身份]：IdM系统向用户发送确认通知，确认从会话中所有处于活动状态的应用服务中退出。

II.5 关联分布式身份信息，确保多因素认证

II.5.1 概述

本使用案例介绍了通过IdM对多项身份信息进行关联和绑定（如，识别符、证书和属性），以确保某个最终用户/签约用户的身份。例如，可关联与签约用户（如用户身份）、签约用户装置（如装置身份）以及位置信息相关的身份信息，以提供更高的签约用户保证。

II.5.2 使用示例

图II.6介绍了一个绑定用户身份与装置身份并将现状与位置信息相互关联的使用案例，为身份及身份相关的权利提供了更高水平的保证。

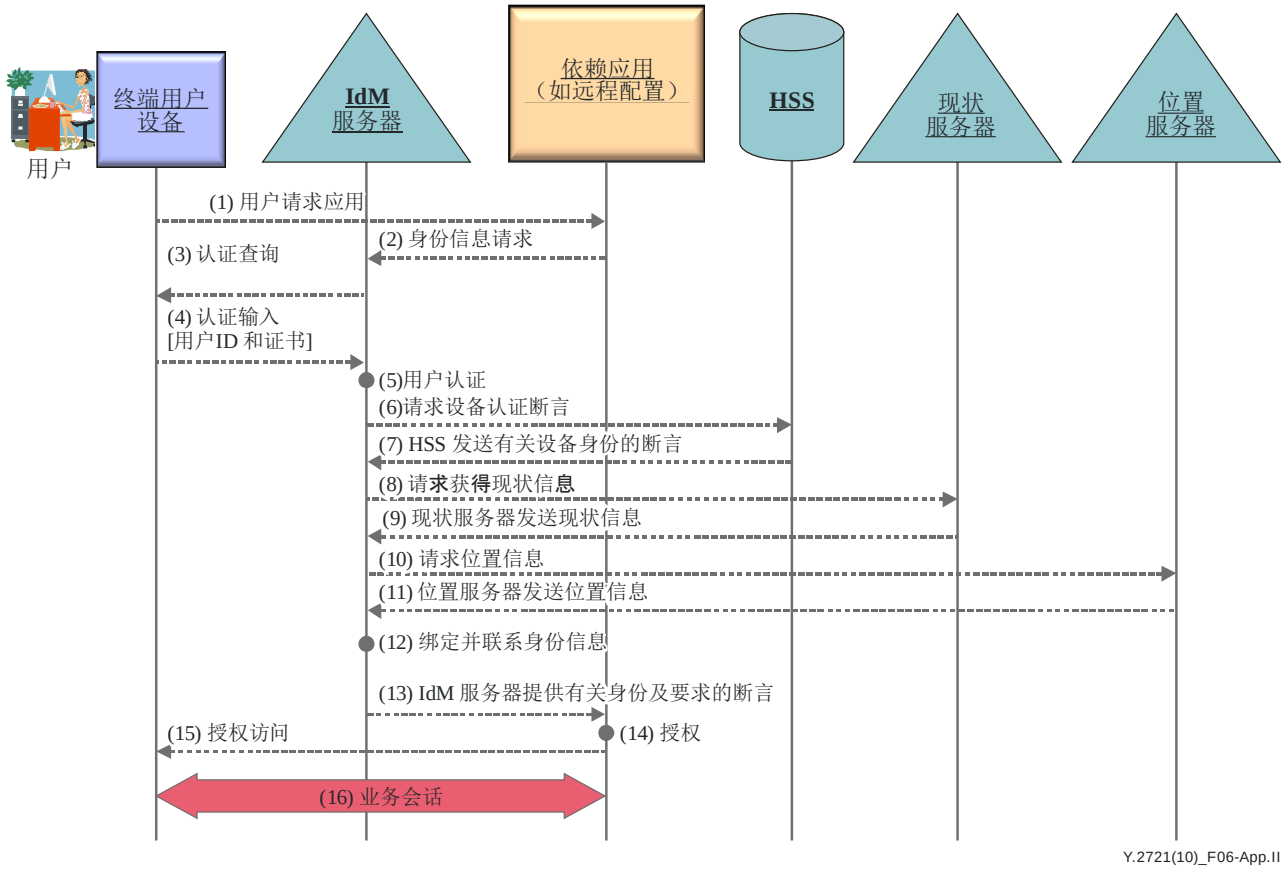


图 II.6 – 身份信息的相关性

在本示例中，最终用户/签约用户试图访问一项应用，该应用要求较高水平的用户身份及与身份相关特权的保证，因为允许对该应用或资源的非授权访问可导致代价极大的安全风险。

呼叫流程示例如下：

1) 用户请求访问该应用
2) 该应用向服务器发送请求，以断言用户身份以及与用户身份相关的权利
3) IdM服务器向用户发送认证要求
4) 用户向IdM服务器提供认证输入（如，用户身份和证书）
5) IdM服务器对用户进行认证
6) IdM服务器向HSS发送请求，要求断言用户装置身份（注：假定用户装置通过正常程序向该网络进行注册和认证）
7) HSS发送用户装置身份断言
8) IdM服务器向现状服务器发送有关现状信息的请求
9) 现状服务器向IdM服务器提供现状信息
10) IdM服务器向位置服务器发送关于位置信息的请求
11) 位置服务器向IdM服务器提供位置信息

12) IdM服务器将用户身份与用户装置身份信息进行绑定。将综合后的身份与现状和位置信息相关联，以核实与身份相关的权利（如，特权）

13) IdM服务器向应用提供有关用户身份以及与该身份相关权利的断言

14) 应用确定该用户是否获得访问授权

15) 该户用被准许访问应用

16) 业务会话得以建立。

II.6 跨对等网络/业务提供商域强制执行对个人可识别信息（如，特权）的用户控制

II.6.1 概述

保护PII对于最终用户/签约用户十分重要。IdM的一个重要特色是帮助最终用户/签约用户向业务提供商及IdSP提供有关建立、采集、使用及传播其身份信息的条件、限制、同意、授权等信息。

II.6.2 使用案例描述

本使用案例与强制执行适当的政策有关，如，有关匿名或假名身份信息的政策。

图II.7介绍了一个应用示例，其中用户请求使用匿名。

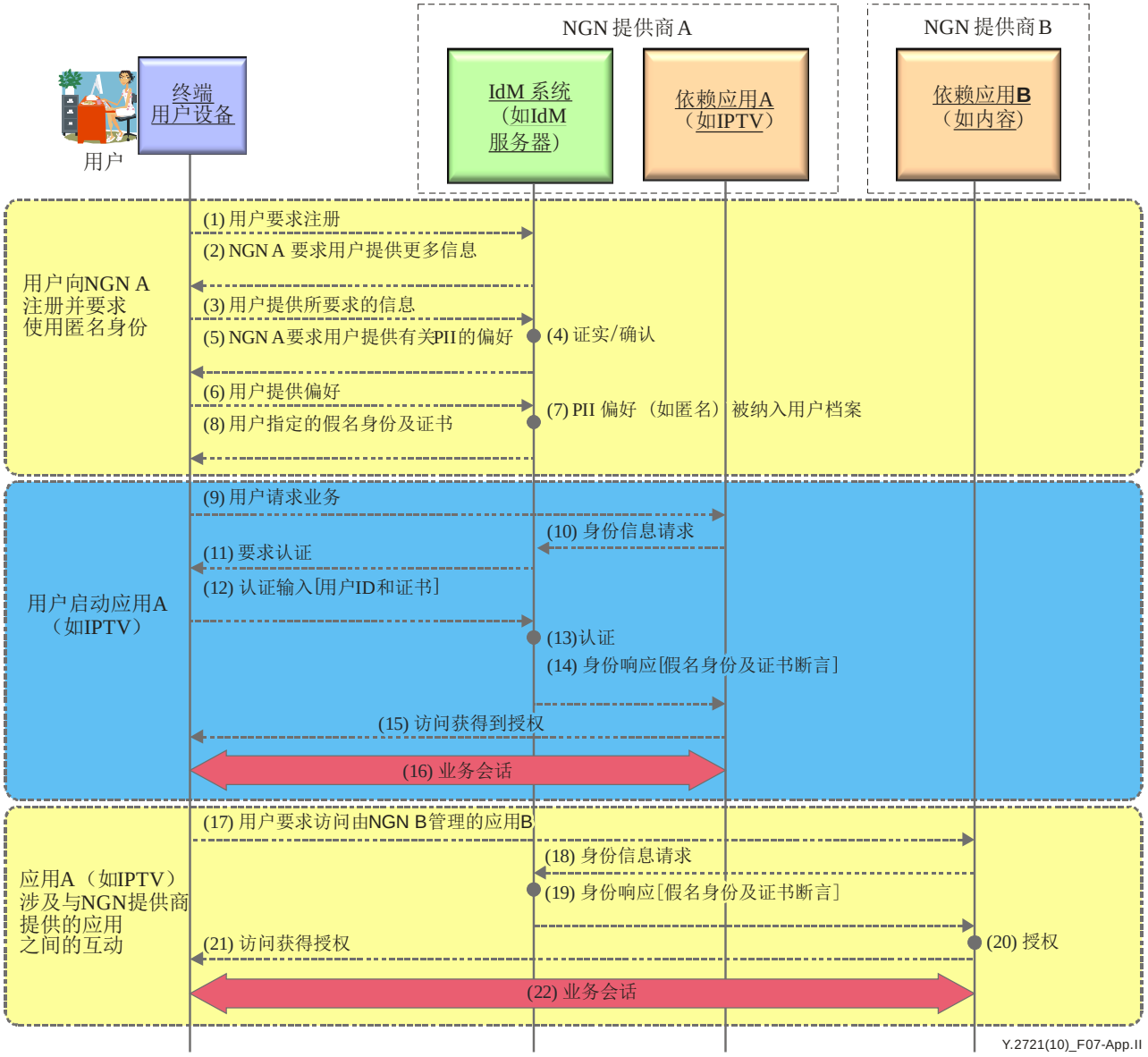


图 II.7 – 匿名用户身份

注 – IdM系统一词取其一般性含义，表示任何可能提供IdM功能并具有不同的实现/实施可能性的网元。

应用示例表明，根据最终用户/签约用户使用匿名的请求，NGN提供商（NGN提供商A）使用假名指定一个身份。该假名身份被用于与NGN提供商B进行互动，以保护最终用户/签约用户的个人可识别信息。

呼叫流程示例如下：

1) 用户请求获得NGN提供商A的吸纳
2) NGN提供商A督促用户提供额外信息
3) 用户向NGN提供商A提供所要求的信息
4) NGN提供商A证实并审核该信息
5) NGN提供商A督促用户提供有关个人可识别信息（PII）偏好的信息
6) 用户表明匿名偏好

7) NGN提供商A将匿名偏好纳入用户描述信息

8) 用户被指定一个假名身份以及约束该身份的证书

9) 用户调用一个由NGN提供商A管理的应用A（如，IP电视）

10) 依赖应用A要求从IdM系统（如，IdM服务器）获得有关用户身份的信息

11) IdM系统向用户发送认证要求

12) 用户向IdM系统提供认证输入（如，用户身份和证书）

13) IdM系统对用户进行认证

14) IdM系统向依赖应用A发送用户身份及证书断言
（注 — 仅提供假名身份信息以执行匿名）

15) 用户获得访问应用A的授权

16) 业务会话

17) 用户要求访问NGN B管理的应用B

18) 应用B向IdM系统发送请求，要求获得断言用户身份及相关权利的信息

19) IdM系统提供用户身份及相关权利的断言。为执行匿名政策，仅发送假名身份信息

20) 应用B验证该信息以便授权

21) 向用户提供访问授权

22) 业务会话得以建立。

II.7 异质IdM系统之间的桥接/映射

II.7.1 概述

为帮助用户获得由下一代网络（NGN）各组成部分提供的多种业务，NGN需要在不同的IdM系统之间进行桥接的机制。下节所述使用案例即描述了这一需求。

II.7.2 使用案例描述

本案例中的情境描述了一个NGN签约用户通过其手机访问位于一个企业网络中的资源（如，目录服务器）。由于NGN和企业网络采用了不同的IdM机制，因此有必要在这些网络的IdM系统之间进行桥接。

在说明这一情境的示例中，涉及到以下实体：

- NGN的IdM系统。对该系统的修改使其不仅能够支持对用户手机进行基于AKA的相互认证，还可向企业网络的IdM系统提供认证证书
- 企业网络的IdM系统（如，密钥分配中心）
- 位于企业网络中的企业目录服务器（EDS）
- 用户手机

- 这些实体执行以下互动：
  - 用户手机和移动网络通过AKA方法进行相互认证
  - 用户使用手机向位于企业网络中的企业电话目录服务器（EDS）发送一项请求
  - EDS回复认证请求
  - 基于AKA认证结果，用户从NGN的IdM系统获得认证证书（如，一张Kerberos票据），可用于向企业IdM系统进行认证。

如，用户手机获得了进入企业网络密钥分配中心（KDC）的一张票据。具体而言，该票允许用户获得作为KDC一部分的票据授权服务器（TGS）的认证

- 用户从TGS请求获得一张向EDS做出认证的票据
- TGS验证提交证书的有效性，并发给用户一张进入EDS的票据
- 最终用户通过从TGS获得的票据响应EDS的认证请求
- EDS对用户进行认证，以自己的认证证书以及对所请求业务的确认回复用户。在验证EDS证书有效后，用户可进入EDS

II.7.3 隐含的要求

- NGN的IdM系统必须支持AKA认证机制以及企业网络所使用的认证机制（如，Kerberos）
- NGN的IdM系统必须能够向最终用户装置发行认证证书（如，Kerberos票据），用于向企业IdM系统认证该用户
- NGN的IdM系统必须管理用户的身份及证书
- 企业IdM系统必须管理服务器的身份及证书。

注 – a) 3G网络不必具备新的能力（这可作为一个范例）；

b) 此处的要求仅适用于支持上述使用案例。

II.8 在一个服务提供商的网络内支持融合业务（如，固定和移动接入）

II.8.1 概述

下一代网络的期许之一是支持固定和移动接入网络上名目繁多的融合业务。用户因而可在某一特定时刻方便地使用一个接入设备和身边的网络调用一项业务。（反之，业务提供商也将扩大其客户群并增加营收。）由于固定和移动环境所适用的潜在安全机制一般来说是不同的，因此，一个可协调这些差异的融合的 IdM 系统将发挥重要作用。该融合 IdM 将对最终用户和网络服务器的身份和证书加以管理，而无论接入技术如何。

II.8.2 使用案例描述

本案例涉及的情境描述了一个3G网络签约用户通过其手机访问一项位于一个固定网络的资源（如，视频点播服务器）。在这一情境中，3G网络以及固定网络中的资源支持不同的IdM相关机制。在说明这一情境的示例中涉及以下实体：

- 3G网络的IdM系统。对该系统的修改使其不仅能够支持对用户手机进行基于AKA的相互认证，还可向视频点播服务器提供认证证书
- 位于固定网络中的VoD服务器
- 用户3G手机
- 这些实体进行下述互动：
  - 用户手机和移动网络通过AKA方法进行相互认证
  - 用户使用手机向VoD服务器发送一项请求
  - VoD服务器向用户发出一项认证请求
  - 用户从3G网络的IdM系统获得基于AKA认证结果生成的认证证书（如，一张Kerberos票据）
  - 用户向VoD服务器回复认证证书（票据）
  - VoD服务器对用户进行认证，向用户确认所请求的业务

II.8.3 隐含的要求

- 3G网络的IdM系统必须支持AKA认证机制以及VoD服务器使用的认证机制（如，Kerberos）
- IdM系统必须能够向用户装置发行认证证书（如，票据），以便对VoD服务器进行用户认证
- 3G网络IdM系统必须管理用户的身份及证书
- 3G网络IdM系统必须管理VoD服务器的身份及证书

注 – 此处的要求仅适用于支持所述使用案例。

II.9 使用案例 – 用户对NGN提供商的认证和授权（相互认证和授权）

图II.8介绍了一个使用案例，其中涉及用户对NGN提供商的认证。本使用案例假定一个NGN提供商能够向用户推介其业务的开放业务环境。这一使用案例说明了在一个开放业务和多提供商环境中用户进行NGN提供商认证（或相互认证）和授权的能力差距或欠缺。

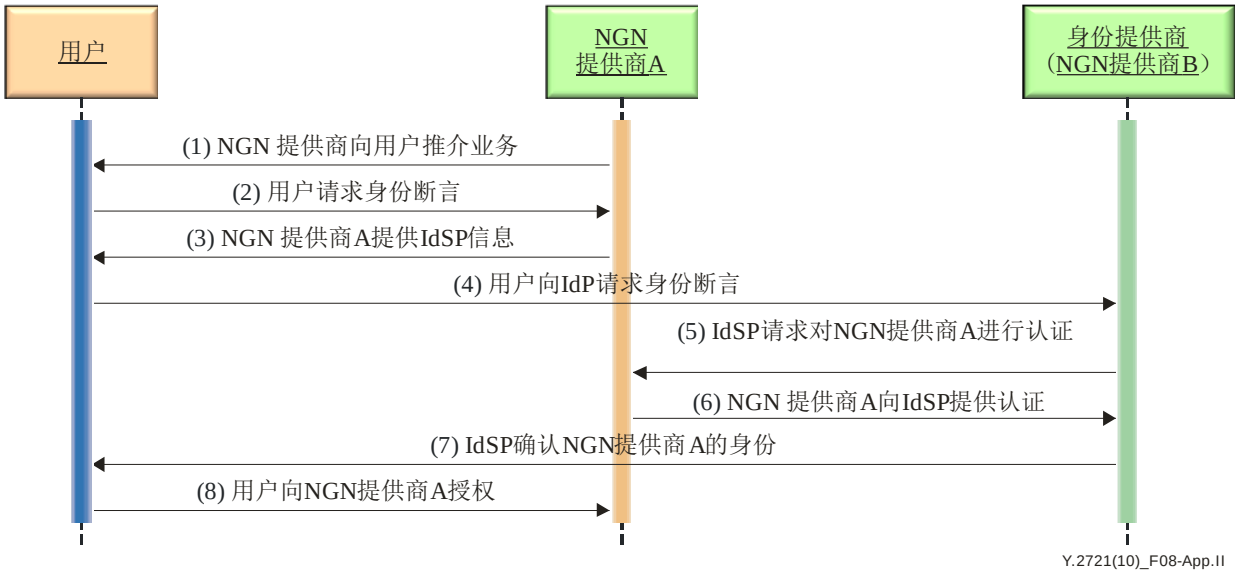


图 II.8 – 使用案例：用户对NGN提供商的认证和授权

现将示例的呼叫流程归纳如下：

1) NGN提供商A向用户推介业务
2) 用户请求断言NGN提供商A的身份
3) NGN提供商向用户提供身份服务提供商（IdSP）的地址
4) 用户向IdSP发送请求，以获得NGN提供商A的身份断言
5) IdSP向NGN提供商A发送请求进行认证
6) NGN提供商提供认证信息
7) IdSP向用户发送信息，验证NGN提供商A的身份
8) 用户授权NGN提供商A提供服务。

注 – 本示例并未显示NGN提供商认证和验证或用户相关流程。

II.10 使用案例 – 对等用户断言（非现金交易）

目前，NGN缺乏允许用户认证通信发生或数据来源的IdM能力。一般而言，目前正在受到规范的IdM方法主要集中于针对现金交易和电子商务的IdM。NGN将需要为范围更广的交易和通信提供IdM能力保障。对于必须得到NGN支持的某些应急业务而言，这一点尤为重要。图II.9显示了一个使用案例，说明了NGN IdM能力的必要性，使用户能够相互断言身份，以开展对等通信及非现金交易。如，用户可能需要对来源或收到的消息（如，电子邮件或及时消息）、通信请求（如，语音、视频或数据通信）或收到的数据进行认证。而目前缺乏支持这类IdM能力的NGN规范。

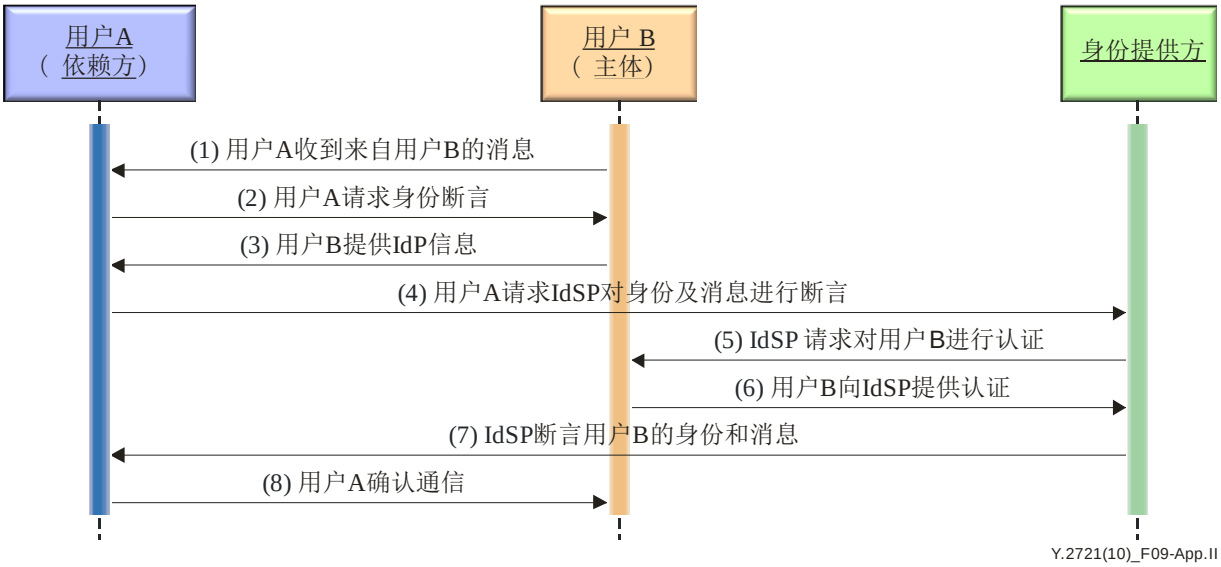


图 II.9 – 使用案例：对等用户断言（非现金交易）

图II.9所述使用案例假定用户收到了来自用户B的一条消息或一项请求，希望对用户B的身份及所收到的数据进行断言。现将示例的呼叫流程归纳如下：

1) 用户A收到来自用户B的消息或通信请求

2) 用户A请求获得用户B的身份断言并对从用户B收到的信息进行认证

3) 用户B向用户A提供身份服务提供商（IdSP）的地址信息

4) 用户A向IdSP发送请求、以断言用户B的身份并认证所收到的信息

5) IdSP向用户B发送认证请求

6) 用户B向IdSP做出回复并进行认证

7) IdSP回复用户A，断言了用户B的身份及所收到的信息

8) 用户A向用户B认可通信

II.11 IdM使用案例 – 最终用户装置的身份和完整性保证

NGN将支持形形色色的用户装置（如，固定电话、无线手机、个人电脑、PDA、IP电视机顶盒）。连接到NGN的装置包括各类复杂程度不一的硬件和软件组件。万一被盗并受损，它们可被用于发起各种各样的攻击。

可设计并采用专用安全能力，将之作为最终用户装置中防止篡改的硬件组件，以加密形式保存身份管理数据并支持专用安全能力，从而验证最终用户装置的身份和完整性。本节介绍的使用案例设计和采用了专用安全硬件组件，作为最终用户装置的一部分，为身份管理业务提供支持，从而：

1) 保证最终用户装置的身份

2) 保证最终用户装置的完整性（如，核实所配置的软件和硬件并未受损）

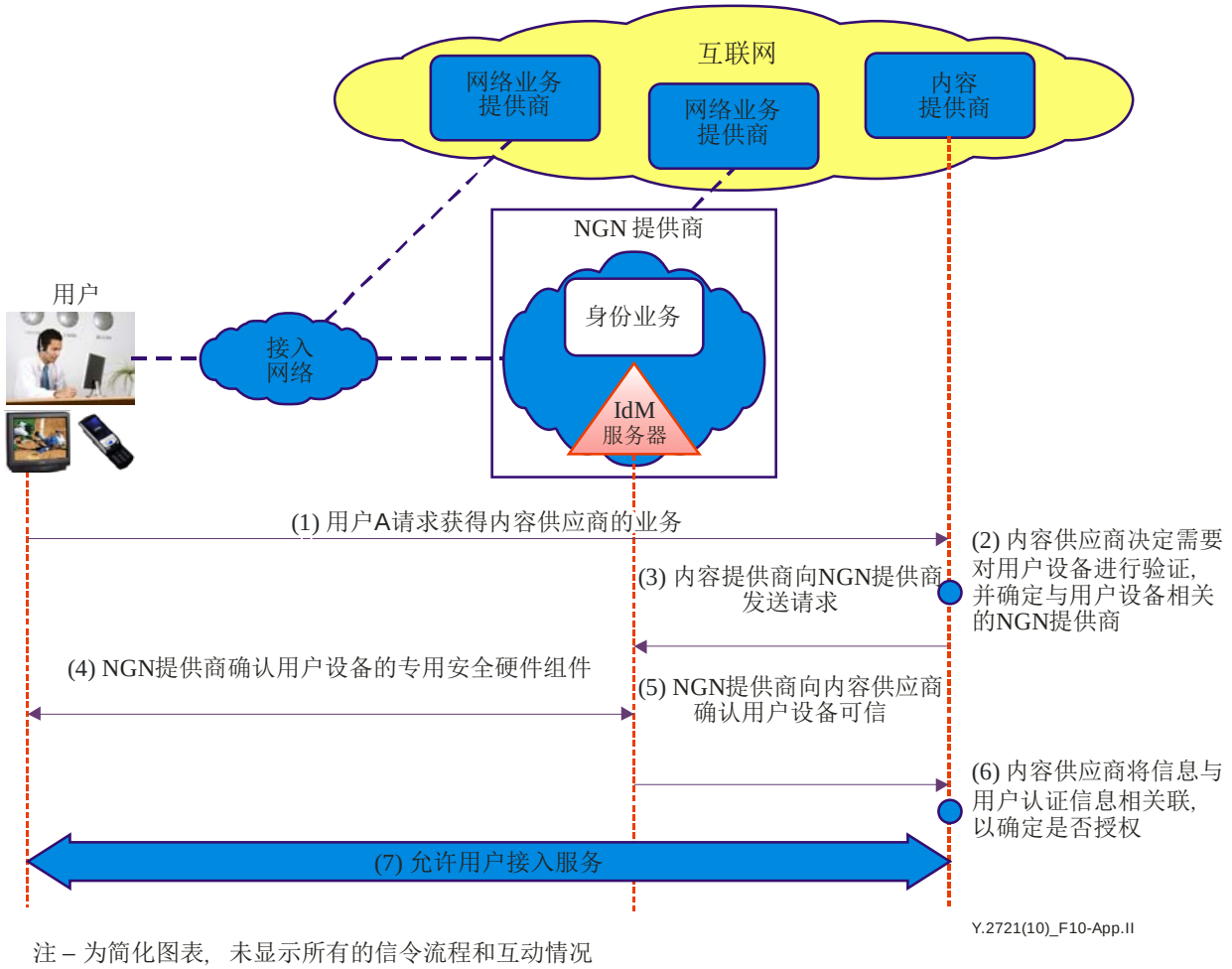
3) 允许用户在最终用户装置上对PII及其它敏感数据进行加密和保护。

II.11.1 使用案例 – 用户和装置的认证保证

本使用案例涉及支持最终用户装置中专用的防篡改硬件组件，为装置提供独一无二的身份确认。例如，密码、数字秘钥以及证书可储存在装置的专用防篡改硬件组件中，为装置提供独一无二的身份确认。专用硬件组件可支持标准化应用协议接口（API），支持安全应用服务将专用硬件组件作为最终用户装置的信任锚。

可将对防篡改硬件组件的独特确认和认证以及对用户的确认和认证相互关联，在多业务提供商环境中提供更高程度的访问控制保证。

图II.10介绍了一个使用案例，其中在最终用户装置中设计并采用了一个专用防篡改硬件组件，为设备提供独一无二的身份确认。在本实例中，假定NGN提供商通过与签约用户签订协议，对专用防篡改硬件组件进行控制。经限定用户同意，NGN/IdSP提供商可向其他服务提供商（如，内容提供商、网络业务提供商和第三方服务提供商）及合作伙伴提供身份服务，为最终用户装置的身份和认证提供保障。业务提供商将因此对最终用户装置的身份和认证产生信任。可将用户装置的身份和认证信息与用户认证联系起来，以获得更高程度的保障和信任。



注 – 为简化图表，未显示所有的信令流程和互动情况

图 II.10 – 关联用户和装置认证以获得保证

现将呼叫流程归纳如下：

1) 用户请求获得内容提供商的业务。

2) 内容提供商决定有必要核实用户装置，以便允许其访问业务，并确定NGN提供商与)用户装置有关

3) 内容提供商向NGN提供商发送要求断言用户装置身份和认证的请求

4) NGN提供商确认并认证用户装置的专用安全硬件组件（如，核实装置防篡改安全硬件组件中存储的证书）

5) NGN提供商回复内容提供商，验证用户装置的身份和认证

6) 内容提供商将NGN提供的信息与用户认证信息相关联，确定对业务进行授权

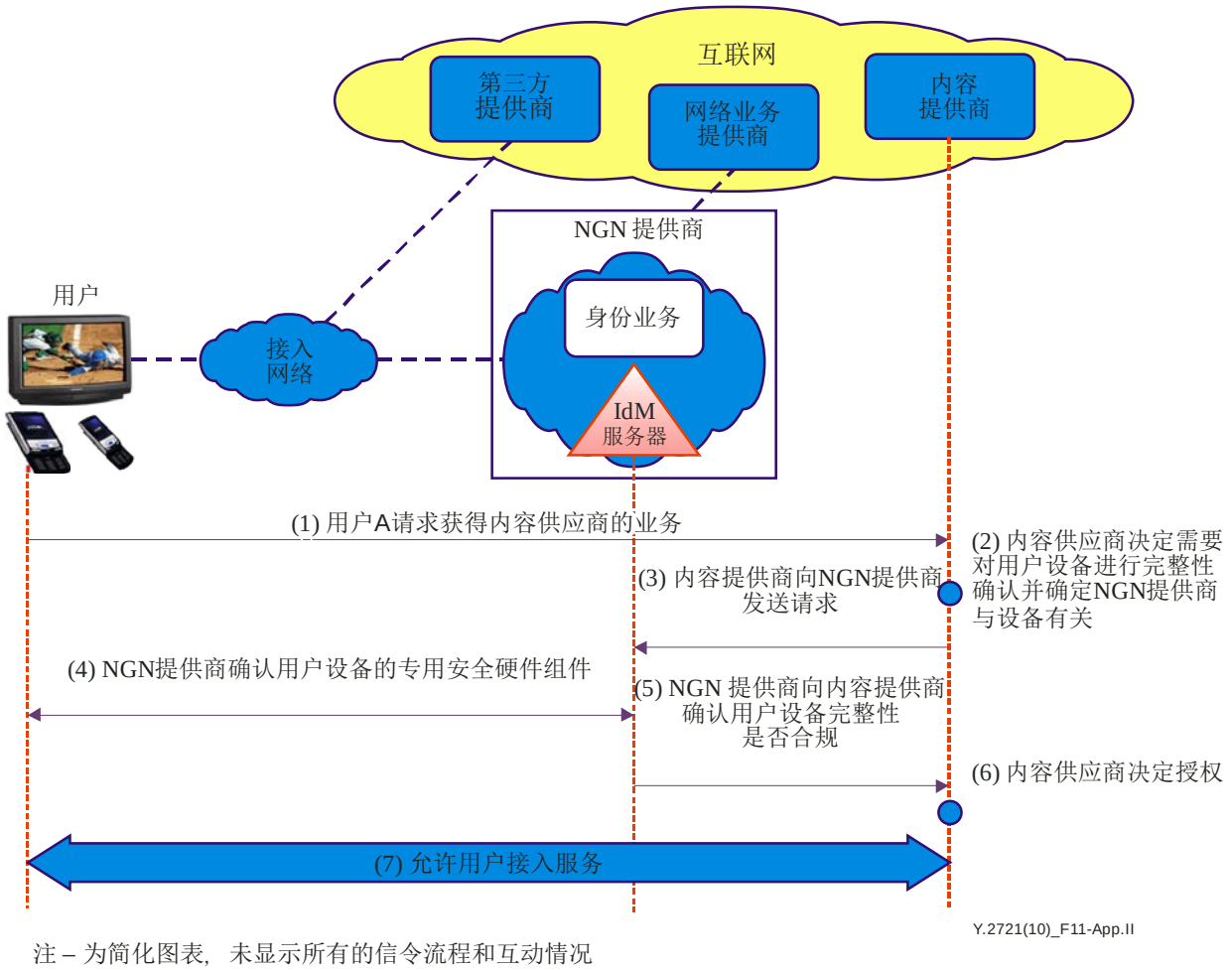
7) 允许访问业务（如，内容）。

II.11.2 使用案例 – 用户装置的完整性保证

在当今的安全环境中，签约用户利用不同的装置（如，固定电话、无线手机、个人电脑、PDA、IP电视机顶盒）连接到网络。在用户/签约用户不知情的情况下，最终用户装置的完整性（如，所配置的软件和硬件）很容易遭受损害。流行的互联网应用程序（如，在签约用户装置上执行的、帮助用户与业务及本地装置的特性发生互动的网络浏览器和电子邮件）一旦引入漏洞，便极有可能损害装置的完整性。如，这些应用程序可能含有容易受人利用的内在安全缺陷或支持特色，如文档下载、软件小程序、浏览器插件和嵌入式链接。软件和文档下载（尤其是来自一个不受信任的来源）使签约用户的装置易于受到恶意代码、蠕虫、病毒和木马的攻击。密钥记录器（可记录包括用户名和密码在内的所有密钥输入，然后将信息转发给一个能够利用该信息进行非授权访问的攻击者）即是一种常见的恶意代码。其他类型的恶意代码包括间谍软件（即跟踪用户活动的程序），以及广告软件（通常基于监控用户所采集到的信息推出无用广告的程序）。其中的一些程序会不客气地劫持签约用户装置，通过把自己深藏于操作系统，使人难于察觉其存在。

本使用案例涉及支持最终用户装置中的专用防篡改硬件组件，以进行完整性检查并向应用程序和业务确认装置的完整性。如，专用防篡改硬件组件可能含有厂商为进行完整性损坏检查而设计的特定算法和功能。专用硬件组件可能包含一个参照模型，其中拥有一套已知的良好完整性衡量规范，专门用于识别正确代码并为装置提供参照值。已知的良好完整性衡量规范将配置与实际报告值加以对比，从而确定该装置是否合规。

图II.11介绍了一个使用案例，其中最终用户装置设计并采用了专用防篡改硬件组件，用于核实装置的完整性。在本示例中，假定NGN提供商通过与签约用户签订协议，对专用防篡改硬件组件进行控制。经限定用户同意，NGN/IdSP提供商可向其他服务提供商（如，内容提供商、网络业务提供商和第三方服务提供商）及合作伙伴提供身份服务，对最终用户装置的完整性和合规性进行确认。



注 – 为简化图表，未显示所有的信令流程和互动情况

图 II.11 – 装置的完整性保证

现将示例的呼叫流程归纳如下：

1) 用户向内容提供商请求业务
2) 内容提供商决定有必要核实用户装置的完整性，并确定NGN提供商与用户装置有关
3) 内容提供商向NGN提供商发送请求，要求进行用户装置完整性确认
4) NGN提供商与用户装置专用安全硬件组件发生互动，核实完整性是否合规
5) NGN提供商向内容提供商确认用户装置的完整性
6) 内容提供商决定授权
7) 允许用户访问业务（如，内容）

II.11.3 使用案例 – PII和敏感文档/数据的加密

含有 PII 及其他敏感数据的装置一旦丢失或被盗，可能会给个人、企业和政府企业带来严重后果。用来以独特的方式识别并确认可信赖装置的完整性的专用硬件组件也可用来支持对最终用户装置上的 PII 和其他敏感数据进行加密和保护。由于保密数据经过加密，非授权方无法获得电脑、手机或存储设备上的数据，从而避免了事后的亡羊补牢措施和相关费用。

附录 III

与应急通信服务（ETS）相关的IdM使用案例

（此附录不构成本建议书的组成部分）

III.1 引言

本附录列举了与 ETS 相关的 IdM 使用案例。ETS 是一项需要预先处理的服务。见第 8.4.7 节。

III.2 综合利用设备和用户提供认证保证

认证获授权的 ETS 用户的身份，是保护 ETS 以及相关网络的可用性和完整性的必要条件。目前对遗留的 ETS 应用程序采用的两个基本身份认证方法是：

1) 基于PIN的方法，和

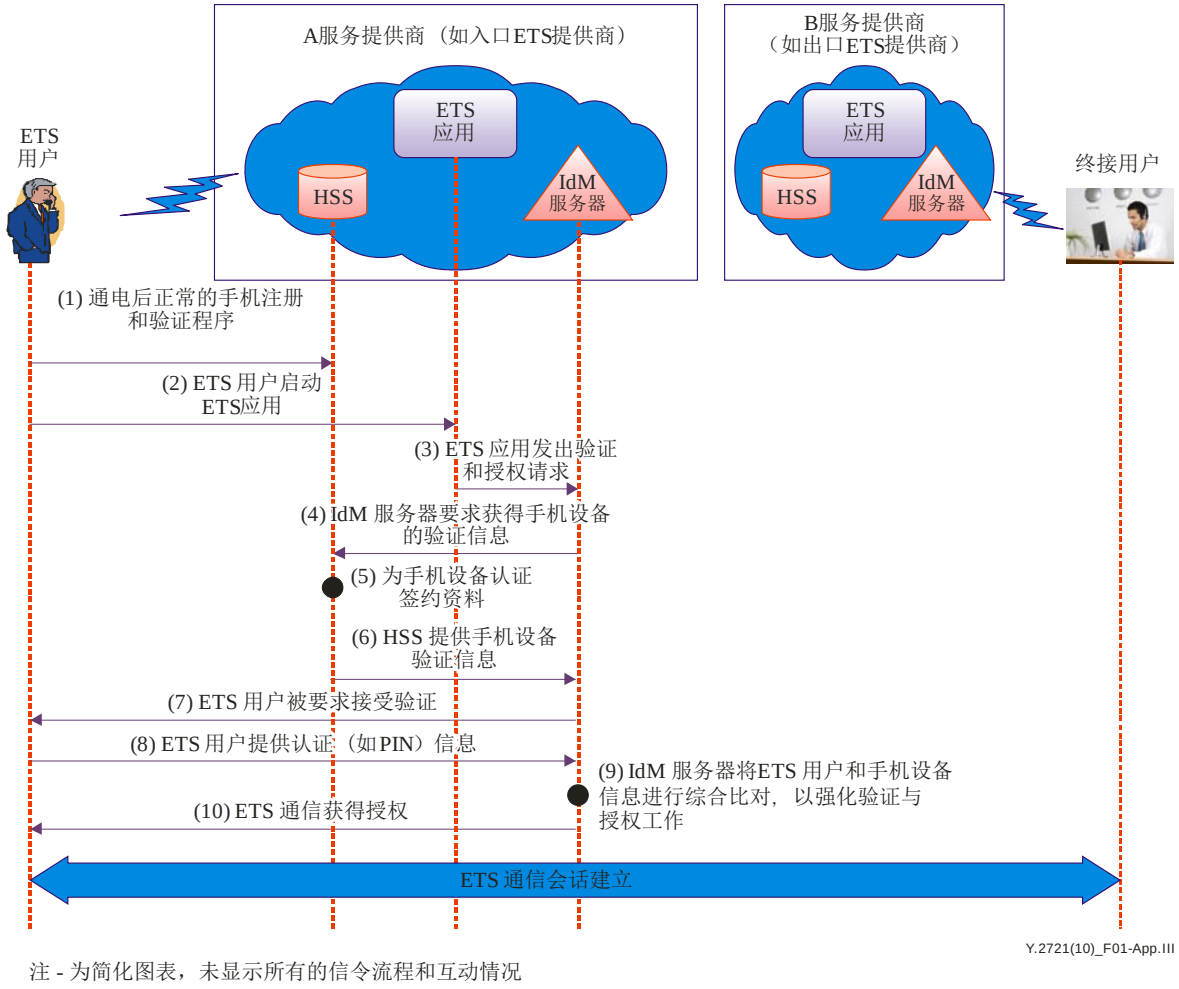
2) 基于签约的方法。

第一种方法涉及利用个人识别号码（PIN）进行认证和授权。对 PIN 的认证可辨识用户的真伪，从而授权用户使用 ETS。这种方法识别的是用户，不是用户装置。因此，它通常用于用户从任意设备获取 ETS 的情况。

第二种方法是根据与具体终端或最终用户装置相关的签约综合信息进行的认证与授权。用户装置或终端的身份认证，是作为下一代网络（NGN）提供商（即 ETS 提供商）的常规注册和认证的一部分进行的，并通过核查服务预订资料授予个体 ETS 呼叫/会议的权力（即认证服务预订是否允许设备提供 ETS 呼叫/会话）。这种方法认证的是用户设备（如无线手机），而非用户。

使用简单的基于 PIN 或基于签约的方法，足以应对遗留的 ETS 应用程序。然而，简单的基于 PIN 或基于签约的方法，则不足以应对 NGN 环境中所有类型的 ETS 应用。具体来说，多媒体优先服务（如数据和视频服务），将需要对 ETS 用户身份和授权级别更有把握与信任，才能动用 ETS 应用程序及其相关资源。因此，除了支持现有的基于 PIN 和基于签约的认证方法外，NGN 还必须支持得到强化的机制认证，并授权 ETS 用户和设备。

一种可考虑采用的 ETS（如优先语音服务）向 NGN 环境过渡的方法，是利用 IdM 将用户认证与用户装置的识别和认证结为一体。这将为访问 ETS 的用户的身份和授权提供更多的保证（即信任）。以下通用案例对这一概念做了说明。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.1 – 用户和设备的综合认证

图 III.1 例举了利用 IdM 进行用户和设备综合认证、使 ETS 用户的授权更有保障的实用案例。

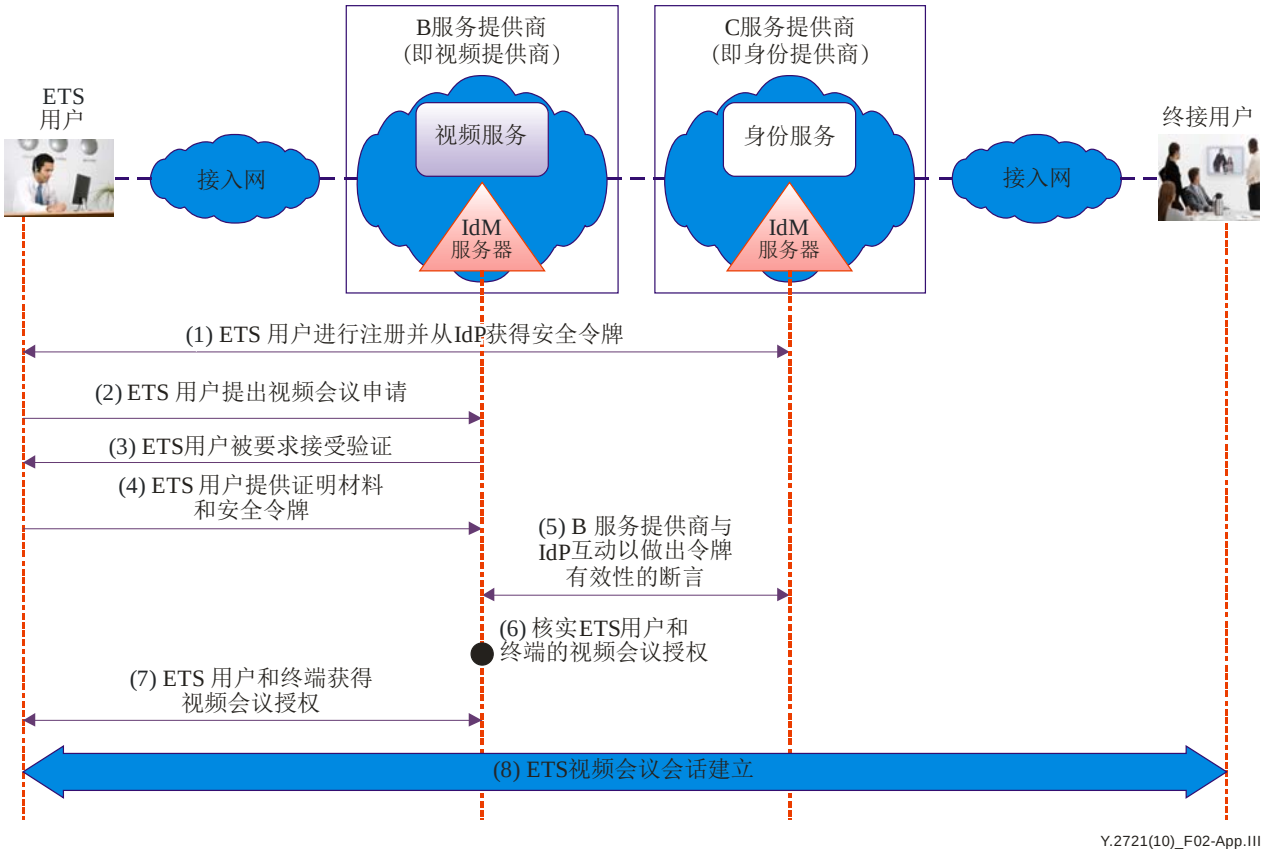
现将呼叫流程示例归纳如下：

1) 用户的手机装置是在带电情况下利用通用程序进行注册和认证的
2) ETS用户启动ETS应用程序
3) ETS应用程序需要IdM服务器的认证和授权
4) IdM服务器需要HSS提供手机装置认证信息
5) HSS认证手机的签约记录
6) HSS向IdM服务器提供手机装置认证信息
7) ETS用户被要求接受认证
8) ETS用户提供认证（如PIN）信息
9) IdM服务器将ETS用户和手机装置信息进行综合比对，以强化认证与授权工作
10) ETS通信会话获得授权。

这一实例流程提高了 ETS 用户身份和服务使用授权的可靠性。将设备的认证与用户相结合需要 ETS 用户为身份认证加强互动，但人们可能视之为一种负担。不过，这并不是所有 ETS 会话所必需的。可以考虑将它用于需要更高级别保障的 ETS 会话。

III.3 为下一代优先业务（优先多媒体业务）而强化ETS用户认证

随着通信环境向NGN/IMS环境的过渡，ETS用户需要跟上通信界的技术变革和新趋势。例如，ETS用户越来越多依赖即时通信、短信和电子邮件等超越语音通信的方式开展工作。一般来说，规划和发展阶段实施的举措可以使用户优先获得语音、数据和视频服务等多媒体服务。但是，用于PSTN环境的基于PIN或基于签约的机制，不足以承担NGN/IMS环境中的多媒体服务。具体来说，由于NGN整体环境的安全风险与威胁更大，多媒体优先服务等应用（如数据和视频服务）在ETS应用程序及其相关资源的实用方面，需要更为可靠和可信的ETS用户身份和授权水平。此外，与现有得到PSTN支持的ETS不同的是，下一代多媒体优先服务预计只获准有选择地向部分ETS用户提供。此外，鉴于总体目标是便于ETS用户以用户友好的方式随时随地通过任意设备进行访问，必须酌情考虑和使用更为先进的IdM机制。高度可靠的ETS用户身份，将是在整个灾害和紧急情况期间对ETS多媒体业务和资源以及全部NGN/IMS基础设施的完整性和可用性加以保护的关键。数据和多媒体应用（如网络信息或视频剪辑下载）与语音应用相比，具有带宽和资源密集特性。如果不加以适当控制，对ETS数据和视频应用未经授权的访问，会对ETS应用程序本身和整个通信基础设施造成负面影响。例如，对资源密集型ETS应用程序的擅自访问，有可能被用来造成网络拥塞或发起拒绝服务攻击。因此，应考虑采用特殊安全令牌、数字证书、语音识别和生物识别功能等更先进的方式，进行ETS用户和/或终端的身份认证与授权。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.2 – 对下一代优先服务的强化认证

图 III.2 展示了一个对下一代多媒体优先服务（如视频会议）授权用户强化认证的实用案例。这个案例假设身份证书（即安全令牌或数字证书）是由不同于多媒体服务提供商（虽然服务供应商和 IdSP 可能是同一家公司）的身份服务提供商（IdSP）提供的。如果 IdSP 不是该服务提供商，就必须事先确定必要的业务和信任安排，还需要 IdSP 与该服务提供商的相互认证。

现将呼叫流程归纳如下：

1) ETS用户注册并获得说明多媒体服务的ETS用户及特权的证书（如安全令牌或数字证书）

2) ETS用户提出视频会议申请

3) ETS用户被要求接受认证

4) ETS用户提供证书（如安全令牌或数字证书）

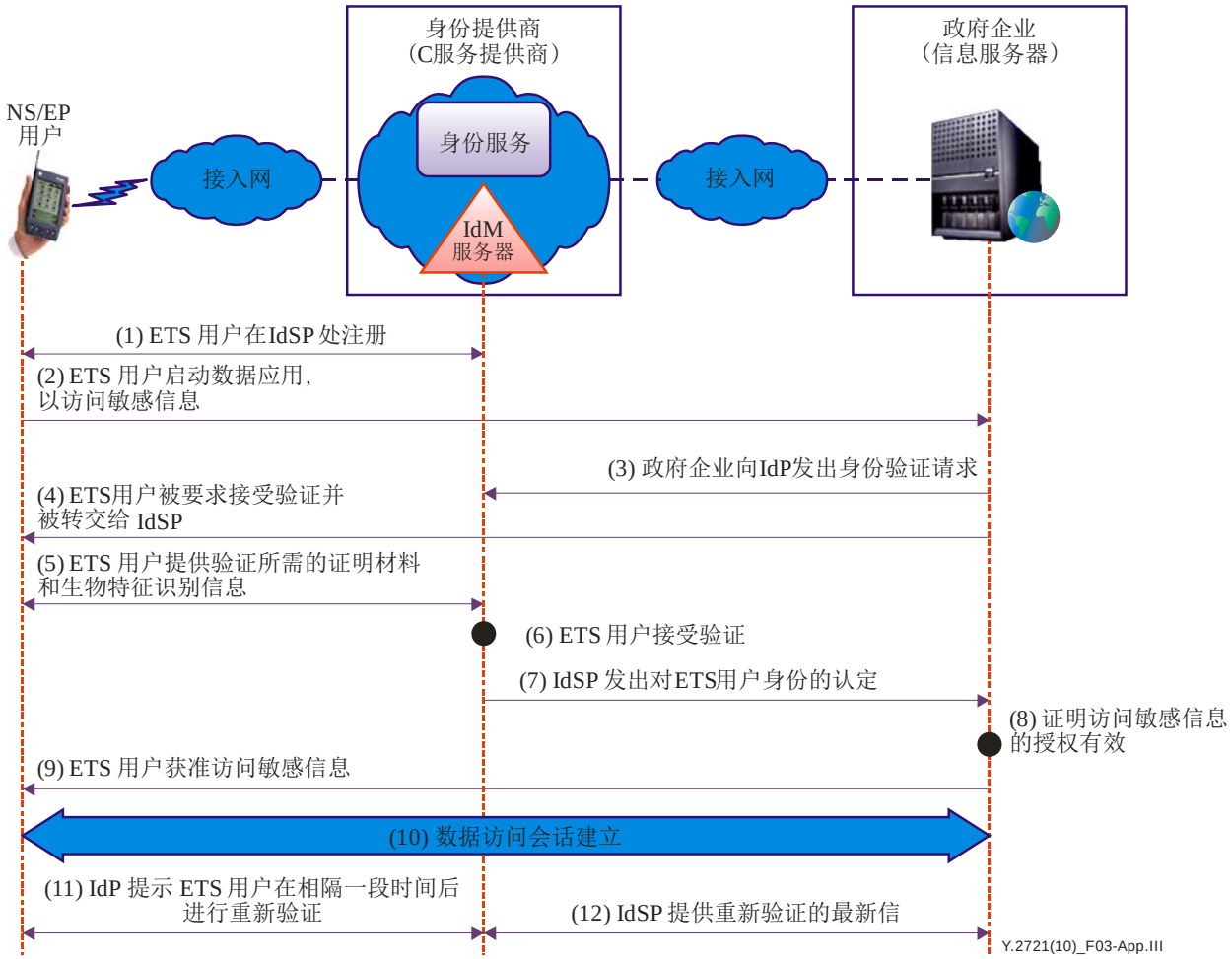
5) B服务提供商与身份服务提供商（IdSP）进行互动，要求认证证书（如安全令牌或数字证书）的有效性

6) B服务提供商处理并认证信息，以确定ETS 用户和终端是否获准使用多媒体优先服务

7) 经认证合格的ETS用户获准启动多媒体优先服务（如视频会议）

8) 多媒体会话得到设置和建立。

某些下一代多媒体通信业务可能需要利用生物特征识别信息来认证经授权的用户。例如，某些敏感性信息或许只能在部分经授权的用户之间共享。在这种情况下，ETS 用户身份认证必须具有高可信度。在这种情况下，生物特征识别机制可能被视为候选的认证技术。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.3 – 生物特征识别案例

图 III.3 显示了关于生物特征识别的案例。例子假设用户手机配备有读取生物特征识别信息的适当功能，还假设 ETS 用户在 IdSP 处进行了预注册，而且获得并存储了必要的生物特征识别信息。但请注意，除使用第三方服务提供商的服务之外，政府企业也可以托管和提供身份服务（如注册和保存 ETS 用户身份和生物特征识别信息）。现将呼叫流程归纳如下：

1) ETS在IdSP处进行了注册，以启动生物特征识别认证服务。这里假设的情况是，采集和证明生物特征识别和其它身份信息的必要程序（如本人亲自登记）已经完成。

2) ETS用户启动了远程访问托管敏感信息的政府企业数据库的通信

3) 政府的安全政策指出，访问许可必须高度可靠，并启动转交IdSP的程序

4) ETS用户受到认证质疑并重定向到IdSP。

5) ETS用户提供认证资料。例如，通过整合无线手机上的专用生物特征识别芯片进行拇指扫描

6) IdSP利用输入信息认证ETS用户

7) IdSP向政府企业发送证明ETS用户身份的信息

8) 政府企业核查ETS的身份是否获准访问托管敏感数据的信息服务器

9) ETS获得访问授权

10) 数据访问会话建立

11) IdSP提示ETS用户根据有关访问政府企业服务器的安全政策，在一具体时段后进行重新认证

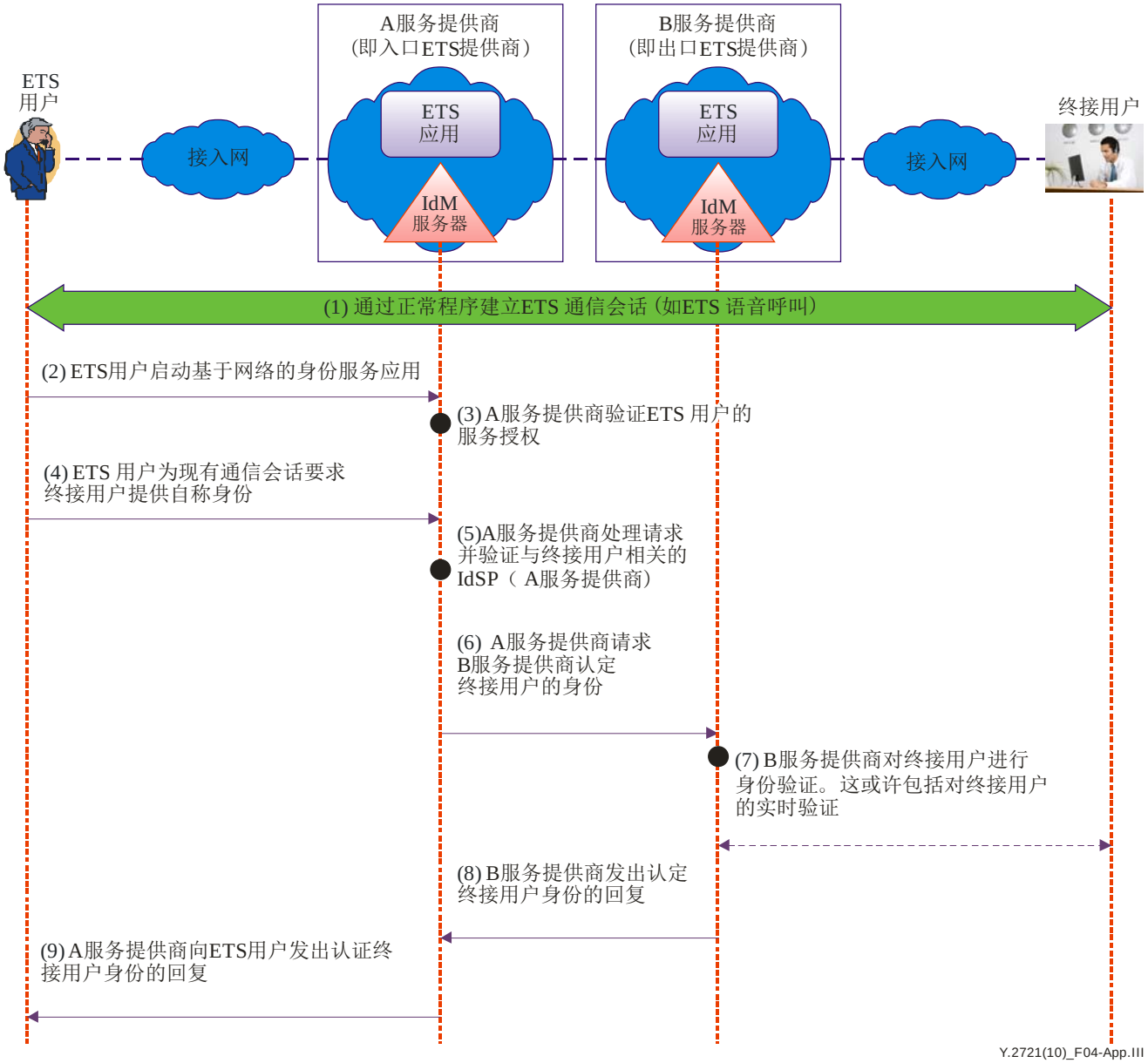
12) IdSP向政府企业提供有关ETS用户重新认证的信息。

III.4 呼叫方和数据通信源的认证

目前，尚没有作为 ETS 自身应用程序一部分的具体机制从事通信会话被叫方（即 ETS 呼叫的终接方）的认证工作。这在封闭的 PSTN 的环境中不算什么问题。然而，在向 NGN/IMS 的 IP 传输环境过渡时，则要考虑到通过假造被叫号码和路由信息形成假冒威胁的可能性。

未来可能利用通信服务提供商（CSP）和第三方服务供应商提供的身份管理服务，对 ETS 通信会话被叫方或终接方进行认证。具体而言，ETS 服务提供商可以支持 IdM 认证用户身份和用户自称身份的身份服务功能。示范性身份信息既可以是粗线条的呼叫方姓名查证，也可以是使用安全令牌、智能卡或数字证书等保护用户身份的更有力的认证机制。

图 III.4 介绍了一个关于 ETS 通信会话（如 ETS 语音呼叫）终接用户自称身份的使用案例。具体来说，这一用例假设 ETS 用户在 ETS 服务提供商那里预注册了基于网络的身份服务。在与一公共网络用户建立 ETS 通信（如 ETS 语音呼叫）联系后，ETS 用户通过门户网站启动身份服务，以认证 ETS 通信另一端的终接用户的身份。在这一用例中，ETS 通信会话的建立独立于用于确认终接用户身份的身份服务。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.4 – 终接用户身份的断言

现将呼叫流程与互动归纳如下：

1) ETS用户启动ETS通信会话（如ETS语音呼叫）。ETS通信会话通过正常程序建立。

2) ETS用户启动基于网络的身份服务（如A服务提供商，即入口ETS提供商的门户网站），对已建立的ETS通信会话的终接端用户进行认证

3) A服务提供商核实ETS用户的服务授权

4) ETS用户请求对已建立的通信会话终接端用户的身份进行认证

5) A服务提供商处理请求并确定与终接用户（即入口ETS提供商）相关的身份服务提供商（IdSP）

6) A服务提供商请求B服务提供商确认终接用户的身份

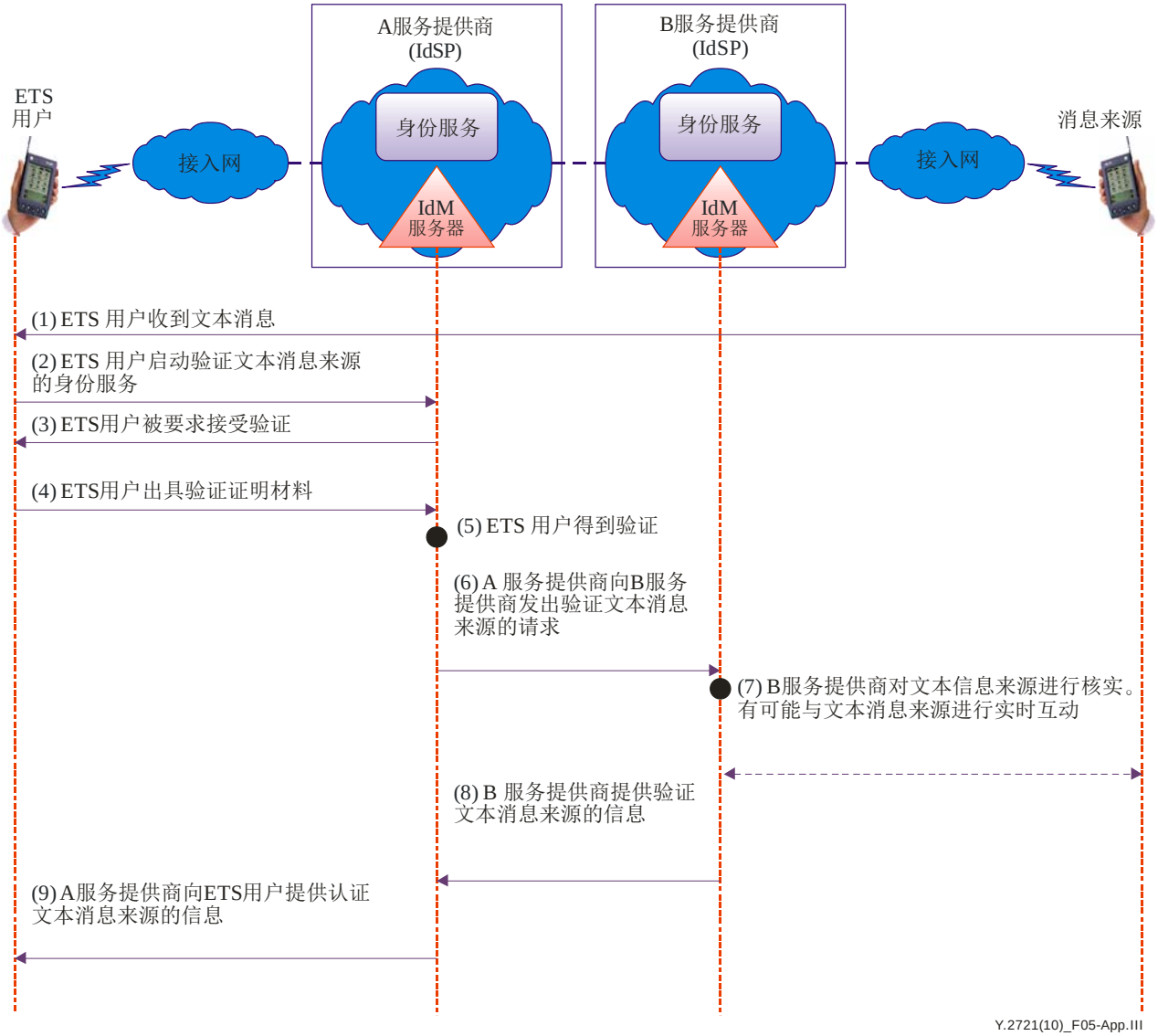
7) B服务提供商对终接用户进行身份认证。这或许包括对终接用户的实时认证

8) B服务提供商发出断言终接用户身份的回复

9) A服务提供商向ETS用户（即虚拟网络显示）发出认证ETS通信会话终接用户身份的回复。

ETS 用户越来越依赖对电子邮件、即时消息和文本消息等数据服务的使用。在某些情况下，或许有必要核实或认证这些数据服务的来源。鉴于存在大量垃圾信息和垃圾邮件，能够在某些灾难情况下区分和确认真实的信息，对 ETS 用户是至关重要的。

图 III.5 介绍了一个确认文本信息来源的案例。该案例假设 ETS 用户收到了文本消息，但无法确定是否来自另一个 ETS 用户。于是采用了服务提供商的身份服务，确认文本信息的来源。身份服务可以确认该文本信息的来源是否是文本信息服务自身的一部分。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.5 – 对文本消息来源的断言

现将呼叫流程与互动归纳如下：

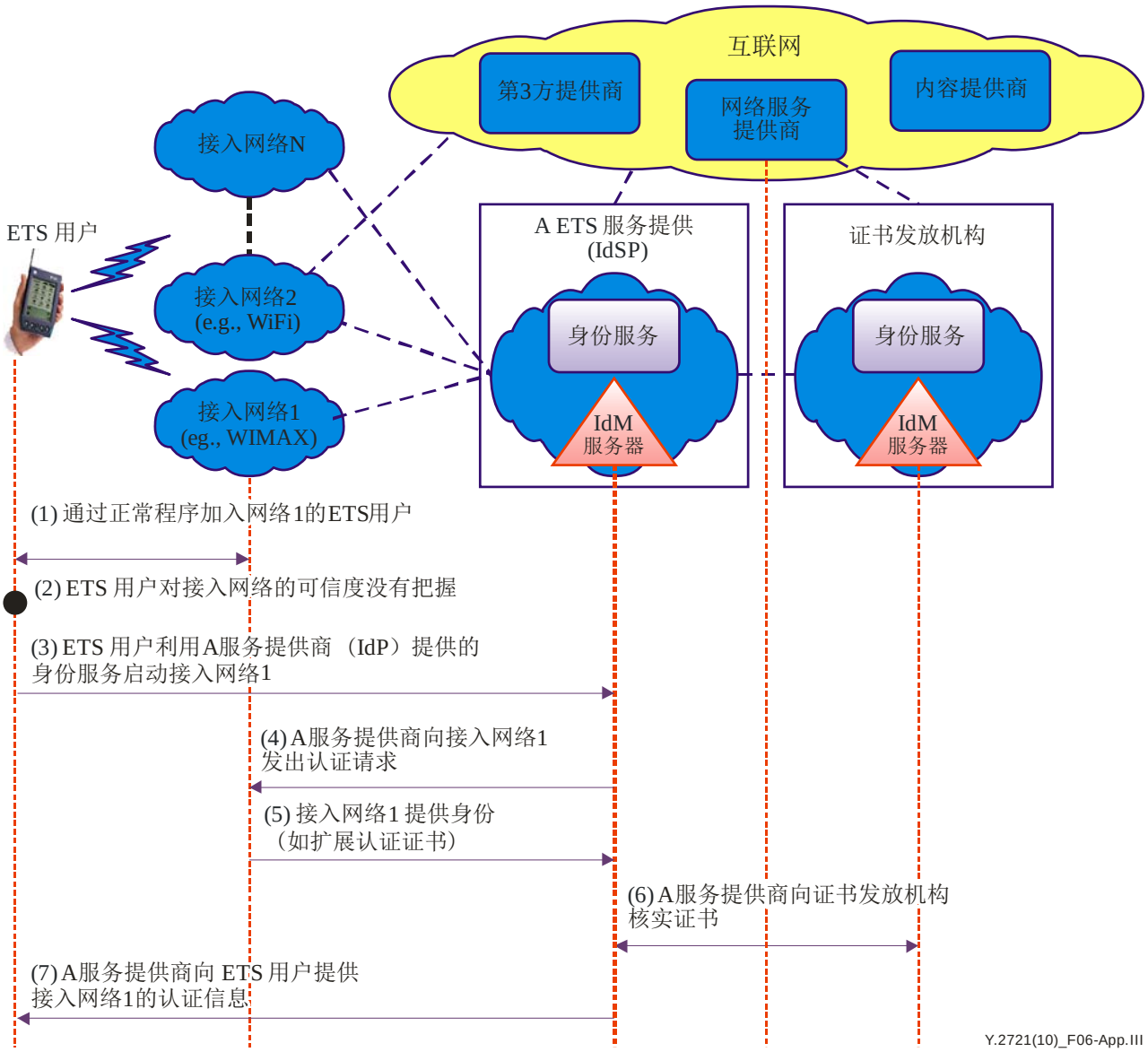
1) ETS用户收到文本消息
2) ETS用户希望核实文本消息来源的真伪，遂启动A服务提供商提供的身份服务
3) ETS用户被要求接受认证
4) ETS用户出具认证证书
5) A服务提供商认证ETS用户并核实身份服务授权
6) A服务提供商向B服务提供商发出断言文本消息来源的请求
7) B服务提供商处理请求并核实文本消息来源。这或许包括与文本消息来源的互动
8) B服务提供商向A服务提供商发出断言文本消息来源身份的回复
9) A服务提供商向ETS用户发出认证文本消息来源的信息。

III.5 对多提供商环境中的服务提供商的可靠证明与认证

当今的通信基础设施已经发展成一个多提供商环境，包括使用不同技术（如 xDSL、电缆、FTTX、WiFi、WiMAX、EV-DO、LTE）的多固定和移动接入提供商、采用“受管理的核心 IP 网络”的通信服务提供商、网络服务提供商、内容提供商和第三方提供商。在这种多提供商环境中，服务提供商的身份可能不会再像封闭的 PSTN 环境那样受到绝对信任。

在开放的多提供商环境中，人们缺乏对服务提供商进行可靠识别、认证和授权的能力，这可能导致非法实体伪装、伪造或假冒合法服务提供商的情况。因此，识别和认证服务提供商的 IdM 功能，对于基础设施的保护至关重要。当服务提供商在向 ETS 提供支持时，这种能力便成为国家安全的关键。

在图 III.6 展示的 ETS 用例中，ETS 用户试图在多提供商环境中接入网络。具体来说，漫游中的 ETS 用户的移动手机装置可加入在该地区提供服务的多个接入网络提供商之一（不是所有的服务提供商都是经授权的 ETS 服务提供商）。此用例假设 ETS 用户加入作为其首选的接入网络 1。加入该网络后，ETS 用户希望先对网络进行认证，再进行任何敏感的 ETS 通信。有多种认证接入网络提供商的选择和形式可供考虑，包括 ETS 用户的直接认证。这个例子假定该系统的用户利用 A ETS 服务提供商的身份认证服务接入网络。此用例中的 ETS 用户信任 A 服务提供商，并将认可 A 服务提供商提供的有关接入网络 1 的认证信息。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.6 – 对接入服务提供商的认证

现将互动情况归纳如下：

1) ETS用户使用具有多种网络（如WiFi、WIMAX、LTE或EVDO）适应能力的的与移动手机进行漫游。ETS用户的移动手机装置加入网络1（即因知名ETS服务供应商和信号强度等因素而成为首选）

2) ETS用户希望在对网络1进行认证之后，再进行服务授权

3) ETS用户利用A服务提供商提供的身份服务启动对接入网络1的认证

4) A服务提供商向接入网络1发出认证请求

5) 接入网1提供身份认证信息（如扩展认证X.509证书）

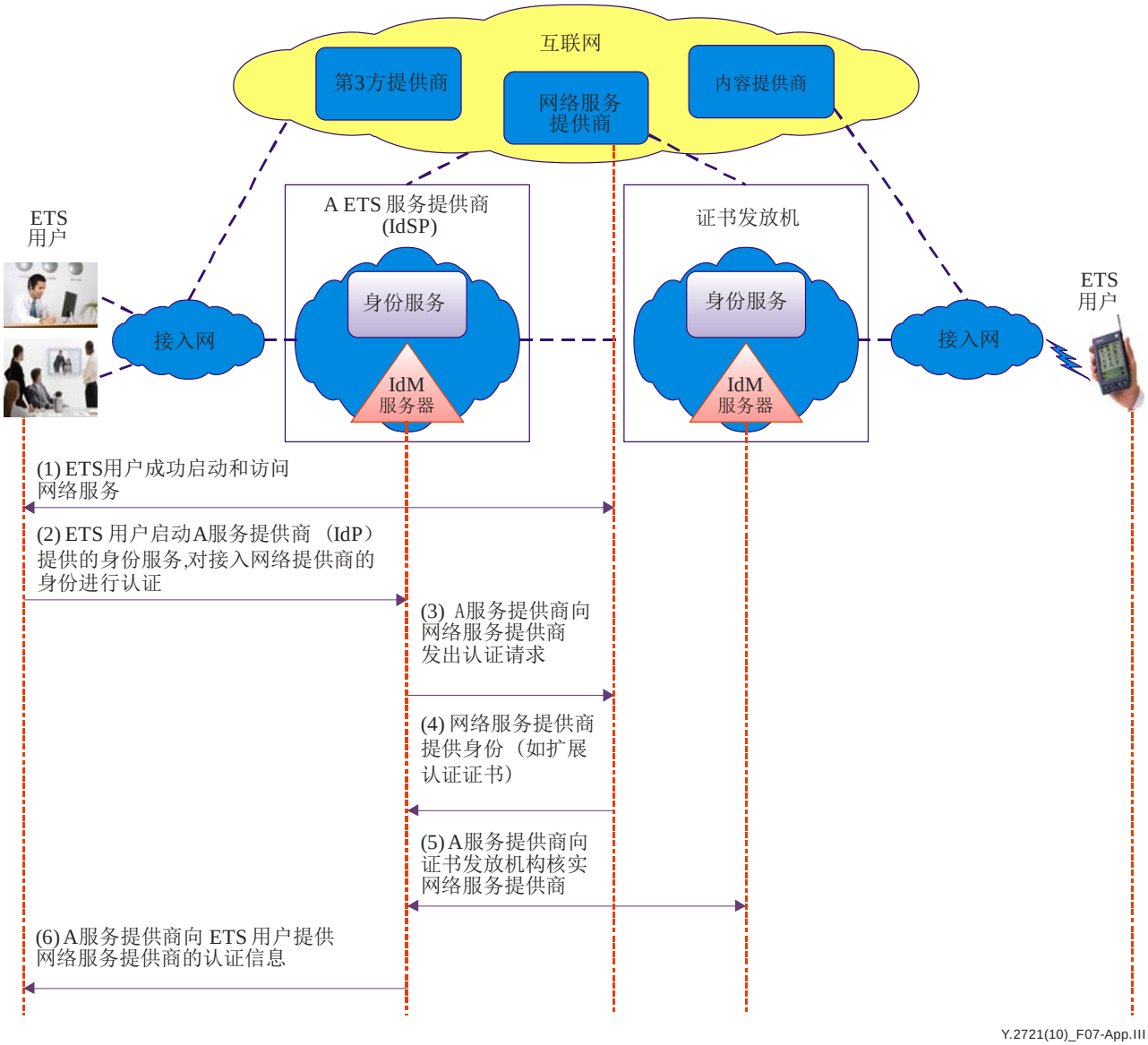
6) A ETS服务提供商向证书发放机构核实网络1的证书

7) A ETS服务提供商向ETS 用户提供接入网1的认证信息。

这使 ETS 用户在采取进一步行动时相信，他的移动手机装置连接的是一个经授权的接入网络。

在接入网络后，ETS 用户可使用多提供商基础设施中的多个服务提供商的服务。例如，ETS 用户可能需要使用网络服务提供商（如地球和其它地图/数据提供商）或内容提供商（如提供监控摄像、天气预报或视频流的服务提供商）的服务。ETS 用户可通过互联网直接或通过下一代网络提供商的服务间接地访问网络服务提供商和内容提供商的服务。在其中的任何一种情况下，ETS 用户都可能需要对具体服务的提供商进行认证。

图 III.7 所举的案例显示，ETS 用户需要认证网络服务提供商的身份。如上述用例所示，有多种认证接入网络提供商的选择和形式可供考虑，包括 ETS 用户的直接认证。这个例子假设 ETS 用户使用 A ETS 服务提供商的身份服务，对网络服务提供商进行认证。正如前一案例所示，ETS 用户信任 A 服务提供商，并将认可 A 服务提供商提供的有关网络服务提供商的认证信息。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.7 – 对网络服务或内容提供商的认证

现将互动情况归纳如下：

1) ETS用户成功启动和访问网络服务。但ETS用户希望对网络服务提供商进行认证，以便提高对数据的信任

2) ETS用户启动A ETS提供商的身份服务，以便对网络服务提供商进行认证

3) A ETS服务提供商向网络服务提供商发出认证请求

4) 网络服务提供商提供认证信息（如扩展认证证书1）

5) A ETS服务提供商向证书发放机构核实信息

6) A ETS服务提供商向ETS用户提供网络服务提供商的身份认证信息。

对网络服务提供商的认证使 ETS 用户对网络服务的身份具有信任，从而使他更加信任从网络服务获得的信息。

III.6 单点登录和单点退出

用户通常需要登录多个托管应用服务（如互联网协议电话、数据和视频）的系统，因此需要同等数量的登录对话，而每个对话都可能涉及不同的用户名和身份认证信息。系统管理员面临的任务是以协调的方式管理每个多系统内的用户帐户，以便将安全政策付诸实施。

ETS 用户可能需要利用 IdM 的“单点登录和单点退出”等项功能。单点登录的前提是，最终用户、设备或最终用户与设备的组合可以凭借一次性登录一项服务（即通过提供认证和授权所需的证书），获得同一下一代网络领域的一项或多项附加服务的身份认证，或在联合提供服务的情况下，使这一认证横跨多个下一代网络领域。单点登录的价值在于最终用户不受逐项服务认证之累。这里使用的“登录”一词与“注册”（“Register with”）、“登记”（“Log-On”）或“登入”（“Log-In”）的意思相同，系指最终用户或设备“注册”、“登记”或“登入”一项服务。同时，“单点登录”还提供了一个全面“退出”一特定会话中的多项应用服务的方法。

单点登录和单点退出功能给 ETS 用户带来的潜在好处包括：

- 缩短用户登录各领域的操作时间，包括减少登录失败的次数。还通过降低用户处理和记忆多组认证信息的需求提高安全性。
- 减少系统管理员添加和删除系统用户或修改其访问权限所用的时间
- 通过增强系统管理员保持用户帐户配置完整性的能力，包括以协调统一的方式抑制或取消个人用户访问所有系统资源的能力

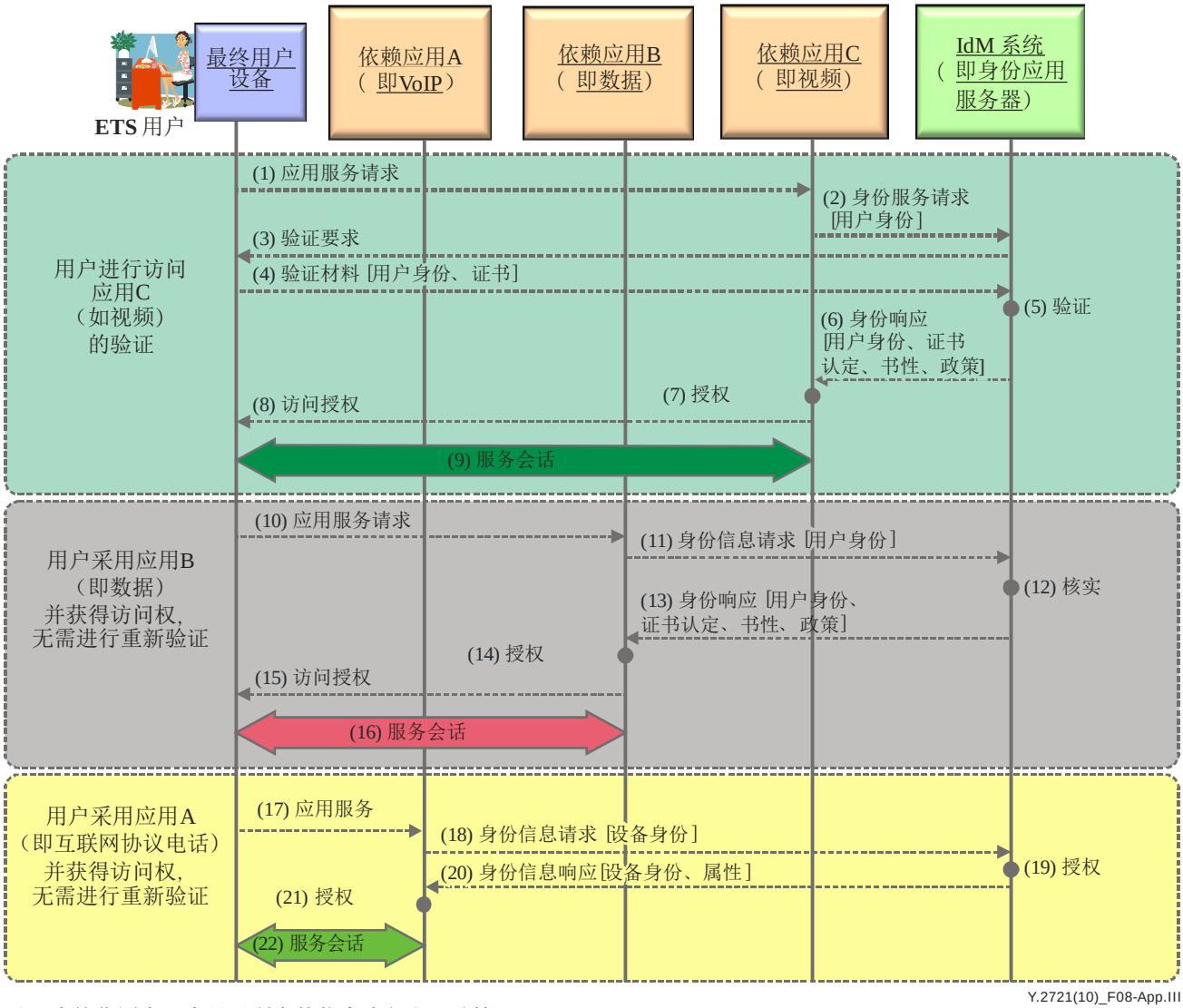
图 III.8 介绍了一个在下一代网络领域中利用 IdM 系统支持连接多应用服务（如互联网协议电话、数据和视频）的“单点登陆和单点退出”的案例。案例涉及以下实体之间的互动：

- 最终用户（即最终用户和/或最终用户装置）
- 依赖系统（即应用服务或网络系统）

---

1 扩展认证证书是特殊类型的X.509证书，要求证书机构在证书发放前对申请实体进行广泛调查。

- IdM系统（即提供诸如注册、认证和授权、签约个人资料信息等IdM服务的网络系统）。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.8 – 单点登录

本案例假设终端用户通过正常程序注册加入下一代网络。

呼叫流程如下：

1) 应用服务请求。这一信息流体现为ETS最终用户采用应用服务C（视频）的请求。

2) 身份信息请求[用户身份]。应用服务C（视频）向IdM系统发送一个断言用户身份的请求，并提供与用户身份相关的属性。其中可能包括服务的历史资料、特权、偏好和政策等信息，例如所有与身份相关的政策或限制。

3) 认证要求。IdM系统要求用户接受认证。

4) 认证材料[证书]。用户提供认证信息（如用户身份和护照或个人识别码）

5) 认证：IdM系统进行认证并获得其它信息，可能包括从其它网络系统（如HSS或其它签约数据库）获得的信息

6) 身份回复[证书的断言、属性、政策]。IdM系统提供证书断言信息。其它信息可能包括与用户身份相关的属性（如特权和偏好）和涉及身份信息的政策（即所有关系使用、显示和传播的限制）。

7) 授权。应用服务C（视频）对信息进行处理，并确定用户获得了这项服务的授权。

8) 访问授权。应用服务C（视频）提示用户：已授予他们服务访问权。

9) 服务会话。用户与应用服务C（视频）的会话已成功建立。

10) 应用服务请求。用户请求使用应用服务B（数据）。

11) 身份信息请求[用户身份]。应用服务B（数据）向IdM系统发送一个断言用户身份的请求，并提供与用户身份相关的属性。其中可能包括服务的历史资料、特权、偏好和政策等信息，例如所有与身份相关的政策或限制。

12) 核实。IdM系统对请求进行处理，确定单点录入功能适用，并核实用户认证依然有效。

13) 身份信息回复[证书的断言、属性、政策]。IdM系统提供证书断言信息。其它信息可能包括与用户身份相关的属性（如特权和偏好）和涉及身份信息的政策（即所有关系使用、显示和传播的限制）。

14) 授权。应用服务B（数据）对信息进行处理，并确定用户获得了这项服务的授权。

15) 访问授权。应用服务B（数据）提示用户：已授予他们服务访问权。

16) 服务会话。用户与应用服务B（数据）的会话已成功启动。

17) 应用服务请求。用户请求使用应用服务A（互联网协议电话）。

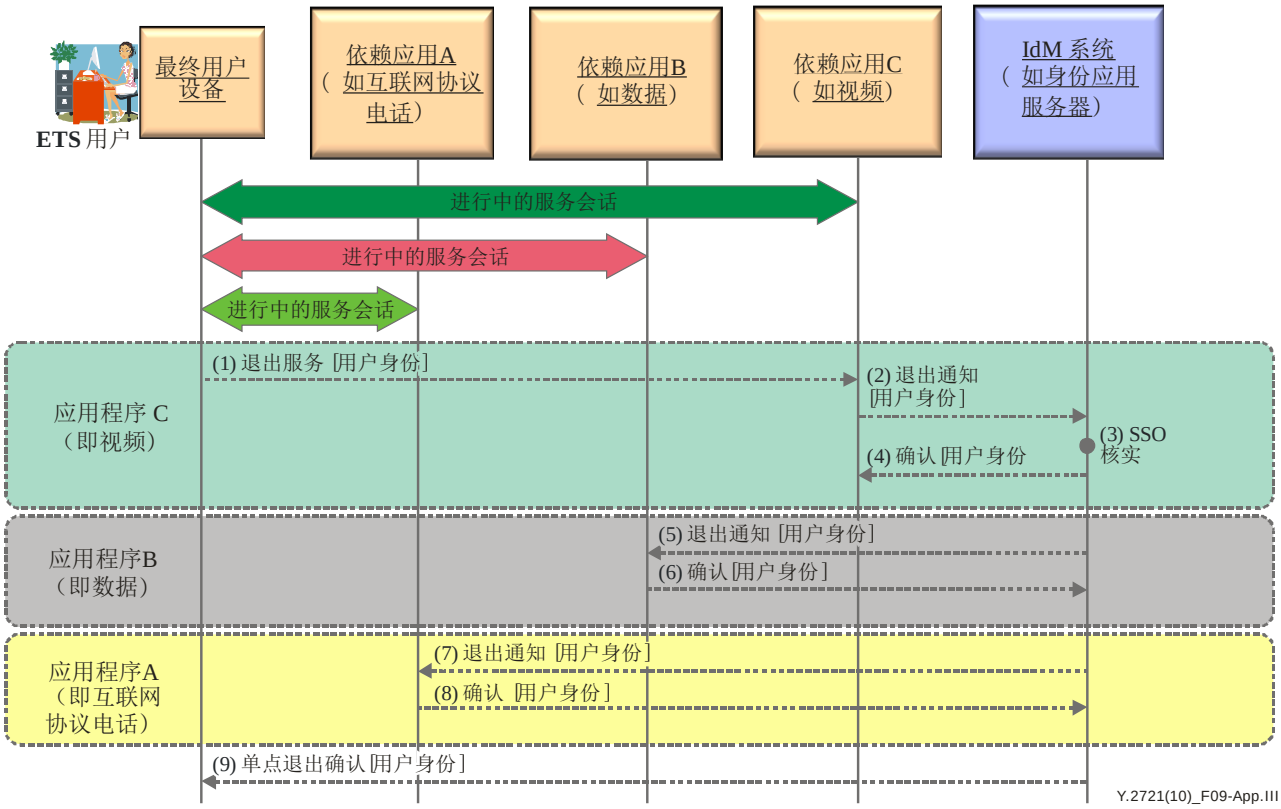
18) 身份信息请求[设备身份]。应用服务A（互联网协议电话）向IdM系统发送一个断言用户身份的请求，并提供与设备身份相关的属性。

19) 核实。IdM系统对请求进行处理，确定单点录入功能适用，并核实用户认证依然有效。

20) 身份信息回复[证书的断言、属性、政策]。IdM系统提供证书断言信息。其它信息可能包括与设备身份相关的属性（如特权和偏好）和涉及身份信息的政策（即所有关系使用、显示和传播的限制）。

21) 授权。应用服务A（互联网协议电话）对信息进行处理，并确定用户获得了这项服务的授权。

22) 应用服务会话。用户与应用服务A（互联网协议电话）的会话已经建立。



注 - 为简化图表，未显示所有的信令流程和互动情况

图 III.9 – 单点退出

图 III.9 说明“单点退出”服务可使用户在自动退出多个应用服务（互联网协议电话、数据和视频）时，无需退出会话中的各项程序。这一用例假定用户正处于进行中的应用服务 A（互联网协议电话）、应用服务 B（数据）和应用服务 C（视频）的服务会话当中。

呼叫流程如下：

1) 退出服务[用户身份]。ETS用户发出请求终止服务会话的信号。

2) 退出通知[用户身份]。应用服务C（视频）向IdM系统通报用户的退出请求。

3) SSO核实：IdM系统确定单点退出功能适用，并核实进行中的应用服务。

4) 确认[用户身份]。IdM系统向应用服务C（视频）发出终止服务会话的确认。

5) 退出通知[用户身份]。IdM系统将退出的情况通知应用服务B（数据）。

6) 确认[用户身份]。应用服务B（数据）对退出进行确认。

7) 退出通知[设备身份]。IdM系统将退出的情况通知应用服务A（互联网协议电话）。

8) 确认[设备身份]。应用服务A（互联网协议电话）对退出进行确认。

9) 单点退出确认[用户身份]。IdM系统向用户发出退出会话中所有现行应用服务的确认。

附录 IV

与移动相关的使用案例

（此附录不构成本建议书的组成部分）

IV.1 引言

本节提供了与移动相关的 IdM 使用案例。本节的案例是以美洲 3 代技术白皮书“*身份管理：移动和固定互联网标准与技术概论*”[b-3G美洲白皮书]为依据的。

IV.2 使用案例

IV.2.1 使用得到UICC支持的3G设备的移动用户，通过访问移动网络运营商（MNO）门户网站（网络商店）购买铃声。

参与方：

- 移动用户
- 移动网络运营商（MNO）
- 服务提供商（SP）是移动网络运营商

用户所得实惠：

- 单点登录不同移动网络运营商服务的体验。

主要制约因素：

- 服务提供商和移动网络运营商同处于一个信任圈（据自由联盟认为）。

IV.2.2 使用得到UICC支持的3G设备的移动用户访问移动网络运营商（MNO）门户网站上的网络商店；他浏览网站上的数字商品目录，找到了特别促销商品（如一种移动网络运营商拥有全部内容经销权的视频游戏）并进行了采购；他随后同意将这笔支出记入他的移动电话账单；用户可从由移动网络运营商转向内容提供商的安全链路下载游戏。

参与方：

- 移动用户
- 移动网络运营商
- 服务提供商-a是移动网络运营商；服务提供商-b是外部内容（即游戏）提供商

用户所得实惠：

- 单点登录移动网络运营商和外部厂商门户网站的体验。
- 能够利用其移动网络运营商提供的有关他的证书完成与外部内容提供商的交易。

主要制约因素：

- 作为移动网络运营商的服务提供商-a以及作为视频游戏提供商服务提供商-b同处于一个信任圈。

IV.2.3 移动用户正在使用其得到UICC支持的3G智能手机在另一国家漫游；在上网冲浪时，他订购了一本外国的汽车杂志并将支出记入信用卡（有选择地披露其移动网络运营商掌握的他的用户资料属性，以完成杂志订阅申请程序）；信用卡公司代表移动用户授权支付汽车杂志公司。

参与方：

- 移动用户
- 移动网络运营商
- 服务提供商-a是内容提供商；服务提供商-b是信用卡公司

用户所得实惠：

- 单点登录移动网络运营商和信用卡公司的体验。
- 能够利用其移动网络运营商提供的有关他的证书授权其信用卡公司进行支付，完成与外部内容提供商的交易。
- 能够再次利用其移动网络运营商从其用户资料中提取的有关他的个人属性信息完成外部服务的订购，从而最大限度地避免这类细节的重复操作。

主要制约因素：

- 移动网络运营商和作为服务提供商-b的信用卡公司同处于一个信任圈。
- 作为服务提供商-a的外国汽车杂志提供商不在信任圈内。

IV.2.4 移动用户使用其得到UICC支持的3G 笔记本在另一国家漫游，在机场候机时，他订购了几个小时的机场WiFi服务；由于那里的WLAN运营商与移动用户的移动网络运营商有联盟关系，因而同意将用户的WiFi使用费记入其移动电话账单；而移动用户在使用WiFi服务时，访问了多个他经常联系互动的门户网站，包括一家银行、一家旅行社和一家金融投资公司的门户网站；用户希望无需再登录地使用这些网络商家提供的服务，并能够安全地交换保密的个人信息。

参与方：

- 移动用户
- WLAN运营商
- 移动网络运营商
- 服务提供商-a是移动网络运营商；服务提供商-b是银行；服务提供商-c是旅行社；服务提供商-d是金融投资公司。

用户所得实惠：

- 单点登录移动网络运营商和WiFi运营商的体验。
- 能够利用其移动网络运营商提供的有关他的证书授权支付WiFi服务费。
- 能够通过简单的登录程序访问多个与移动网络运营商无从属关系的网络服务提供商，并安全传送私人信息。

主要制约因素：

- 移动网络运营商和WLAN运营商同处于一个信任圈。
- 作为服务提供商-a的银行、作为服务提供商-b的旅行社和作为服务提供商-c的金融投资公司不处于同一信任圈。

IV.2.5 移动用户在国内使用其得到UICC支持的3G 笔记本，利用其住宅宽带DSL服务在网上冲浪，并访问了其移动网络运营商的门户网站；他（利用其有预先授权记录的信用卡）支付了移动帐户服务费，并在其移动服务签约中增加了一项新特性；随后他又访问了一家电影租赁网站，其费用也记入他的信用卡（无预先授权）。

参与方：

- 移动用户
- 固定网络DSL运营商
- 移动网络运营商
- 服务提供商-a是移动网络运营商；服务提供商-b是电影租赁门户网站；服务提供商-c是信用卡公司。

用户所得实惠：

- 单点登录其固定网络运营商和移动网络运营商的体验。
- 能够利用其固定网络运营商提供的有关他的证书认证其移动服务账户，并增购移动网络运营商的服务。
- 能够授权利用其信用卡帐户支付外部服务提供商（如电影租赁）收取的内容购置费。

主要制约因素：

- 移动网络运营商、固定网络运营商和作为服务提供商-b的信用卡公司同处于一个信任圈。
- 作为电影租赁提供商的服务提供商-a不在同一信任圈内。

IV.2.6 使用其得到UICC支持的3G设备的移动用户希望访问一企业网内的资源（如企业目录服务）。

参与方：

- 移动用户
- 移动网络运营商
- 企业IdM系统
- 企业目录服务服务器（EDS服务器）

以下介绍了这些参与者间的高层互动。移动用户请求 EDS 服务器提供服务：

- EDS服务器请用户提供身份认证。
- 得到移动网络运营商系统认证的用户获得系统提供的认证证书，用于进入企业IdM系统的认证程序。
- 用户向企业IdM系统提交证书，并在通过认证之后，从该系统获得须交EDS服务器认证的证书。
- 用户利用企业IdM系统提供的证书回复EDS服务器的请求。
- 经认证的用户从EDS服务器获得他所需要的服务

用户所得实惠：

- 移动用户能以经济有效的方式利用其企业网上的资源（如企业目录服务），同时满足企业信息技术（IT）环境特有的苛刻安全要求。

主要制约因素：

- 除移动网络运营商提供的用户证书外，企业IdM系统可能还需要进行双重认证（如uid/password/PIN）。
- 移动网络运营商的IdM和企业IdM系统处于同一个信任圈。

附录 V

示范性IdM交易模型

（此附录不构成本建议书的组成部分）

V.1 引言

本附录提供了示范性 IdM 的交易模型。[b-ITU-T X.1250]对这些模型作了介绍。在本附录所列的模型之外，还可能存在其它模型。

V.2 可能的身份管理交易模型示例

如图 1[b-ITU-T X.1250]所示，常见于多数结构性信息交换过程中的基本查询响应程序，是身份管理的主要交易之一。最基本形式的信息交换涉及双方使用经认可的协议和信息模型。

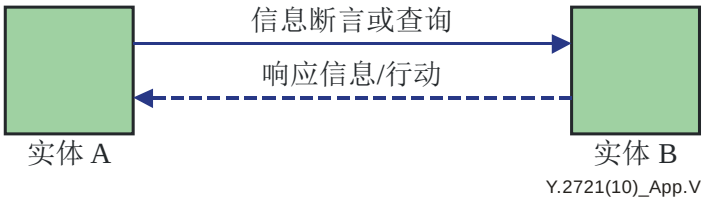


图 V.1 – 基本查询/响应信息交换过程

参与这一过程的各方可以是任何类型的实体。一个实体可以是一个自然人、动物、法人、组织，主动或被动物体、设备、软件应用、服务等，也可以是由件上述个人组成的团体。在电信领域，实体的例子包括接入点、订户、用户、网元、网络、软件应用、服务和设备、接口等。它们可以是任何物理或虚拟物件，如网络设备、软件、终端设备、传感器，主动标注的物理物件（如使用 RFID 或光代码）和被动标注的物件。例如，网络设备可被视为代表最终用户、提供商和政府机构接受 IdM 特别功能的实体。在数字权力管理方面，该实体可能是多媒体或 IPTV 内容等受知识产权或版权保护的资料。群体是一种特殊类型的实体，其身份是群体成员身份（共性）的汇集。

多数身份管理案例涉及复杂的模型。倘若原来接受断言的依赖方不是身份服务提供商，正如图 2A 或 2B[b-ITU-T X.1250]所示，身份服务提供商的职能是独立于和不同于依赖方的。依赖方对身份服务提供商的回应做出评估，并确定是否提供了充分的实体认证保证。服务提供商的主要职能是创建、更新、核实、暂停和废止身份信息。

可行的身份信息交换模型种类繁多。一个通常使用的模型是图 2a[b-ITU-T X.1250]所示的三方查询响应模型。该模型对一些新的开放式 IdM 协议作了预测。

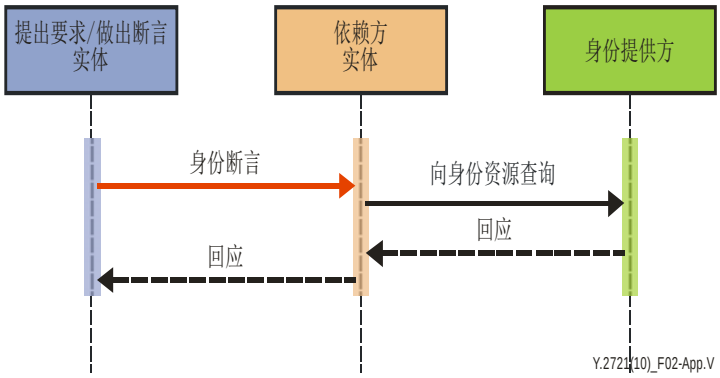


图 V.2 – 三方身份管理模型示例

图 2a [b-ITU-T X.1250]描述了应一方要求强化身份关系管理的另一种身份管理模型。

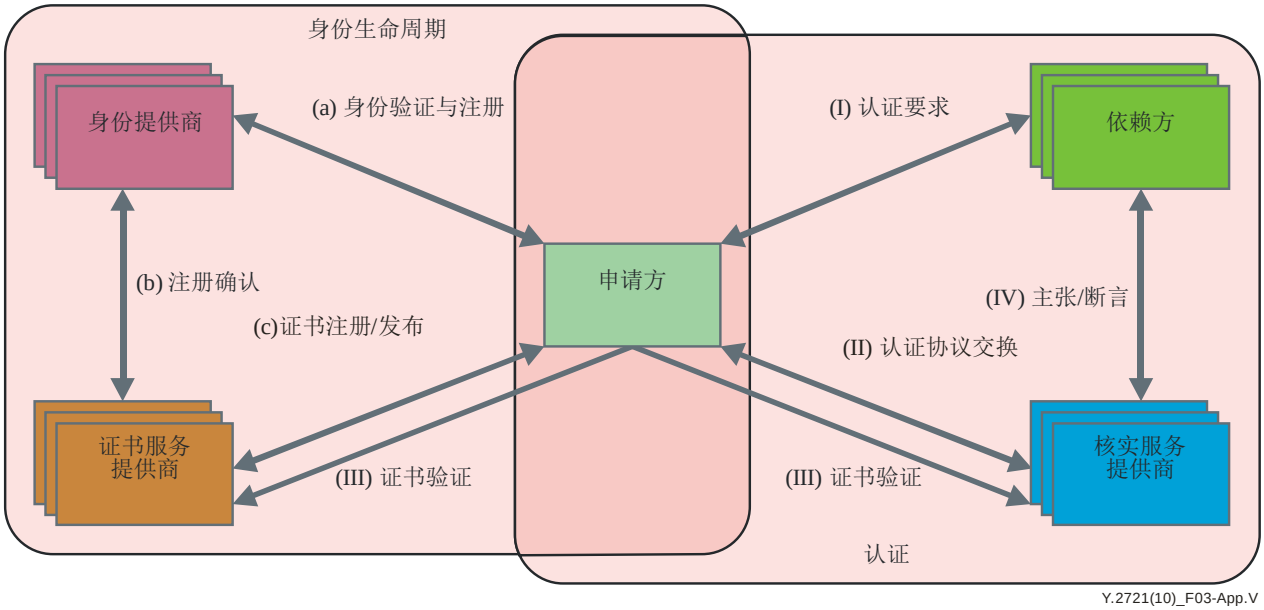


图 V.3 – 以用户为中心的五方身份管理模型示例

“以用户为中心”的模式（即需要申请方实现对其身份使用的全面管理）目前极受关注，并可能在国家和区域管辖范围内颁布施行。图 2b [b-ITU-T X.1250]显示了不同服务提供商提供身份管理专项职能的例子。所有查询/回应都要经转申请方。就此类模型而言，各种实体被定义为：

- 身份服务提供商：一个为其它实体（如最终用户、机构和设备）维护和管理并可能创建可靠身份，同时提供基于身份的服务的实体。这一负责分配和发布属性（即涉及针对具体情境的身份（如证书提供商的用户））– 亦称登记 – 的实体，负责身份的生命周期管理，包括身份的认证、注册和维护，也包括其撤销。

- 证书服务提供商：行使与发布证书和令牌（如将令牌与可核查的标识码和属性相结合的证书）相关职能的实体。
- 认证服务提供商：行使身份信息（如断言和证书）评估职能并确定其有效性级别的实体。
- 依赖方[ITU-T Y.2720]：一个在某种请求的范围内，依赖提出要求/作出断言的实体所作的身份陈述或断言的实体。

附录 VI

在下一代网络中部署IdM的示例

（此附录不构成本建议书的组成部分）

VI.1 引言

本附录提供了在下一代网络中部署 IdM 的示例。

VI.2 IdM结构的部署

NGN 可利用网络服务能力和自由联盟及 OpenID 定义的规范，部署具有支持向用户提供基于身份服务功能的 IdM 基础设施。例如，IdM 具有允许其用户享用不同服务和应用提供商提供的包括联合应用等服务的功能。此外，下一代网络可支持 IdM 向其他应用和服务提供商提供身份服务提供商（IdSP）服务（如用户装置身份和认证的断言、地点和其它关系身份信息）的功能。

支持 IdM 的 IdSP 服务提供能力和/或与根据不同语义、模式、机制和技术采用不同类型 IdM 系统的服务提供商结盟，需要有利于互操作性的适当衔接和互通能力。例如，为了支持其他应用和服务提供商（如网络服务和内容提供商）的 IdM 服务和应用，下一代网络可支持以下功能：

- 与自由联盟框架互通的3GPP GBA；
- 与OpenID互通的3GPP GBA；
- 与OpenID和自由联盟框架互通的其它机制。

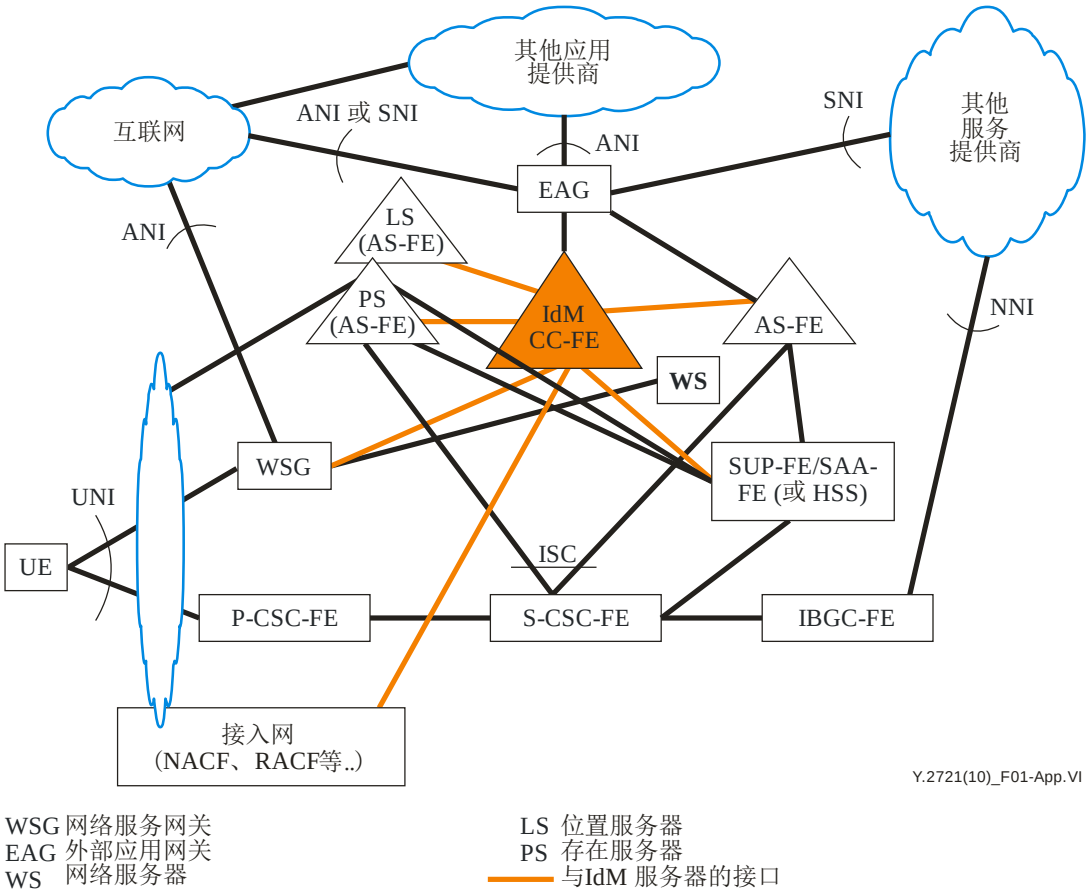


图 VI.1 – 在下一代网络中部署IdM的示例

图 VI.1 列举了在下一代网络中部署 IdM 的示例，说明 IdM 服务器既可以是一个独立的机箱，也可以是一套分布式或内置于 HSS 的功能。IdM 服务器与为 NGN 定义的网元支持功能实体进行对接和互动。例如，IdM 服务器可能连接：

- 支持位置服务器（LS）或存在服务器（PS）等应用程序服务器的服务或其它应用，以提供更高水平的认证保证，并支持基于身份的应用程序服务
- 用于认证保证和政策管理的政策和网络依附和控制服务器。

注 — 对于某些特定国家法规，这可能意味在NGN的不同层面上分别实现 IdM功能。

为了支持订户/用户的某些 IdM 服务和提供 IdM 服务或与其它应用程序和服务提供商合作，下一代网络需要支持控制访问和与其它应用和服务提供商（如网络服务和内容提供商）进行 IdM 交换的具体功能。这一示例显示了利用网络服务网关（WSG）和外部应用程序网关（EAG），支持某些利用或联手其他应用程序和服务提供商 IdM 服务的情况。具体来说，图 VI.1 显示 IdM 服务器通过网络服务网关（WSG）面对用户，对用户进行认证，并向用户提供一个用来管理他/她的身份资料的界面。IdM 服务器还连接外部应用程序网关（EAG），使用户能够访问下一代网络或其它应用程序或服务提供商提供的基于网络的服务。

参考资料

[b-ITU-T X.1141] ITU-T X.1141建议书（2006年），安全断言标记语言（SAML 2.0）。

[b-ITU-T X.1250] ITU-T X.1250建议书（2009年），强化全球身份管理信任和可互操作性的基本功能。

[b-ITU-T X.1251] ITU-T X.1251建议书（2009年），用户的数字身份控制框架。

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

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDSPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), *Identity Management, Overview of Standards and Technologies for Mobile and Fixed Internet*.

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
2012年，日内瓦