



联合国国际贸易法委员会  
第四工作组（电子商务）  
第五十五届会议  
2017年4月24日至28日，纽约

与身份管理和信任服务有关的法律问题

与身份管理和信任服务有关的术语和概念

秘书处的说明

目录

	页次
一. 导言.....	2
二. 与身份管理和信任服务有关的术语和概念.....	3
A. 与身份管理有关的定义.....	3
B. 与信任服务有关的定义.....	7



## 一. 导言

1. 委员会在 2015 年第四十八届会议上指示秘书处就身份管理和信任服务、云计算和移动商务进行准备工作，包括为此举办学术讨论会和专家组会议，以便今后在关于电子可转让记录的目前工作完成之后在工作组级别进行讨论。委员会还请秘书处向第四工作组呈报这一准备工作的成果，以期征求关于准确范围、可能方法和优先事项的建议，供委员会第四十九届会议审议。<sup>1</sup>
2. 委员会 2016 年第四十九届会议收到了秘书处关于与身份管理和信任服务有关的法律问题的说明 (A/CN.9/891)，其中概述了 2016 年 4 月 21 日和 22 日在维也纳举行的贸易法委员会关于身份管理和信任服务所涉法律问题专题讨论会期间的讨论情况以及其他补充材料。委员会还获知，根据委员会 2015 年第四十八届会议上提交的一项建议 (A/CN.9/856)，<sup>2</sup>已经在专家一级启动关于云计算所涉合同问题的工作。
3. 在第五十四届会议上 (2016 年 10 月 31 日至 11 月 4 日，维也纳)，工作组一致认为，今后在身份管理和信任服务方面的工作应当限于为商业目的而使用身份管理系统，这一工作不应考虑身份管理服务供应商的私营或公营性质。工作组还一致认为，虽然身份管理方面的工作可以先于信任服务方面的工作进行，但鉴于身份管理和信任服务这两者之间关系密切，应当同时对这两方面的相关术语加以确定和定义。还一致认为，侧重点应当是多方身份系统以及自然人和法人，但不排除酌情对两方身份系统以及实体对象和数字对象进行审议。此外，会议一致认为，工作组应当为继续开展工作而进一步明确项目目标，具体指明项目范围，确定所适用的一般原则，并拟订必要的定义 (A/CN.9/897，第 118-120，122 段)。
4. 本说明载有与身份管理和信任服务有关的一些术语的定义。提出这些术语是为了能够基于对基本概念的共同理解进行讨论，而不是为了提议就这些概念具有法律约束力的定义进行讨论。同样，这些术语并非意在表明贸易法委员会在身份管理和信任服务领域今后工作的范围。
5. 关于所界定术语的来源，凡有出处的都明确注明。由于来源不同，同一术语可能包括不止一个定义。未指明来源的术语是在专家协商期间提出的。国际上已作定义的术语优先考虑。所界定术语可出自其他来源，尤其是国内来源。
6. 所界定术语列于不同部分只是为了便于编排而已，不影响工作组就这些术语对身份管理或信任服务所涉法律问题讨论的相关性作出决定。
7. 所界定术语各有渊源，故此不应将其解读为一套相互关联的统一术语。相反，每一术语均应看作自成体系的定义单独解读，从而为工作组讨论提出一种可供参照的定义。所界定术语可查到的来源都作了注明，以便从原始来源文件收集进一步信息。
8. 同义词仅为方便使用而列出。并非所有同义词都是本说明界定的术语。

<sup>1</sup> 《大会正式记录，第七十届会议，补编第 17 号》(A/70/17)，第 358 段。

<sup>2</sup> 同上，《第七十一届会议，补编第 17 号》(A/71/17)，第 229 段。

9. 术语按本说明英文文本字母顺序列出。其他语文文本保持同样顺序，以确保段落对应，从而便于工作组讨论期间查找。

## 二. 与身份管理和信任服务有关的术语和概念

### A. 与身份管理有关的定义

10. “保证水平”指对实体和所介绍的身份信息之间关联性的置信程度。来源：Rec. ITU-T X.1252。同义词：身份保证。

11. “属性”指与主体关联的一条信息或数据。属性的例子包括诸如姓名、地址、年龄、头衔、工资、净值、驾照号码、社保号、电邮地址、移动电话号码之类信息，以及诸如主体的网络存在、主体所使用的设备、网络所知悉的主体惯常住宅所在地之类数据，等等（对人而言）；公司名称、主要办公地址、注册名称、注册管辖地，等等（对法律实体而言）；牌号和型号、序号、所在地、性能、设备类型，等等（对设备而言）。同义词：身份属性。

12. “属性提供方”指作为主体身份一项或多项属性来源行事的企业或政府实体。属性提供人通常是负责分配、收集或保持此种属性的实体。属性提供人的例子包括保持出生登记处或头衔登记处的政府机构、征信所、保持商业营销数据库或公司登记处的企业，以及诸如移动电话运营商、银行、公共事业和保健提供人之类持有经核证的用户数据并且（可能且须经客户同意）验证这些属性或者向第三方提供这些数据的实体。

13. “认证”指(a)对实体与所介绍身份之间关联性实现充足信任的过程。来源：Rec. ITU-T X.1252；(b)使主体的声称身份与实际主体相关联的过程，或是直接确认主体与一证书的关联（“主动认证”），或是通过主体正在互动的环境确认主体与一证书的关联（“被动认证”或“适应性认证”）。例如，输入与一用户名关联的秘密口令，即可假定认证输入该秘密口令的个人系被签发该口令之人。同样，将出示护照的人与该护照上出现的照片比对就是用来认证（即确认）该人系护照上所描述之人。

14. “认证保证”指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。来源：Rec. ITU-T X.1252。注：在有些情况下，“身份保证”和“认证保证”概念被视为“保证水平”总体概念的单独组成部分。

15. “认证因素”指用以认证或验证实体身份的一条信息和过程。来源：ISO/IEC 19790。注：认证因素分四类：(a)实体拥有内容（如设备签名、护照、含证书的硬件设备、私钥等）；(b)实体所知内容（如口令、密码等）；(c)实体本身（如生物识别特征等）；或(d)实体一般可为（如行为模式等）。来源：Rec. ITU-T X.1254。

16. “认证元素”指用以验证主体与证书关系的元素。主动认证元素通常是主体所知内容（如秘密口令）、主体拥有内容（如智能卡）或主体本身（如照片或生物识别信息），并用以捆绑主体和身份证书。例如，口令起着用户名验证元素作用，照片起着护照或驾照验证元素的作用。被动认证元素通常是环境所知内容，例如，

移动网络知道用户与网络相连、用户处于惯常位置、用户正在使用移动设备、用户未被禁止使用网络，等等。

17. “权威来源”指被公认为准确和及时信息来源的数字贮存器。来源：Rec. ITU-T X.1254。

18. “授权”指(a)基于通常由依赖方确定的标准将权利和特权准予经认证主体的过程。例如，一旦主体经过认证，该人即可被准予进入某一保密数据库。来源：A/CN.9/WG.IV/WP.120，附件；(b)授予权利，并根据这些权利准予接入。来源：Rec. ITU-T Y.2720 和 Rec. ITU-T X.800。

19. “证书”指：(a)作为声称身份和/或权利的证明而出示的一组数据。来源：Rec. ITU-T X.1252；(b)作为主体声称身份的证明而出示的数字形式或有形形式的数据。纸介证书的例子包括护照、出生证、驾照、雇员身份卡等。数字证书的例子包括用户名、智能卡、移动身份和数字证书等。来源：A/CN.9/WG.IV/WP.120，附件。同义词：电子身份识别手段、身份证书。

20. “证书提供方”或“证书服务提供方”指(a)向主体发布证书的实体；(b)发布和/或管理证书的可靠参与方。注：证书服务提供方（CSP）可包括注册机构（RAs）和其营运的验证方。证书服务提供方可以是独立第三方，也可发布自用证书。来源：Rec. ITU-T X.1254。

21. “吸纳”指(a)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。来源：Rec. ITU-T X.1252；(b)证书提供方（或其代理）在向主体发布证书之前验证该主体身份主张的过程。

22. “实体”指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。来源：Rec. ITU-T X.1252。一实体可有多个标识符。

23. “联邦”指(a)用户、服务提供方和身份服务提供方的关联。来源：Rec. ITU-T X.1252；(b)身份提供方、依赖方、主体和其他各方的组合，其同意根据系统规则（或信任框架）中具体规定的兼容政策、准则和技术运营，以使身份提供方提供的主体身份信息能够为依赖方理解和信任。同义词：身份联邦、多方身份系统。

24. “身份识别”指在特定环境下收集、验证并核证一特定主体的充足身份属性以确定并确认其身份的过程。同义词：身份证明、注册。

25. “标识符”指(a)用来在语境中识别实体的一个或多个属性。来源：Rec. ITU-T X.1252。(b)用来在具体情境中以独特方式描述一实体特征的一个或多个属性。来源：Rec. ITU-T X.1254。

26. “身份”指(a)与实体相关的一系列属性。来源：ISO/IEC 24760；(b)关于特定主体的信息，以一个或多个属性的形式允许在特定情况下充分区分主体；(c)在特定环境下以独特方式描述某人的一系列属性。同义词：数字身份。

27. “身份主张”指源自身份提供方并发给依赖方，其中包含主体标识符（如姓名、帐号、手机号码、所在地等）、认证状态以及适用的身份属性的电子记录。属性一般是依赖方要求提供的关于交易所涉主体的个人和非个人信息。
28. “身份保证”指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。来源：Rec. ITU-T X.1252。同义词：保证水平。注：在有些情况下，“身份保证”和“认证保证”概念被视为“保证水平”总体概念的单独组成部分。
29. “身份联邦”指身份提供方、依赖方、主体和其他各方的组合，其同意根据系统规则（或信任框架）中具体规定的兼容政策、准则和技术运营，以使身份提供方提供的主体身份信息能够为依赖方理解和信任。另见：联邦、多方身份系统。
30. “身份管理”指(a)用以在网上环境中管理个人、法律实体、设备或其他主体的身份识别、认证和授权的一套程序。来源：A/CN.9/854，第6段；(b)用于(一)保证身份信息（如标识符、证书、属性）；(二)保证实体身份；以及(三)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）。来源：Rec. ITU-T Y.2720。
31. “身份证明”指(a)指在特定环境下收集、验证并核证一特定主体（个人、法律实体、设备、数字对象或其他实体）的充足身份属性信息以确定并确认其身份的过程。可以通过自我主张或者根据现有记录进行身份证明；(b)证书颁发方向证书应用实体证实充足信息的过程。来源：Rec. ITU-T X.1252。(c)注册机构(RA)为证实一实体具有规定或认可的保证等级而捕获和确认足够信息的过程。来源：Rec. ITU-T X.1254。同义词：身份识别、注册。
32. “身份提供方”指(a)负责确定个人、法律实体、设备和（或）数字对象的身份，签发相应身份证书并维护和管理主体的此类身份信息的实体。来源：A/CN.9/WG.IV/WP.120，附件；(b)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。来源：Rec. ITU-T Y.2720。同义词：证书服务提供方、身份服务提供方。
33. “身份系统”指由一套系统规则（又称信任框架）加以规范的身份管理交易的网上环境，在这种环境中，个人、组织、服务机构和设备由于权威来源确定并认证其身份而能够彼此信任。来源：A/CN.9/WG.IV/WP.120，附件。身份系统涉及以下方面：(a)一套规则、方法、程序和惯例、技术、准则、政策、过程，(b)适用于一组参与实体，(c)对收集、验证、存储、交换、认证以及依赖关于个人、法律实体、设备或数字对象的身份属性信息进行规范，(d)目的是便利身份交易。同义词：身份管理系统（“IdM系统”）、身份联邦、电子身份识别方案。
34. “身份交易”指涉及两个或多个参与方参与身份信息确定、验证、发布、主张、吊销、发送或依赖的任何交易。
35. “身份认证”指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。来源：Rec. ITU-T X.1252。
36. “保证等级”指指定对身份识别和认证过程的信任程度——即(a)对用以确定被签发证书实体的身份的调查过程的置信程度，和(b)对使用某一证书的实体系统

签发该证书的实体的置信程度。保证反映了所使用方法、程序和技术可靠性。保证方案的一些等级以数字界定保证等级，即等级 1 至 4，等级 1 是最低保证等级，等级 4 是最高等级。其他方案以“低”、“中”、“高”指定保证等级。同义词：身份保证、信任等级。

37. “多因素认证”指通过至少两个独立认证因素进行的认证。注：认证因素分四类：(a)实体拥有内容(如设备签名、护照、含证书的硬件设备、私钥等)；(b)实体所知内容(如口令、密码等)；(c)实体本身(如生物识别特征等)；或(d)实体一般可为(如行为模式等)。来源：ISO/IEC 19790；Rec. ITU-T X.1254。

38. “多方身份系统”指主体可使用若干身份提供方中任何一方签发的身份证书对多个不相关依赖方进行认证的身份系统，又称身份联邦；一种允许一个或多个身份提供方与多个依赖方使用所签发的身份证书以及所主张的身份信息的身份系统。来源：A/CN.9/WG.IV/WP.120，附件。同义词：身份联邦。

39. “参与方”指参与身份系统或参与使用此种系统的身份交易的任何个人或法律实体。参与方包括主体、身份提供方、属性提供方、证书提供方、依赖方、身份系统运营人及其他方。与信用卡系统参与方一样，身份系统参与方一般以合同形式约定对其作用适用一套系统规则(常称之为信任框架)。

40. “证明”指在吸纳新的实体进入身份系统时验证或核实信息。来源：Rec. ITU-T X.1252。同义词：身份证明、身份识别。

41. “假名”指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。来源：Rec. ITU-T X.1252。

42. “注册”指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。来源：Rec. ITU-T X.1252。

43. “注册机构”指在联邦(即多方)身份系统的环境中，通常为身份提供方提供吸纳和/或身份证明服务的实体。

44. “依赖方”指(a)依赖身份证书或身份主张就特定应用情况下可采取什么行动——如处理一项交易或准予访问信息或系统——作出决定的个人或法律实体。来源：A/CN.9/WG.IV/WP.120，附件；(b)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。来源：Rec. ITU-T X.1252；(c)依赖于电子身份识别或信任服务的自然人或法人。来源：欧洲议会和欧盟理事会 2014 年 7 月 23 日关于内部市场电子交易的电子身份识别和信任服务的第 910/2014 号条例(欧盟)(eIDAS)，第 3(6)条，该条例撤销第 1999/93/EC 号指令。

45. “存储库”指接受数字实体交存的接口，有助于保留数字实体并通过其识别符安全获取数字实体。来源：Rec. ITU-T X.1255。

46. “角色”指身份系统参与方的类型(或种类)，如主体、身份提供方、证书提供方、依赖方，等等。一个参与方可有多个角色。例如，在对其员工的身份识别方面，雇主既可以是身份提供方也可以是依赖方。

47. “自称身份”指由实体本身自称的身份。来源：Rec. ITU-T X.1252。

48. “主体”指其身份在特定身份证书中确定并可由身份提供方认证和保证的个人、法律实体、设备或数字对象（即实体）。来源：A/CN.9/WG.IV/WP.120，附件。同义词：用户、数据主体。

49. “系统规则”：见“信任框架”。

50. “信任”指在一定语境内，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。来源：Rec. ITU-T X.1252。

51. “信任框架”指(a)针对身份系统的系统规则，包含对参与和运作特定身份系统进行规范的商业、技术和法律规则。此类规则往往由私人制定（如特定身份系统的身份系统运营人），并通过合同而对各参与方具有约束力和可执行性。来源：A/CN.9/WG.IV/WP.120，附件；(b)供交换身份信息各方使用的一系列要求和执行机制。来源：Rec. ITU-T X.1254；(c)一种 IdM 系统，在该系统中，一项交易所涉不同各方的每一方都向其交易对手做出一系列可核实的承诺，这些承诺需要包括：(一)有助于确保承诺得到实现的控制机制以及(二)不履行这些承诺的补救措施。来源：Rec. ITU-T X.1255。同义词：系统规则、运行规则、方案规则。

52. “信任框架提供方”指为特定身份系统创建或采用系统规则和关联合同框架的实体或组织。信任框架提供方还可验证遵守这些系统规则的参与方。例如，信用卡和借记卡发放人可在信用卡和借记卡使用圈内发挥类似作用；它们负责系统规则的制定和遵守。

53. “可信赖第三方”指(a)其他活动方面（例如与安全相关的活动）可为其他参与方所信任的机构或其代理。来源：Rec. ITU-T X.1254；(b)为交易各方接受、可充当公正、可信赖的中间人促进各方之间互动的实体。

54. “用户”指(a)证书的主体；依赖方所提供服务的客户；(b)使用如系统、设备、终端、流程、应用或公司网络等资源的实体。来源：Rec. ITU-T X.1252。

55. “核证”指验证并确认身份证书有效的过程（例如，证书未过期或者未被吊销）。

56. “验证”指(a)通过将提供的信息与过去确证的信息进行比较的信息检验过程。来源：Rec. ITU-T X.1254；(b)确认声称实体的过程或实例。注：（身份）验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。来源：Rec. ITU-T X.1252。

## B. 与信任服务有关的定义

57. 以下定义可能与信任服务所涉法律问题的讨论具体相关。不过，身份管理所涉法律问题的讨论中列出的相关定义可能也有一些与信任服务所涉法律问题的讨论有关（见上文第 6 段）。

58. “验证服务商”指签发证书和可能提供与电子签名有关的其他服务的人。来源：《贸易法委员会电子签名示范法》第 2 条(e)项。<sup>3</sup>

<sup>3</sup> 联合国出版物，出售品编号：E.02.V.8。

59. “电子登记交付服务”指使得能够通过电子手段在第三方之间传输数据并提供与处理被传输数据相关证据的服务，这种服务保护被传输数据免于丢失、盗窃、损毁或任何未经授权更改的风险。来源：eIDAS，第 3(36)条。
60. “电子印章”指附于电子形式的其他数据或与之有逻辑联系，以确保这些其他数据的来源和完整性的电子形式数据。来源：eIDAS，第 3(25)条。
61. “电子签名”指(a)附于电子形式的其他数据或与之有逻辑联系，并由签名人用以签署的电子形式数据。来源：eIDAS，第 3(30)条；(b)在数据电文中，以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息。来源：《贸易法委员会电子签名示范法》第 2 条(a)项。注：《联合国国际合同使用电子通信公约》(2005 年，纽约)<sup>4</sup>第 9 条第(3)款(a)项提及表明签名人对电子通信所含信息的意图。
62. “电子时戳”指将电子形式的其他数据与某一特定时间相关联，从而确立可证明这些特定数据在该时间存在的证据的电子形式数据。来源：eIDAS，第 3(33)条。
63. “依赖方”指可能根据某一证书或电子签名行事的人。来源：《贸易法委员会电子签名示范法》第 2 条(f)项。
64. “信任服务”指(通常为付酬而提供的)一种电子服务，其中包括：(a)电子签名、电子印章或电子时戳、电子登记交付服务以及与这些服务有关的证书的创建、验证和核证，或者(b)网站认证证书的创建、验证和核证；或者(c)电子签名、电子印章或者与这些服务有关的证书的保全。来源：eIDAS，第 3(16)条。
65. “信任服务提供方”指[作为合格或不合格信任服务提供方]提供一项或多项信任服务的自然人或法人。来源：eIDAS，第 3(19)条。
66. “时戳”指代表与共同参考相关的时间点的可靠时间变量参数。来源：Rec. ITU-T X.1254。
67. “核证”指核实和确认电子签名或印章有效的过程。来源：eIDAS，第 3(41)条。

---

<sup>4</sup> 大会第 60/21 号决议，附件。