国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2720

(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）身份管理框架

ITU-T Y.2720建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T Y.2720建议书

下一代网络（NGN）身份管理框架

摘要

本建议书提供了下一代网络（NGN）中身份管理（IdM）的框架。该框架的主要目的是描述一种设计、定义和实施身份管理解决方案的结构化方法并协助在不同环境中实现互操作。

实体身份信息（如标识符、证书、属性）的管理并不是一个新问题。但是，随着我们步入一个随时随地皆可接入的网络融合环境，在各个地方，业务都基于前后关系、角色，身份信息的保证、安全和管理变得越来越复杂。此外，可能存在着不同的、相互独立的解决方案，因此存在着互操作的必要性。因而，出于以下原因，需要新的、改进的、自动的可互操作能力：

- 最终用户使用多个身份的情况在增加；
- 这些身份可能与不同的前后关系和业务特权相关联；
- 身份也许只能部分表明最终用户的身份；
- 可能在任何地方、任何时间使用这些身份；
- 这些身份在提供商之间可能不能互操作。

身份管理（IdM）即针对这种情况，是用于以下目的的一系列功能和能力（如管理、管理和维护、发现、通信交换、关联和绑定，政策执行、认证和维护等）：

- 保证身份信息（如标识符、证书、属性）；
- 保证实体（如用户/订户、组、用户设备、机构、网络和业务提供商、网络元素和物件、虚拟物）身份；以及
- 实现业务和安全应用。

该框架旨在用于制定和确定IdM特定方面（如详细要求、所需的机制和程序）的基础。它也提供了一个清晰的、前后一致的NGN中IdM的全景总览。

本建议书中提供的框架用于Y.2001建议书（NGN总体概述）中所定义的NGN（即受控的分组网络）。但是，也可酌情适用于其它类型的网络（如企业网）。

注 – 本建议书中使用的有关身份管理（IdM）的术语“身份”不表示本身的含义，尤其不能构成通常对个人身份的认证。

来源

ITU-T Y.2720建议书由ITU-T第13研究组（2009-2012年）于2009年1月23日按照“电信标准化全会”（WTSA）第1号决议程序批准。

前言

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

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

WTSA第1号决议规定了批准建议书须遵循的程序。

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

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

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

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T Y.2720建议书

NGN身份管理框架

1 范围

本建议书为下一代网络（NGN）提供了一个身份管理（IdM）框架。本建议书的主要目的是描述用来组织和指导为NGN提供有组织的解决方案的有关IdM的基本概念、功能构成和能力。本建议书的范围包括：

- 阐述IdM服务的商业动机、好处和优势以及用来提供身份保证的通用特性，同时定义适用于NGN的IdM概念。本建议书以b-ITU-T Y.2012-第1版本NGN的功能要求和架构 – 所规定的NGN功能要求及架构（FRA）为基础；
- 确定并描述支持NGN的IdM服务和能力的功能实体、角色、关系、使能因素及通信；
- 确定并描述NGN中支持IdM服务和能力的（网内）关系；
- 确定并描述NGN服务提供方之间（如，在联邦架构内）和NGN提供方与其它提供方（如联邦架构间）之间在支持IdM服务和能力中的关系。

本建议书提供的框架针对[b-ITU-T Y.2001]“NGN概述”所定义的NGN（即，受到管理的分组网络）。然而，该建议书还可酌情用于其它类型的网络（如，私营公司和企业网络）。

本框架旨在用来作为开发和确定NGN IdM各个具体方面（如详尽要求、必要的机制和程序）的基础。同时，它为NGN中的IdM概念提供了一个清晰而完整的描述。

注 – 本建议书中使用的有关身份管理（IdM）的术语“身份”不表示本身的含义，尤其不能构成通常对个人身份的认证。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，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 Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

3 定义

3.1 其它国际电联建议书定义的术语

本建议书使用了其它文件定义的以下术语：

3.1.1 匿名[b-ITU-T X.1121]：允许匿名获取服务的能力，这种能力可避免对用户位置、服务使用的频率及其它用户个人信息和用户行为的跟踪。

3.1.2 认证[b-ITU-T X.811]：对所宣称的实体身份提供保证。

3.1.3 授权[b-ITU-T X.800]：授予权力，其中包括根据接入权授予的接入。

3.1.4 要求者[b-ITU-T X.811]：要求认证的实体或该实体的代表。要求者包含代表主要实体进行认证交流所必需的功能。

3.1.5 分派[b-ITU-T X.911]：向另一对象分配权利、责任或功能的行动。

3.1.6 标识符[b-ITU-T Y.2091]：标识符是用来识别用户、使用者、网元、功能、提供服务/应用的网络实体或其它实体（如，物理或逻辑对象）的系列数位、字符和符号或其它形式的数据。

3.1.7 下一代网络（NGN）[b-ITU-T Y.2001]：下一代网络是一个能够提供电信业务并能使用多种宽带、可实现服务质量（QoS）的传输技术的分组网络。在此网络中，有关服务的功能独立于底层传输技术。它使用户不受约束地接入网络及竞争服务提供商和/或其所选择的服务。它支持一般性移动，由此可为用户提供连贯一致的及无处不在的服务。

3.1.8 主实体[b-ITU-T X.811]：身份可认证的实体。

3.1.9 安全域[b-ITU-T X.810]：指一套元素、安全政策、安全授权和一组与安全相关的活动，其中有关元素须符合相关活动的安全政策，而安全政策则受到有关安全域中安全机构的管理。

3.1.10 证明者[b-ITU-T X.811]：需要认证身份的实体或实体代表。证明者包括进行认证交流所必需的功能。

3.2 其它非国际电联标准中定义的术语

3.2.1 属性[b-ETSI TS102 042]：规定实体条件、质量等特性的描述性信息或与实体相关的其它信息。

3.3 本建议书定义的术语

本建议书定义了以下术语：

3.3.1 保证：通过身份管理能力的安全功能和架构实现的一定的信心，它执行依赖方和身份提供方达成共识的安全政策。

3.3.2 认证保证：见保证。

3.3.3 保证水平：依赖方和身份提供方之间达成一致的保证程度。

3.3.4 证书：可识别对象，用来认证要求者的身份并对要求者授予接入权利。

3.3.5 发现：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结合。发现的目的是寻找适当的服务资源。

3.3.6 实体：任何可单独识别的独立生存的东西。在IdM范畴内，实体包括用户、使用者、网元、网络、软件应用、服务和设备。一个实体可能具有多个标识符。

3.3.7 联邦：在两个或多个实体间建立一种关系或由多个服务提供方和身份提供方构成的联合体。

3.3.8 联邦身份：用来接入通过政策和联邦条件捆绑一起的一组服务或应用的身份。

3.3.9 身份：有关一实体的信息，通过这些信息足以在特定环境下识别该实体。

3.3.10 身份提供方：创建、维护和管理其它实体（如，使用者/用户、组织和设备）可信赖身份信息的实体，它基于信任、业务和其它类型的关系提供与身份相关的服务。

3.3.11 身份管理：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、相关和捆绑、政策执行、认证和声明）：

- 身份信息（如，标识符、证书、属性）保证；
- 实体身份（如，使用者/用户、组、用户设备、组织、网络和服务提供方、网元和对象及虚拟对象）的保证；
- 实现业务和安全的应用。

3.3.12 模式：由与参与识别或提供识别的实体的行为推出的结构表述，其中可能包括实体信誉。模式可能只与某个实体相关，或与一组实体相关。

3.3.13 个人可识别信息：与任何生活中的个人相关的信息，该信息可使人们识别这样一个个人（包括当与其它信息综合甚至有关信息不能清晰地描述个人时还得以识别个人的信息）。

3.3.14 现状：一套说明一实体现状的属性。

3.3.15 隐私：对个人可识别信息的保护。

3.3.16 依赖方：依赖于身份表述或申请声明实体的实体。

3.3.17 信任：对某个人或某物特性、能力、优势或真实情况一定的依赖。

4 缩写词

本建议书使用了下列缩写字母缩略语：

API 应用程序界面（Application Programming Interface）
BSS 业务支持系统（Business Support System）
CSCF 呼叫会话功能（Call Session Control Function）
FRA 功能要求和架构（Functional Requirements and Architecture）
GBA 一般性自举架构（General Bootstrapping Architecture）
IdM 身份管理（Identity Management）
IdP 身份提供方（Identity Provider）
NGN 下一代网络（Next Generation Network）
OAM&P 操作、管理、维护和提供（Operation, Administration, Maintenance and Provisioning）
OSS 操作支持系统（Operations Support System）
PII 个人可识别信息（Personally Identifiable information）
PSTN 公众交换电话网（Public Switched Telephone Network）
QoE 体验质量（Quality of Experience）
QoS 服务质量（Quality of Service）
RP 依赖方（Relying Party）
SAML 安全声明标记语言（Security Assertion Markup Language）
SBC 会话边界控制器（Session Border Controller）
SIP 会话启动协议（Session Initiation Protocol）
SP 服务提供方（Service Provider）
SS7 7号信令系统（Signaling System No. 7）
URI 统一资源标识符（Uniform Resource Identifier）
VoIP 互联网协议电话（Voice over Internet Protocol）

5 引言

5.1 身份管理IdM概述

实体身份信息（如，标识符、证书和属性）的管理并非新鲜事物。但是，随着向融合网络的发展，身份信息的保证、安全和管理日益复杂，因为在融合的网络环境中，服务以境况和角色为基础并可随时随处获取。此外，由于解决方案各不相同，而且相互独立，因此需要可互操作性。新的增强型、自动并可互操作的能力必不可少。本框架的主要目的是描述在异构环境中用来促进设计、确定和实施可互操作性解决方案的结构方式。

身份管理（IdM）解决的就是这个问题。它是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、相关性和绑定、政策执行、认证和声明）：

- 身份信息的保证；
- 实体身份的保证；
- 实现业务和安全的应用。

图1是有关IdM的概览。

图1 – IdM概览

与实体相关的身份信息可组合如下：

- 标识符（如，用户身份、电子邮件地址、电话号码、URI和IP地址）；
- 证书（如，数字证书、令牌和生物特征）；
- 属性（如，角色、要求、特权、模式和位置）。

IdM功能和能力用来保证身份信息，保证实体的身份并实现业务和安全应用，包括基于身份的服务。

此外，IdM服务和能力还能使使用者/用户实体控制其身份信息的使用和分发。IdM亦可使联邦身份信息获得共享并得到联邦成员（如，商业伙伴）的使用，从而支持联邦服务。

IdM可用来开发不同的应用。应用示例包括但不局限于：

- 商业应用
  - 单点登录和退出（如，无需对各应用或服务平台进行单独认证的情况下接入多项应和服务）
  - 联邦服务（如，通过不同联邦或NGN提供方接入服务）

- 基于身份的服务
  - 标识符、证书和属性服务
  - 桥接服务（在异构环境中对身份信息的映射和连通）
  - 模式信息服务
- 安全应用
  - 网络和应用服务（如，VoIP、IPTV和数据）的接入控制
  - 对信息、资源和资产基于角色的接入控制
  - 授权和特权管理
  - 安全保护服务（如，保护网络基础设施资源和使用者/用户身份信息及资产的安全功能）
  - 个人可识别信息（PII）的保护

在一个多服务提供方和连邦环境中，IdM服务和能力将用来发现并沟通信息，从而在不同网络和安全域内建立对不同网络实体（如，用户/要求者、依赖方（如，使用者、服务提供方和网络提供方）及身份服务提供方（如，证书提供方和核验提供方））中的实体身份建立信任。举例而言，与一身份相关的标识符、证书和属性可通过个别身份提供方（如，认证/证明提供方）进行核验并通过生命与依赖方（如，服务提供方）进行沟通，从而促进接入控制、商业决定及试行政策（如，隐私和个人可识别信息的保护）的执行。

5.2 业务驱动因素和动机

除作为NGN安全的使能因素外，IdM还能实现并促进新的NGN商业应用和服务（如，融合的固定和移动应用及万维网应用）。具体而言，IdM服务、能力和功能支持大量的最终用户/用户、商业企业（如，网络、服务提供方、企业）和公司企业应用及服务（见图2）。

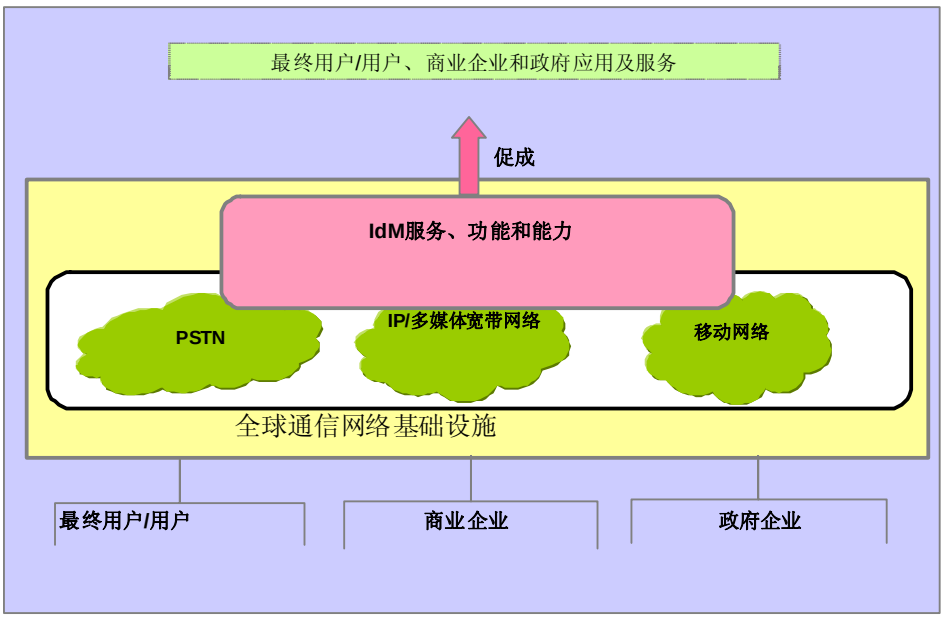

图2 – IdM服务的使用

IdM是管理NGN安全并实现对NGN业务和应用游牧式随需接入的关键组成部分，代表了最终用户对信息时代的期望。与其它防范机制（如，防火墙、入侵检测系统和病毒保护）一起，IdM在保护NGN基础设施和服务及应用免受欺诈和身份盗窃等网络犯罪的威胁中发挥了重要作用。此外，由于使用者确信NGN交易的安全性和可靠性，IdM将促成新的基于身份的服务提供。因此，使用IdM将有力地增强现有的服务和网络能力。IdM的驱动因素和动机概括如表1。

表1 – IdM 驱动因素和动机

方面	IdM驱动因素和动机
最终用户/用户	• 个人信息的用户控制和个人可识别信息的保护 – 提供了控制允许谁能接入的能力（即，同意接入个人信息及如何使用个人信息）。 • 单点登录/退出 – 提供了接入多项应用/服务和进行跨服务提供方/联邦结构接入的统一方法。 • 灵活的网络和应用服务（如，VoIP、IPTV和数据）接入控制。 • 社交网 – 提供安全接入社交网服务的动态和灵活的身份能力。 • 安全 – 建立交易信心，包括防止身份窃取。

表1 – IdM驱动因素和动机

方面	IdM驱动因素和动机
商业企业（如，NGN提供方）	• 实现随时随处和通过任何设备对服务预定的接入。 • 提供身份保证功能和能力，从而支持多项应用和服务。 • 相对于建立服务协议的双方安全，实现多伙伴（如，最终用户、受访和家庭网络）之间动态/自动化连接，交流身份信息并执行政策。 • 实现新的应用和服务（如，固定移动融合），包括基于身份的服务，如向用户和其它服务提供方提供的标识符、证书和属性服务。 • 在多厂商和服务提供平台间实现标准API和应用设计数据模式。 • 实现联邦身份和服务。 • 提供对应用服务、网络基础设施和资源的保护。 • 方便符合规定要求。
政府企业	• 实现身份保证服务和能力并增强对身份的信任和信心水平，从而支持： – 电子政务（eGovernment）服务（如，万维网交易） – 公众安全服务（如，应急911服务） – 执法服务（如，合法侦听） – 应急通信服务 – 早期预警服务 – 国家安全服务 • 实现联邦政府服务 • 提供对通信基础设施的保护（即，防范网络安全威胁）

5.3 身份提供方（IdP）

本建议书未限制由谁提供身份提供方（IdP）服务。

IdP是一实体，它负责创建、维护并管理其它实体（如，使用者/用户、组织和设备）的可信赖身份信息，同时提供基于信任、业务和其它类型关系的身份服务。

在多服务提供方的环境中，NGN提供方可能是一个身份提供方。NGN提供方还可以提供IdP服务（如，身份服务）给其它提供方。此外，可以使用第三方IdP服务。

5.4 NGN功能架构和标识符的使用

如[b-ITU-T Y.2012]-“第1版本NGN的功能要求和架构”所述，NGN包含多项使用实体标识符履行功能的功能元素，以便支持并促进服务和应用。图3显示出映射至NGN功能框架内的身份，即，[b-ITU-T Y.2012]所示的NGN架构。

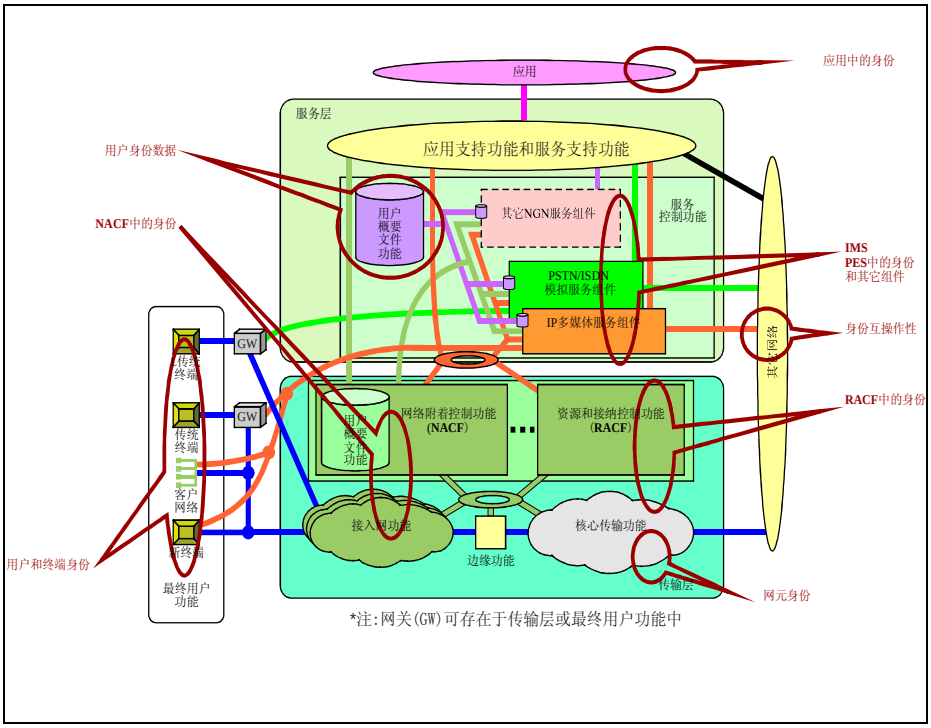

图3 – NGN身份示例

由于所有NGN操作使用上述不同身份，保持这些身份的完整性非常重要。IdM提供保证服务能力及功能，以维护NGN身份完整性和使用。

NGN网络环境中，一个单一实体内可能存在多个身份属性。这些身份属性可能由不同网元使用（如，在不同NGN提供方域中或NGN不同层（即，服务层或传输层）中）及不同位置内不同实体使用。因此，IdM有必要提供可以保证实体之间（和/或与位置之间），如依赖方（如，应用、服务或其提供方）和身份提供方（IdP）之间的安全信息交流。请注意，NGN提供方也可以是一个IdP。IdM信息的交流以规定的政策和多服务提供方环境中上述实体之间达成的信任为基础。这种信任基于对分布式NGN中各实体身份的声明和验证。IdM还提供保护实体信息（如，具体身份属性）隐私的能力，同时确保在NGN中仅传播授权信息。

6 IdM框架概述

框架的组织见图4。

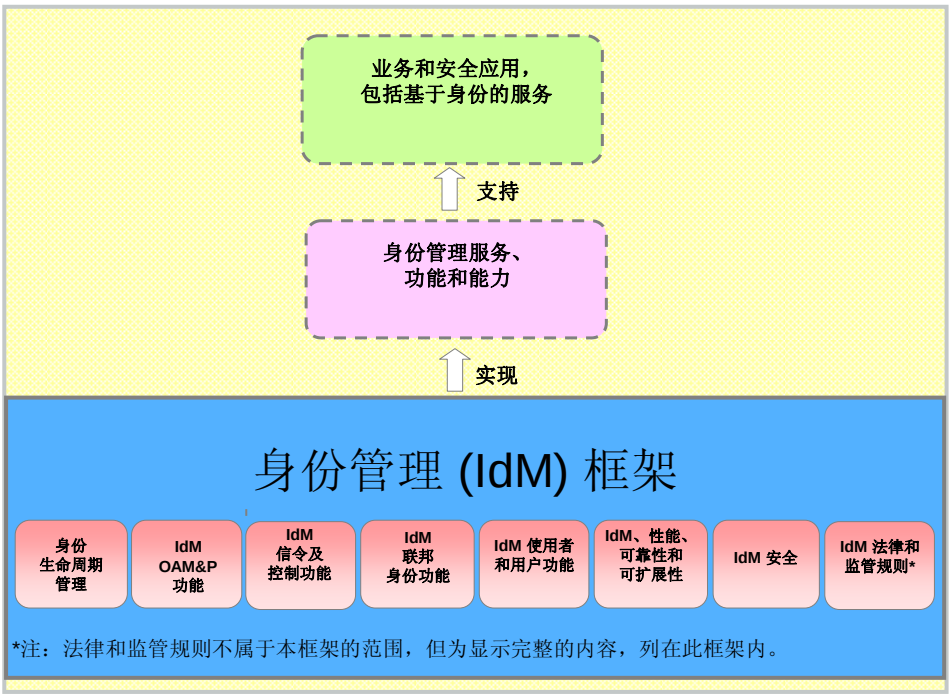

图4 – IdM框架概览

该框架包含以下IdM功能和能力：

1) 身份生命周期管理：

这包括有关身份和身份信息（如，标识符、证书和属性）的生命周期管理程序和功能。身份生命周期管理涉及与登记和颁布身份、或数据和与一实体身份相关的信息相关的程序和过程。

2) 身份管理（IdM）操作、管理、维护和提供（OAM&P）功能：

这包括为支持IdM而进行的操作、管理、维护和提供（OAM&P）管理功能及能力。OAM&P是一组管理功能，提供系统或网络故障指示、性能监测、安全管理、诊断功能、配置和用户调配。具体而言，它包含网络管理系统，特别是被称为OSS（操作支持系统）和BSS（业务支持系统）的管理系统所支持的功能和能力。

3) 身份管理（IdM）信令和控制功能：

这包括用来支持IdM服务、能力和功能的信令和控制功能及能力。它涉及实时和接近实时的通信信令和控制。

4) 身份管理（IdM）联邦身份功能：

这包括身份联邦和支持联邦服务的功能和能力。

5) 身份管理（IdM）使用者和用户功能：

这包括与最终用户和用户对其身份信息（如PII、个人喜好和位置）进行控制的功能和程序。它涉及控制、分配和授权使用及传播身份信息的功能。

6) 身份管理（IdM）的性能、可靠性和可扩展性：

这包括涉及IdM系统和解决方案的性能、可靠性和可扩展性的功能和程序。

7) 身份管理（IdM）安全：

这包括涉及IdM系统、服务和能力的安全保护的功能和程序。

8) 身份管理（IdM）的法律和监管规则：

法律和监管规则不属于本建议书的范围。

注 – 为完整起见，在此使用了该术语。

对各项内容的详细说明见第8节。

7 NGN架构和参考模型中的IdM

7.1 与NGN架构和服务的总体关系

图5介绍了在更广泛的NGN网络环境内，IdM框架的关系。

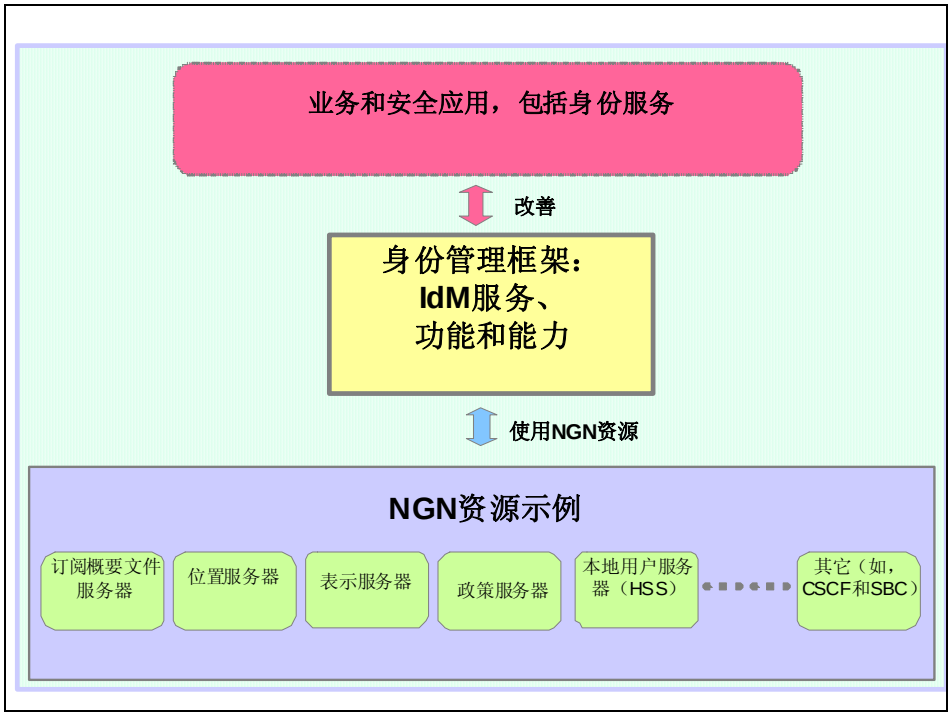

图5 – 与NGN架构和服务的关系

如框图所示，该框架使用NGN网络资源（如，订阅信息、位置、政策、现状和本地用户服务器及其它诸如呼叫会话控制功能（CSCF）和会话边界控制器（SBC）等网元）。该框架提供的IdM服务、功能和能力用来支持并加强业务和安全应用，包括身份服务。

7.2 ITU-T Y.2011建议书（NGN的一般性原则和通用参考模型）参考模型

本节阐述了在[ITU-T Y.2011]-“下一代网络的一般性原则和通用参考模式”中定义的NGN架构模型和参考中的IdM服务、功能和能力。

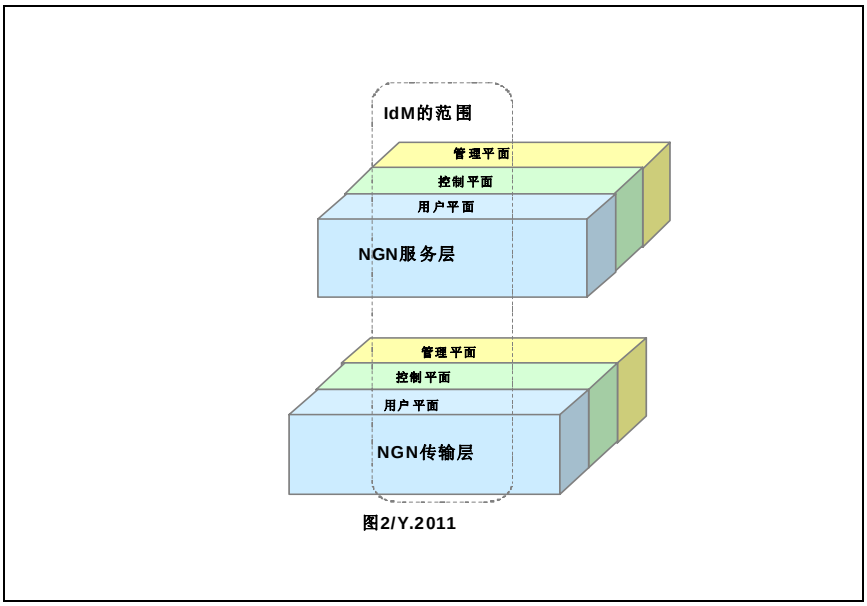

图6 – [ITU-T Y.2011]图2环境下IdM的范围

图6显示了[ITU-T Y.2011]图2所定义的NGN参考架构模型环境下的IdM范围。该图表明，IdM功能可能存在于用户、控制和管理层面。

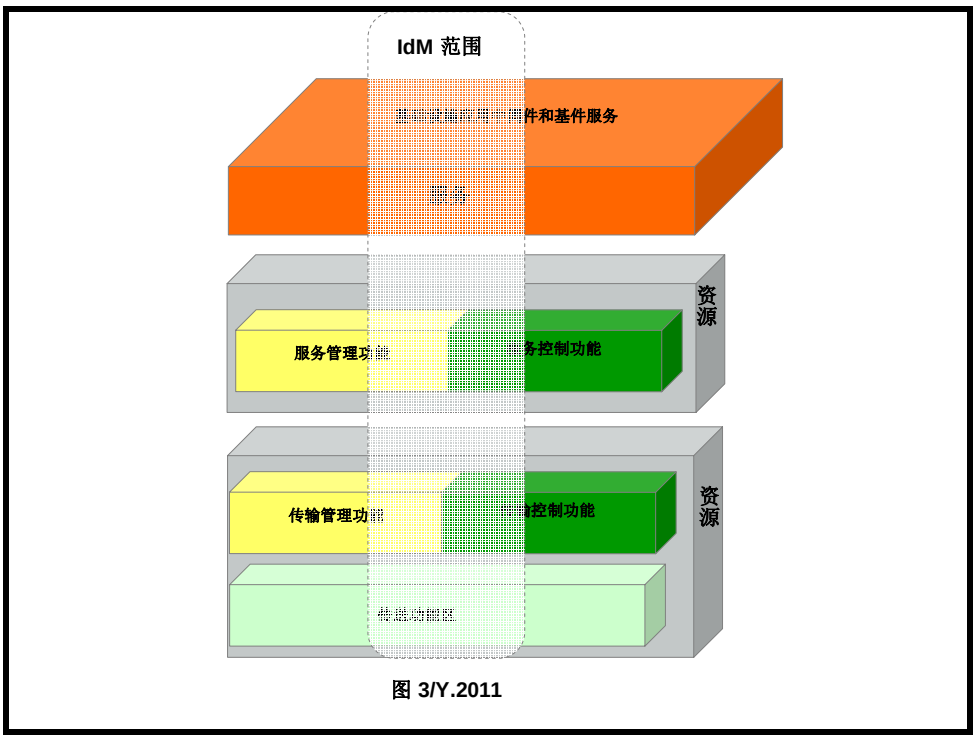

图7 – [ITU-T Y.2011]图3环境下的IdM

图7显示了[ITU-T Y.2011]图3定义的NGN参考架构模型环境下IdM的范围。该图表明，IdM功能可能包含在NGN架构所有纵向层面中。

8 身份管理框架

本节详细阐述了第6节所述功能组。

8.1 身份生命周期管理

8.1.1 验证和登记

创建实体（如，用户、设备、组织、NGN提供方或对象）身份的第一步是身份或证书的验证和登记过程。这一过程旨在按照特定场景（如，角色）注册与某一实体相关的身份或证书。

对于最终用户而言，这一过程是指申请者申请成为IdP或NGN提供方的用户。

对于最终用户，用户名可能是一个经验证的名称。验证的名称与一实体身份相关。在申请者收到证书或与验证名相关的登记令牌之前，须显示该身份是一个真实的身份，而且该实体有权使用上述身份。这个过程称之为身份验证。当名称得到验证后，可以与假名相关联，从而进行匿名操作。

验证包括认证与身份相关的属性和要求。当将实体登入身份系统时，需要认证和证实信息的过程和程序。

IdM的总体有效性首先取决于验证和登记过程，同时，还需要完善的保证要求以及适当的政策和管理程序，确保总体登记程序得到适当设计和实施。

需考虑的导则包括：

- 登记过程中人员的培训
- 文件及其它支持实体登记的证据质量
- 避免在登记中出现欺骗的程序
- 避免对同一实体进行多重或重复登记的程序。

8.1.2 颁发和吊销

成功完成登记程序后将授予证书，使有关实体得以在未来得到认证。举例而言，IdP（或NGN提供方）颁发的证书将与身份或实体身份相关属性（如，特权或要求）相互捆绑。

身份吊销是取消身份及相关证书的过程。颁发身份或证书的一方或系统（如，IdP或NGN提供方）负责维护并保护与身份相关的信息。吊销手段是为防止身份或证书在无效的情况下继续使用或出现违背安全原则的问题。

需考虑的导则包括：

- 为颁发和吊销确定标准；
- 确定更新和修改标准；
- 同步身份信息；
- 建立颁发和吊销的流程和程序；
- 审计并审议颁发和吊销流程；
- 通知颁发、更新和吊销身份或证书的程序和流程（即，所有建立身份使用的系统和过程必须能够确定有关身份已吊销的情况）；
- 制定完善的颁布和吊销身份或证书的流程和程序及适当的政策。同时，还需要管理程序以确保整个过程得到适当设计和实施。
- 保护吊销流程和程序免受安全威胁的机制。

8.2 身份管理OAM&P功能

8.2.1 数据模型和方案

每个NGN提供方、联邦或企业均可拥有自己的格式、方案、定义或语句用来表示或分享与身份相关的数据和信息。例如，有关生日的同样信息可能在两个系统（如，月/日/年或日/月/年）中的表示不同。另外，申请或交流有关身份的信息使用的语句、格式和协议也有可能不同，导致可互操作性问题，例如，公众交换电话网（PSTN）中的身份信息，如呼叫方号码和主叫身份是使用具体的语句来表示的，并使用具体的协议（如，7号信令）进行检索，在基于SIP的VoIP系统中，它们各不相同。

为解决使用不同数据模式的异质IdM系统之间的可互操作性问题，结构和模式至关重要。

需考虑的导则包括：

- 促进一个NGN提供方域内异质IdM系统（如，身份数据来源）之间互操作性的数据模型和方案（即，不同提供方产品）。
- 促进不同NGN提供方（网络间）之间互操作性的数据模型和方案。
- 促进不同联邦（如NGN提供方和万维网服务提供方）之间互操作性的数据模型和模式。

8.2.2 标识符管理

实体（如，使用者/用户、组织、联邦、企业、服务提供方、设备和对象）的身份可能具有一个或多个需要管理和维护的、与身份相关的标识符。

标识符是一个用来表示实体身份（如，用户身份、网络身份、电子邮件地址、假名、小组名称等）的表示法。举例而言，以下标识符可与一个使用者/用户身份相关：

- 用户身份
- 电子邮件地址
- 电话号码
- URI
- IP地址。

IdM的总体有效性取决于每个标识符的有效性，而这些标识符与实体身份相关并对此提供保证。因此，需要认真制定管理标识符的要求和程序。

IdM设计和实施需考虑的导则包括：

- 应管理好具有不同特性的不同类型的标识符，例如，一些标识符可能具有共性（即，跨联邦的独特性），对于某一系统有意义的假名或只在短期内有效的一次性标识符。
- 标识符的不同特性可能具有隐私含义，应防范不适当的用户行为。

8.2.3 属性管理

身份属性是对实体的类型、经常使用的IP地址、域、地址信息、电话号码的描述。属性中可能还包含要求、权利、特权、分配清单和特殊限制。其它类型的属性包括入侵检测需跟踪的信息，如失败的身份声明，重新按键次数等。

IdM的有效性取决于对属性的保证。属性应与实体身份相关并对此进行保证。这包括属性的存储和提供。因此，需制定适当的要求和程序以便管理属性。

模式是一种特殊类型的属性，它是与实体行为相关的特性。模式信息可由IdM系统根据声誉及以往的交流情况加以分配，而不是由实体本身确定的。模式信息可用来评估身份保证程度，包括IP地址、接入点、位置信息、使用时间和所接入的系统。智能化功能可能还将目前的事件考虑在内，以便对未来的使用模式进行预测。

属性管理需考虑的导则包括：

- 可将模型信息视为PII；
- 管理模型信息的严格要求和程序；
- 为减少身份盗取而使用模型信息；
- 符合PII政策。

8.2.4 证书管理

证书用来认证提出要求的实体。证书包括：

- 用户名/密码；
- 数字证书；
- 令牌和智能卡；
- 安全提示；
- 与PKI相关的信息，如密钥、证书、签署证书授权、加密信息等；
- 生物特征。

身份证书管理包括创建、颁发和管理用来认证身份要求信息的所有操作活动。IdM的有效性取决于证书管理过程、程序和能力。因此，需制定适当的证书管理要求和程序。

证书管理需考虑的导则包括：

- 确定并维护证书政策；
- 证书生命周期管理过程和程序（第8.1节所述IdM生命周期的子集）；
- 在多服务/网络提供方环境中的政策和服务协议（谈判证书政策、符合联邦要求、出版证书信息，如公共密钥）。

8.2.5 登录和审计

登录和审计功能及能力对于有效实施IdM解决方案而言至关重要。审计和合规措施包括维护安全日志以满足问责制要求，保护并适当使用个人信息并向适当系统或实体提供通知（如，身份所有者）。

登录和审计需考虑的导则包括：

- IdM相关事件（如，访问身份信息、非授权访问尝试、更新时间标记等）的登录和审计以便用于取证分析；
- 实现反向追踪的机制和程序；
- 检查对现行政策不合规的情况；
- 确保符合国家规定要求。

8.3 身份管理信令和控制功能

8.3.1 引言

信令和控制功能用来发现并沟通与实体（如，使用者/用户、组、组织、网元、服务提供方）相关的可信赖身份信息（如，标识符、属性、要求），从而支持IdM服务、功能和能力。

本节阐述了与IdM相关的信令和控制功能。

8.3.2 身份信息的发现

在NGN这种分布式环境中，身份信息可能存在于不同网元（如，订购服务器、位置服务器、表示服务器、本地订购服务器等）中。发现身份信息来源的结构方式是IdM不可分割的一部分。对于使用身份信息的应用，它需了解身份信息是否存在。在一个动态和不断发展的NGN环境中，身份信息及身份信息来源也在不断变换。因此，依赖方和实体（如，应用）需要采用结构式手段了解身份信息的存在并予以发现。这还包括发现IdM功能服务及能力。

规定和实施发现能力需考虑的导则包括：

- 在NGN提供方域（网络内）内发现；
- 在不同NGN提供方域（网络间）内发现；
- 在不同联邦成员之间发现。见第8.4.2节-联邦发现。

发现还包括寻找或定位身份提供方（IdP）的能力。在NGN IdM框架中发现是必不可少的能力，因为有很多IdP。在只有一个IdP（如，企业）的情况下，没有必要进行发现操作，因为可以知道从哪里获得身份属性。此外，在一个单一的NGN提供方网络中，可能有多个提供不同身份管理功能的系统及适当的发现功能。

发现功能类似于在万维网中对身份的搜索。在搜索引擎中的输入就是身份特性，而输出则是一个标识符列表以及与要求相匹配的IdP。这种查询和响应情形通常需要IdP将自身注册为某种用户/设备身份服务的提供方。

现有支持发现和接入相关需求的方法分为两个类型：1)重叠寻根方式和/或2)推理发现。前者依赖于使用支持服务器担当名称空间总注册处角色的某些实体，而后一种方法依赖于众所皆知的规则，通过该规则可反向获得支持服务器的地址。同时还可以使用混合方法。

8.3.3 IdM通信

IdM通信包括发现和交流在NGN提供方网络内位于不同网络系统（如，订购服务器、位置服务器、表示服务器等）中一实体身份相关信息（如，标识符、证书和属性）的能力和功能。通过相关和验证（即，使用IdM应用服务器提供认证和相关功能）提供身份保证能力。身份和相关属性（如，要求和特权）可传达给依赖系统（如，应用服务）声明以便获得控制决定。这将使不同的应用服务（即，不同厂商平台的）利用通用IdM基础设施，而不是使用独立的，即自主的解决方案。通信关系需考虑的问题包括：

- 网络内：与NGN提供方域的通信（如，网元之间）；
- 网络间：两个不同NGN提供方之间的通信；
- 联邦：联邦成员之间的通信。

8.3.3.1 实时和接近实时的通信

用来发现和交流身份信息的解决方案需考虑到是否需要实时或接近实时的通信。这将取决于获得支持的具体的应用。

8.3.3.2 信令和控制协议及界面

图8显示了适用于支持IdM通信的外部界面，例如，用来交流身份信息或控制IdM服务功能和能力的界面。

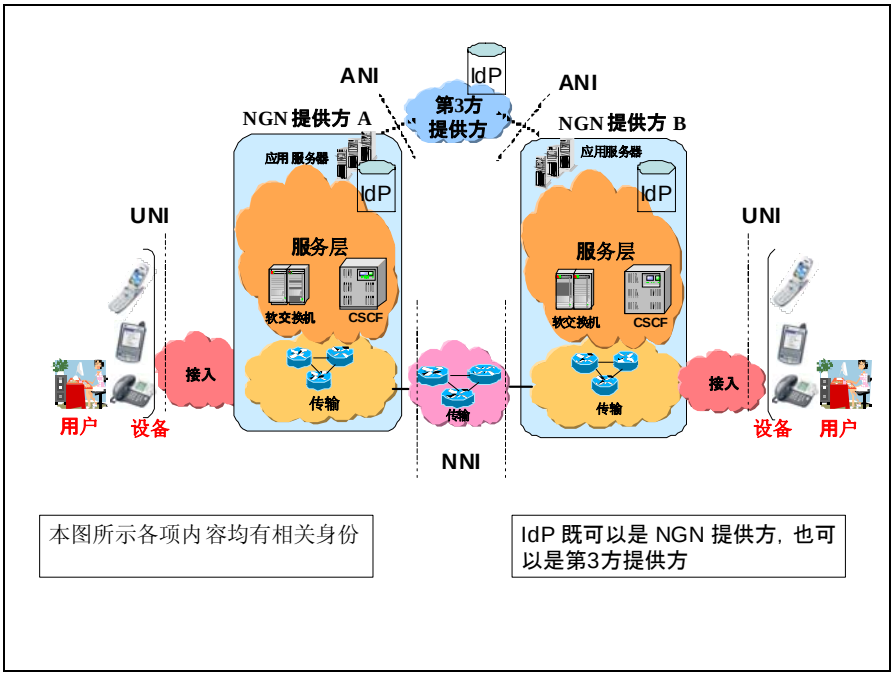

图 8 – 外部界面

外部界面包括：

- 用户与网络界面（UNI）
- 应用与网络界面（ANI）
- 网络与网络界面（NNI）。

所使用的具体要求和协议取决于具体的界面、沟通的信息或所采用的控制功能。具体的要求和协议选项及概要文件应加以确定和规定以便于实现互操作性。界面解决方案取决于具体应用和服务需求（如实时或接近实时）、协议解决方案（如，SAML、Diameter、RADIUS）及机制和手段（如，[b-ITU-T X.509]、通用及一般性自展架构（GBA））等因素。

除外部界面外，内部界面对于总体解决问题亦非常重要。在NGN网络中，身份信息可置于不同网元和应用服务（如，订购、位置和表示服务器及其它网元，如CSCF和SBC）中。用来发现和交流身份信息的内部界面和协议是多厂商，互操作性需考虑的重要方面。

8.3.3.3 机制和程序

用来实施具体IdM功能或能力的机制和程序应得到确定和规定。应确定和规定具体的机制或协议以及如何使用这些机制和协议。机制和协议示例包括：

- SAML
- X.509
- GBA
- E.115

8.3.4 相关和捆绑

通过相关身份信息（如，标识符、证书和属性）可建立捆绑关系，以保证实体的身份。与用户相关的身份信息（如，用户ID）、用户设备（如，设备ID）和位置信息可通过建立相关关系形成捆绑，从而为用户提供更高的保证。

在规定和实施相关和捆绑中需考虑的导则包括：

- 执行现行政策（如，匿名或隐私政策）。

8.3.5 认证

认证是对实体身份建立信心的过程。实现认证保证的一种手段是描述量化实体本身或其所宣称内容的风险所必须的目标和导则。这包括确定哪些标识符在确认过程中更加重要，以及为什么一些认证使用的标识符不应具备同样的认证价值。

传统上实现信任的方法是通过为每个系统颁布用户身份和密码对。但是，在NGN 中，这种方法不适用，操作起来无效，而且还能导致不安全隐患。在确定和实施认证中需考虑以下导则：

- 保密性和认证机制的完整性
- 各系统足以信任的证书。

8.3.6 认证保证

认证保证是对提供给信息系统的身份和要求建立信心的过程。并非所有认证使用的信息均应得到同等对待或具有相同的保证价值。例如，对使用生物特征进行认证的信息不同于使用用户身份/密码进行的认证。因为每个标识符分配基于基本原则的相关价值，从而使人们量化认证有效实体的信心。

认证保证的目的是量化实体本身或其所宣称内容可能的风险。并非所有在认证决策过程中使用的标识符均应得到同等对待或具有同样的认证价值。此外，随着认证错误所致后果的严重，认证保证所必要的程度应根据认证错误的风险含义（如，重要影响）而提高。

量化和沟通和认证保证的机制将使依赖方就认证过程的信心做出决定，从而认证身份或身份要求。

认证保证的主要好处包括有能力决定对一实体在其整个生命周期内的信心程度。指定和沟通相关认证过程保证值的标准、机制和跨联邦数据（如，密码、证书、生物特征）对于支持联邦服务和网络安全保护起到非常关键的作用。

认证保证流程应考虑到以下各方面：

- 认证机制：静态密码不如一次性密码，带有密码的硬件令牌一般来说比软件令牌更好。
- 认证协议：防止攻击的协议或基于加密操作的协议一般而言更加有力。
- 用来认证的设备特性：信任部分来源于用户和使用设备的特性，即由相关组织或专用防篡改设备拥有和控制的商用现成计算机比大众可获取的商用现成设备更好。
- 得到认证的实体位置：用户位置应得到考虑，如，在一组织区域或公共服务台或网吧内等。如信息亭内公众终端难以说服使服务器相信其处于某组织的物理边界内，可提高认证信心。
- 通信路径：认证一般涉及所认证实体和提供认证和/或接入决定的服务器之间的通信路径（无线网络、商用租用线路等）。用于认证的信息应可靠地传递给认证服务器并不受攻击者网络钓鱼的影响。
- 恶意行为启动认证操作的相对简便性：重要的是要评估与加密与密钥相关的风险。

8.3.7 分派

分派涉及将特权转移，以便代表主实体采取某些行动和过程。该实体拥有另一实体所不具备的特权。

举例而言，分派授权始于决定哪些帐户可以进行某些管理行动（如创建新的帐户）或管理具体功能（如变更帐户密码）等的能力。因此，当具有分派行动或进行管理的能力时，目的是提供一个使任务得以安全和负责任地完成的环境。

8.3.8 政策执行

IdM解决方案的设计和实施应考虑到适行政策的执行。政策执行通常关系到：

- 匿名和隐私；
- 身份信息的创建和收集；
- 身份信息的使用和散发。

8.3.9 支持需要优先处理的服务

IdM 解决方案的设计和实施应考虑到对应用服务和需要优先处理的诸如应急通信服务(ETS)等应用服务和通信会话的支持。任何与 IdM 系统旨在建立和保持 ETS 通信会话的交流都应得到优先处理。有关需要优先处理的服务和能力信息请查阅[b-ITU-T E.107]和[b-ITU-T Y.2205]。

8.4 身份管理联邦身份功能

8.4.1 联邦身份

联邦的总体概念是使各联邦成员保持独立的同时促进对某些身份信息的共享，从而实现联邦服务。一些用户/使用者（如，用户概要文件的子集）的身份信息可以得到联邦处理（即，提供给联邦成员）。

8.4.2 联邦发现

联邦发现包括发现和交流联邦身份信息的功能和机制。一些有关使用者/用户的身份信息可进行联邦处理，做为用户概要文件信息的子集。

联邦发现的主要内容是确定并发现与某一实体相关的某些身份信息的权威来源，即，备选IdP（如，位置信息）。

在任何拥有多个IdP的架构中或IdP位置可能处于动态的情况，发现都是必要的。如只存在一个身份提供方（如，企业），没有必要进行发现操作，因此，任何RP/SP都会知道在哪里获取有关实体的身份信息。

8.4.3 桥接和互通

一般情况下，各NGN提供方、企业或联邦成员均有自己的格式、模式、定义或语句用来表示或分享身份数据和信息。如生日这种同样的信息可能在两个系统中有不同的表示。同时，用来要求和交流身份信息的语句、模式和机制也各不相同，由此导致可互操作性问题。因此，适当允许不同联邦之间桥接和互通的能力应必不可少。

8.5 身份管理使用者和用户功能

允许最终用户/用户提供有关控制其身份信息的功能对于有效的IdM解决方案而言是必不可少的。这包括使最终用户/用户得以向服务提供方和IdPs提供有关其身份信息的条件、限制、许可、创建授权、收集、使用和分发信息的功能和能力。

这些功能涉及现行政策的执行，如有关 PII保护、匿名或假名身份信息政策。

需考虑的导则包括：

- 最终用户/用户向NGN提供方传达有关控制其身份的信息的手段；
- 符合现行PII保护的政策；
- 方便最终用户/用户的使用。

8.6 性能和可靠性

8.6.1 性能

IdM能力和功能将用来支持和加强广泛的业务和安全应用。IdM功能可用来在允许通信会话（如，VoIP、IPTV或数据会话）之前进行通信实体身份的保证。因此，在更高层应用服务（如，VoIP、IPTV、数据）上的IdM 性能对于该解决方案至关重要。IdM不应对受到支持的更高层应用服务造成不良影响，由此影响最终用户/用户的总体服务质量（QoS）和体验质量（QoE）。

性能管理是IdM 解决方案设计中的重要考虑因素。性能管理包括为性能监测收集并分析统计数据。性能监测是对网络系统通过连续收集并分析适当性能数据完成其指定功能的系统评定。性能监测程序旨在捕捉因网络设备逐步退化而造成的瞬间错误和故障。性能监测等积极的维护技术可在问题严重之前实现早期发现。

8.6.2 时间标记准确性

时间标记是IdM的一个因素。审计阐述了在各时间框架内发生的事件。在审计中，时间标记是必不可少的。审计数据的质量及其可用性也是由时间标记的精确性决定的。

时间标记的精确性决定于三个因素 – 本地时间标记时钟的读取精度、本地时钟对参考时钟的可追踪性和本地时钟相对于参考标准的数字不确定性。

8.6.3 可靠性和可用性

提供IdM功能和能力的网源和系统的可靠性及弹性是设计和实施解决方案的重要内容，因为，IdM将用来支持并加强可应性要求各不相同的大量业务和安全应用。因此，包括以下在内的可靠性因素的要求和导则需得到考虑：

- 系统稳健性和弹性设计（如，冗余）；
- 有关可用性的多样性（如，地理多样性）。

此外，IdM 解决方案的设计和实施还应考虑到防障措施。可依赖的应用可引起某些限制性特权的使用，如整个 IdM 系统出现故障或不可用。

8.7 IdM安全

8.7.1 提供IdM的网元的安全保护

由于身份信息和资源非常宝贵、敏感且用于支持商业应用和服务，提供IdM 服务的网元、功能和能力将成为安全攻击的目标，因此需要安全保护。

保护提供IdM 功能服务和能力的网元和系统的适当要求和措施必不可少。安全考虑包括：

- 对IdM服务、功能和能力的安全保护；
- 对信令和通信界面的安全保护；
- 对IdM 系统管理界面的安全保护（即，用来配置身份信息的界面）。

8.7.2 个人可识别信息（PII）的保护

保护PII是IdM非常重要的内容。保护PII的具体能力应得到确定和实施。这涉及到有关按照国家和区域性规定保护PII的适行政策的实施。需考虑的功能和能力包括：

- 使用者/用户交流有关PII喜好的能力；
- 提供透明度的能力（即，确保只有授权实体能够获取或观察PII的能力）；
- 提供有关散发和使用身份信息通知的能力。

参考资料

[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 E.115] Recommendation ITU-T E.115 (2008), *Computerized directory assistance.*

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

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 1081-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

[b-ITU-T X.911] Recommendation ITU-T X.911 (2005) | ISO/IEC 15414:2006, *Information technology – Open distributed processing – Reference model – Enterprise language*.

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

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

[b-ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN.*

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

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2008), *Next Generation Networks – Emergency telecommunications – Technical considerations.*

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

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[b-ETSI EG 202 072] ETSI EG 202 072, V1.1.1 (2002), *Universal Communications identifier (UCI); Placing UCI in context; Review and analysis of existing identification schemes*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=14108>

[b-ETSI EG 202 236] ETSI EG 202 236, V1.1.1 (2003), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Design guide; Use of non-numeric names*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17732>

[b-ETSI EG 284 004] ETSI EG 284 004, V1.1.2 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21139>

[b-ETSI TS 102 042] ETSI TS 102 042, V1.3.4 (2007), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27736>

[b-RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*.
<http://www.ietf.org/rfc/rfc3650.txt?number=3650>

[b-NIST] NIST SP800-63, v6.3.3, *Electronic Authentication Guidelines.*
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OGIM] The Open Group, *Identity Management White Paper* (03/2004).
<http://www.opengroup.org/bookstore/catalog/w041.htm>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	**全球信息基础设施、互联网协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2009年，日内瓦