联合国 A/CN.9/WG.IV/WP.158

大 会

Distr.: Limited
1 February 2019
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十八届会议
2019 年 4 月 8 日至 12 日，纽约

关于跨境承认身份管理和信任服务的条文草案的解释性说明

秘书处的说明

目录

页次

一. 导言 2
二. 条文草案所寻求的主要政策目标 2
三. 关于条文草案的解释性说明 3
A. 第一章－适用范围（第 1 至 3 条草案） 3
B. 第二章－总则（第 4 至第 7 条草案） 4
C. 第三章－身份管理（第 8 至 13 条草案） 5
D. 第四章－信任服务（第 14 至 18 条草案） 10
E. 第五章－国际方面（第 19 至 20 条草案） 12

V.19-00601 (C) 180219 180219

请回收

一. 导言

1. 本说明就 A/CN.9/WG.IV/WP.157 号文件所载关于跨境承认身份管理和信任服务的条文草案作了说明。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.156 号文件第 6-15 段。

二. 条文草案所寻求的主要政策目标

2. 过去二十年见证了网上活动呈指数的增长。网上商业活动——即企业之间、企业与消费者之间以及企业与政府之间的电子交易——的增加，就其所代表的价值而言尤为显著。全球电子商务从 1999 年的 640 亿美元增长到 2015 年的 25 万亿美元。[1]这一增长与个人和企业对互联网的使用增加相吻合。例如，拥有互联网接入的家庭比例从 2002 年的 35%增加到 2017 年的 83.6%。[2]电子政务（包括与贸易有关的服务）、电子银行和电子支付的提供量也相应增加.

3. 这种增长需要有对网上环境信任感的支持。网上信任的一个重要组成部分是能够以可靠方式识别每一方的身份，特别是在没有任何事先面对面互动的情况下。多年来，人们就网上身份识别的需要提出了各种解决方案，由此造成用于管理身份的方法、技术和设备激增。在全球一级处理身份管理所涉及的法律问题，不仅有可能将这些不同的解决方案联系起来，而且可以不论私人或政府运作，促进身份管理系统之间的互操作性。

4. 在更广泛地使用身份管理和信任服务方面存在若干障碍。其中一些是法律性质的障碍，包括：(1)缺乏赋予身份管理和信任服务法律效力的立法；(2)针对身份管理的法律和做法不同，其中包括基于特定技术要求的法律；(3)法规要求为进行网上商业交易提供纸质身份识别文件；(4)缺乏对身份管理和信任服务进行跨境法律承认的机制（A/CN.9/965，第 52 段）。

5. 工作组工作的主要目标是通过制定统一的法律规则来解决这些障碍。这些规则有若干目的：提高效率；降低交易成本；提高电子交易的安全性和法律确定性，从而建立信任；以及弥合数字鸿沟。

6. 工作组的工作通过这种方式促进执行“可持续发展目标”。具体而言，“可持续发展目标”16 确认了身份的重要性，其中的具体目标 9 要求为所有人提供法律身份。在数字经济中，这将成为一项对数字身份的权利。身份管理和信任服务方面的法律框架将促进数字身份的安全运作。通过促进对网上环境的信任，这一框架还将有助于可持续发展和社会包容，这与（除其他外）涉及促进创新的“可持续发展目标”9 是一致的。

[1] 资料来源：贸发会议，“2001 年电子商务和发展报告”，联合国文件：UNCTAD/SDTE/ECB/1，第 44 页；贸发会议，“2017 年信息经济报告”，联合国文件：UNCTAD/IER/2017，第 28 页。

[2] 资料来源：国际电联，信通技术统计，2001-2018 年全球信通技术发展，查阅网址：https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx。

三. 关于条文草案的解释性说明

A. 第一章——适用范围（第 1 至 3 条草案）

1. 使用身份管理的目的（第 1 条第(1)款草案）

7. 可以要求为不同目的——即为监管合规——而进行身份识别，以确定商业书证的有效性并遵守合同义务（A/CN.9/965，第 82-83 段；另见 A/CN.9/WG.IV/WP.153，第 32-34 段）。**工作组似宜审议如何为监管合规目的而适用条文草案。**

2. 跨境法律承认和国内法律承认（第 1 条第(1)款草案）

8. 对外国身份管理和信任服务的承认得益于国内法律框架的存在。这是因为此种框架确立了与承认机制有关的法律概念。如果国内立法载有基于共同一般原则的协调规则，即便不是相同条款，也可进一步促进跨境承认。此外，身份管理的跨境承认，以及不考虑任何跨境或外国因素的身份管理跨系统承认，都会带来一定程度的共同性。正是出于这些原因拟订了条文草案，以期为一项国际协定和将在国内颁布的示范立法提供基础。

3. 相关实体（第 1 条第(2)和(3)款草案）

(a) 公共实体

9. 虽然工作组工作的主要重点是商对商交易，但还应考虑到在与商业操作有关的其他背景下——特别是在诸如海关业务单一窗口等与贸易相关的政府服务方面——建立的身份管理系统（A/CN.9/965，第 83 段）。出于这些原因，有必要将公共实体列为可适用条文草案的实体。

10. **工作组似宜审议，公共实体参与身份管理交易或信任服务是否会引起具体问题，**同时铭记适用技术中性原则（见下文第 23 段）和当事人意思自治（见下文第 24 段）。

(b) 架构的识别

11. 有建议提出，工作组的工作应有利于可靠地识别交易的主体（即自然人和法人）和架构（即物理架构和数字架构），对架构的识别或许有助于识别交易的主体。鉴于架构不具有法律人格且不能承担赔偿责任，无论如何都应保持主体与架构之间的明确区分（A/CN.9/965，第 11 段）。

12. 第(3)款中提及“验证身份”反映了工作组的决定：工作组的工作应侧重于交易身份，并在这方面侧重于承认问题，即验证身份而不是验证其属性（A/CN.9/965，第 10 段）。A/CN.9/WG.IV/WP.153 号文件第 7-10 段对交易（或次要）身份和基本（或主要）身份作了更详细的说明。

4. 不新设身份识别义务（第 2 条第(1)款草案）

13. 贸易法委员会电子商务法规共有的一条一般原则与实体法（如一般适用于商业交易的法律）不受影响这一事实有关。

14. 对于身份管理或信任服务，这一原则的要求是，关于身份管理的立法不应就身份识别提出任何新的义务，关于信任服务的立法不应就使用任何特定类型信任服务提出任何新的义务，并且现有义务不应受到影响。

15. 据指出，不就身份识别规定新义务的原则与当事人意思自治原则之间存在密切关联（A/CN.9/965，第 110 段）。还指出，可能由于使用特定信任服务而产生新的身份识别义务，但是，任何情况下都应在自愿基础上使用此种信任服务（同上）。

5. 对隐私和数据保护法的提及（第 2 条第(2)款草案）

16. 工作组强调了数据保护制度对于身份管理和信任服务的重要性。第 2 条第(2)款草案具体提及隐私和数据保护法，以反映工作组对这些法律的重视。

B. 第二章——总则（第 4 至 7 条草案）

1. 定义（第 4 条草案）

17. 第 4 条草案中的定义草案是根据贸易法委员会现有电子商务法规中使用的术语拟订的。

18. 工作组第五十七届会议请秘书处在供今后参考的基本定义清单中列入从《电子身份识别和信任服务条例》第 3 条中摘录的若干定义。[3]这些定义如下：

(a) “电子身份识别”指使用唯一代表自然人或法人或代表作为法人的自然人的电子形式个人身份识别数据的过程。

(b) “电子身份识别手段”指包含个人身份识别数据并用于网上服务认证的物质装置和/或非物质装置。

(c) “个人身份识别数据”指支持确定自然人或法人身份或作为法人的自然人身份的一组数据；

(d) “电子身份识别方案”指向自然人或法人或作为法人的自然人签发电子身份识别手段的电子身份识别系统。

(e) “认证”指支持对自然人或法人进行电子身份识别或对电子形式数据的来源和完整性加以确认的电子流程；

(f) “权威来源”指为提供可用于证明身份的准确数据、信息和（或）证据而能够依赖的任何来源，其形式不予考虑；

(g) “依赖方”指依赖于电子身份识别或信任服务的自然人或法人。

[3] 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认服务的第 910/2014 号条例（欧盟），该条例撤销第 1999/93/EC 号指令。

19. **工作组似宜审议，这些与贸易法委员会所定义的术语不一致的定义是否应当取代或补充第 4 条草案中的定义。**

2. 一般原则和统一解释（第 5 至 7 条草案）

20. 贸易法委员会的法规通常载有一项提及其统一来源的规定和统一解释的义务。第 5 条第 2 款旨在确保在解释和适用法规案文时保持统一性。

21. 工作组确定以下一般原则与其在身份管理和信任服务所涉法律方面的工作有关：(1)不歧视使用电子手段；(2)功能等同；(3)技术中性；(4)当事人意思自治（A/CN.9/936，第 67 段）。

22. 虽然在贸易法委员会现有电子商务法规中阐明了这些在国内一级适用的一般原则（例如，见《电子签名示范法》第 3、第 5、第 6 条[4]），但这些原则同样适用于跨境一级，因为它们所奠定的国内法律基础允许受理国法域对外国身份管理和信任服务准予并维持法律地位。

23. 技术中性原则对于身份管理的重要性已得到充分承认。关于发展中国家，据指出，贯彻这项原则可阻止采用贸易商认为过于昂贵或过于复杂的技术要求（A/CN.9/965，第 38 段）。在身份管理的范围内贯彻技术中性原则，可能要求身份管理系统采用提及系统属性而非特定技术的最低限度系统要求（A/CN.9/936，第 69 段）。

24. 当事人意思自治是一项基本商法原则。但是，这项原则的适用受强制性法律规定的限制（A/CN.9/936，第 72 段）。这些限制特别重要，因为使用身份管理和信任服务所满足的法律要求往往是强制性的。随着工作的进展，**工作组似宜确定哪些核心规则是当事人不得变更或减损的，以增进身份管理和信任服务跨境承认的确定性和可预测性**（A/CN.9/965，第 109 段）。为此原因，没有拟订一项关于当事人意思自治的条文草案（例如，基于《电子签名示范法》第 5 条）。不过，第 3 条草案反映了当事人意思自治原则的要素。

25. 当事人意思自治原则还旨在支持合同协议的可执行性，如身份管理系统规则和信任服务系统规则及框架。系统规则可能对身份管理系统联盟特别重要（见 A/CN.9/WG.IV/WP.154，第 39 段）。

C. 第三章——身份管理（第 8 至 13 条草案）

1. 在功能等同的基础上对身份管理的法律承认（第 8 条草案）

26. 功能等同原则要求确定电子记录、方法或流程为履行与纸质概念相同的功能而必须满足的要求。据指出，关于功能等同的条文只在涉及纸质身份识别的情况下适用（A/CN.9/965，第 69 段），而且可能需在该条文中体现与非网上身份管理流程的关联（A/CN.9/965，第 66 段）。

[4] 《贸易法委员会电子签名示范法》（联合国出版物，出售品编号：E.02.V.8）。

27. 在第五十七届会议上，强调了赋予身份管理法律效力的功能等同条文的一些要素：提及非网上使用的身份识别物理要素（无论是文件、登记处还是其他权威来源）；提及身份管理流程的所有阶段（即身份识别和认证）；以及提及用以评估对正确身份识别的置信度的保证级或其他标准（A/CN.9/965，第 70-78 段）。

28. 工作组内对法律承认的对象表达了不同意见（A/CN.9/965，第 25 段），这又决定了功能等同条文的重点。就身份管理而言，法律承认的对象可以是：(a) 身份管理系统；(b)身份管理系统签发的身份证书；或(c)使用身份管理系统的身份识别流程（即身份交易）的结果（A/CN.9/965，第 24 段）。

29. 普遍看法是，工作组应侧重于对流程（即系统）的承认以及对身份管理和信任服务的结果的承认（A/CN.9/965，第 94-99 段）。在这方面还作出的解释是，对身份管理系统、证书以及身份识别流程结果的法律承认是互为补充的（A/CN.9/965，第 26 段）。因此，如果身份管理系统得到承认，那么用于身份识别的证书得到承认，身份识别流程的结果也是如此。工作组第五十七届会议讨论的第 8 条草案的两个备选案文都反映了这一做法。

30. 可能存在着身份识别完全在网上进行、功能等同可能不适用的情形（A/CN.9/965，第 62 段）。为了处理所有情况，建议工作组应当讨论一种可接受的身份识别方法的特点，而不是试图详细拟订功能等同条文（A/CN.9/965，第 69 段）。

2. 可靠性标准（第 9 条草案）

31. 功能等同条文中与确定方法可靠性有关的要素包括：(a)合同协议，以适用法律允许为前提；(b)核证和监督；(c)保证级。

(a) 核证

32. 对身份管理和信任服务提供人的核证可大大有助于建立对这些提供人及其服务的信任。核证选项包括：自我核证；独立第三方核证；经认可的独立第三方核证；以及国家机构核证。选择最合适的核证形式可能会受到所涉服务类型、成本以及所寻求保证级的影响。在商对商情况下应当提供所有核证选项，包括无核证，因为商业伙伴应当能够选择最适合其需要的选择，同时认识到每种选择都将产生不同的法律效力（A/CN.9/965，第 112 段）。

33. 不过，有建议提出，在使用分布式分类账技术的情况下，任何以中央核证、资格鉴定或监督机构为前提的解决方案未必合适，因为在确定有资格提出核证请求的机构及评估机构以及在采取纠正和强制执行行动等方面存在困难（A/CN.9/965，第 114、129 段）。

34. 在以事前方法（见下文第 47-49 段）为基础的现有法律承认机制中（见 A/CN.9/WG.IV/WP.153，第 61-73、76-79 段），核证（包括自我认证）是使用基于结果的标准来评估身份管理系统的必要条件。

35. 核证也可能与事后法律承认相关（见下文第 44-45 段）。例如，《电子签名示范法》第 10 条(e)和(f)项提到而不是规定，资格鉴定、审计和自我核证的存在是评估认证服务提供商所使用系统可信赖性的因素。

36. 关于让公共机构参与核证过程是否可取，表达了不同意见。一方面，据指出，自愿核证不一定涉及公共实体，而可能依赖独立核证（A/CN.9/965，第 112 段）。

37. 另一方面也指出，国家监督私营部门核证机构的活动对于防止竞争风险和滥用风险至关重要，对较小市场参与者尤为重要（A/CN.9/965，第 115、128 段）。另外还指出，由国家当局认可核证机构是为了确保这些机构活动的独立性、公正性和公平性。对此提出的建议是，独立机构或许更有条件实现这些目标（A/CN.9/965，第 115 段）。

38. 《电子签名示范法》第 10 条所采取的办法是模式中性的产物。加入强制性监管条款可能被视为妨碍采用基于信任服务自我监管的市场模式。

(b) 监督

39. 对身份管理系统的监督是常见的，因为这种监督的存在被认为对于建立对服务提供人及其所提供服务的信任是有用的，甚至是必需的。然而，设立这样一种机构会带来行政和财政方面的影响。而如果使用替代或补充机制，如第三方核证，则可能有助于在降低相关成本的同时实现监督机制所追求的目标。

40. 据指出，公共当局目前不仅越来越多地参与监督，而且越来越多地参与发展和部署身份管理系统并提供身份管理和信任服务，这就需要将监督职能与公共当局履行的其他职能分开（A/CN.9/965，第 128 段）。

(c) 保证级和映射

41. 保证级是对身份识别和认证过程置信度的一种衡量方式，因此，是确立身份管理系统可靠性的关键（A/CN.9/965，第 61 段）。关于提及保证级是否可取，表达了不同意见（见 A/CN.9/965，第 63-68 段）。

42. 可以在功能等同条文（即第 8 条草案）或在确定身份管理系统可靠性标准的条文（即第 9 条草案）中提及保证级。**工作组似宜审议，如果提及保证级，一般提及是否足以，还是说是否需要提及不同保证级，**就后一种情形而言，是否应将每一保证级与不同法律效力相关联（见 A/CN.9/965，第 59-60 段）。

43. 工作组在其第五十七届会议上讨论了将“映射”作为一种验证身份管理系统是否符合某一保证级一般说明的方法（见 A/CN.9/965，第 43-48、54 段）。A/CN.9/WG.IV/WP.153 号文件第 80 段给出了映射工作如何操作的实际例子。

3. 事后确定可靠性（第 9 条草案）

44. 第 9 条草案旨在以事后方法确定身份管理系统的可靠性。事后方法仅在发生实际争议时对身份管理制度进行评估，但依据的是预先确定的条件。贸易法委员会法规对信任服务采用了这一方法（例如，见《电子通信公约》第 9 条第(3)款）。

45. 关于事后方法的进一步资料，可参见 A/CN.9/965 号文件（第 40-45 段）和 A/CN.9/WG.IV/WP.153 号文件（第 74-75 段）。

4. 可靠性的推定（第 10 条草案）

46. 第 10 条草案是以《电子签名示范法》第 6 条第(3)款为基础，其中就满足某些要求的电子签名给出可靠性推定。第 10 条草案可适用于事后和事前方法。事后方法支持执行第 9 条草案，所表述的是允许更易于确定可靠性的客观技术标准。但是，同样标准可由指定机构事先进行评估。在后一种情况下，第 10 条草案与第 11 条草案结合起来运用。

5. 事前确定可靠性（第 11 条草案）

47. 第 11 条草案旨在以事前方法确定身份管理系统的可靠性。

48. 这种方法的前提是，事先确定身份管理系统必须满足哪些条件方可被列入获得承认的身份管理系统合格名单。有意见认为，在使用较高保证级时最好采用事前办法（A/CN.9/965，第 47 段）。

49. 工作组对这一方法的讨论提出了两个问题：(1)需要一种集中化的机构机制来评估身份管理系统；(2)公共当局的参与。关于执行事前方法的机构机制的进一步资料，可参见 A/CN.9/965 号文件（第 40-45 段）和 A/CN.9/WG.IV/WP.153 号文件（第 61-73 段）。关于公共当局参与的进一步资料，可参见 A/CN.9/965 号文件（第 49-50 段）。

6. 身份管理系统运营人的义务（第 12 条草案）

50. 第 12 条第(1)款草案就确定身份管理系统运营人的基本义务提供了初步要素。该条受到《电子身份识别和信任服务条例》相应条款的启发。

(a) 安全违规的通知义务

51. 第 12 条第(2)款草案规定了安全违规的通知义务。此项义务是透明度原则的一个方面（A/CN.9/936，第 88 段）。

52. 安全违规会影响系统和交易。适当的安全违规通知机制已被确定为关系到绩效的改善和增进对身份管理和信任服务的置信度（A/CN.9/965，第 123 段）。

53. 安全违规通知与数据泄露通知有共同之处，但也有重大区别。A/CN.9/WG.IV/WP.154 号文件（第 43-44 段）给出了现行立法就安全违规披露制度作出规定的例子。

(b) 服务提供情况的披露义务

54. 工作组在其关于透明度原则的讨论中审议了服务提供情况的披露义务（A/CN.9/965，第 121 段）。服务提供情况透明度不仅对用户重要（使其能够作出知情选择），而且对竞争对手和其他有关实体也很重要（例如，监测市场竞争情况）（A/CN.9/965，第 121 段）。以目前的写法，第 12 条第(1)款草案没有就披露服务提供情况单独规定一项独立义务。

55. 加入联盟或以其他方式获得其服务证书的身份管理系统运营人将披露大量信息。可以对其他提供人规定最低限披露义务。例如，《电子签名示范法》第 9 条第(1)款载有认证服务提供商必须向依赖方披露的信息清单。

7. 身份管理系统运营人的赔偿责任（第 13 条草案）

56. 据指出，只要工作组的工作载有在国家一级适用的规则，就有必要处理赔偿责任分配问题（A/CN/965，第 116 段），因为适用的赔偿责任制度可能对促进身份管理和信任服务用于商业和非商业方面产生重大影响。

57. 在这方面，工作组确定了有待解决的下列问题：确定负有赔偿责任的实体，同时考虑到公共实体的特别赔偿责任制度；对遵守预先确定的要求的当事方限制赔偿责任的可能性；限制赔偿责任的法定机制（例如，通过免责或举证责任倒置）；合同规定的赔偿责任限制（A/CN.9/936，第 85 段）。A/CN.9/WG.IV/WP.154 号文件对涉及身份管理系统运营人赔偿责任的立法作了简短说明（第 23-30 段）。

58. 第 13 条第(1)款草案所贯彻的一般原则是，身份管理系统运营人未能提供商定的服务或未按法律规定的其他要求提供服务，应对所造成的后果承担赔偿责任（A/CN.9/965，第 117 段）。然而，在某些情况下，对身份管理系统运营人进行识别可能并非易事（例如，在使用分布式分类账技术的情况下）。

59. 按照该条文目前的写法，公共实体在作为服务提供人行事时可能要承担责任。当公共实体履行监督职能和签发基本身份证书时，可能会产生不同的赔偿责任分配方式。

60. 第 13 条草案目前只将赔偿责任分配给身份管理系统运营人。**工作组似宜审议，赔偿责任规则是否也应适用于其他相关实体**（例如，用户和第三方依赖人），还是说应对这些实体适用一般赔偿责任规则。工作组还似宜审议，是否应为提高透明度而强制要求向用户和其他相关实体披露适用的赔偿责任制度。

61. 第 13 条草案规定故意和疏忽是赔偿责任的依据。在《增进对电子商务的信心》这份文件中载有关于公钥基础设施运营人赔偿责任方面谨慎标准的论述，其中包括一般过失和推定过失以及严格赔偿责任。[5]

62. **工作组似宜审议，是否应制定关于举证责任和损害定义的补充规则，**还是说应在适用的国内法中寻找这些规则。

63. 第 13 条第(2)款草案限制身份管理系统运营人对由于使用量超过身份管理系统运营人披露的限额而造成的损害的赔偿责任。这项规定补充了服务提供情况的披露义务，此种披露是透明度原则的一个方面。《增进对电子商务的信心》这份文件讨论了公钥基础设施运营人在合同上限责或免责的能力。[6]

64. 第 13 条第(3)款草案规定了一种鼓励身份管理系统运营人采用某些标准的机制，要求使用这些标准作为免责条件。另一种办法是，该条文可以提及使用更高保证级。

---

[5] 《增进对电子商务的信心：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 179-201 段）。

[6] 同上，第 202-210 段。

65. 第 13 条第(3)款草案受第 13 条第(4)款草案的限制。“重大过失或故意不当行为”的标准体现在《弗吉尼亚电子身份管理法》中（见 A/CN.9/WG.IV/WP.154，第 29 段）。

66. 处理赔偿责任问题的其他方法包括建立一个基于保险的机制，根据这种机制，保险人对因使用身份管理系统而产生的损害作出赔偿。另一种可用机制设想在满足某些条件的情况下自动发放预先约定的赔偿金或定额罚金。

D. 第四章——信任服务（第 14 至 18 条草案）

67. 作为初步事项，**工作组似宜审议，是否应着手拟订一个基于“信任服务”共同定义的敞开式清单，还是提供适用于所有信任服务的共同规则和适用于其中每项服务的具体规则**。信任服务敞开式清单可包括：电子签名、电子印章、电子时戳、电子登记交付、网站认证、电子存档、电子托管、在场电子证据。

1. 在功能等同基础上对信任服务的法律承认（第 14 条草案）

68. 为了就一项信任服务拟订适当的功能等同规定，有必要确定该信任服务所要履行的具体功能。第 14 条草案载有针对每一项具体确定的信任服务的功能等同基本规定。**工作组似宜审议，关于信任服务功能等同的条文是否应述及：(a)通用或具体的可靠性标准；(b)可靠性推定；(c)可靠性事前评估；(d)关于不可否认的安全条款**。

(a) 电子签名

69. 第 14 条第(1)款草案涉及电子签名这种常见的信任服务形式。贸易法委员会所有电子商务法规都载有关于使用电子签名的规定。

70. 某些类型的电子签名和某些类型的其他信任服务（如电子存档）可为数据电文完整性提供保证。在贸易法委员会法规中，保持数据电文完整性是一项关于与纸质“原件”概念功能等同的要求。**工作组似宜审议，是否应将完整性保证作为一项单独的信任服务加以处理**。

(b) 电子印章

71. 《电子身份识别和信任服务条例》中使用电子印章为法人签发的电子文件的来源和完整性提供证据（《条例》第 59 条）。此外，“电子印章可用于认证法人的任何数字资产，如软件代码或服务器”（《条例》第 65 条）。

72. 贸易法委员会关于信任服务的法规适用于自然人和法人。此外还建议，工作组目前的工作也应适用于物理架构和数字架构，从而将软件代码或服务器也涵盖在内。

73. 《电子商务示范法》第 8 条要求保持完整性，以实现与纸质“原件”概念的功能等同。[7]《电子签名示范法》第 6 条第 3 款在提及“完整性”概念时规定，对签名的法律要求的目的是就签字所涉信息的完整性提供保证。

74. 鉴于以上所述，**工作组似宜审议，是否应将电子印章视为一项单独的信任服务，**还是可将其视为电子签名的一个子集。

(c) 电子存档

75. 第 14 条第(3)款草案涉及电子存档服务，而电子存档服务又涉及电子记录的保存。将要保存的电子记录可能是第一次以电子方式生成，也可能重现最初在书面上发布的信息。电子存档服务还可为存档的电子记录的完整性以及归档时间提供保证。

76. 电子存档所要履行的功能是，在发生争议时以及为满足其他需要，为存档电子记录的有效性提供法律确定性。据建议，电子存档的法律承认机制可限于确保遵守需要使用存档记录的法域的法律要求（A/CN.9/965，第 126 段）。如果工作组希望审议一项关于电子存档的规定，建议使用《电子商务示范法》关于数据电文留存的第 10 条作为讨论基础。

77. 此外，法律可能要求能够迁移已存档的电子记录，以便无论技术发展如何都可访问。这一结果可通过适用技术中性原则以及与“完整性”概念功能等同的要求来实现，即：当需要展现信息时，该信息能够显示给被展现该信息的人（《电子商务示范法》第 8 条第(1)款(b)项）。

(d) 其他信任服务

78. 第 14 条第(2)款草案中所涉及的电子时戳旨在就印章与数据绑定的日期和时间提供证据。电子时戳还可就绑定日期和时间的数据的完整性提供证据。

79. 第 14 条第(4)款草案所涉及的电子登记交付服务旨在就身份确定的发送人发出电子通信和身份确定的收件人收到电子通信提供证据。电子登记交付服务还可就所交换数据的完整性以及数据的发送和接收时间提供证据。

80. 第 14 条第(5)款草案涉及网站认证。根据《电子身份识别和信任服务条例》，“网站认证服务提供了一种籍以向网站访问者保证网站背后有一个真实、合法实体存在的手段”（《条例》第 67 条）。**工作组似宜审议，是否应将网站认证视为一项单独的信任服务，**还是可将其视为电子签名的一个子集。

81. 第 14 条第(6)款草案涉及托管服务，其中包括保管一项资产，并在符合托管协议规定的条件时将其发放给权利人。托管服务用于支付款项和发放软件源代码。例如，货物价款的支付可能会推迟到买方收到货物；同时，卖方将收到价款到账并在货物交付和验收后发放价款的确认通知。

82. 电子在场证明服务旨在证明某一时间主体在某一特定地点。结合电子遗嘱讨论了这项信任服务。这项服务还可能与网上注册有关，如银行服务注册。**工作组似宜审议，是否应拟订一项关于电子在场证明服务的专门规定。**

[7] 《贸易法委员会电子签名示范法》（联合国出版物，出售品编号：E.99.V.4）。

2. 信任服务可靠性的推定（第 15 条草案）

83. 《电子签名示范法》和若干关于电子签名的国内法律根据信任服务所具有的可靠度对信任服务加以区分。具体而言，这些法律对满足某些要求并因此被视为具有更高可靠度的电子签名规定了法律后果。为避免混淆，建议工作组的工作在讨论信任服务时提及可靠度，并建议仅在提及身份管理系统时使用“保证级”一词。

84. **工作组似宜审议，是否应将保证级概念适用于对信任服务的承认，**还是应适用其他一些概念来确定某一特定信任服务的可靠性。据指出，具有高保证级的身份证书可为具有不同可靠度的信任服务所使用（A/CN.9/965，第 106 段）。因此，电子身份识别的保证级与信任服务的可靠度之间不存在相互关系。

3. 信任服务提供人的赔偿责任（第 18 条草案）

85. 作为一般原则，信任服务提供人未能提供商定的服务或未按法律规定的其他要求提供服务，应对所造成的后果承担赔偿责任（A/CN.9/965，第 117 段）。所提供的信任服务类型将决定这一赔偿责任的范围。

86. 《电子签名示范法》载有关于签名人的行为（第 8 条）、认证服务提供商的行为（第 9 条）以及依赖方的行为（第 11 条）所产生的赔偿责任的条款。 这些条款规定了参与电子签名生命周期的每个实体的义务。此外，《电子签名示范法》承认认证服务提供商有可能限制其赔偿责任的范围或程度。

87. A/CN.9/WG.IV/WP.154 号文件对涉及信任服务提供人赔偿责任的立法作了简短说明（第 33-35 段）。

E. 第五章——国际方面（第 19 至 20 条草案）

1. 跨境法律承认（第 19 条草案）

88. 对于跨境法律承认，可以用不同方式来理解（见 A/CN.9/WG.IV/WP.153，第 55 段）。在工作组第五十七届会议上指出，给予国民待遇应当是跨境法律承认更可取的办法（A/CN.9/965，第 30 段）。第 19 条草案是根据这一办法拟订的。

89. 适用的赔偿责任制度可能与评估外国身份管理系统的等同性有关。因此，据建议，为了便利对身份管理的跨境承认，有必要确定赔偿责任制度的适用法律（A/CN.9/965，第 116 段）。这可能要求制定一项专门的国际私法规则或提及现有规则。**工作组似宜审议，跨境法律承认是否意味着将国内赔偿责任制度适用于外国身份管理和信任服务。**

90. 第 19 条草案没有明确涉及责任限制。可以适用其他可能限制此类合同条款效力的规则，包括根据强制性法律适用这些规则。

91. 第 19 条第(2)款草案规定可靠度是评估外国身份管理系统或身份证书等同性的标准。其中提出两个备选案文：外国身份管理系统提供了相同的可靠度；或者提供了基本等同的可靠度。“基本等同的可靠度”概念取自《电子签名示范法》第 12 条。

工作组似宜审议，是否应参照保证级概念和映射方法的使用，就身份管理的承认提供更多指导。

2. 机构合作机制（第 20 条草案）

92. 机构合作机制可有助于实现身份管理系统和信任服务的相互法律承认和互操作性。

93. 第 20 条草案提到以国家间合作的形式进行的机构合作。合作可包括交流信息、经验和良好做法，特别是在技术要求和保证级方面，对身份管理系统进行同行审查，以及审查相关发展情况。《电子身份识别和信任服务条例》的一项实施法案[8]提供了关于信息交流和同行审查的更多细节，包括指出，如果披露可能违反公共安全或国家安全事项，或者泄露商业、专业或公司机密，成员国可以不提供所需要的信息。

94. 另一种形式的合作可以通过身份管理系统联盟来实现。联盟通常以合同协议为基础，但法定条款可能有助于促进联盟。关于身份管理系统联盟的更多信息，另见 A/CN.9/WG.IV/WP.154 号文件第 39 段。

95. 身份管理系统联盟基于技术互操作性和由一组系统规则界定的共同法律框架进行操作。合同规则和立法规则的统一可能有助于建立这一共同法律框架（A/CN.9/965，第 120 段）。

96. 据指出，如果法律承认采用事先机制，也可能导致某种形式的机构合作。

[8] 欧盟委员会 2015 年 2 月 24 日第 2015/296 号执行决定，该决定确立了成员国之间电子身份识别合作的程序安排。