国 际 电 信 联 盟

ITU-T X.1252

(04/2021)

国际电信联盟
电信标准化部门

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

身份管理基准术语和定义

ITU-T X.1252 建议书

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
消息处理系统	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	X.1080–X.1099
安全应用和服务（1）	
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（1）	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	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400 – X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1252 建议书

身份管理基准术语和定义

摘要

ITU-T X.1252建议书定义了用于身份管理（IdM）的关键术语。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，ITU-T X.1252建议书中规定的术语仅限于那些被认为是最重要和最常用的、与IdM相关的基准术语。ITU-T X.1252建议书包含的附件A解释了某些关键术语的理论基础。

ITU-T X.1252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，尽可能使之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。

历史沿革

版本	建议书	批准日期	研究组	唯一识别标识*
1.0	ITU-T X.1252	2010-04-16	17	11.1002/1000/10440
2.0	ITU-T X.1252	2021-04-30	17	11.1002/1000/14642

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en.

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）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，国际电联已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 X.1252 建议书

身份管理基准术语和定义

1 范围

本建议书定义了身份管理（IdM）中普遍使用的一套基准术语和定义。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注释。附件A包含了某些关键术语和定义的理论基础。

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建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

汇编后的IdM术语和定义在第6部分列出。

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：

CID 加密标识符

DDO DID对象描述符

DID 去中心化标识符

DLT 分布式账本技术

ID 标识符

IdM 身份管理

IdP 身份提供方

IdSP 身份服务提供方

IH 身份枢纽

PII 个人可识别信息

PKI 公钥基础设施

RA 注册机构

RE 请求实体

RP 依赖方

SIM 签约用户身份模块

SSI 自我主权身份

URL 统一资源定位符

ZKP 零了解证明

5 惯例

无。

6 术语和定义

6.1 访问控制：按照预先确定的规则和请求方的具体权利或相关授权，主管部门可用来限制对资源、设施、服务或信息访问的程序。

6.2 地址：确定某一个网络终接点，可用于选路至公众或专用网络中该物理和逻辑终接点。

注 – 基于[b-ITU-T E.101]。

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：仅使用一次的标识符。

6.6 匿名性：一实体无法在一组实体中被识别的性质。

注 – 匿名性可防止对实体或其行为（如用户位置、服务使用频率）的跟踪。

6.7 断言：一实体在没有有效性凭证的情况下做出的声明。

注 – 术语“声称”和“断言”[名词]被一致认为非常相似。

6.8 保证

注 – 见认证保证和身份保证。

6.9 保证等级：实体与所介绍身份信息之间关联性的置信程度。

6.10 属性：针对一实体并说明该实体特性的信息。

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

6.12 属性值 [b-ITU-T X.501]：由属性类型说明的信息类别的一个特别实例。

6.13 认证 [b-ISO/IEC 24760-1]：验证的正式过程，如果成功，将为某实体产生一个经认证的身份。

注 – 在身份管理情境中使用术语认证是指实体认证。

6.14 认证保证：旨在提供置信度的、认证过程中的肯定确认，表明沟通伙伴是其声称或预期的实体。

注 – 保证基于在沟通实体和显示的身份之间绑定的信任程度。

6.15 授权：权利的授予以及基于这些权利授权的接入。

注 – 基于[b-ITU-T X.800]。

6.16 绑定：明确建立的相关性、捆绑关系或纽带。

6.17 生物特征识别，生物特征[b-ISO/IEC 2382-37]：基于对生物和行为特性的观察而对个人进行的自动识别。

6.18 证明：由安全机构或可信任的第三方发布的一组安全相关数据，配合用来提供有关数据的完整性和数据来源认证服务的安全信息。

注 – 基于对“安全证书“的定义。

6.19 声称：［*名词*］关于一个实体对自己或另一个实体［*动词*］所做的身份属性的数字声明。

注 – 术语“声称”和“断言”[*名词*]被一致认为非常相似。

6.20 声明方：作为认证主体的实体或实体代表。

注1 – 声明方包括代表主体参与认证交流的必要功能。

注2 – 基于 [b-ITU-T X.811]。

6.21 声称定义：一种机器可读的、关于声称语义结构的定义。

注 – 声称定义有助于声称和证明在多个发布方、持有方和依赖方之间的互操作性。

6.22 情境：确定实体存在和互动的边界条件的环境。

6.23 关联：与实体相关或在组合后变得与实体相关的各种信息片段的组合。

注 – 关联与识别紧密相关。相关可促进识别和推断关于不由给定数据直接提供的实体的信息。

6.24 证书：作为被声称的身份和/或权利的证明的一组数据。

注 – [b-ISO/IEC 29115]是与[b-ITU-T X.1254]相似的文本，并包含由相关小组提出的相同的证书定义。

6.25 数据最小化：将与实体关联的标识符、属性和其他数据的收集、存储和使用限制在仅执行身份认证所需的范围内，并将与实体关联的数据（包括请求的上下文信息）的任何交换和透露限制在仅响应请求所需的范围内，以及限值在仅对与请求关联的依赖方上。

6.26 去中心化标识符（DID）：指的是一种全球唯一的标识符，由于它已通过分布式账本技术或其他形式的去中心化网络进行注册，因此不需要一个集中/中心化的注册机构。一个DID仅与一个DID对象描述符相关。

注 – 见[b-W3C-DIDs]。

6.27 DID对象描述符（DDO）：指的是用于描述去中心化标识符（DID）主体的一组数据，包括诸如公钥等机制，DID主体或DID代理可用来认证自己并证明其与DID的关联。

6.28 委托：将权利、责任或功能指配给另一个实体的行动。

6.29 数字身份：有关某个资源、特定的人、群体或组织的信息的数字表述。

6.30 分布式账本 [b-ITU-T X.1400]：指的是一种以分布式和去中心化方式共享、复制和同步的账本类型。

6.31　去中心化的密钥管理系统（DKMS）：基于去中心化标识符的可互操作加密密钥管理的标准。

6.32　域：实体可以使用一组属性进行标识和其他用途的环境。

注 – 域提供情境。

6.33　登记：使某实体开始进入某情境的过程。

注1 – 登记可包括对实体身份的认证以及对情境身份的确立。

注2 – 同时，登记是注册的前提，在很多情况下，后者用来描述两个过程。

6.34　实体：单独和独立存在的某个事物，在情境中可被识别。

注1 – 可以有一个物理或逻辑具象的实体。

注2 – 实体可以是一个真人、动物、法人、组织、有源或无源之物、设备、软件应用、服务等或者上述实体的一个组合。在电信情境下，实体的例子包括接入点、签约用户、用户、网络元素、网络、软件应用、服务和设备和接口。

6.35　实体认证：对实体和所述身份之间的绑定实现验证和充分信任的过程。

注 – 在身份管理情境中使用术语认证是指实体认证。

6.36　联邦[b-ITU-T Y.2720]**：**在两个或更多实体，服务提供方和身份提供方之间建立关联。

6.37　持有方：已由发布方发出一份声称的实体。如果声称支持零了解证明（ZKP），则持有方也是证明方。

6.38　标识[b-ISO/IEC 24760-1]**：**识别特定域中某实体有别于其他实体的过程。.

6.39　标识符（ID）[b-ITU-T E.101]**：**用来唯一标识某个签约用户、用户、网络元素、功能、网络实体、业务或应用的一系列数字、字符和符号。标识符可用于注册或授权。标识符可以是所有网络的公共标识符或者是某个特定网络的专用标识符（专用ID通常不披露给第三方）。

注 – 标识符可以是一个专门创建的属性，其值在域内指配为唯一。

6.40　身份：以一个或多个属性的形式来表示一个实体，使实体足以在情境内区分开来。出于身份管理的目的，术语“身份”被理解为情境下的身份（属性的子集），即属性的多样性受限于实体存在和互动的边界条件（情境）所定义的框架。

注 – 各实体通过一个综合身份来表示，它包括用于表征此类实体（属性）的所有可能的信息元素。不过，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，因为所有可能的属性数量是无限的。

6.41　身份保证：在用来确立发布证书之实体身份的身份认证和验证过程中提供的置信度，以及有关使用证书的实体就是被颁发或被指配证书的实体的置信度。

6.42 基于身份的安全策略 [b-ITU-T X.800]：基于用户、一组用户或代表用户和所访问资源/对象之实体的身份和/或属性的安全策略。

6.43 身份管理（IdM）：用于保证身份信息（如标识符、证书、属性）、保证实体身份并支持商业和安全应用的一系列功能和能力（如行政、管理和维护、发现、通信交换、关联和绑定、政策执行、认证和断言等）。

注 – 基于 [b-ITU-T Y.2720]。

6.44 身份所有者：可以负责的一个实体。身份所有者必须是个人或组织。与事务互斥。

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

6.46 身份证明[b-ISO/IEC 29115]：注册机构（RA）获取并验证足够信息以确认某实体具有特定或所认为保证的过程。

6.47 身份提供方（IdP）：

注 – 见身份服务提供方（IdSP）。

6.48 身份服务桥提供方：作为其他身份服务提供方中可信中介的身份服务提供方（IdSP）。

6.49 身份服务提供方（IdSP）：验证、维护、管理并可能创建和指配其他实体身份信息的实体。

6.50 身份验证：使用以往经证明的信息对所提供的身份声称进行比较以确认声称之身份正确性的过程。

6.51 独立者：直接控制管理去中心化身份所需之私钥和主钥的个人。

6.52 个人：作为自然人的身份所有者。与组织互斥。

6.53 发布方：发布一个声称的实体。

6.54 发布方密钥：发布方发布一份支持零了解证明的声称所需的特殊类型的加密密钥。

6.55 密钥链：指的是保护设备中可信硬件单元上私钥或数据存储安全的任务。

6.56 合法身份：在至少一个辖区内，出于法律责任目的，足以识别一个身份所有者的一组信息。出于临时网络的目的，可以通过参考一个或多个可公开访问的互联网资源（例如，网站、博客、社交网络配置文件或其他提供足够信息来满足此测试要求的网页）来建立一个合法身份。

6.57 可链接性：在一组信息中区分两个或多个属性、标识符、身份或其他数据的能力，与足够有用的概率相关。

6.58 表征：所观察到的或所发现的（即非自我断言的）的实体表述。

注 – 相比断言。

6.59 相互认证[b-ISO/IEC 29115]：两个实体（如客户端和服务器）相互确保对方身份。

6.60 名称：名称是字符的一个组合，用来标识可能转化为或转译为地址的实体（如签约用户、网络元素）。字符可包括号码、字母和符号。

注1 – 名称在某个情境内使用，不能假设为唯一的或无歧义的。当名称用于路由目的时，可转化/转译为一个地址。

注2 – 基于 [b-ITU-T E.101]。

6.61 不可否认性：防止参与过某项活动的实体之一拒绝承认曾参与整个或部分行动的能力。

6.62 模式

注 – 见“身份模式”。

6.63 持续：存在和可以在发布指配方直接控制之外在服务中使用，没有确定的时间限制。

6.64 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；或者c) 该信息能够直接或间接地与一个自然人相关联。

6.65 主体：身份可被认证的一个实体。

注 – 此项出现在 [b-ITU-T X.811]、[b-ITU-T Y.2702]和 [b-ITU-T Y.2720]中。

6.66 隐私政策：确定保护接入和发布个人可识别信息的要求和如何使用其个人信息的个人权利的政策。

6.67 私钥 [b-ITU-T X.509]**：**（在公钥加密系统中）一个实体密钥对中只有该实体知晓的那个密钥。

6.68 特权：指的是一种权利，当授予某个实体时，允许该实体执行某项行动。

6.69 证明：对声称的密码验证。数字签名是证明的一种简单形式。加密哈希也是证明的一种形式。证明是两种类型之一：透明或零了解。透明证明可揭示声称中的所有信息。零了解证明可以选择性地透露声称中的信息。

6.70 证明方：用声称发布一份证明的实体。证明方也是声称的持有方。

6.71 化名 [b-ISO/IEC 24760-1]**：**指的是一个标识符，包含足以允许验证方将之确立为指向某已知身份的一条链路的最小身份信息。

注1 – 一个化名可以是一个标识符，其值由人来选择或随机指配。

注2 – 可以使用化名来避免或减少与使用标识符绑定相关的隐私和安全风险，这些标识符绑定可能会揭示实体的身份。

6.72 公共数据 [b-ITU-T L.1410]**：**公众可获得的数据，不受成员要求、保密协议或类似限制的局限。

6.73 公钥 [b-ITU-T X.509]**：**实体密钥对中公开的那个密钥。

6.74 公共概况：描述服务提供商的信息，包括其法律身份、徽标或者其他商标、位置、营销信息、互联网链接，以及信任框架为确保有关提供商的法律身份和资格完全透明而需要的任何其他信息。

6.75 注册：实体请求和被指配使用某项服务或资源的特权的过程。

注 – 登记是注册的前提。登记和注册功能可组合使用或相互分离。

6.76 依赖方（RP）：在一些请求情境内依赖身份表述或请求或断言实体所做声称的一个实体。

注 – 基于[b-ITU-T Y.2720]。

6.77 否认：有关实体之一拒绝承认曾参与全部或部分行动。

6.78 请求实体（RE）：在一些请求情境内向依赖方做出身份表述或声称的一个实体。

6.79 撤销：由有权人取消以往做过的某件事情。

6.80 角色：描述可被一个实体执行的能力或功能的一系列特点或属性。

注 – 每个实体都可以有或扮演多个角色。能力可以是固有的或指配的。

6.81 安全审计 [b-ITU-T X.800]：对系统记录和活动的独立审查和检查，以便测试系统控制是否恰当，以确保符合所建立的政策和操作程序、监测安全违规情况，并对控制、策略和程序提出修改建议。

6.82 安全域：指的是一系列元素、安全策略、安全授权和一系列与安全相关的活动，活动中按照安全策略来对各元素进行管理。

注 – 基于[b-ITU-T X.810]。类似定义见 [b-ITU-T Y.2701]和[b-ITU-T Y.2720]。

6.83 安全区域：指的是一个受保护的区域，它通过操作控制、位置以及与其它设备或网络元素的连通性来刻画。

注 – 基于[b-ITU-T Y.2701]。

6.84 安全域主管部门 [b-ITU-T X.810]：指的是一个安全主管部门，它负责实施针对某个安全域的安全策略。

6.85 自称身份：由实体宣称是自己的身份。

6.86 事物：一个无法追究法律责任的实体。事物可以是动物（例如，宠物、牲畜）、自然物体（例如，房屋、汽车、电话）或数字对象（例如，软件程序、网络业务、数据结构）。与身份所有者互斥。

6.87 信任：一个当事方或实体对另一当事方或实体将以明确定义的方式表现的信心，不会违反身份管理系统中商定的规则、策略或法律条款。

6.88 信任锚：可以充当去中心化可信网络起点的身份所有者。信任锚具有两个独特的特权：

- 将新的身份所有者添加到网络；和
- 发出信任锚邀请。

信托锚必须满足信任锚资格并同意信任锚框架中定义的信任锚义务。所有受托人和管理人都是自动的信任锚。

6.89 信任框架：指的是一系列可合法执行的规范、规则和协议，用于管理一个身份系统。

注 – 基于[b-OIX-TFIS]。

6.90 可信任第三方：在安全策略背景下，在一些安全相关活动中可信任的安全机构或安全代理。

注1 – 基于[b-ITU-T X.810]和[b-ITU-T Y.2702]。

注2 – 见[b-ITU-T X.800]。

6.91 **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度量。

6.92 **用户**：使用诸如系统、设备、终端、流程、应用或公司网络等资源的任何实体。

6.93 **以用户为中心**：身份管理系统为用户提供控制和执行各种管理用户数据（包括用户的个人可识别信息）的策略的能力。

6.94 **验证方节点**：指的是一个节点，用于验证身份记录的新交易，并使用账本共识协议主动地将有效交易写入账本。

6.95 **可验证的声称**：包含发行方证明的一个声称。通常，该证明采用数字签名的形式。可以通过与发行方去中心化标识符相关联的公开密钥来验证可验证的声称。

注 – 基于[b-W3C-VC]。

6.96 **验证** [b-ISO/IEC 24760-1]：确立与某特定实体关联的身份信息是正确的过程。

注1 – 识别过程将验证应用于所声称或所观察到的属性。

注2 –（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、实体关联性等检查。

注3 – 验证时信息是正确的。

6.97 **验证方** [b-ISO/IEC 24760-1]：执行验证的实体。

6.98 **钱包**（身份钱包）：指的是一个应用程序，它主要允许用户通过在用户设备上存储相应的私钥来持有标识符和证书。

6.99 **零了解证明（ZKP）**：指的是一个证明，它使用密码学和一个主密钥来允许有选择地透露一组声称中的信息。一个ZKP可证明一组声称中的某些或全部数据是真实的，而无需透露任何其他信息，包括证明方的身份。

注 –“选择性透露”的概念意味着针对透露有广泛的选择范围。例如，ZKP可用于证明对机密数据的众多声称，例如：(1) 成年，而不透露出生日期；(2) 偿付能力（未破产），而未显示投资组合构成；(3) 资产的所有权，而不透露或链接到过去的交易。

注2 – 基于[b-ITU-T X.1403]。

附件A

身份管理基本术语的要点和理由

（本附件是本建议书的组成部分）

背景

有关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，本附件记录了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IdM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分的信任。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*（RE）和依赖于已确认实体的实体 – RP。管理实体的第三方亦可介入 – IdSP。

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（ID）或属性描述某一情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，我们必须清楚地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1 – 实体可以拥有实体或逻辑表达。

注2 – 实体可以是一个真人、动物、法人、组织、有源或无源之物、设备、软件应用、服务等或者上述实体的一个组合。

在电信情境下，实体的例子包括接入点、签约用户、用户、网络元素、网络、软件应用、服务和设备和接口。

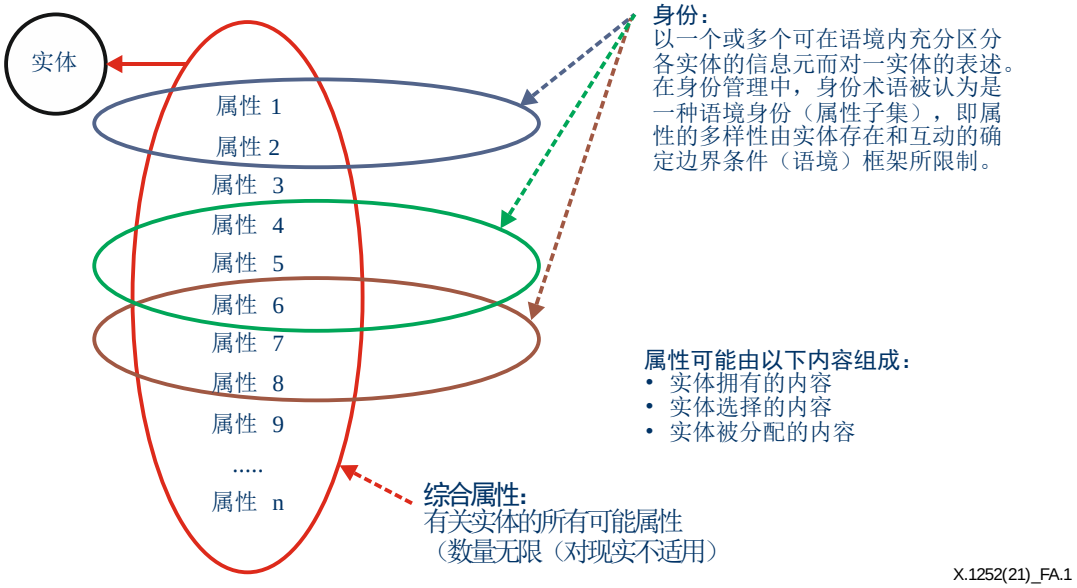
根据实体属性确定的信息可用来识别实体。属性的定义是：与一实体关联的信息，规定了该实体的特性。实际上，实体的标识往往基于一套属性子集，因为标识受限于环境，即实体存在和互动的环境。环境越窄，边界条件越清晰，标识所需要的属性数量越小。情境的定义为：实体存在和互动时边界条件明确的环境。

由于实体定义基于识别能力，有必要对标识予以适当定义：在与其它实体不同的特定域进行的实体识别过程。

为区分实体，可以使用充分说明情境的属性子集。这就是身份，其定义为：以一个或多个可在情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情境身份（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情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。



图A.1 – 实体、身份和属性之间的关系

如上所述，认证涉及IdM。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，地区或领域，
  - 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明确区别开来，在需要时这种区分可定期得到重新评定。

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RE，实体X作为RP。

X的认证：实体X作为RE，Y作为RP。

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RP沟通的知识，
- 充分信任RP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）。

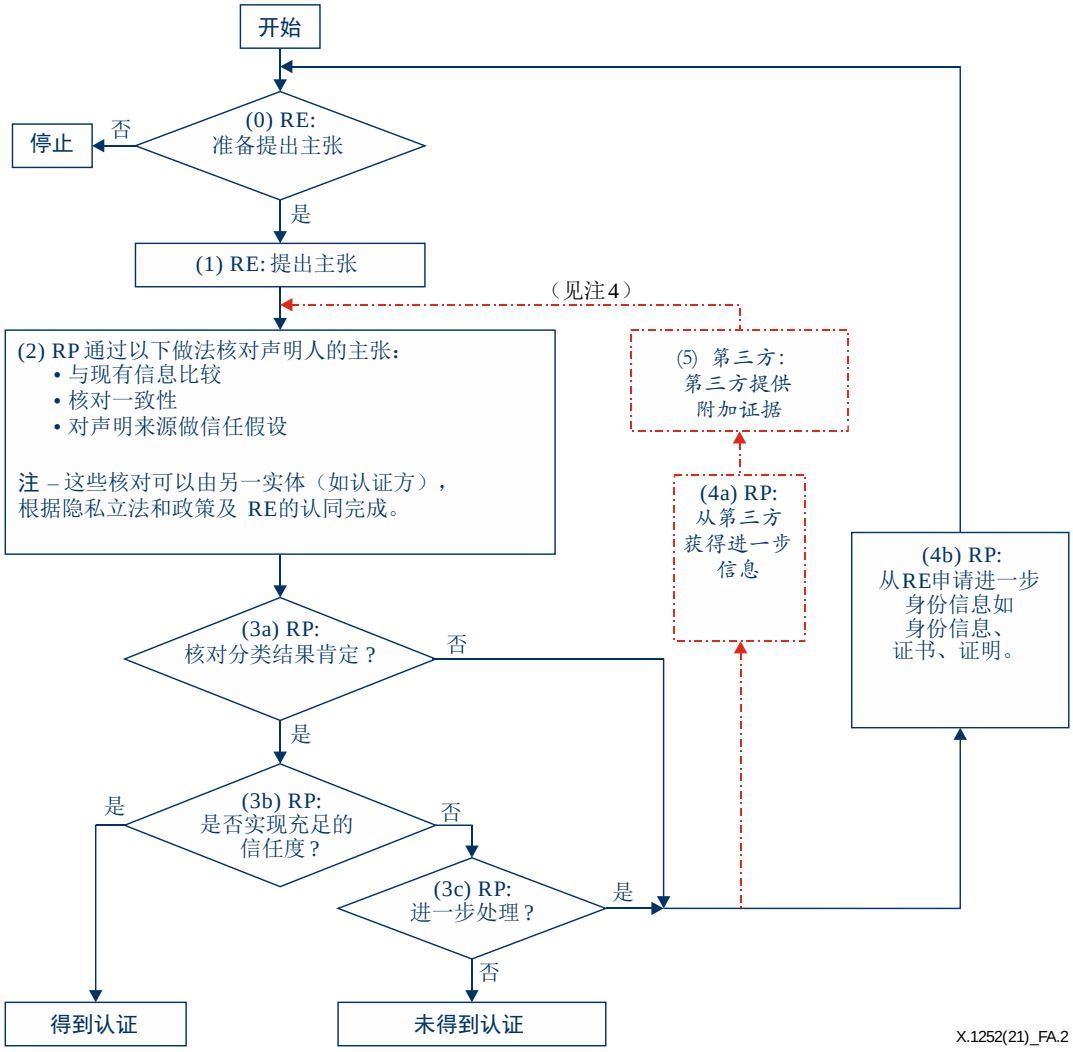
在一些情况下（但不是以用户为中心的系统中），第三方可直接参与提供信息，作为向RP提供的证据，从而提高对RE属性的信任。

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。



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。 ( )

X.1252（21）_FA.2

图A.2 – 单向认证过程

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RE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IdM时，有必要对有关实体及其目的了如指掌，由此可将情境和实体（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签约用户身份模块（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情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 声称或断言

术语“声称”和“断言”的含义相近，但意义略有不同。在一些情况下，“断言”被认为比“声称”更“强硬”。例如，按以下方法定义“声称”：

a) 说明情况，但无法提供证据。

b) 说明情况如此，

而“断言”的定义为：有信心和强硬的说明。但是，在数字环境中，形容词“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。无论是声称还是断言都无任何授权而言，需要由RP决定是否基于RP（或应RP要求由认证方）通过认证而接受声称或断言。

A.3 登记和注册

登记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，尽管它们可能用在一个步骤中，但实际是两个不同的过程。登记是在情境内启动（或建立）一实体的过程。

登记可能包括对实体身份的认证和情境身份的确立。注册为实体请求并指配到使用服务或资源的特权的过程。登记是注册的前提。

在现实世界中，用户可在一定程度上被登记使用一般银行服务，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（即登记）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（IdP）和IdSP为常用术语。尽管IdP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，属性是指配的。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。

IdSP一词因此被认为比IdP更具描述性，因此更受欢迎。将IdP目前的定义用于IdSP，同时保留IdP的术语，但不对此定义，而是将其指向IdSP便可以完成这一修改，这对现有文件产生的影响微乎其微。

A.5 身份模式

通常来说，模式被认为是观察到的或经认可的信息，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的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”的两个定义为：“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，但不限于观察到的或认识到的信息。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：“停在左后角落里的那辆”。

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地方，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。

附件B

去中心化实体管理基本术语的要点和理由

（本附件是本建议书的组成部分。）

B.1 去中心化身份

附件A中提出的身份模式以IdP为中心。该模式假定用户依赖IdP来建立、维护和提供其身份，以用于其在线交互。这种以IdP的身份方法要求用户信任IdP及其身份。在以IdP为中心的方法中，IdP提供联邦业务以重用身份。重用用户身份的能力受到联邦成员的限制。身份联邦将提供方放在信任的中心，其焦点在保护商业模式上，而不是启用允许用户负责其身份和关系的、真正去中心化身份回显系统。以IdP为中心的身份模式需要对中心式IdP的隐式信任。因此，该模式不灵活也不动态。

另一方面，在去中心化身份模式中，系统使用户能够掌控自己的身份。在去中心化方法中，提供方专注于断言有关特定身份的声称。当前分布式账本技术（DLT）的发展推动了去中心化身份模式的发展。

为了启用跨参与域的服务，中心式身份模式专注于在一个域中提供身份认证服务，以允许通过身份联邦桥来访问另一个域。在在线交互中，压力在基于身份的系统上，以确认所声称的实体身份，而不是提供访问控制。因此，去中心化身份系统的一个主要功能是提供一种模式，以便能够提交关于用户身份的断言，该模式可以方便地在提供方间使用。

以用户为中心的身份模式由跨多个身份域的个人或行政控制组成，而无需一个联邦来充当信任圈。以用户为中心的身份旨在为实体创建一个持久的在线身份，该实体专注于创建更好的在线体验，同时通过使用去中心化信任模式来为用户提供对其身份的更好控制。不过，由于缺乏简单性和缺少诸如DLT之类的技术，因此以用户为中心的模式未获成功。

自从引入DLT以来，以用户为中心的身份这一概念便开始受到关注。正在开发基于DLT的协议栈，以实现真正的去中心化身份基础设施。这些系统可以通过公共、专有、无需许可或经过许可的DLT来赋能，以实现数字身份的管理。目标是将身份断言的控制权移交回用户，同时保持系统的安全性、完整性和私密性。

B.2 去中心化身份模式

去中心化身份是一种模式，可推动在任何数量机构（包括IdP）间的个人控制（具有委托控制的能力）。一种特定的去中心化身份模式称为自我主权身份（SSI），它具有表B.1所列假设：

表B.1 – 自我主权身份假设

存在	用户必须独立存在
控制	用户必须控制其身份
访问	用户必须有权访问自己的数据
透明性	系统和算法必须透明
持续性	身份必须长期存在
可移植性	有关身份的信息和服务必须可传输
可互操作性	身份应尽可能广泛地使用
同意	用户必须同意使用其身份
最小化	对声称的透露必须最小化
保护	用户的权利必须得到保护

所期望的与DLT可提供的非常一致。去中心化身份实施方案通常基于声称和认证，当中参与者通常可以扮演不同的角色。

去中心化身份系统可用于促进可信的在线交易。去中心化身份系统使用户能够通过使用可验证的声称（认证）来向服务提供方证明有关其自身的属性（反之亦然）。整个过程可以通过技术堆栈的使用，以可互操作和可信的方式来完成，技术栈使分发可信的声称成为可能，而无需交易参与者之间的直接关系。

在去中心化身份系统中，服务提供方充当RP，而声称则由认证发布方来提供，后者发布所需的缺失认证。认证是关于另一个声明集准确性的声明集。原始声明集也可以称为声称。认证的接收方应能验证认证方对声称的承诺。因此，该承诺应是一种数字签名的形式或是一个指向分布式账本中数据的指针。

标识网络中的节点通过去中心化的标识符（DID）来进行。DID对参与网络和进行交易而言至关重要。这是标识某人的数字/名称/字符串。加密标识符（CID）是一种DID，它通过密码链接到某个私钥。

如今，大多数基于身份的解决方案对身份、透明性和可移植性的控制的支持都是有限的，原因是具有专有系统的第三方身份提供方可以简化此类解决方案。完全符合身份系统可能不会在不久的将来出现，但这并不排除需要建立关于主权的基本原则。

为了启用SSI，将带来新一波的去中心化身份管理协议和解决方案的标准化工作，如B.2.1至B.2.5款所述。

B.2.1 去中心化标识符

去中心化标识符（DID）是可验证的、去中心化身份系统的ID，包括“自我主权”数字身份。通常，DID是用户生成的并且是自有的。DID具有独特的特性，可以提供更大的不变性保证，并且具有防篡改功能。DID完全处于DID主体的控制下，独立于任何中心化注册机构、IdP或证书机构。DID是统一资源定位符（URL），它将DID主体与用于和该主体进行可信交互的方式相关联。

通常，DID分为两类：公共DID和成对DID（将它们视为半私有）。

1) 公共DID是那些选择将自己与打算供公众共享的数据链接起来的用户使用的ID。例子包括在社交媒体上的公开简介或对诸如医生之类的职业的验证。公共DID允许用户支持其认为适合与他人共享并可由他人验证的活动。 例如，我可验证我自己的私人医生拥有DID。公共DID在互联网上是可跟踪和可链接的。

2) 成对DID是作为一个关系或一组交互的一部分生成的，因此，用户希望进行相互交易。成对DID隔离用户并防止关联。对大多数用户而言，成对DID将是进行基于身份的交互的主要机制。

DID解析为DID文档，DID文档是描述如何使用特定DID的简单文档。每个DID文档至少包含三件事：加密材料、认证套件和服务端点。加密材料与认证套件相结合，提供了一组对DID主体进行认证的机制（例如，公钥和化名生物特征识别协议）。服务端点启动与DID主体的可信交互。

为将DID与特定的分布式账本或网络一起使用，需要在一个单独的DID方法规范中定义一种DID方法。一种DID方法规定一组规则，这些规则用于控制在该特定的账本或网络中如何注册、解析、更新和撤销一个DID。

这种设计减少了对有关ID的中心化注册机构以及有关密钥管理的中心化认证机构 – 层次化公钥基础设施（PKI）的标准模式的依赖。由于DID驻留在分布式账本上，因此每个实体都可以充当自己的机构。

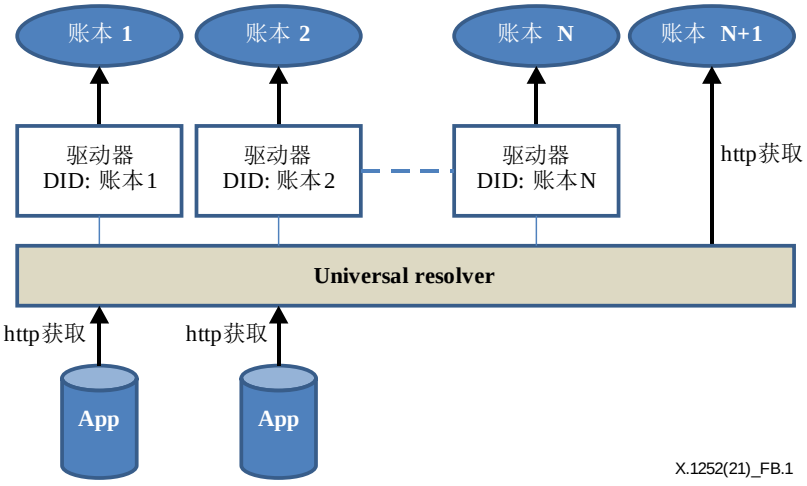
注意：还可以为在联邦化或中心式IdM系统中注册的ID开发DID方法。就其本身而言，所有类型的ID系统都可以添加对DID的支持。这在中心化、联邦化和去中心化标识符世界之间建立了一座互操作性的桥梁。

B.2.2 身份枢纽

身份枢纽（IH）[1]是负责存储有关主体的身份断言的组件。IH基于去中心化模式，来存储任何对象的语义表示，然后将其公开为特定的URL。IH体系结构可以将存储在从云目录到设备的不同提供商上的身份汇集在一起。

B.2.3 通用去中心化标识符解析器

通用DID解析器就像一个分布式系统一样，可以解析多个DLT或区块链上的DID。通用DID解析器的目的与域名系统中的绑定机制相似。通用DID解析器不使用域名，而是专注于解决SSI，这些SSI可以由它们引用的实体来直接创建和注册。该概念在图B.1中描述。



图B.1 – 通用DID解析器

B.2.4 可验证的证书

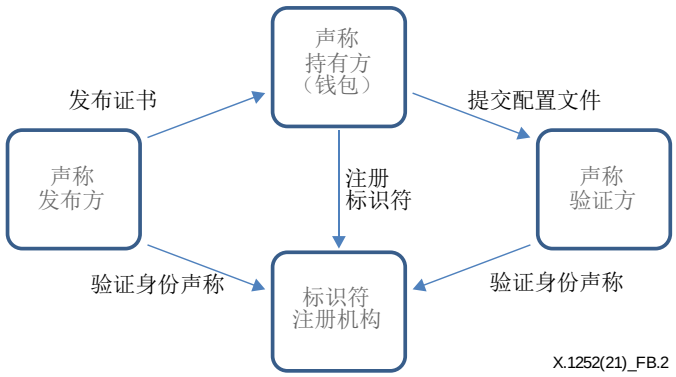
当实体需要证明它们有以下情况时，可验证的声称会很有用：

- 超过一定年龄；
- 能够驾驶某种特定的汽车；
- 要某种特定的药物；
- 经培训并获电工认证；
- 有专业的行医许可；以及
- 获准国际旅行。

可验证的声称生态系统由四个主要角色组成：

1) 发布方，发布有关特定主体的、可验证的证书，
2) 持有方，持有代表某个主体的证书。持有方通常也是证书的主体，
3) 验证方，请求一个有关主体的配置文件。配置文件包含一组特定的证书。验证方确认配置文件中提供的证书适合于目的，
4) ID注册，一种用于发布主体ID的机制。

图B.2是该生态系统的直观描述。



图B.2 – 生态系统

B.2.5 去中心化钱包

在该模型中，用户可以通过以令牌形式向服务提供方（RP）提供其ID来访问服务。RP通过对ID的哈希值与其存储在DLT中的相应哈希记录进行比较来验证身份。RP根据验证结果来同意或拒绝访问。在更高级的场景中，用户可以从主私钥中获取单独的密钥对，以生成用于不同关系的单独ID，从而实现隐私友好的交互。

图B.3描述了支持基于身份的服务的总体身份交互。该图描述了去中心化身份事务处理中的以下步骤：

- 用户决定使用身份信任系统的去中心化身份服务进行交互。如图B.3去中心化账本框中所述，DLT提供的服务使最终用户能够建立一个DID以及与账本的一个关系。为用户建立一个DID的任务将为该用于保存一个账本地址，并创建用于与该用户交互的公共私钥对。账本还将维护DID文档，并建立用户规定之所需链接数据的JavaScript对象符号链路。账本提供核心身份服务，使服务能够发现如何与用户钱包进行交互，以便在用户控制下查询可用的声称。
- 在账本上创建一个DID的行为将创建一个钱包，供用户用来向RP提供经验证的声称。钱包持有由DID方法确定的用户私钥、公钥和其他身份配置文件。零了解技术的使用确保可以以保护隐私的方式来验证声称，并与传统的纸质证书和文档的当前用法相符。例如，在餐厅，用户可以使用驾驶证来证明其年龄，而无需驾驶证签发方参与交易。接下来几段提供所需的步骤。钱包可以是虚拟钱包，其中钱包的一部分在用户的移动设备上，另一部分可以在云上。这种配置使得能够通过创建代理来代表用户采取行动和提供服务，而无需用户的直接参与。

  1) DID注册：用户下载与DLT核心服务提供方关联的钱包，并在账本上注册其DID。DLT生成与身份钱包关联的私钥和公钥对。此外，作为注册过程的一部分，将创建一个地址并将其存储在DLT中。

  2) 身份初始化：对于要在去中心化身份系统中使用的DLT，假定存在一个信任框架，该信任框架为参与者规定可用的身份服务集。在这方面，用户可以依赖可验证服务身份之发布方（可信方）的可用性。用户可以在初始声称的基础上收集来自多个提供方的声称，以纳入其钱包中，并增强其在系统内的身份有效性。从图B.3可以看出，每种关系都受到发布方、持有方（用户）和验证方之间相互DID的保护。

  3) 验证：如果持有方（用户）想访问RP提供的某项服务，则RP（验证方）将请求用户提供可用声称。验证方而后咨询账本，以便通过使用与DID相对应的并和交易相关的公钥来验证经签名的声称。本步骤包括其他层面的认证，尤其是系统的工作方式，依据有关持有方私钥的知识，系统假定钱包是真相的来源。系统假定进行了适当的认证，以确保合法的钱包所有者是执行交易的实体。

  4) 声称验证：RP使用钱包提供的声称，以使用基于PKI的签名和哈希验证技术来验证用户的身份和属性。

  5) 授权：RP根据身份验证的结果来确定可以访问哪些服务。

- DID设计要求具有任何DID的通用解析器的功能。DLT社区仍在实施这项要求。在去中心化身份模式中，需要建立可互操作的DID认证层。这项工作仍在进行中。

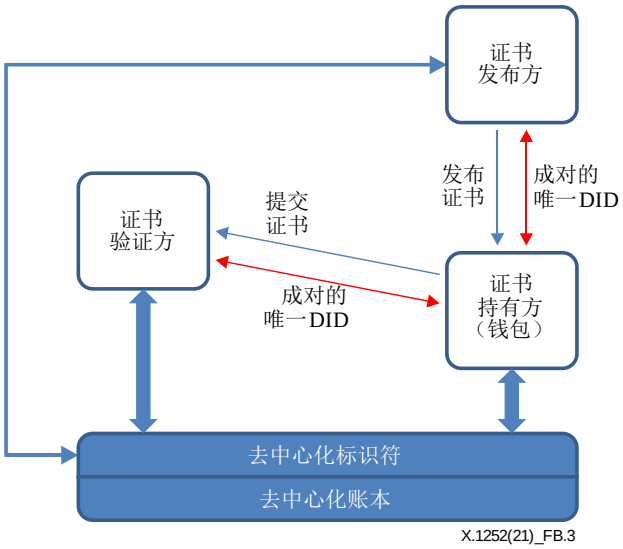
- DID认证使身份所有者能够在与RP交互期间控制DID。这要求RP执行以下步骤：

  1) RP将身份所有者的DID解析为一个DID文档；

  2) RP尝试使用在DID文档中找到的认证对象来对身份所有者进行认证；

  3) 在身份所有者的证明被建立为一个加密签名的情况下，认证对象可以纳入或参考一个公钥对象。

- 就身份所有者如何证明对DID的控制而言，必须将DID认证理解为是可扩展的。



图B.3 – 具有可验证声称的去中心化身份钱包

参考资料

[b-ITU-T E.101] Recommendation ITU-T E.101 (2009), *Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations*.

[b-ITU-T L.1410] Recommendation ITU-T L.1410 (2014), *Methodology for environmental life cycle assessments of information and communication technology goods, networks and services*.

[b-ITU-T X.501] Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *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 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Authentication framework*.

[b-ITU-T X.1254] ITU-T X.1254 (2020), *Entity authentication assurance framework*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management*.

[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-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT Security and Privacy – A frame work for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information Technology – Security techniques – Entity authentication assurance framework*.

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). *Trust frameworks for identity systems*, White paper, Trust framework series. London: Open Identity Exchange. 18 pp. Available [viewed 2021-05-17] at: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [Untitled], Decentralized identifiers (DIDs) … Cambridge, MA: World Wide Web Consortium. Ayailable [viewed 2021-05-15] at: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases*. Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-17] at: http://www.w3.org/TR/vc-use-cases/

ITU-T 系列建议书

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦