联合国 A/CN.9/WG.IV/WP.157

大 会

Distr.: Limited
28 January 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

秘书处的说明

目录

页次

一. 导言 2

附件一 关于跨境承认身份管理和信任服务的条文草案 3

V.19-00492 (C) 180219 180219

一. 导言

1. 在第五十七届会议上，工作组要求秘书处今后编写的文件应载有核心问题的条文草案，以促进工作组在与身份管理和信任服务有关的法律问题上的工作取得进展。

2. 根据这一要求，本说明附件一载有工作组迄今讨论的一系列问题的条文草案。在可能的情况下，这些条文以工作组第五十七届会议的讨论（A/CN.9/WG.IV/WP.153）为基础。关于这些问题和其他相关问题的补充评述载于 A/CN.9/WG.IV/WP.158 号工作文件。

附件一

关于跨境承认身份管理和信任服务的条文草案

第一章　适用范围

第 1 条　适用范围

[第(1)款备选案文 A

1.　本[文书草案]适用于[当国际私法规则导致适用颁布法域的法律时]营业地位于不同国家的当事人之间的商业交易使用身份管理系统和信任服务。

[第(1)款备选案文 B

1.　本[文书草案]适用于跨境承认在商业活动中使用的[身份管理系统][身份证书]和信任服务。[1]

2.　本[文书草案]还适用于在与贸易有关的政府服务中使用身份管理系统和信任服务。[2]

3.　本[文书草案]适用于对自然人和法人身份以及物理架构和数字架构身份的验证。

第 2 条　不受本[文书草案]影响的事项

1.　本[文书草案]中的规定概不要求某人验证主体的身份或使用信任服务，亦不要求验证主体的身份或使用提供某种程度可靠性的信任服务。

2.　除本[文书草案]另有规定外，本[文书草案]概不影响对[身份管理和信任服务]适用[身份管理和信任服务]所适用的任何法律规则[，包括适用于隐私和数据保护的任何法律规则]。[3]

第 3 条　自愿使用身份管理和信任服务

1.　本[文书草案]中的规定概不要求主体在未予同意的情况下[使用身份管理系统][接受身份证书]或使用信任服务。

2.　就第 1 款而言，可根据主体的行为[及其他情形]推断主体是否同意。[4]

---

[1] 工作组内部对其身份管理工作中法律承认的“对象”发表了不同意见。工作组第五十七届会议认为身份管理系统、身份证书和身份交易是法律承认的可能对象。

[2] 该条文草案旨在强调，身份管理和信任服务可以在纯商业环境之外使用。

[3] “包括适用于隐私和数据保护的任何法律规则”一语旨在解决工作组对适用隐私和数据保护法的关切。

[4] “及其他情形”一语是指主体不能自主行为的情形，即物理架构或数字架构。在这些情况下，不应将同意归因于主体，而应归因于对该主体负有法律责任的自然人或法人（A/CN.9/965，第 109 段）。

第二章　总则

第 4 条　定义

在本[文书草案]中：

(a)　“属性”指与主体关联的一条信息或数据；[5]

(b)　“身份识别”指收集、验证并核证关于主体的充分身份属性以在特定环境下确定并确认主体身份的过程；[6]

(c)　“身份”指关于主体的一组属性，其在特定环境下[允许充分区分主体][对主体作出[独一]描述]；[7]

(d)　“身份证书”指[作为声称身份的证据而出示的一组数据][主体为在网上环境中验证或认证其身份可出示的数据或数据可能驻留的物理架构][8]；[9]

(e)　“[电子]身份管理”指在网上环境中对主体的身份识别、认证[和授权]进行管理的一套流程；[10]

(f)　“身份管理系统运营人”指运营身份管理系统的人；

(g)　“保证级”表示对身份识别和认证过程的置信度——即(a)对用以确定被签发证书主体的身份的审查过程的置信度，和(b)对使用该证书的主体系被签发该证书的主体的置信度。这种保证反映了所使用方法、流程和技术的可靠性；[11]

(h)　“依赖方”指可在身份管理或信任服务的基础上行事的人；

(i)　“主体”指在特定身份证书中识别并可由身份提供方认证和担保的人或架构；[12]

---

[5] 见 A/CN.9/WG.IV/WP.150，第 13 段。

[6] 见 A/CN.9/WG.IV/WP.150，第 29 段。工作组似宜审议，是否应说明该定义包括在身份管理系统中登记以及签发身份证书。

[7] 见 A/CN.9/WG.IV/WP.150，第 38 段。在讨论“身份”定义时，工作组似宜审议，就工作组关于这一专题的工作而言，是否需要独一性要求，其依据是：(a)独一性是基本身份的一种特性，(b)基本身份目前被排除在工作范围之外（A/CN.9/965，第 10 段）

[8] 该定义根据《弗吉尼亚电子身份管理法》第 59.1 至 550 条（《弗吉尼亚法典》第 59.1 篇第 50 章）中的定义改拟。

[9] 见 A/CN.9/WG.IV/WP.150，第 21 段。“身份证书”一词与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）（《电子身份识别和信任服务条例》）第 3 条第(2)款所界定的“电子身份识别手段”大致同义，该条例撤销第 1999/93/EC 号指令，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”。

[10] 见 A/CN.9/WG.IV/WP.150，第 35 段。在工作组第五十七届会议上指出，该定义可能表明，有必要累加提及“身份识别”、“认证”和“授权”，同时，这些要素中的任何一项都已足够。为此，据指出，《电子身份识别和信任服务条例》中的“电子身份识别”定义更可取（A/CN.9/965，第 91 段）。《电子身份识别和信任服务条例》第 3 条第(1)款将“电子身份识别”这一术语定义为指“使用唯一代表自然人或法人或者代表作为法人的自然人的电子形式个人身份识别数据[即本文件中所定义的“身份证书”]的过程”。

[11] 见 A/CN.9/WG.IV/WP.150，第 42 段。

[12] 见 A/CN.9/WG.IV/WP.150，第 38 段。

(j) “信任服务”[13]指就数据品质提供一定程度可靠性的电子服务；

(k) “信任服务提供人”指提供一项或多项信任服务的人。

第 5 条 解释

1. 对本[文书草案]的解释应以下列一般原则为指导：

(a) 不歧视使用电子手段；

(b) 技术中性；

(c) 功能等同；

(d) […]

2. 在解释本[文书草案]时，应考虑到其国际性以及促进其统一适用和遵守诚信的必要性。

3. 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，应按照本[文书草案]所依据的一般原则加以解决，[无此种原则的，应按照依国际私法规则适用的法律]加以解决。[14]

第 6 条 不歧视使用电子手段

1. 不得仅以[身份证书][身份验证结果][身份管理系统]是电子形式为由而否定[身份证书][身份管理系统]的法律效力、有效性、可执行性或证据可采性。[15]

2. 不得仅以信任服务是电子形式为由而否定信任服务的法律效力、有效性、可执行性或证据可采性。

第 7 条 技术中性

为身份管理或提供信任服务而使用的任何[技术、方法或系统]，凡满足本[文书草案]提及的要求[或以其他方式符合适用法律要求][16]的，本[文书草案]规定的适用概不排除、限制或剥夺其法律效力。

---

[13] 工作组似宜审议，是否应在英文中使用“trusted service”（“信任服务”）的提法，以避免与“trust”（“信托”）这一非常确定的法律概念有任何混淆（见 A/CN.9/965，第 14、101 段）。

[14] 所添加的案文“无此种原则的，应当按照依国际私法规则适用的法律”，对于跨境情形可能特别有用。

[15] 身份证书和身份管理系统的取舍，与法律承认的对象是身份证书还是身份管理系统有关（见上文脚注 1，以及 A/CN.9/WG.IV/WP.158 关于法律承认一节）。或者，如果法律承认的对象是身份识别过程（即“身份交易”）的结果，则该条文可改为提及这一过程。

[16] “或以其他方式符合适用法律要求”一语，可见于《贸易法委员会电子签名示范法》（《电子签名示范法》）第 3 条（联合国出版物，出售品编号：E.02.V.8），其中提及，文书草案以外的法律可能在某些确定情况下规定可使用与文书草案所列要求不同的要求。

第三章　身份管理

第 8 条　对身份管理的法律承认

[第 8 条备选案文 A

法律或一方当事人要求[17]按照某种方法识别主体身份的，就身份管理而言，如果使用了一种可靠方法，验证主体的相关属性符合该方法所保证的相同级，即为满足了这一要求。][18]

[第 8 条备选案文 B

当事人希望或法律要求当事人对主体进行身份识别的，为此目的使用身份管理系统，具有与适用为此目的而被承认的非电子程序等同的法律效力，条件是身份管理系统使用了一种可靠方法，验证主体的属性与这一目的相关。][19]

第 9 条　身份管理承认方面的可靠性标准

在为第8条所述要求之目的确定身份管理系统的可靠性时，应考虑到所有相关情形，包括：

(a)　当事人之间的任何协议；

(b)　就身份管理系统提供的任何监督或核证；

(c)　与身份管理系统关联的保证级；[20]

(d)　[…]

第 10 条　身份管理可靠性的[推定]

1.　符合下列条件的，[身份管理系统即满足了第 8 条所述要求][为满足第 8 条所述要求之目的，即推定身份管理系统是可靠的]：

(a)　[说明关于身份管理系统应当如何运作，包括关于审计、保险、认证、赔偿责任、终止和与确定保证级有关的其他问题的一套最低限度适当规则]；

(b)　[说明可确保并验证各参与方遵守规则的机制]；以及

(c)　[说明可确保公示身份管理系统遵守最低限度适当规则情况的机制]。[21]

---

[17] 工作组似宜审议，功能等同条文是否应延伸适用于法律“允许”该事的情形，并确认提及“要求”暗指不做该事的法律后果。

[18] 见 A/CN.9/965，第 77 段。工作组似宜明确，“某种方法”的提法是否意在与纸质身份识别手段建立关联。

[19] 见 A/CN.9/965，第 78 段。

[20] 该条文旨在顾及事后承认方法。

[21] 该条文与事前承认和事后承认方法兼容。

[2. 第 1 款不限制任何人在下列方面的能力：

(a) 为满足第 8 条所述要求之目的，以其他任何方式确立身份管理系统的可靠性；或者

(b) 举出身份管理系统不可靠的证据。][22]

第 11 条 身份管理系统可靠性的确定

1. [颁布国指明的个人、公共或私人机关或机构]可确定哪些身份管理系统满足了第 8 条所述要求。[23]

2. 依照第 1 款作出的任何确定应与公认国际标准一致。

第 12 条 身份管理系统运营人的义务

1. 身份管理系统运营人应：

(a) 将相关身份证书归属于适当人；[24]

(b) 确保身份管理系统流程的在线可用性和正确操作。

2. 身份管理系统运营人应毫不拖延地将对所提供的身份证书或认证过程或对其中保持的个人数据有[重大]影响的任何安全违规或完整性受损事件通知[监管机构][其受影响的客户[25]和依赖方][，任何情况下，通知应在得知该事件后[…]天内发出]。

3. 在发生重大安全违规或完整性受损事件时，身份管理系统运营人应暂停提供受影响的服务[，直至[…]]。

4. 如果发生下列情况，身份管理系统的用户[26]应通知身份管理系统运营人：

(a) 身份证书或认证过程已失密；或者

(b) 用户所知悉的情况导致身份证书或认证过程有重大失密风险。[27]

第 13 条 身份管理系统运营人的赔偿责任

1. 在不影响依据法律可能产生的赔偿责任的情况下，身份管理系统运营人应对由于未遵守本[文书草案]对其规定的义务[故意或因疏忽而]给任何人造成的损害[承担赔偿责任][承担法律后果]。

---

[22] 该条文草案是以《电子签名示范法》第 6 条第(3)款为基础。如果第 1 款确立了可靠性推定，则适用该项。

[23] 该条文草案是以《电子签名示范法》第 7 条为基础，旨在顾及事前承认方法。

[24] 工作组似宜审议是否将这项义务扩大到属性的归属。

[25] 工作组似宜考虑界定“用户”和“客户”概念。

[26] 工作组似宜考虑界定“用户”和“客户”概念。

[27] 关于必须发出通知的时限规定、确定需通知的当事人，以及确定触发通知义务的服务、身份证书或个人数据受影响程度，该条文草案提供了可选措辞。还可以确立一种义务，规定直至泄密或受损得到控制或建立起新的认证或类似流程，必须暂停身份管理系统。

2. 对于因服务的使用超出对[可能使用身份管理系统的交易的目的或价值]的限制而造成的损害，身份管理系统运营人不应承担赔偿责任，前提是身份管理系统运营人提供了合理可及的手段，使[用户[28]或]第三方能够确认这些限制。[29]

3. [身份证书的签发或]一项身份属性的归属符合下列各项的，身份管理系统运营人[应推定为不承担赔偿责任][不应承担赔偿责任]：

(a) [适用的身份管理标准；]

(b) [任何合同协议的适用条款；和]

(c) [其作为成员的身份信任框架的任何书面规则和政策]。

[4. 如果身份管理系统运营人的作为或不作为构成[重大过失或故意不当行为]，第3款不予适用。]

第四章 信任服务

第14条 对信任服务的法律承认

电子签名[30]

[第(1)款备选案文A

1. 法律要求[31]有某人签名的，如果使用了一种可靠方法识别该人身份并表明该人对[电子通信]所包含信息的意图，即为满足了该要求。[32]]

[第(1)款备选案文B

1. 法律要求有某人签名的，如果符合下列条件，即为满足了该要求：

(a) 使用了一种方法识别该人身份并表明该人对[电子通信]所包含信息的意图；以及

(b) 所使用的这种方法：

㈠ 从各种情形来看，包括根据任何相关协议，对于生成或传递[电子通信]所要达到的目的既是适当的，也是可靠的；或者

[28] 工作组似宜考虑界定“用户”和“客户”概念。

[29] 该条文草案旨在维护关于责任限制的合同协议。

[30] 工作组似宜审议，是否应将电子印章视为一种单独的信任服务，还是可将其视为电子签名的一个子集。

[31] 工作组似宜审议，功能等同条文是否应延伸适用于法律“允许”该事的情形，并确认提及“要求”暗指不做该事的法律后果。

[32] 该条文草案是以《贸易法委员会电子可转让记录示范法》（《电子可转让记录示范法》）第9条为基础（联合国出版物，出售品编号：E.17.V.5），可加以调整，以确定在使用每项信任服务时所履行的功能。该条文草案没有就可靠性标准提供指导，可以在适用于所有信任服务的单独条款中规定这一标准（例如，见《电子可转让记录示范法》第12条）。

㈡ 其本身或结合进一步证据，事实上被证明已履行前述(a)项中所说明的功能。[33]]

电子时戳

2. 法律要求将[某些文件、记录或信息]与某一时间和日期关联的，如果使用了一种可靠方法将该时间和日期与[某一电子通信]关联，[对于该电子通信而言，]即为满足了这一要求。[34]

电子存档

3. 法律要求留存[某些文件、记录或信息]的，通过留存数据电文即为满足了这一要求，前提是满足下列条件：

(a) 其中所包含信息能够调取供日后查用；

(b) 以生成、发送或接收数据电文的格式留存数据电文，或以能够被证明可准确重现所生成、发送或接收信息的格式留存数据电文；以及

(c) 任何此种信息的留存可支持查明数据电文的来源和目的地以及数据电文的发送或接收日期和时间。[35]

电子登记交付服务

4. 法律要求提供[某一文件、记录或信息]的发送和接收证据的，如果使用了一种可靠方法传递[某一电子通信]，[对于该电子通信而言，]即为满足了这一要求。[36]

网站认证

5. 法律要求识别网站所有人身份的，如果使用了一种可靠方法识别网站所有人的身份并将该人与该网站关联，即为满足了这一要求。

电子托管

6. 法律要求使用托管服务的，如果使用了一种可靠方法**[**，将托管资产置于保管之下并将其发放给权利人**]**，即为满足了这一要求。

第 15 条 信任服务可靠性的推定[37]

1. 符合下列条件的，为满足第 14 条所述要求之目的，推定某一方法是可靠的：

---

[33] 这一备选案文是以《联合国国际合同使用电子通信公约》（2005 年，纽约）第 9 条第(3)款为基础，提供了关于可靠性标准的一般性指导。(b)(2)项包括一项安全条款，目的是在电子签名事实上已达到其功能的情况下避免否认。

[34] 工作组似宜审议是否应提及电子通信、数据电文或其他概念。

[35] 这一条件不适用于其唯一目的是支持发送或接收电文的信息：见《贸易法委员会电子商务示范法》第 10 条第 2 款，联合国出版物，出售品编号：E.99.V.4。

[36] 工作组似宜审议是否应提及电子通信、数据电文或其他概念。

[37] 按目前写法，该条文草案适用于电子签名，但经调整可适用于其他信任服务。

(a) 签名制作数据在其所使用范围内与签名人而不是与其他任何人关联；

(b) 签名制作数据在签名之时处于签名人而不是处于其他任何人控制之下；

(c) 凡在签名时间后对电子签名作出的更改均可被察觉；以及

(d) 如果对签名的法律要求的目的是就签名所涉信息的完整性提供保证，凡在签名时间后对该信息作出的更改均可被察觉。[38]

2. 第 1 款不限制任何人在下列方面的能力：

(a) 为满足第 14 条所述要求之目的，以其他任何方式确立电子签名的可靠性；或者

(b) 举出电子签名不可靠的证据。[39]

第 16 条 信任服务可靠性的确定[40]

1. [颁布国指明的个人、公共或私人机关或机构]可确定哪些电子签名满足了第 14 条的规定。

2. 依照第 1 款作出的任何确定应与公认国际标准一致。

第 17 条 信任服务提供人的义务

1. 信任服务提供人应确保其所提供的信任服务的可用性和正确操作。

2. 信任服务提供人应毫不拖延地将对所提供的信任服务或对其中保持的个人数据有[重大]影响的任何安全违规或完整性受损事件通知[监管机构][其受影响的客户[41]和依赖方][，任何情况下，通知应在得知该事件后[…]天内发出]。

3. 在发生重大安全违规或完整性受损事件时，信任服务提供人应暂停提供受影响的服务[，直至[...]]。

4. 如果发生下列情况，信任服务的用户应通知信任服务提供人：[42]

(a) 信任服务制作数据已失密；或者

(b) 用户所知悉的情况导致信任服务制作数据有重大失密风险；[43]

---

[38] 凡要求信任服务提供完整性保证的，均可使用该条文草案。

[39] 该条文草案是以《电子签名示范法》第 6 条第(3)款为基础。其中载有对那些符合某些标准的签名的可靠性的推定。如果对签名的法律要求的目的是就签名所涉信息的完整性提供保证，则这些标准提及完整性。

[40] 该条文草案使得能够对电子签名的可靠性进行事前评估。按目前写法，该条文草案适用于电子签名，但经调整可适用于其他信任服务。

[41] 工作组似宜考虑界定“用户”和“客户”概念。

[42] 工作组似宜考虑界定“用户”和“客户”概念。

[43] 关于必须发出通知的时限规定、确定需通知的当事人，以及确定触发通知义务的服务或个人数据受影响程度，该条文草案提供了可选措辞。还可以确立一种义务，规定直至泄密或受损得到控制或建立起新的认证或类似流程，必须暂停信任服务。

第 18 条　信任服务提供人的赔偿责任

1.　在不影响依据法律可能产生的赔偿责任的情况下，信任服务提供人应对由于未遵守本[文书草案]对其规定的义务[故意或因疏忽而]给任何人造成的损害[承担赔偿责任][承担法律后果]。

2.　对于因服务的使用超出对[可能使用信任服务的交易的目的或价值]的限制而造成的损害，信任服务提供人不应承担赔偿责任，前提是信任服务提供人提供了合理可及的手段，使[用户[44]或]第三方能够确认这些限制。[45]

第五章　国际方面

第 19 条　对外国身份管理和信任服务的法律承认

1.　在确定[身份管理系统][身份证书]或信任服务是否或在多大程度上具有法律效力时，不应考虑：

(a)　[签发或使用身份证书][运行身份管理系统]或提供信任服务的地理位置；

(b)　[签发人][身份管理系统运营人]、信任服务提供人或主体的营业地地理位置。

2.　在[颁布法域]境外[运行的身份管理系统][签发的身份证书]或提供的信任服务，如果具有[基本等同的][相同的]可靠度，应在[颁布法域]境内具有与在[颁布法域]境内[运行的身份管理系统][签发的身份证书]或提供的信任服务相同的法律效力。

3.　在确定[身份证书][身份管理系统]或信任服务是否提供[基本等同的][相同的]可靠度时，应考虑到[公认国际标准]。[46]

第 20 条　合作

[颁布国指明的个人、公共或私人机关或机构][应][可]与外国实体合作，交流与身份管理和信任服务有关的信息、经验和良好做法，特别是在以下方面：

(a)　核证身份管理系统和信任服务；

(b)　界定身份管理系统的保证级和信任服务的可靠度；以及

(c)　审查相关发展情况。

---

[44] 工作组似宜考虑界定“用户”和“客户”概念。

[45] 该条文草案旨在维护关于责任限制的合同协议。

[46] 工作组似宜确认，如果颁布上述规定，其效果是将颁布法域法律的所有规定适用于身份管理系统或身份证书，例如，包括法规或合同中规定的责任限制规则。