联合国 A/CN.9/WG.IV/WP.153

大 会

Distr.: Limited
6 September 2018
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十七届会议
2018 年 11 月 19 日至 23 日，维也纳

目录

V.18-05867 (C) 260918 260918

一. 导言

1. 本说明介绍了工作组所确定的同审议身份管理和信任服务相关法律问题有关的若干专题的某些方面（A/CN.9/936，第 58 段），以便利进一步讨论。它尤其力求着重说明某些关键问题并就可能的解决办法提出建议，而无意限制审议更多专题或酌情一并审议某些专题的可能性。A/CN.9/WG.IV/WP.154 号工作文件介绍了由工作组确定的事关其审议身份管理和信任服务相关法律问题的其他专题的某些方面。

2. 关于身份管理和信任服务相关法律问题工作组工作情况的背景资料见 A/CN.9/WG.IV/WP.152 号工作文件，第 6-17 段。更多相关文件的清单见 A/CN.9/WG.IV/WP.152 号工作文件，第 18 段。

二. 身份管理和信任服务所涉法律问题今后工作的相关问题

A. 工作范围

3. 依照工作组的建议，委员会请工作组开展关于身份管理和信任服务所涉法律问题的工作，以期编拟一份促进跨境承认身份管理和信任服务的案文。委员会所提请求的措辞足够宽泛，除了已经确定的方面外，还可包括在法律上对待身份管理和信任服务的各个方面（见上文，第 1 段）。

4. 身份管理和信任服务跨境承认法律机制是数字经济扶持性法律框架的一个基本组成部分，缺乏这些机制可能促成数字鸿沟进一步扩大。因此，工作组似宜考虑其工作对处理数字鸿沟问题所产生的更广泛影响。

5. 在这方面，工作组似宜考虑，缺乏扶持利用身份管理和信任服务的国内法律框架是否会对身份管理和信任服务的跨境法律承认构成挑战。在这种情况下，工作组似宜确定为充分实现对身份管理和信任服务的跨境法律承认而应在国内立法中颁布的法律条文，并讨论最适合实现该目标的法律文本的类型（如条约、示范法或对两者兼容并蓄）。

6. 而且，对身份的跨境法律承认与对各类身份管理系统的身份的法律承认有着共同的要素，而不论其外国要素如何。因此，工作组似宜考虑是否应讨论酌情顾及外国要素的允许在法律上承认各类身份管理系统的机制问题。在这种情况下，工作组的工作成果可以在国家和国际层面上就身份管理问题提供指导。

1. 基础身份和交易身份

7. 工作组似宜回顾，有人建议对主要身份确定和次级身份确定加以区分（A/CN.9/WG.IV/WP.149，第 29 段）。

8. 主要身份确定或者说基础身份确定涉及实体产生背景及其产生时间的身份归属问题。基础身份因而通常独一无二并且无可替代。主要身份确定的实例包括:政府在民事登记和生命统计记录中登记自然人；有关主管机构在例如注册商业公司登记处等专门登记处对法人进行登记；以及将数字对象标识符归属于数字对象。

9. 次级身份确定，或交易身份，是指使用身份来履行特定的功能（例如，签订合

同；由自动柜员机分发现金；由公共机构颁发证书）。

10. 虽然基础身份可能不常用于商业交易，但身份提供者可以使用它来建立交易身份。例如，贸易法委员会关于电子签名的规定要求识别签名人的身份。在某些情况下，对签名人身份的可靠识别可能基于身份证书的使用和基于基础身份证书确立身份的认证过程。因此，对基础身份的跨境和跨身份管理系统的法律承认可能是有用的，或甚至是必要的。

2. 相关实体

11. 工作组就同其工作有关的各类实体也就是说其工作成果所可适用的实体展开了初步讨论（A/CN.9/936，第 63-65 段）。参与贸易包括跨境贸易的自然人和法人的相关性得到普遍承认。没有明确的法人资格但与商业活动有关的实体也可以考虑在内。例如，在最不发达国家非正规部门经营的贸易商可以使用移动身份作为他们的主要身份识别手段。

12. 鉴于诸如海关业务跨境单一窗口等某些企业对政府交易和政府对政府交易在国际贸易上的相关性，公共实体的参与可能是合理的。工作组似宜考虑公共实体参与身份管理和信任服务是否会引起一些具体问题，同时特别铭记技术中性原则的适用（见下文，第 38-40 段）、当事人意思自治（见下文，第 41-47 段）及电子身份识别手段与所追求的功能的相称性（见下文，第 46 段）。

13. 对于识别实物和数字物体是否属于这项工作的范围，人们表达了不同的观点。一种观点认为，应当将实物和数字物体排除在外，因为它们不具有法人资格，不能自行承担责任。然而，也有一种观点认为，身份识别不需要自主法人资格，也不需要对被识别物体追究责任（A/CN.9/936，第 64 段）。

14. 另一种观点认为，可以在工作组处理完人的身份识别问题之后再考虑识别物体的问题（A/CN.9/936，第 65 段）。在这方面，应当指出的是，根据“物联网”模型，物体是大数据的主要来源，在该模型下，数据的可靠归属可能具有特别的相关性。例如，医疗设备被越来越多地用于在日常活动中远程监控患者的状况。确保由这些设备生成的信息属于正确的患者是至关重要的。同样，对于药品不仅在使用时而且在整个生产周期过程中都需要加以追踪，目的是确保对药品进行适当的识别，并保证其来源和内容。对药物及其成分加以可靠识别同样是至关重要的。

B. 定义

15. 关于可能有助于委员会审议的有关身份管理和信任服务的术语和概念清单，工作组似宜参考 A/CN.9/WG.IV/WP.150 号文件。该清单并不妨碍工作组按照工作的进展对相关术语的定义展开审议。

16. 关于身份管理和信任服务，载于 A/CN.9/WG.IV/WP.150 号文件的下述定义可能特别有助于工作组审议本说明提出的问题。

17. “身份”指(a)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；(b)在特定情况下以独特方式描述某人的一系列属性（A/CN.9/WG.IV/WP.150。第 31 段）。

18. 工作组似宜审议这些定义与基础身份和交易身份的概念之间的关系（见上文，第 7-10 段）以及这些概念同其今后工作的相关性。在这方面，工作组似宜澄清唯一性是否是基础身份的一种属性。

19. “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（A/CN.9/WG.IV/WP.150，第 35 段）。

20. “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（A/CN.9/WG.IV/WP.150，第 38 段）。

21. “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、签发、主张、吊销、发送或依赖的任何交易（A/CN.9/WG.IV/WP.150，第 39 段）。

22. 工作组似宜参照“身份管理”、“身份系统”和“身份交易”的概念，以澄清其关于身份管理法律承认的工作是否应参照身份系统或身份交易或对这两者一并参照（见下文，第 57-59 段）。

23. “保证等级”指指定对身份识别和认证过程的信任度——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被签发该证书的实体的置信程度。保证反映了所使用方法、程序和技术的可靠性（A/CN.9/WG.IV/WP.150，第 42 段）。

24. 工作组在讨论该专题时不妨参照“保证等级”的定义（见 A/CN.9/WG.IV/WP.154，第 10-19 段）。工作组为此还似宜考虑到“保证等级”的下述定义：“对实体与所显示的身份信息之间关联性的置信程度”（A/CN.9/WG.IV/WP.150，第 12 段）以及对该定义所做的这样的说明，即解释“身份保证”和“认证保证”的概念可被视为“保证等级”总体概念的独立组成部分。

C. 一般原则

25. 工作组为此确定了同其在身份管理和信任服务所涉法律方面工作有关的以下一般原则：不歧视使用电子手段；功能等同；技术中性；和当事人意思自治（A/CN.9/936，第 67 段）。

1. 不歧视使用电子手段

26. 将不歧视使用电子手段的原则放在贸易法委员会的文本中是很合适的。在身份管理和信任服务情况下该原则可被表述为：[1]

> 在通过使用身份[证书][管理系统]和信任服务进行身份验证时，不得仅以这些身份[证书][管理系统]和信任服务是电子形式为由而否认其法律效力、有效性或可执行性。

[1] 插入条文草案仅为举例说明，绝不妨碍工作组就其工作的可能形式向委员会提出建议，也不妨碍委员会就该形式作出决定。

27. 条文草案包含了在“身份证书”和“身份管理系统”之间的选择，如何选择取决于在身份识别方面究竟是应参照使用证书，还是应参照使用整个身份管理和信任服务系统（见下文，第 57-59 段）。

2. 功能等同

28. 在电子商务领域，功能等同原则确立了为行使与纸质概念相同的功能电子记录、方法或流程所必须满足的要求。

(a) 身份管理

29. 身份管理方面的一个可能的功能等同规则可以被理解为：

> 在法律要求或允许识别实体的情况下，如果使用可靠方法[以核实实体的[相关]属性]，则应满足在[电子][数字]身份管理方面的这一要求。

30. 功能等同条文在身份识别上的预期效果是，将适用于纸质身份识别的身份识别要求转用于电子环境。工作组似宜考虑插入“[相关]”一词，以表明只有为离线身份识别所要求的那些属性才是成功实现在线身份识别所必需的。工作组还似宜澄清是否应参照“电子身份”或“数字身份”。

31. 可就确定方法可靠性的相关要素提供进一步指导，包括：(a)合同协议，如果为适用法律所允许的话；(b)第三方认证和自我认证；及(c)参照保证等级。在功能等同条文中参照使用“可靠方法”可能要求使用在在线和离线识别中提供同等可靠性的方法。

32. 有关身份管理功能等同规则的讨论可获益于对利用身份管理的案例的参照。在这方面应当指出的是，可能需为不同目的或功能而进行身份识别。一个目的是遵守法规。这类要求的实例是，在金融、电信和其他商业部门以及在电子采购领域使用“了解你客户”的规则，因为在这些领域，正确识别潜在的供应商和客户的身份是防止欺诈和串通及实施禁令的必要条件。

33. 进行识别的另一目的是确定商业文件的有效性。举例说，适用于提单的法律可能要求确定某些当事人的身份。《联合国海上货物运输公约》（1978 年，汉堡规则）（《汉堡规则》）[2]第 15 条和《联合国全程或部分海上国际货物运输合同公约》（2008 年，纽约）（《鹿特丹规则》）[3]第 36 条即有此规定。

34. 而且，网上交易当事人可商定使用某些程序和方法在没有任何法律要求的情况下为风险管理目的准确识别彼此的身份。识别义务以合同为依据。

35. 在离线识别虽获使用但并非完全令人满意的情况下，可做出有关采纳更高识别标准的政策性决定，以更好落实识别义务。工作组似宜考虑以下两者之间的互动关系：即采纳有关识别的功能等同规定与视可能对在线识别提出较之于离线识别的适用要求更为严格的要求。

---

[2] 联合国，《条约汇编》，第 1695 卷，第 29215 号，第 3 页。

[3] 大会第 63/122 号决议，附件。

(b) 信任服务

36. 贸易法委员会的文本载有针对某些信任服务的功能等同规则，即针对电子签名的《贸易法委员会电子商务示范法》（《电子商务示范法》）[4]第七条、《贸易法委员会电子签名示范法》（《电子签名示范法》）[5]第六条和《联合国国际合同使用电子通信公约》（2005 年，纽约）（《电子通信公约》）[6]第九条第三款和《贸易法委员会电子可转让记录示范法》[7]第九条以及针对保存和存档的《电子商务示范法》第十条。工作组似宜考虑是否应当就各类信任服务的产出编拟专门规定，或是否能够或应当草拟一条功能等同一般规则（见 A/CN.9/WG.IV/WP.154，第 58 段）。

37. 工作组还似宜考虑是否应当有一条关于确定身份信息归属的规定，或有一条功能等同的规则是否便已足够，其原因是，身份信息将被确定为属于相同实体，一如在离线环境下，并且无论如何都不应被认为属于身份服务提供商。《电子商务示范法》第 13 条提供了处理归属问题的规定的范例。

3. 技术中性

38. 技术中性原则是贸易法委员会文本以及处理电子通信使用问题的许多其他立法文本的基石。在身份管理和信任服务的背景下，可能有必要参照系统特点而并非具体技术提供关于最低系统要求的指导（A/CN.9/936，第 69 段）。或者，如果选择交易做法（见下文，第 57-59 段），可能需要参照交易特点就最低身份交易要求提供指导。在信任服务背景下，技术中性原则的执行可能要求确定各项信任服务所应当实现的具体目标，同时没有强行规定实现这些目标究竟应当使用哪一项特定技术。

39. 一项关于平等对待身份管理和信任服务技术、方法和系统的条款可以被理解为：

> 本[文书草案]的适用概不排除、限制或剥夺可用于满足本文书草案所述要求[，或以其他方式符合适用法律要求的]关于身份管理和信任服务的任何[技术、方法或系统]的法律效力。

40. 见于《电子商务示范法》第三条中的“或符合适用法律的要求”一语指的是，文书草案以外的法律在某些确定的情况下，可能会规定使用有别于文书草案所述的要求。[8]

4. 当事人意思自治

41. 当事人意思自治原则所造成的一个后果是，身份和信任服务的使用是可选的。虽然这一原则可能完全适用于商业服务，但由于政策原因，在获得公共实体提供的服务或与这些实体互动方面，这一原则的适用可能会受到限制。

---

[4] 联合国出版物，出售品编号：E.99.V.4。

[5] 联合国出版物，出售品编号：E.02.V.8。

[6] 联合国，《条约汇编》，第 2898 卷，

[7] 联合国出版物，出售品编号：E.17.V.5。

[8] 《贸易法委员会电子签名示范法》及其颁布指南，（联合国出版物，出售品编号：E.02.V.8），第 107 段。

42. 关于对身份和信任服务的使用可供选择的一条可能规定的内容如下：

1. 本[文书草案]概不要求某一实体在未经该实体同意的情况下使用或接受身份[证书][管理系统]和信任服务。

2. 某一实体同意使用身份[证书][管理系统]和信任服务可以从该实体的行为[和其他情况中推断出来]。

[第 1 款不适用于……]

43. 条文草案包含了在“身份证书”和“身份管理系统”之间的选择，如何选择取决于在身份识别方面究竟是应参照使用证书，还是应参照使用整个身份管理系统（还见下文，第 57-59 段）。

44. 在该条文草案第 2 款中，插入“[和其他情况]”一词，以指实体不能自主行为的情况（例如，实物或数字物体）。在这些情况下，不得认为同意来自于该实体，而是应认为来自于控制该实体的自然人或法人。

45. 当事人意思自治原则的适用受制于强制性法律所述限制（A/CN.9/936，第 72 段）。这些限制之所以特别重要，是因为对身份管理和信任服务的使用所满足的立法要求往往是强制性的。有鉴于此，建议根据《电子商务示范法》第五条制定该项原则：

本[文书草案]的规定可经由协议加以删减或改变其效力，除非根据适用法律，该协议无效或不产生效力。

46. 当事人意思自治原则的另一种适用涉及选择更适合当事人履行职能的身份和信任服务的自由（所谓的“相称原则”）。服务类型的选择自由也与技术中性原则密切相关。

47. 当事人意思自治原则还旨在支持诸如身份管理系统的规则与信任服务系统的规则和框架之类合同协议的可执行性。因此，在身份管理系统联邦的背景下，系统规则可能特别具有相关性（见 A/CN.9/WG.IV/WP.154，第 39 段）。“身份联邦”的在用定义是指身份提供方、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所理解和信任（A/CN.9/WG.IV/WP.150，第 28 段）。

5. 识别义务

48. 贸易法委员会在电子商务上的各项文本所共有的另一项一般原则涉及例如通常适用于商业交易的法律等实体法不受影响的事实。

49. 就身份管理和信任服务而言，这项原则要求关于身份管理的立法不应该引入任何新的识别义务，关于信任服务的立法不应该引入使用任何特定类型信任服务的任何新的义务，而且现有的义务应该仍然不受影响。

50. 可以按照如下措词拟定一项条文：

[文书草案]概不要求某一当事人[核实][识别]另一实体的[身份]或使用信任服务。

6. 统一解释

51. 贸易法委员会的文本通常载有提及其统一来源和进行统一解释义务的条文。这项条文旨在确保在统一解释和适用立法案文时保持统一。

52. 可以按照如下措词拟定一项条文：

> 1. 在解释本[文书草案]时，应考虑到其国际性和促进其适用的统一以及在国际贸易中遵守诚信的需要。
>
> 2. 涉及本[文书草案]所管辖事项的问题，未在本文书草案中明确解决的，应当按照本文书草案所依据的一般原则加以解决，在无此种原则时，应当按照国际私法规则指定的适用法律加以解决。

53. 在条文草案第二段中，提及“根据国际私法规则适用的法律”在跨境情况下可能特别有用。

D. 法律承认要求和机制

54. 总的来说，可以将法律承认理解为界定了在某一法域获得法律地位所必须满足的要求。对在国内层面上给予法律承认可能需要制定实体规则。

55. 可以将跨境法律承认理解为：(a)在接收法域给予与起始法域相同的法律地位；(b)给予与接收法域相同的法律地位，而不论有任何外国要素；或(c)在专门文书中界定法律承认的效力。而且，跨境法律承认可以是相互的，即对等的，也可以是单方面的。在这两种情况下，它都可能受到一些条件的制约。

56. 对身份管理方案和信任服务的法律承认是工作组工作的核心问题，应当在法律上实现身份证书和信任服务的互操作性以及身份和信任在身份管理方案之间的可移植性等技术特征。如上所述（第 6 段），对身份的跨境法律承认与对各类身份管理系统的身份的法律承认有着共同的要素，而不论其外国要素如何。

57. 法律承认的对象可以是身份管理和信任服务的系统和计划。在这种情况下，可能需要就这些系统和计划为取得法律承认而必须遵守的特征提供法律指导。因此，交易中使用的这些系统和计划的产出，即电子识别手段和特定的信任服务，也可以受益于法律承认。

58. 法律承认的对象也可以是获得身份管理和信任服务使用之便的交易。在这种情况下，可能需要就对身份证书和验证及信任服务的产出给予法律承认所应满足的条件提供法律指导。贸易法委员会关于电子商务的现有文本主要涉及交易事项。例如，《电子商务示范法》主要涉及对电子签名的交易性使用，仅部分涉及电子签名系统的特征。

59. 工作组似宜考虑其关于法律承认的工作是否应适用于身份管理与信任服务系统和方案及获得身份管理和信任服务之便的交易，或是否对两者一并适用。

60. 工作组还似宜考虑其工作是否应仅设想只有一种跨境法律承认机制，还是也应处理国内跨系统法律承认问题。

1. 身份管理问题

(a) 事先法律承认

61. 目前所可利用的有关身份管理方案的法律承认机制设想事先建立一份被承认身份管理方案的清单以及获列该清单所应满足的条件清单。该做法通常要求建立一个集中管理的评估和许可体制机制以评估身份管理方案。

62. 也可用于信任服务的这种做法，可以让究竟哪些方案和服务能够跨系统和跨境使用得以实现清晰和可预测性。然而，它可以拒绝对虽获使用但不在清单上的这些计划和服务给予法律承认。视其管理情况而定，它对发展的反应可能不会像技术进化所要求的那样快，从而可能阻碍创新，并可能导致强加一些技术特定要求。

63. 实施该做法所需体制机制要求确定成为评估实体的必要条件并界定以下方面的情况：身份管理方案评价标准及其更新机制、决策评价过程和筹资来源。根据包括先前存在的体制安排等一些因素，许可证制度的管理可能有些复杂并且成本高昂。

64. 而且，如果规模相对有限并在更广的经济一体化倡议框架内运作，集中管理的许可证制度可能会更有效，但如果在全球层面上实施，这类制度可能会带来挑战，因为这可能需要成员的高度合作。

65. 在全球层面采用集中管理的许可证制度可能需要通过一项条约或具有类似约束力的国际法文书。基于条约的机制的优点包括可预测性并有可能更容易适用于公共机构；其缺点涉及体制机制的建立和维护费用、就参与该方案收取费用以及争取足够多国家、计划和用户的支持的需要。基于条约的机制可能特别适合确保为长期财政义务供资，虽然仍有可能从用户手中收回成本。

66. 最近通过的专门的身份管理法律依靠集中监督来确认身份管理方案的法律效力。

67. 《电子身份识别和服务条例》[9]是专门处理身份管理跨境问题的唯一的一项法规。具体而言，《电子身份识别和服务条例》第 6 条允许欧盟某一成员国使用电子识别手段，在满足某些条件的前提下，获取另一个成员国公共部门机构在线提供的服务。其中一个条件是要求根据电子识别方案发布电子识别手段，该方案应通报欧盟委员会，并且应符合欧盟委员会规定的互操作性要求。同行审查即是通报过程的一部分。

68. 其他身份管理法律力图在不具体提及跨境问题的情况下处理身份管理问题。应当就此指出的是，虽然《电子身份识别和服务条例》并不影响现有的身份管理方案，而是力图实现这些计划之间的跨境相互法律承认，但是关于身份管理的国家法律给身份管理方案的运作创造了条件。

69. 贝宁第 2017-20 号法律载有关于身份管理的一条，涉及电子识别方案的保证等级、电子识别方案通报资格、违反安全规定、赔偿责任和互操作性。这些规定通常受到关于内部市场电子身份认证和电子交易信任服务条例相应条文的启发。

[9] 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电子身份识别和信任服务的第 910/2014 号条例（欧盟），该条例撤销第 1999/93/EC 号指令。

70. 弗吉尼亚电子身份管理法令[10]依赖于身份信任框架运营商如果符合若干监管和法定要求即可据以回避赔偿责任的某种机制（见 A/CN.9/WG.IV/WP.154，第 28-29 段）。关于法律效力，使用符合弗吉尼亚联邦、合同陈述和联邦规则所定标准的身份证书或身份属性即为满足《统一电子交易法》和《统一计算机信息交易法》所述关于商业上合理的安全或归属程序的任何要求。[11]

71. 佛蒙特州第 205-2018 号法令创建了一种称作个人信息保护公司的新型专用商业实体，负责管理个人信息，即为交易目的向第三方提供有关个人消费者的各项个人信息，并提供个人信息认证或验证服务。

72. 该法所声称的一个目标是，个人信息保护公司的运营应“是为消费者的根本利益并保护和造福于消费者”（第 2451 条第(3)款(B)节）。第 205-2018 号法令第 2452 条规定，个人信息保护公司在提供个人信息保护服务时负有对消费者的信托关系。

73. 佛蒙特州金融监管局对个人信息保护公司拥有监督权，该局可通过关于这些公司提交报告的时间和内容的规则。它还可以通过关于保护和保障个人信息以及与第三方交换信息的规则。

(b) 事先法律承认

74. 或者，法律承认可以经由通常允许交换和评估关于唯在发生争议时基于预先确定的标准使用身份管理方案和信任服务是否适宜的相关信息的机制而得以实现。贸易法委员会的文本遵行了这种做法，例如为此实施了所谓的“事后”可靠性测试（例如见《电子通信公约》第 9 条第 3 款）。

75. 这种做法的好处是，为交易各方提供了在选择技术和方法上的最大灵活性。而且，它不需要建立体制机制，从而避免产生相关费用，并且可以分散管理。另一方面，它的缺点是需要第三方裁决程序的干预来评估身份管理方案或信任服务是否适合跨境使用，而这种评价也可能成本高昂、耗时甚多，并给各当事方造成不确定性。

(c) 基于摸底调查的法律承认

76. 有一项建议提及按照共同模板摸底调查身份管理系统的可能性。开展摸底调查工作的法律要求及其效果都将由接收法域和身份管理系统界定。

77. 在开展摸底调查工作时，可参照对保证等级的通类说明来确保摸底调查以实效为基础，从而确保将适用技术中性原则。

78. 摸底调查工作将不依赖于中央主管机构的批准，而是可以由包括私人和商业实体等任何相关当事方进行。摸底调查工作的结果将发表在一份对外公开的受信任清单上。

79. 开展摸底调查工作时所应考虑的某些要素，可以是在《电子身份识别和服务条例》框架内运作的欧盟委员会第 2015/1502 号执行条例所确定的要素。这些要素是：

[10] 弗吉尼亚电子身份管理法，VA 代码 2.2-436-2.2-437 和 VA 代码 59.1-550-59.1-555。

[11] 2000 年和 2002 年修订的 1999 年《统一电子交易法》和 1999 年《统一计算机信息交易法》是美国全国统一州法专员会议编写的示范法。

登记、电子身份识别手段管理、认证以及管理和组织。每个要素包括几个次级要素。同样，工作组似宜审议是否以及在何种程度上可以提供关于摸底调查工作所应遵循的规格和程序的指导。

80. 一个实际例子可以说明摸底调查工作究竟是如何进行的。如上所述，“了解你的客户”是各种商业部门的常见要求。根据拟进行的交易，为满足“了解你的客户”的要求，通常使用符合“二级”或“高级”保证等级或“三级”或“实质性”保证等级的证书（关于对不同等级的保证的描述，见 A/CN.9/WG.IV/WP.154，第 13-14 段）。

81. 在身份管理方案没有正式的相互承认机制的情况下，使用另一法域签发的身份证书可能通常无法满足这些要求。对照有关保证等级的通用描述就证书展开摸底调查，就有可能核实身份证书可否满足在特定交易中为了解你的客户而需要的保证等级的要求。

82. 例如，身份系统运营商 A 可以提交一份认证书，证明其电子识别方案 X 符合保证等级 2 或更高的保证等级，并且其电子识别方案 Y 符合等级 3 或实质性等级，从而可以将电子识别方案 X 和 Y 插入受信任清单中。希望与金融机构 C 以电子方式开展业务的法人 B 可以根据交易的要求使用根据电子识别方案 X 或电子识别方案 Y 签发的证书。金融机构 C 可以对电子识别方案 X 和 Y 被插入受信任清单及相关保证等级加以核实，并由此接受根据这些电子识别方案而颁发的证书。

83. 如果国内法没有具体规定有关电子身份识别方案法律承认及其等同性的要求，上述例子也可在国别语境下予以适用。

84. 所设想的机制可以基于分别涉及插入受信任清单的先决条件和此种插入所产生之效果的两则条文。

85. 关于插入受信任清单的先决条件的可能条文的内容如下：

1. 如果身份管理和信任服务提供方打算着手提供其服务，他们则应向[……][监管机构]提交一份意向通知和一份认证书。

2. 该认证书应至少列入以下内容：

(a) 评估报告的类型；

(b) 评估实体的资格；

(c) 服务交付所用技术规范和格式，包括所参考的保证等级和消息传递标准。

3. [监管机构][……]应建立、保存和公布受信任清单，包括与身份管理和信任服务提供方及其所提供之服务有关的信息。

86. 工作组似宜考虑条文草案中的“认证”一词是否也可指自我认证，这可能适用于担保水平较低的服务（见 A/CN.9/WG.IV/WP.154，第 3-9 段）。

87. 该条文草案要求指定保存受信任清单的实体。如果建立了负责任的国家实体通知机制，该机制就可能是一个国家实体。

88. 关于插入受信任清单的法律效力，可以从《电子商务示范法》第十二条中收集一些有用的要素。而且，一项关于法律承认效力的条文也可以纳入这样一项原则，即对于外国身份和信任服务，唯有其提供的保证等级等于或高于寻求承认的国家所要求的等级，才应予以承认（所谓“对等原则”）。可以按照如下措词拟定一项条文：

> 在[接收国]以外提供并被列入根据第…条建立的受信任清单中的身份或信任服务，应在[接收国]享有同等法律效力，一如[接收国]所提供的身份或信任服务[同等保障等级的[……]]。

89. 工作组似宜考虑是否应就如何使用摸底调查程序并参照保证等级的概念来确定有关外国身份和信任服务的法律效力提供额外指导。工作组似宜就此审议，参照《电子商务示范法》第十二条所载“大体等同的可靠性”的概念是否适宜的问题。

90. 工作组在审议时似宜考虑有关利用身份管理方案的各种实例：由于在国内交易和跨境交易中均有可能出现该问题，工作组似宜一并考虑这两种情况。特别是，它不妨考虑经常出现的这样一些挑战，也就是说似乎产生于对遵守公共当局所规定的强制性要求的需要，而这些要求在合同协议中可能不易实现。例如，如上所述（第80-83 段），银行可能希望知道究竟哪些身份管理方案可用于满足“了解你的客户”的要求。

91. 总而言之，与法律承认机制可能有关的要素包括：通知和插入受信任清单；有待满足的要求，包括参照保证等级；使用认证书以提供要求已获实现的证据；中央监督和许可证管理机构；摸底工作。

92. 工作组似宜审议法律承认机制所应依据的做法问题。委员会还似宜就此进一步讨论该法律承认机制究竟应仅适用于跨境制度还是也应适用于国内各种制度的问题（见上文，第 60 段）。

2. 信任服务

93. 关于信任服务，已经设计了若干法律机制来实现对电子签名的法律承认。应当就此指出，有一种观点认为，并非所有电子签名均是信任服务的产出，而只有那些需要第三方信任服务提供方参与的签名才可被认为是信任服务的产出。另一种观点认为，所有电子签名都是信任服务的产出。工作组似宜审议该事项。

94. 关于贸易法委员会的文本，电子签名功能等同规则（见上文，第 36 段）提供了国内层面上的法律承认。

95. 关于跨境法律承认，基于“大体等同”做法的《电子商务示范法》第十二条[12]要求不得因电子签名的外国要素而出现任何歧视。《电子通信公约》第 9(3)条规定了确立手写签名和电子签名功能等同的要求，但其本身并不能确定签名在寻求承认的法域的法律地位。[13]

[12] 关于实质性等同的更多信息载于贸易法委员会出版物《增进对电子商务的信心：关于国际使用电子认证和签名方法的法律问题》（联合国出版物，出售品编号：E.09.V.4，第 158-161 段）。

[13] 《联合国国际合同使用电子通信公约》的解释性说明（联合国出版物，出售品编号：E.07.V.2），第 156 段。

96. 另一种跨境承认电子签名的机制依赖于订立专门的国际协议，或者经授权订立谅解备忘录。例如，《电子身份识别和服务条例》第 14 条要求，只有在国际协议承认的情况下，欧洲联盟之外设立的提供方所提供的信任服务才能被承认为与在欧洲联盟内设立的合格提供方所提供的服务在法律上等同。印度 2008 年《信息技术法》第 19 条就承认外国核证机构做了如下规定：

> “(1) 在符合规章条例所规定的条件和限制的前体下，审计主管可在中央政府事先批准下，并通过在官方公报上发布通知，承认任何外国核证机构为本法令所涉核证机构。
>
> (2) 凡核证机构在第(1)款下获得承认，这类核证机构签发的电子签名证书就本法令而言即为有效。
>
> (3) 审计主管如深信任何核证机构违反了其据以在第(1)款下获得承认的任何条件及限制，则可基于须以书面记录的理由，通过官方公告上发布通知而撤销该项承认。”

97. 确保基于公钥基础设施跨制度或跨境承认电子签名的其他方法是交叉承认和交叉核证。[14]交叉承认系互操作性安排，公钥基础设施领域的依赖方可以使用另一公钥基础设施领域的权威信息来认证前一个公钥基础设施领域中的对象。[15]交叉认证指的是通常以合同的形式承认另一认证服务提供者的公钥达到约定信任程度的做法。[16]这些基于合同的方法可能会得到一项专门法律条文的支持。例如，哥伦比亚 1999 年第 527 号法律第 43 条指出：

> 对于由他国验证机构签发的数字签名证书，可以按照法律就本国验证机构签发证书所规定的相同条款和条件予以承认，条件是此类证书得到获得授权的本国验证机构的承认，该验证机构对他国证书细节的准确性及其效力和有效性予以保证，一如其自己签发的证书。

98. 上述机制已经存在了一段时间，但尚未完全实现对电子签名的跨境识别。颁布《电子商务示范法》的州为数有限，并且通常没有采纳第十二条。各国对《电子通信公约》的参与虽然稳步增加，但仍然有限。基于法令的相互承认机制很费时间和资源，而且很少使用。基于公钥基础设施的交叉承认和交叉核证仅适用于谈判此类承认和核证的核证机构，如果没有所有相关法域的法规支持，可能就不符合强制性立法要求。

---

[14] 关于交叉承认和交叉认证的更多信息见《增进对电子商务信心》的出版物，引文，第 165-172 段。

[15] 《增进对电子商务的信心》，引文，第 165 段。

[16] 《增进对电子商务的信心》，引文，第 169 段。