

国 际 电 信 联 盟

**ITU-T**

国际电信联盟  
电信标准化部门

**X.1252**

(04/2010)

X系列：数据网、开放系统通信和安全性  
网络空间安全 – 身份管理

---

## 身份管理基准术语定义

ITU-T X.1252建议书

ITU-T



ITU-T X 系列建议书  
数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
<b>身份管理</b>	<b>X.1250–X.1279</b>
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T 建议书目录。

## 身份管理基准术语和定义

### 摘要

ITU-T X.1252建议书提供了用于身份管理（IdM）的关键术语定义。这些术语来源广泛，但均被认为通用于IdM领域。本建议书并不是要成为与IdM相关术语的一个大纲要。相反，本建议书中规定的术语仅限于那些被认为是最重要最常用的与IdM相关的基准术语。本建议书包含的附件A解释了某些关键术语的理论基础。

本建议书的主要目的是为了促成各有关IdM标准制定小组（正在或计划制定）之间就这些术语达成共识。制定这些定义时，尽可能使它们与实施或具体的环境无关，这样就适合作为任何IdM领域的基准定义。应当承认，在某些情况和环境下，某个特殊术语可能会要求更详细的细节，这样的话可以考虑详细描述基准定义。

### 沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1252	2010-04-16	17

## 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/>。

© 国际电联 2010

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

## 目录

	页码
1 范围 .....	1
2 参考文献 .....	1
3 定义 .....	1
4 缩写词和首字母缩略语 .....	2
5 惯例 .....	2
6 术语和定义 .....	2
附件 A – IdM基本术语的主要问题和理论基础.....	7
A.1 认证和信任 .....	7
A.2 声称/主张 .....	12
A.3 吸纳和注册 .....	12
A.4 身份提供方和身份服务提供方 .....	12
A.5 身份模式 .....	13
参考资料.....	14

## 引言

IdM术语和定义表的汇编工作始于2007年。该清单已经过反复调整，收到很多文稿和意见并已经过多次复审。这些术语和定义来自四面八方，其中一些（并非全部）列在参考资料中。在一些情况下，原有定义恰如其分，因此纳入其中，但在很多情况下，这些定义经过修改或与其他定义综合形成了“最好的”的术语。

为确保这些术语与其他IdM建议书 | 国际标准中的术语保持同一含义，我们付出了艰辛的努力。这意味着，在一些情况下，用词虽然有所不同，但含义应完全相同。

由于一个术语可用于多个不同场景，而定义只局限于该术语的基本含义或简单描述，不包含其他内容或可能发生的变异。如需要进一步详情或澄清，可按要求予以补充。

形成定义的基本要素详见附件A。

## 身份管理基准术语和定义

### 1 范围

本建议书包含身份管理（IdM）普遍使用的一套术语和定义。有关定义是对相关术语的基本描述，即旨在表述基本含义，不包含细节或举例。但例外情况是，为澄清有关定义使用了一些示例。附件A包含了某些关键术语/定义的理论基础。

注 – 本建议书中使用的与IdM相关的术语“身份”不表明它的绝对含义，尤其不构成对人做出的任何肯定验证。

### 2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

- [ITU-T X.501] ITU-T X.501建议书（2005年）| ISO/IEC 9594-2:2005，《信息技术 – 开放系统互连 – 号码簿：模型》。
- [ITU-T X.800] ITU-T X.800建议书（1991年），《CCITT应用的开放系统互连的安全体系结构》。
- [ITU-T X.810] ITU-T X.810建议书（1995年）| 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》。
- [ITU-T X.811] ITU-T X.811建议书（1995年）| 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 Y.2701] ITU-T Y.2701建议书（2007年），《下一代网络（NGN）第1阶段的安全要求》。
- [ITU-T Y.2702] ITU-T Y.2702建议书（2008年），《下一代网络（NGN）第1阶段的认证和授权要求》。
- [ITU-T Y.2720] ITU-T Y.2720建议书（2009年），《下一代网络（NGN）的身份管理框架》。

### 3 定义

该段有意保留空白。

## 4 缩写词和首字母缩略语

本建议书采用下列缩写词和首字母缩略语：

IdM	身份管理
IdP	身份提供方
IdSP	身份服务提供方
NGN	下一代网络
PII	个人可识别信息
RP	依赖方

## 5 惯例

本段有意保留空白。

## 6 术语和定义

**6.1 接入控制：**用来确定一实体是否应按照预先确定的规则和请求方的具体权利或相关授权被授予获得资源、设施、服务或信息的程序。

**6.2 地址 [ITU-T Y.2091]：**地址是用于特定终接点的识别码（用于路由至该终接点）。

**6.3 代理：**代表另一实体行事的实体。

**6.4 联盟：**两个或多个独立实体之间达成的协议，确定其相互关系及如何共同开展活动。

**6.5 匿名：**一实体无法在一组实体中被识别的性质。

注 – 匿名性防止对实体或其行为（如用户位置、使用服务频率等）的跟踪。

**6.6 主张：**（一实体）在没有有效性凭证<sup>1</sup>的情况下做出的声明。

**6.7 保证：**见认证保证和身份保证。

**6.8 保证水平：**表明对实体和所介绍的身份信息之间关联性的置信程度的量化表示。

**6.9 属性：**针对一实体并说明该实体特性的信息。

**6.10 属性类型 [ITU-T X.501]：**属性的组成部分，说明由属性确定的信息类型。

**6.11 属性值 [ITU-T X.501]：**由属性类型说明的某一类信息情况。

**6.12 （实体）认证：**对实体与所介绍身份之间关联性实现充足信任的过程。

注 – 在IdM语境内使用术语认证是指实体认证。

---

<sup>1</sup> 术语声称和主张被一致认为非常相似。

**6.13 认证保证：**是声称或预期为沟通伙伴的实体，在认证过程中实现的信任度。

注 – 信任是基于在沟通实体和显示的身份之间绑定的信任程度。

**6.14 授权 [ITU-T Y.2720、X.800]：**权利的授予以及基于这些权利授权的接入。

**6.15 关联：**明确形成的相关性、捆绑关系或纽带。

**6.16 生物特征 [b-ISO/IEC CD 2382-37]：**根据对行为和生物（解剖学和生理学）特点的观察而对真人进行的自动识别。

**6.17 证明 [ITU-T X.810]：**由安全机构或可信赖第三方发布的一组安全数据，配合用来提供有关数据的完整性和数据来源认证的安全信息。

**6.18 声称 [b-OED]：**声明情况如此，无法提供证据。<sup>1</sup>

**6.19 声明人 [ITU-T Y.2720、X.811]：**作为认证主体的实体或实体代表。

注 – 声明方包括代表主体参与认证交流的必要功能。

**6.20 语境：**确定实体存在和互动的边界条件的环境。

**6.21 证书：**作为被声称的身份和/或权利的证明的一组数据。

**6.22 分配：**将权利、责任或功能分配给另一实体的行动。

**6.23 数字身份：**有关某个人、群体或组织的信息的数字表述。

**6.24 吸纳：**使实体开始进入语境的过程。

注1 – 吸纳可包括对实体身份的认证及语境身份的确立。

注2 – 同时，吸纳是注册的前提，在很多情况下，后者用来描述两个程序。

**6.25 实体：**单独和独立存在的任何事物，可在语境内识别。

注 – 实体可以为真人、动物、法定人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。在电信中，实体的例子包括接入点、订户、用户、网源、网络、软件应用、服务和设备、接口等。

**6.26 实体认证：**对实体和所介绍身份之间关联性实现充足信任的过程。

注 – 在IdM语境中使用术语认证是指实体认证。

**6.27 联邦：**用户、服务提供方和身份服务提供方的关联。

**6.28 标识：**通过语境特性识别实体的过程。

**6.29 标识符：**用来在语境中识别实体的一个或多个属性。

**6.30 身份：**以一个或多个信息元素表示一实体，使实体足以在语境内得到区分。在IdM中，术语身份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，它包括所有描述这类实体（属性）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。

**6.31 身份保证：**用来确定获得证书的一实体身份的身份认证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。

**6.32 基于身份的安全政策 [ITU-T X.800]：**基于用户、一组用户、或代表用户的实体的身份和/或属性的安全政策和所访问的资源/对象。

**6.33 身份服务桥提供方：**作为其他身份服务提供方中可信赖的中介身份服务提供方。

**6.34 身份管理 [ITU-T Y.2720]：**是用于保证身份信息（如标识符、证书、属性）、保证实体以及支持商业和安全应用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）。

**6.35 身份模式：**对实体属性的结构表示（如实体行为），可用于一些识别过程。

**6.36 身份证明：**证书颁发方向证书应用实体证实充足信息的过程。

**6.37 身份提供方 (IdP)：**见身份服务提供方 (IdSP)。

**6.38 身份服务提供方 (IdSP)：**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。

**6.39 身份认证：**通过使用以往经认证的信息比较所提供的身份声明确认一声称身份的过程。

**6.40 证明：**所观察到或发现的（即非自我声称的）一实体的表述（与声称情况比较）。

**6.41 相互认证：**两个实体（如客户机和服务器）相互认证对方身份的过程。

**6.42 名称：**一个实体被公开提及或涉及时的表达式。

注 – 名称在某个语境内使用，不能假设为唯一的或无歧义的。当名称用于寻址时，可转化/转译为地址。

**6.43 非拒绝：**防止参与整个或部分行动的实体之一拒绝的能力。

**6.44 模式：**见身份模式。

**6.45 持续：**现存的可以在发行分配方直接控制以外的服务中使用，没有确定的时间限制。

**6.46 个人可识别信息 (PII) :** 任何信息a) 识别或能用于识别、联系或定位与该信息相关的个人; b) 从这些信息能够获得某个人的识别或联系信息; 或c) 该信息能够直接或间接与一个自然人相关联。

**6.47 主体 [ITU-T Y.2720、X.811、Y.2702]:** 身份可认证的实体。

**6.48 隐私:** 个人控制或影响收集、管理、保留、接入和使用或分配与其相关的个人信息权利。

**6.49 隐私政策:** 确定保护接入和发布个人可识别信息 (PII) 要求的政策和个人有关如何使用个人信息权利。

**6.50 特权:** 执行特别许可 (行为) 的权利。

**6.51 证明:** 在吸纳新的实体进入身份系统时证实或信息认证。

**6.52 假名:** 与实体的关系未知或仅在其所用语境小范围内知晓的标识符。

注 – 使用假名能够避免或降低隐私泄露风险, 这种风险与使用可能暴露实体身份的标识符绑定有关。

**6.53 注册:** 实体请求或被分配使用服务或资源特权的过程。

注 – 吸纳是注册的前提。吸纳和注册功能可综合使用或相互分离。

**6.54 依赖方 (RP) [ITU-T Y.2720]:** 在一些请求语境内依赖身份表述或请求/声称实体主张的实体。

**6.55 拒绝:** 参与全部或部分行动的有关实体之一的拒绝。

**6.56 请求实体:** 在一些请求语境内向依赖方做出的身份表述或声称。

**6.57 吊销:** (由有权人) 取消以往做过的事情的行为。

**6.58 角色:** 描述可被执行的一实体能力的一套特点或属性。一实体开展的行动, 各实体可扮演多种角色。

注 – 每个实体可以有/扮演许多角色。能力可以是固有的或指配的。

**6.59 安全审计 [ITU-T X.800]:** 对系统记录和活动的独立审议和审查, 从而测试系统控制是否充足, 保证符合所确定的政策和操作程序, 监测安全违规并对控制、政策和程序提出建议修改说明。

**6.60 安全域 [ITU-T Y.2720、Y.2701、X.810]:** 按照安全政策管理元素的一套元素、安全政策、安全认证和一套与安全相关的活动。

**6.61 安全区域 [ITU-T Y.2701]:** 受到保护的区域, 按操作控制、位置和与其它设备/网元连接性定义。

**6.62 安全域授权 [ITU-T X.810]:** 负责实施安全域安全政策的安全授权。

**6.63 自称身份：**由实体本身自称的身份。

**6.64 信任：**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。

**6.65 信任水平：**对某人或某物特性、能力、力量或真实度信赖程度的一致性量化水平。

**6.66 可信赖第三方 [ITU-T Y.2702]、X.800、X.810]：**在一些安全相关活动中可信任的安全机构或安全代理。

**6.67 用户：**使用如系统、设备、终端、流程、应用或公司网络等资源的实体。

**6.68 以用户为中心：**身份管理（IdM）系统提供用户控制和执行各种不同隐私和安全政策能力，这些政策管理诸如用户个人可识别信息（PII）的实体间身份信息交换。

**6.69 认证：**确认声称实体的过程或实例。

注 – (身份)认证可能包含与实体相关联的有效性、正确来源、原始数据、（未被改变的）、正确性等检查。

**6.70 认证方：**认证和验证身份信息的实体。

# 附件A

## IdM基本术语的主要问题和理论基础

(本附件是本建议书的组成部分)

### 背景

有关身份管理 (IdM) 的讨论表明人们在对身份管理的目的、所使用的基本程序和术语及定义方面的理解存在差异。这些差异导致在IdM标准化过程中的误解和争论不休的讨论。

为避免今后出现此类误解，本附件概括了ITU-T在讨论这些基本概念和术语时达成的一些一致意见，从而有助于解释本建议书所含术语的演进（或在某些情况下接受）过程。请注意，本附件不包括或说明有关身份管理的全面观点。

### 引言

身份是所有其他IdM术语衍生的基础。在现实生活中，与数字世界不同的是，自然人的身份随时可以获得接受，因为它基于一套广泛的特性或属性。一些特性为物理特性，如身高、头发颜色、外表、举止、行为等；其他特性，如生日、出生地点、家庭住址、电话号码也可得到使用。在沟通过程中，双方一般需要对对方具有充足的信任。寻求这种信任的过程往往需要两个或更多个人或“实体”，待确认身份的实体 – 请求实体和依赖于已确认实体的实体 – 依赖方。管理实体的第三方亦可介入 – 身份服务提供方。

在数字或“在线”世界中，与现实世界一样，“身份”也是由属性构成的。然而，在此情况中，“身份”可能限于单一特性，或具有多重特性，它将取决于其所出现的环境。这适用于无生命对象以及自然人，因此用户往往被称为实体。

通常，标识符和/或属性描述某一语境内实体的具体特性。因此，一实体可能具有多重不同身份，其中一些为其他身份的子集。

### A.1 认证和信任

认证过程是IdM的重要组成部分。下文有助于说明认证过程及其与信任的关系。

请注意，当对现实程序和应用采用该模式时，我们必须了解相关沟通伙伴及其可适用的信任链。

认证过程可描述如下：

多数沟通过程需要沟通伙伴充分信任或相信他们的确在与所设想的伙伴进行沟通。因此，在沟通开始时，伙伴努力基于现有有关伙伴的身份信息给予充足的信任，即对实体和所介绍的身份之间的关联性给予信任。

确定信任的过程对于天各一方，仅依赖通信链路连接进行沟通的双方尤其重要。认证过程的执行旨在通过充足的信任保证沟通伙伴所显示的身份确属其人。

通信总是涉及两个或更多的相互交流信息的伙伴。由于伙伴的多样性（如人和事物），需定义一个一般性术语。我们所选择的术语是身份。它的定义是：独立存在并可在环境内得到识别的任何事物。

注 -

- 实体可以为真人、动物、法律人、组织、主动或被动之物、设备、软件应用、服务等或上述个体的组合。
- 在电信环境中，实体的例子包括接入点、用户、订户、网元、网络、软件应用、服务和设备、接口等。

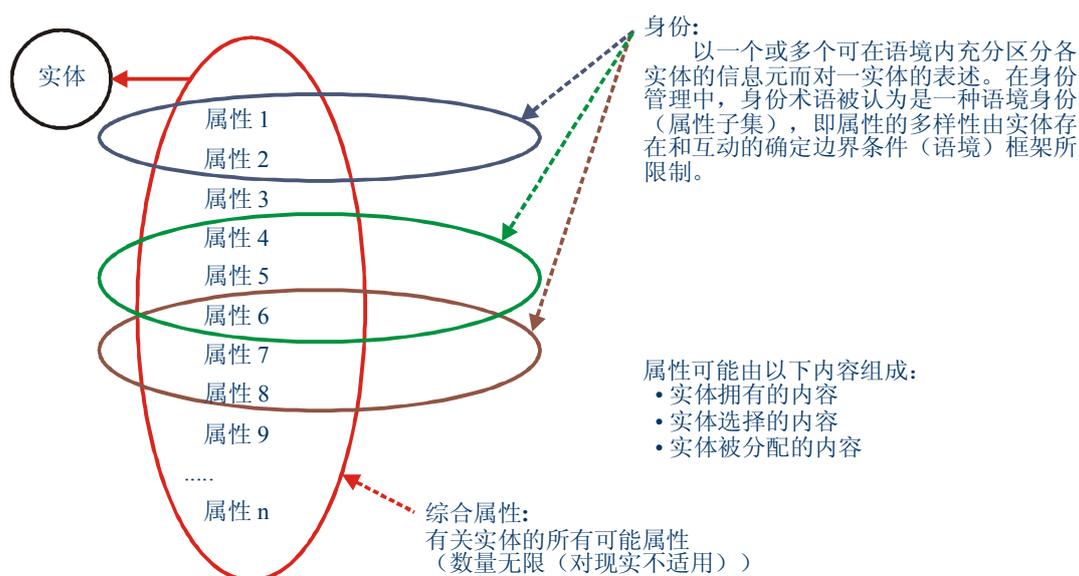
根据实体属性确定的信息可用来识别实体。属性的定义是：与一实体关联的信息，规定了该实体的特性。在实际上，实体的标识往往基于一套属性子集，因为标识受限于环境，即实体存在和互动的环境。环境越窄，边界条件越清晰，标识所需要的属性数量越小。语境的定义为：实体存在和互动时边界条件明确的环境。

由于实体定义基于识别能力，有必要对标识予以适当定义：由语境确定特性的实体识别过程。

为区分实体，可以使用充分说明语境的属性子集。这就是身份，其定义为：以一个或多个可在语境内充分区分各实体的信息元对一实体的表述。在身份管理中，身份术语被认为是一种语境身份（属性子集），即属性的多样性由实体存在和互动的确定边界条件（语境）框架所限制。

身份可以是另一身份的子集。身份之间可能亦有交叉。然而，处于各种原因（如对隐私的担心）用于不同目的或在不同语境下使用的身份交叉可能受到明确限制，甚至受到排斥。

图 A.1显示了实体、身份和属性之间的关系。



X.1252(09)\_FA1

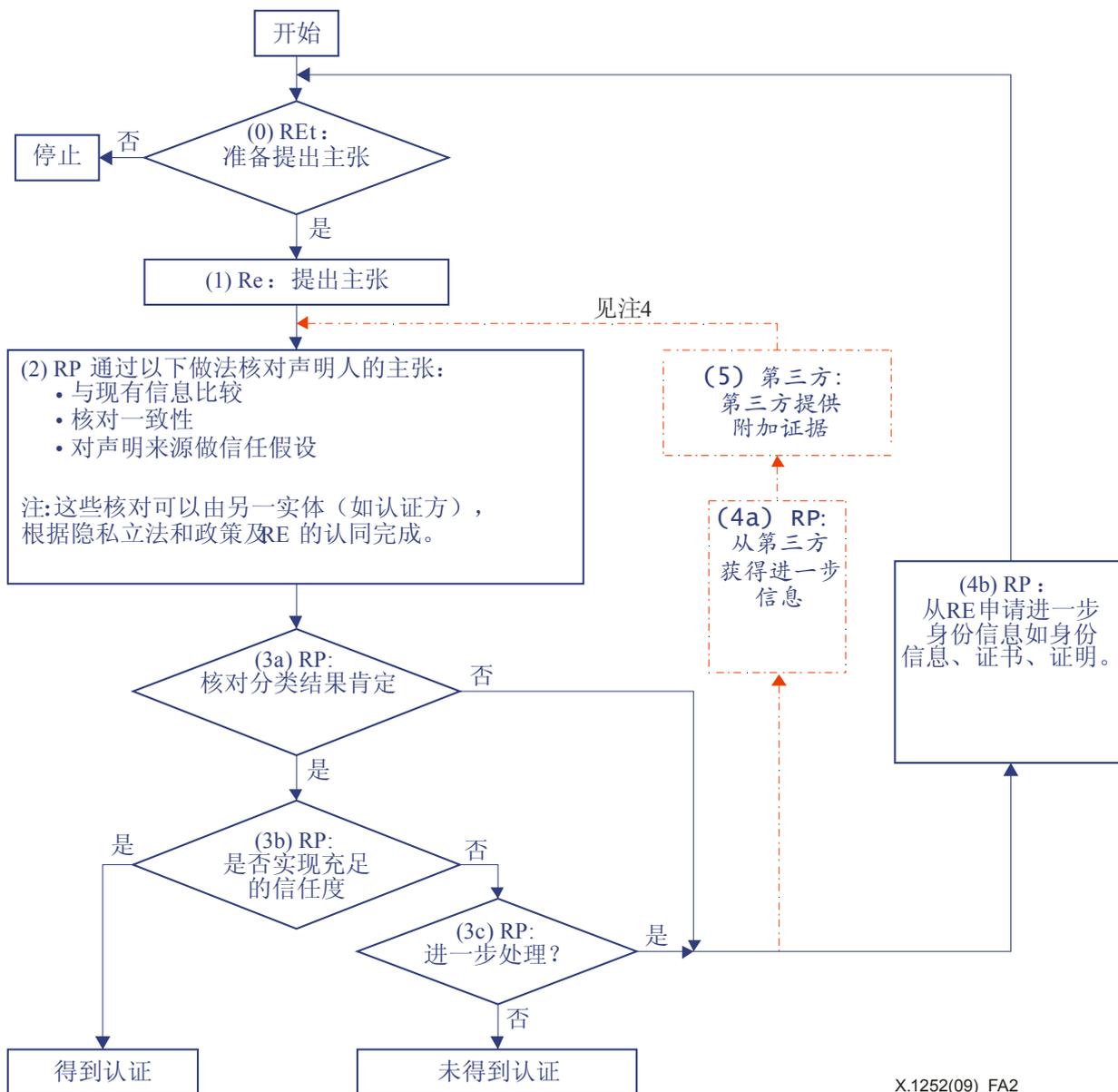
图A.1 – 实体、身份和属性之间的关系

如上所述，认证涉及身份管理。它是为与既定伙伴进行沟通而实现充分信任的过程。实际信任程度取决于应用的敏感性和/或与错误伙伴沟通导致的伤害风险。

不同目的分配到的权利和特权不同：

- 并非针对所有人的交流或信息提供，
- 授权获取：
  - 信息；
  - 房间/领域/地域；
  - 服务；
  - 对资源的使用；
- 签订合同。

赢得这种信任需能将沟通伙伴与其他可能的沟通伙伴区别开来，在需要时这种区分可定期得到重新评定。



X.1252(09)\_FA2

注1:该图显示了基本单向认证过程。通常，该过程相互同时进行，/或交织进行。  
 注2：如不需要信任水平，可放弃第二步。  
 注3：该流程可执行多次，上述循环还可以用时间/地点区分开来。  
 注4：第三方参与取决于隐私立法和政策及Re 的认同。( - - - - - )。

图A.2 – 单向认证过程

一般情况下，实现信任的过程，即认证过程是一个相互的过程。这意味着，图A.2所示认证过程由每个实体按每个角色完成两次，即：

Y的认证：实体Y作为请求实体（RE），实体X作为依赖方（RP）

X的认证：实体X作为请求实体，Y作为依赖方

为简化和方便理解，图A.2所示认证过程只用单向表示。然而，上述两个过程的流动是相互交织的。

交织在一起的过程使各方可以在显示潜在信任属性之前核对前提条件。这些条件可以是：

- 如何与信赖方沟通的知识，
- 充分信任信赖方无误（如在输入用户名和密码信息之前，用户应在一定程度上相信，他们在适当的网页上）。

在一些情况下（但不是以用户为中心的系统中），第三方可直接参与提供信息，作为向依赖方提供的证据，从而提高对请求实体属性的信任。

身份由属性构成。这些内容可以是：

- 实体拥有内容（如代码卡）
- 实体所知内容（如密码）
- 实体本身（如颜色、尺寸）
- 实体可为（如具体加密）
- 实体的位置
- 上述内容的组合

身份可由以下内容予以核对

- 信息本身的一致性
- 与其它支撑信息的一致性
- 与已知信息的比较

属性还可根据身份模式予以规定，这是一实体属性的结构性表述（如实体行为），可用于一些识别过程。

特别要注意的是，如图A.2所示，永远由RP决定是否接受请求实体或不以认证过程为基础。其他人无法做出此确定。

一般而言，每个沟通伙伴都应能够确定实现特权所需要的置信度。但是，在一些情况下，权利是有限的，必须使用立法予以规定。

在通信伙伴之间存在巨大不对等性的情况下，更强的一方可能会滥用局面，因此要求不太高的置信度，或拒绝其自身认证。因此，认证有必要在技术上以对称机制为基础，从而避免不对称性。此外，应加强监管，防止一方主导并在不对称的局面中滥用主导局势。

总之，在进行身份管理时，有必要对有关实体及其目的了如指掌，由此可将语境和实体（一套属性）限制于具体的目的。

有关专门用于电信的置信度，只要客户相信其已连接至指定的传输或服务提供方，而服务提供方相信所使用的服务是得到许可的服务而且能够计费并得到支付就可满足要求。后者可通过对接入点或用户账户认证予以实现，用户账户不一定与服务实际用户相符。在一些情况下预付电话卡或预付SIM卡不需要认证。

在认证过程中，可能需要出示证书作为一定语境下身份的部分或全部属性证据。证书定义为：作为所声称身份和/或权利证据的一组数据。但是，有必要明确区分两类证书：

- 1) 作为所声称身份的证据的一组数据，它用于认证目的（如护照）。这类证书通过证书颁发方确认，用以提高对属性的信任；
- 2) 作为特权证据的一组数据，仅用于认证（如音乐会或球赛门票）。它可以行使特权（如允许凭票参加活动），没必要披露出示该证书的实体身份。

一些证书可能包括两种功能，但两类证书可能采用不同的认证过程。

## A.2 声称/主张

术语“声称”和“主张”的含义相近，但略有不同。在一些情况下，“主张”被认为比“声称”更“强硬”。例如，牛津英语字典这样定义“声称”：

- a) 说明情况，但无法提供证据。
- b) 说明情况如此，

而“主张”的定义为：有信心和强硬的说明。但是，在数字环境中，“信心”和“强硬”是没有什么意义的。

在开放的网络中，做出声明的一方（即展示身份信息一方）和依赖信息的一方之间的关系更加复杂和含糊不清。因此，任何令人疑惑的声明都需认证或要求得到进一步证据。无论是声明，还是主张都无任何授权而言，需要由依赖方决定是否基于依赖方（或应依赖方要求由认证方）通过认证而接受声明或主张。

## A.3 吸纳和注册

吸纳和注册是两个密切相关的过程，二者之间有所重叠。这些术语有时交互使用，尽管他们可能用在一个步骤中，但实际是两个不同的过程。吸纳是在语境内启动（或建立）一实体的过程。

吸纳可能包括对实体身份的认证和语境身份的确立。注册为实体请求并分配到使用服务或资源的特权的过​​程。吸纳是注册的前提。

在现实世界中，用户可在一定程度上被吸纳使用一般银行服务，之后在晚些时候注册在线金融服务。此外，用户在开立新的账户时完成身份（和相关）手续（即吸纳）并在同时注册在线银行服务。

## A.4 身份提供方和身份服务提供方

对目前做法的审查表明，身份提供方和身份服务提供方为常用术语。尽管身份提供方在现有ITU-T一些建议书和建议书草案中有所使用，它可以意味着提供身份的实体，而不是管理身份的实体。此外，该术语容易产生误导，因为身份是不能提供的，它本身就存在或在演进中，属性是分配的。此外，服务提供方一词广泛用于认证服务提供方、证书服务提供方、金融服务提供方等。

身份服务提供方一词因此被认为比身份提供方更具描述性，因此更受欢迎。将身份提供方目前的定义用于身份服务提供方，同时保留身份提供方的术语，但不对此定义，而是将其指向身份服务提供方可以完成这一修改，这对现有文件产生的影响微乎其微。其缩略语应为 IdSP。

## A.5 身份模式

通常来说，模式被认为是观察到或经认可的信息，且用于能被检测到的结构或适合已知的结构中。因此，身份模式可以被认为是描述一个观察到或经认可的实体信息，且用于能被检测到的结构或适合已知的结构中。

例如，术语“模式”在字典上的两个相关定义为：“一个规则的或重复的格式、顺序或安排”；以及“一个人、组织或机构的特性、行动、趋势或其他可观察到的特性范例”。

关于模式的一般观点以及上述定义意味着模式不只有一个元素，但是单个属性在时间上的重复也构成一个模式。某一个属性只发生一次不能构成一个模式，但一个或多个属性同时发生的状态能够形成一个模式。另外，一个身份模式可以基于多个活动或行为，但不限于经观察或认识到的信息。当然它可以基于任何一种（多种）属性。例如，一个轮胎外形有一个明确可检测的结构，因此，在这种情况下，可以把该属性本身认作为一个身份模式。这样的情况也不是必须的：一个模式必须不止一次地观察到为有用。例如，两个人在经销商的展示厅谈论一辆车，他们能够鉴别车并这样谈论它：“停在左后角落的那辆”。

模式是可以重复使用的，但人们也能够设想模式只用过一次的情况，例如一次性密码。

虽然有争论认为，所有属性都有某种结构，但属性和身份模式之间明显的不同是，由观察者发现和导出某种结构，但该结构不必让其他实体知道，甚至被观察实体本身也不必知道。

身份模式不仅可用于识别的目的，而且在某些情况下，还可用于认证或简单地对实体分类或划分。后者的一个实例是通过认真观察消费者行为来确定他们购买了哪些产品以及他们多长时间购买一次。在这样一个“市场营销”的环境中，使用模式来对与某些实体组有关的实体分类，但是如果把这样的样式结合在一起，可以据此识别简单的实体。

用于识别一个实体的元素必须让该实体在环境中十分与众不同。如果要使用身份模式对个人（与组群相对应）进行识别或认证，则身份模式需要是唯一且明确的。然而，在某些情况下，例如，当身份模式用于授权时，则身份模式可以不必是唯一或明确的。举例说，在有必要限制某些特殊服务用户的方面，例如参加运动会。可能有必要设置一些限制，例如，使用某些药物的行为。

## 参考资料

在拟定IdM术语和定义清单时，引证了大量IdM出版物、作品和现有词汇，其中包括以下清单所列内容，但该清单并非完整清单：

- [b-ISO/IEC CD 2382-37] ISO/IEC CD 2382-37, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary.*
- [b-ANSI] American National Standards Institute <http://www.ansi.org/>
- [b-AusCert] AusCert Conference 2005
- [b-Carnegie] Carnegie Mellon® Computing Services  
[www.cmu.edu/acs/documents/idm/](http://www.cmu.edu/acs/documents/idm/)
- [b-NSS] Committee on National Security Systems Glossary Working Group
- [b-Edentity] Edentity <http://www.edentity.co.uk/>
- [b-ETSI] ETSI Terms and Definitions Database Interactive –  
<http://webapp.etsi.org/Teddi/>
- [b-EU] EU Commission eGovernment Unit DG Information Society and Media
- [b-ICANN] ICANN <http://www.icann.org/en/general/glossary.htm>
- [b-Identity] Identity Commons [http://wiki.idcommons.net/Main\\_Page](http://wiki.idcommons.net/Main_Page)
- [b-IETF] IETF Trust (2007) Network Working Group
- [b-ISO/IEC] ISO/IEC JTC 1/SC 27/WG5
- [b-ITU-T Id Mgmt] ITU-T Identity Management Focus Group
- [b-ITU-T Terms] ITU-T Terms and Definitions Database –  
<http://www.itu.int/ITU-T/dbase>
- [b-Cameron] Kim Cameron's Laws of Identity  
<http://www.identityblog.com/?p=354>
- [b-Liberty] Liberty Alliance Technical Glossary
- [b-Modinis] Modinis <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome>
- [b-NetMesh] NetMesh® Inc. <http://www.netmesh.us/>
- [b-NIST] National Institute of Standards and Technology  
<http://www.nist.gov/index.html>
- [b-OASIS] OASIS <http://www.oasis-open.org/committees/security/ipr.php>
- [b-OED] Oxford English Dictionary
- [b-OECD] OECD Recommendation on Electronic Authentication
- [b-Mobile] Open Mobile Alliance™  
<http://www.openmobilealliance.org/UseAgreement.html>
- [b-STORK] STORK-eID Consortium [http://www.eid-stork.eu/index.php?option=com\\_frontpage&Itemid=1](http://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1)

[b-Trusted]

Trusted Computing Group <http://www.trustedcomputinggroup.org/>

[b-IAAC]

UK Information Advisory Council  
<http://www.iaac.org.uk/Default.aspx?tabid=1>





## 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
<b>X系列</b>	<b>数据网、开放系统通信和安全性</b>
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