联合国 A/CN.9/WG.IV/WP.160

大 会

Distr.: Limited
16 September 2019
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十九届会议
2019 年 11 月 25 日至 29 日，维也纳

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

V.19-09429 (C) 071019 071019

一. 导言

1. 本文件附件所载关于身份管理和信任服务的条文修订草案纳入了工作组第五十八届会议（2019 年 4 月 8 日至 12 日，纽约）的审议情况以及秘书处应工作组要求与专家协商的结果（A/CN.9/971，第 67 段）。为此，秘书处召开了一次专家组会议（2019 年 7 月 22 日至 23 日，维也纳），讨论对身份管理系统获得法律承认所要求的标准和程序，以及条文草案中涵盖的其他事项，特别是身份管理系统的可靠性，以及身份管理服务提供人的义务和责任。

2. 关于第四工作组目前工作的背景资料载于 A/CN.9/WG.IV/WP.159 号文件，第 6-17 段。

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　总则

第 1 条　定义

在本[文书]中：

(a) “属性”指与主体关联的一条信息或数据；[1]

(b) “数据电文”指经由电子手段、电磁手段、光学手段或类似手段生成、发送、接收或存储的信息；

(c) “身份识别”指收集、验证并核证充分属性以在特定环境下确定并确认主体身份的过程；[2]

(d) “身份”指在特定环境下[允许充分辨认主体][对主体作出[独一]描述]的一组属性；[3]

(e) “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而可出示的数据或数据可能驻留的物理架构]；[4,5]

(f) “身份管理服务”指包含在网上环境中对主体的身份识别进行管理的服务；

(g) “身份管理服务提供人”指[提供身份管理服务][提供与身份管理系统相关的服务][负责身份管理系统]的人；[6,7]

---

[1] 见 A/CN.9/WG.IV/WP.150，第 13 段。

[2] 见 A/CN.9/WG.IV/WP.150，第 29 段。工作组似宜审议，该定义是否准确地反映了条文草案（尤其谨记第 9 条草案）中对“身份识别”这一术语的使用，或者是否应对该定义进行修订，以纳入其他身份管理流程，如登记和签发身份证书。

[3] 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，考虑到(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，就工作组此项工作而言是否需要独一性要求（A/CN.9/965，第 10 段）。

[4] 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。

[5] 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”。

[6] 工作组商定使用“身份管理服务提供人”一词，而不是“身份管理系统运营人”（A/CN.9/971，第 97 段）。

[7] 工作组似宜审议，鉴于 A/CN.9/WG.IV/WP.150 号文件第 37 段中“身份提供人”的定义，即(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；(b)创建、维护和管理其他实体（如，用户/订户、组织和设备）可信赖的身份信息，并基于信任、业务和其他类型的关系提供基于身份的服务的实体，是否应按其现在的形式保留该定义；

(h) “身份管理系统”指在网上环境中对主体的身份识别进行管理的一套流程；[8]

(i) “依赖方”指可在身份管理服务或信任服务的基础上行事的人；

(j) “主体”指在特定环境范围内加以识别的人或架构；[9]

(k) “信任服务”[10]指就数据品质提供一定程度可靠性的电子服务；

(l) “信任服务提供人”指提供一项或多项信任服务的人。

第 2 条 适用范围

本[文书]适用于在商业活动[11]以及与贸易有关的[政府]服务[12]中使用和跨境承认身份管理系统和信任服务。[13]

第 3 条 身份管理和信任服务的自愿使用[14]

1. 本[文书]中的规定概不要求主体在其未予同意的情况下[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，可根据主体的行为推断主体是否同意。[15]

---

[8] 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“以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，使用个人身份识别数据[即本文件中所定义的“身份证书”]的过程”。

[9] 见 A/CN.9/WG.IV/WP.150，第 38 段。

[10] 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）。

[11] 按照工作组第五十八届会议商定的意见重拟了该条文，将 A/CN.9/WG.IV/WP.157 号文件第 1 条第 1 款中提出的两项备选案文的内容合并在一起（A/CN.9/971，第 23 段）。委员会第五十二届会议指出，在项目的这一早期阶段，工作组应努力制定一项既适用于国内使用也适用于跨国界使用身份管理和信任服务的文书（A/74/17，第 172 段）。这一立场反映在该条文提及身份管理系统和信任服务的“使用”和“承认”这一点上。

[12] 工作组似宜审议，是否有必要提及“政府”，或者一般提及“与贸易有关的服务”是否足以涵盖那些与贸易有关但并非商业性质的交易，例如，与海关业务电子单一窗口的互动。

[13] 工作组一致认为，文书应表达将此项工作成果用于纯商业环境以外的需要的可能性（A/CN.9/971，第 23 段）。委员会第五十二届会议指出，此项工作的成果对商业交易以外的事项有影响（A/74/17，第 172 段）。

[14] A/CN.9/WG.IV/WP.157 号文件第 2 条草案中涉及“不受本[文书草案]影响的事项”的内容现已并入第 5 和 13 条草案。同样，工作组似宜审议，是否应将目前第 3 条草案的内容并入第 5 和 13 条草案。

[15] 如果主体是没有自主行为能力的物理或数字架构，将由对该主体负有法律责任的自然人或法人作出是否同意的表示（A/CN.9/965，第 109 段）。

第 4 条　解释[16]

1. 在解释本[文书]时，应考虑到本[文书]的国际性以及促进其统一适用和[在国际贸易中]遵守诚信的必要性。

2. 涉及本[文书]所管辖事项的问题，未在本[文书]中明确解决的，应按照本[文书]所依据的一般原则加以解决，其中特别是不歧视电子手段的使用、技术中性和功能等同原则[以及……][17]，[或者，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。[18]

第二章　身份管理

第 5 条　对身份管理的法律承认[19]

1. 不得仅根据下述理由之一而否定[身份证书][身份管理系统][的使用]的法律效力、有效性、可执行性或证据可采性：

(a) [身份验证[20]的结果是][身份管理系统是]电子形式；或者

(b) 身份管理系统不是根据第 11 条指定的身份管理系统。

2. 本[文书]中的规定概不要求某人识别主体身份或使用特定的身份管理服务。

3. 除本[文书]另有规定外，本[文书]中的规定概不影响对身份管理服务适用任何法律规则[，包括适用于隐私和数据保护的任何法律规则][21]。

4. 本[文书]中的规定概不影响按照法律所界定或规定的程序识别主体身份的法律要求。[22]

第 6 条　身份管理服务提供人的义务

身份管理服务提供人应[至少]：[23]

(a) 对主体进行注册，包括以下述方式：

---

[16] 工作组第五十八届会议没有审议关于文书解释的条文（A/CN.9/WG.IV/WP.157 号文件第 5 条草案）。该条文是以贸易法委员会其他法规中的类似条款为基础。工作组似宜审议，是否应提及诚信，如果是，是否具体说明“在国际贸易中遵守诚信”。

[17] 工作组似宜审议，是否应列出其他一般原则，即透明度原则（见 A/CN.9/936，第 88 段）。

[18] 所添加的案文“或者，无此种原则的，应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。

[19] 第 5 条草案第 1 款仿照第 13 条草案，后者又反映了工作组第五十八届会议的审议情况。该条文规定了使用电子手段进行身份识别的法律效力，而不论是否存在非网上身份识别程序。第 2 至 4 款是仿照 A/CN.9/WG.IV/WP.157 号文件第 2 条草案。

[20] 如果保留(a)项中的第一个备选案文，工作组似宜考虑增加对身份“认证”的提及，以与第 1 条中“身份证书”定义中的措辞相一致。

[21] 提到隐私和数据保护反映了工作组对这些问题的重视，同时确认这些问题不在工作组的任务授权范围内（A/CN.9/965，第 125 段）。

[22] 这是一个新条文，处理工作组第五十二届会议提出的一项关切（A/CN.9/971，第 30 段）。

[23] 这些是在专家协助下确定的身份管理服务提供人的基本义务。

㈠ 登记并收集属性；

㈡ 进行身份检验和验证；并且

㈢ 身份证书与主体绑定；

(b) 更新属性；

(c) 根据管辖身份管理系统的规则管理身份证书，包括以下述方式：

㈠ 签发、交付和激活证书；

㈡ 暂时取消、吊销和重新激活证书；并且

㈢ 续订和更换证书；

(d) 对主体进行认证，包括以下述方式：

㈠ 管理认证因素；并且

㈡ 管理认证机制；

(e) 确保身份管理系统的在线可用性和正确操作；并且

(f) 提供对管辖身份管理系统的规则的合理访问权。[24]

第 7 条 身份管理服务提供人在发生数据泄露情况下的义务

1. 如果发生了对身份管理系统（包括其中管理的属性）有[重大]影响的安全违规或完整性丧失情形，身份管理服务提供人应：

(a) 立即向[监管机构][受影响的主体和依赖方] 通知安全违规或完整性丧失情形 ；

(b) 纠正安全违规或完整性丧失情形；

(c) 暂时取消受影响的[身份证书]，直至安全违规或完整性丧失事件得到纠正；

(d) 毫不延迟地重建受影响的[身份证书]；并且

(e) 安全违规或完整性丧失情形无法在[时间范围]内得到纠正的，吊销受影响的[身份证书]。

2. 如果主体向身份管理服务提供人通知了安全违规或完整性丧失情形，则身份管理服务提供人应：

(a) 调查潜在的安全违规或完整性丧失情形；并且

[24] 加入(f)项是为了反映提供身份管理服务方面的透明度原则（另见第 12 条草案第 2 款(b)项）。工作组第五十六届会议确定透明度原则与今后关于身份管理的讨论有关（A/CN.9/936，第 88 段）。

(b) 根据第 1 款采取其他任何适当行动。[25,26]

第 8 条 主体和依赖方的义务

1. 主体应遵守身份管理服务提供人传达的指示，以避免未经授权使用身份证书或认证过程。

2. 有下列情况的，主体应通知身份管理服务提供人：

(a) 主体知道相关身份管理系统的身份证书或认证过程已失密；或者

(b) 主体所知道的情况导致身份证书或认证过程有重大失密风险。

3. 有下列情况的，依赖方应通知身份管理服务提供人：

(a) 依赖方知道相关身份管理系统的身份证书或认证过程已失密；或者

(b) 依赖方所知道的情况导致身份证书或认证过程有重大失密风险。

第 9 条 使用身份管理系统进行的身份识别

法律或一方当事人要求按照某种[方法][政策]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][身份管理系统]识别该主体的身份，即为满足了这一要求。[27,28,29]

第 10 条 与确定可靠性相关的因素[30]

1. 在确定[方法][身份管理系统]的可靠性时，应考虑到所有相关情况，其中可包括：

(a) 身份管理服务提供人遵守第 6 条所列义务的情况；

(b) 身份管理系统的运营规则是否符合包括保证级框架在内的任何公认国际标准和程序，特别是关于以下方面的规则：

㈠ 治理；

---

[25] 该款落实了一项建议，即条文草案应规定身份管理服务提供人有义务在接到安全违规通知后采取行动（A/CN.9/971，第 88 段）。

[26] 关于必须发出通知的时限规定、确定需通知的当事人，以及确立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。

[27] 该条文反映了工作组第五十八届会议商定的工作草案（A/CN.9/971，第 49 段）。工作组似宜审议，是否应提及“身份管理系统”，而不是“可靠的方法”。

[28] 使用可靠的识别方法（或身份管理系统）是文书草案中身份管理法律承认制度的基石。文书草案设想了两种确定可靠性的机制：第 10 条草案提供了事后确定可靠性的相关因素指示性清单；第 11 条草案规定建立事先指定可靠方法（或身份管理系统）的机制。经与专家协商，删除了关于可靠性推定的条文（A/CN.9/WG.IV/WP.157 号文件第 10 条草案），以简化文书草案。A/CN.9/WG.IV/WP.157 号文件第 10 条草案第 2 款的内容已并入第 11 条草案第 5 款。

[29] 工作组似宜审议，第 9 条草案是否涉及需要在网上和非网上身份识别之间建立功能等同的情形。如果不是这样，不妨按以下写法插入一个新条文：“在法律规则要求或允许对主体进行身份识别的情况下，使用一种可靠的身份管理系统即为满足了该规则”。

[30] 该条文的标题反映了工作组第五十八届会议商定的意见（A/CN.9/971，第 59 段）。

㈡ 发布的通知和用户信息；

㈢ 信息安全管理；

㈣ 保持记录；

㈤ 设施和工作人员；

㈥ 技术控制；以及

㈦ 监督和审计；

(c) 就身份管理系统提供的任何监督或核证；以及

(d) 当事人之间的任何协议。

2. 在确定[方法][身份管理系统]的可靠性时，不得考虑：

(a) 身份管理系统运营的地理位置；或者

(b) 身份管理服务提供人营业地的地理位置。[31]

第 11 条 可靠身份管理系统的指定

1. [颁布国指明的主管个人、公共或私人机关或机构]可指定第 9 条所指的可靠[方法][身份管理系统]。[32,33]

2. 根据第 1 款作出的任何指定应符合与确定身份管理系统可靠性相关的公认国际标准和程序，包括保证级框架。[34,35]

3. 在指定一种[方法][身份管理系统]时，不得考虑：

(a) 身份管理系统运营的地理位置；或者

(b) 身份管理服务提供人营业地的地理位置。[36]

4. 使用根据第 1 款指定的身份管理系统签发的身份证书对一主体进行的身份识别，应被承认是该主体身份的可靠证明。

5. 第 4 款不限制任何人在以下方面的能力：

(a) 以其他任何方式确证第 9 条所指的[方法][身份管理系统]可靠性；或者

---

[31] 这是一项基于《贸易法委员会电子签名示范法》(《电子签名示范法》) 第 12 条的不区别对待地理位置的条文，其本意是支持跨境承认身份管理系统。

[32] 该条文作了修订，以反映工作组第五十八届会议商定的修改意见（A/CN.9/971，第 76 段），另外由于与专家协商后对该条文作了修改还加入提及第 9 条的内容。加入了“第 9 条所指的可靠的”字样。

[33] 工作组似宜审议，文书是否应涉及因使用根据第 11 条草案所指定的可靠系统而产生的损害赔偿责任。

[34] 该条文作了修订，以反映工作组第五十八届会议商定的修改意见（A/CN.9/971，第 76 段）。

[35] 工作组似宜澄清，第 10 条草案所列要素是否以及如何适用于根据第 11 条草案指定可靠的身份管理系统（即，是否要求指定人/机关/机构考虑到第 10 条第 1 款所列的情况）。

[36] 这是一项基于《电子签名示范法》第 12 条的不区别对待地理位置的条文，其本意是支持跨境承认身份管理系统。

(b) 就依据第 1 款指定的[方法][身份管理系统]的不可靠性举出证据。

第 12 条 身份管理服务提供人的赔偿责任

1. 身份管理服务提供人应对由于故意或因疏忽而未遵守其[因提供身份管理服务而产生的][在第 6 条之下的]义务而给任何人造成的损害承担赔偿责任。[37]

2. 虽有第 1 款的规定，身份管理服务提供人不应对由于使用身份管理系统而造成的损害承担赔偿责任，但限于以下情况：

(a) 这种使用超出[对可能使用身份管理系统的交易的目的或价值的]限制；并且

(b) 身份管理系统提供人提供了合理可及的手段，使[[用户[38]或]第三方][39]能够确认这些限制。[40]

3. 如果[身份证书的签发或属性的归属]符合以下规定，则身份管理服务提供人不应对由于使用根据第 11 条指定的身份管理系统而给任何人造成的损害承担赔偿责任：

(a) 其因提供身份管理服务而产生的义务，包括第 6 条所列义务；

(b) 身份管理系统的运营规则，包括第 10 条第(1)款(b)项所列规则；以及

(c) 当事人之间的任何协议。

[4. 如果损害归因于构成[重大过失或故意不当行为]的身份管理服务提供人的作为或不作为，第 3 款不予适用。][41]

---

[37] 该条文反映了工作组第五十八届会议商定的工作草案（A/CN.9/971，第 101 段）。该条文作了进一步修订，以澄清导致规定赔偿责任的损害的原因。

[38] 如果使用该词，工作组似宜考虑界定“用户”一词。

[39] 工作组似宜审议，是否应当在该条草案中指明应当能够确认这些限制的当事人，如果是这样的话，这些当事人是否应当对应于身份管理系统提供人可能对其承担赔偿责任的当事人。

[40] 该条文草案是基于《电子签名示范法》第 9 条第(1)款(d)项㈡目。

[41] 该款取自 A/CN.9/WG.IV/WP.157 号文件第 13 条草案第 4 款。工作组似宜审议，鉴于第 1 款，是否可以删除第 4 款。

第三章　信任服务[42]

第 13 条　对信任服务的法律承认[43],[44]

1.　对于通过使用信任服务或在信任服务支持下交换、验证或认证的[信息][数据][45]，只要该信任服务[符合[本章的]要求，]不得仅根据下述理由之一而否定其法律效力、有效性、可执行性[或证据可采性][46]：

(a)　其为电子形式；或者

(b)　其不为根据第 24 条指定的可靠的信任服务所支持。

2.　本[文书]中的规定概不要求某人使用特定的信任服务。[47]

3.　除本[文书]另有规定外，本[文书]中的规定概不影响对信任服务适用任何适用于信任服务的法律规则[，包括适用于隐私和数据保护的任何法律规则]。[48]

第 14 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.　如果发生了对信任服务有[重大]影响的安全违规或完整性丧失情形，信任服务提供人应：

(a)　暂停提供受影响的服务，[直至[违规或完整性丧失情形得到控制或建立起新的认证或类似流程]]；并且

(b)　纠正安全违规或完整性丧失情形。

---

[42] 关于信任服务的一章已经修订。这一章现在设有一个关于信任服务的法律承认的总则（第 13 条草案）；一条可靠性一般标准，其中包括旨在便利跨境承认的不区别对待地理位置的条款（第 23 条草案）；一种事先指定可靠信任服务的机制（第 24 条草案），以及将用作“构件”的信任服务清单（第 16-22 条草案），综合起来可以为数据的某些质量提供保证。特别是，电子签名涉及数据的发端人（“谁”）以及发端人创建数据的意图（“为什么”）；电子时戳涉及与数据有关的某些事件发生的时间（“何时”）；一个关于完整性的新条文涉及数据自某一时间点一直没有被更改的保证（“是什么”）；交付服务涉及数据信息在网络空间中的位置（“何处”）。

[43] 加入该条文是为了反映工作组第五十八届会议商定的意见（A/CN.9/971，第 112-115 段）。

[44] 工作组似宜审议，这一非歧视条文的重点是否应放在所交换、验证或认证的信息（或数据）上，而不是用于验证和认证的方法。该条文先前的草案时基于后一种做法，其案文如下：“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”（A/CN.9/WG.IV/WP.157 号文件第 6 条第 2 款）。

[45] 工作组似宜审议，是否应提及“数据”，以使该条文与“信任服务”的定义保持一致。

[46] 建议插入“或证据可采性”，以使该条文与第 5 条草案保持一致。

[47] 第 2 和第 3 款是借鉴 A/CN.9/WG.IV/WP.157 号文件第 2 条草案。

[48] 提到隐私和数据保护反映了工作组对这些问题的重视，同时确认这些问题不在工作组的任务授权范围内（A/CN.9/965，第 125 段）。

3. 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丧失情形通知[监管机构][其受影响的客户[49]和依赖方][，任何情况下，通知应在得知该情形后[……]天内发出]。[50,51]

第 15 条 信任服务提供人在发生数据泄露情况下的义务

如果发生下列情况，信任服务的用户[52]应通知信任服务提供人：

(a) 信任服务制作数据已失密；或者

(b) 用户所知道的情况导致信任服务制作数据有重大失密风险；

第 16 条 电子签名

法律规则要求或允许有[某人][主体]签名的，如果使用了一种可靠方法进行以下操作，[就一项数据电文而言，]即为满足了该规则的要求：[53]

(a) 识别该人的身份；并且

(b) 指明该人对于该数据电文中包含的信息的意图。[54]

第 17 条 电子印章[55]

法律规则要求或允许某人加盖印章的，如果使用了一种可靠方法进行以下操作，[就一项数据电文而言，]即为满足了该规则的要求：

(a) 识别该人的身份；并且

(b) 检测加盖印章后对该数据电文的任何更改。

---

[49] 工作组似宜考虑界定“客户”概念。

[50] 该款取自 A/CN.9/WG.IV/WP.157 号文件第 17 条草案第 2 款。工作组似宜审议，是否可将其中所载义务改为第 2 款(c)项，以与第 7 条草案一致。

[51] 关于必须发出通知的时限规定、确定需通知的当事人，以及确立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。

[52] 工作组似宜考虑界定术语“用户”。

[53] 与评估身份管理系统可靠性所采用的方法相似的是，条文草案为确定信任服务的可靠性预见了两种机制：第 23 条草案提供了一个事后确定可靠性的相关因素指示性清单；第 24 条草案规定建立一种事先指定可靠的信任服务的机制。同样与身份管理系统所采用的方法相似的是，删除了关于推定可靠性的条文（A/CN.9/WG.IV/WP.157 号文件第 15 条草案），以求简化文书草案。A/CN.9/WG.IV/WP.157 号文件第 15 条草案第 2 款的内容已并入第 24 条草案第 5 款。

[54] 在第五十八届会议上提出，加入“以第三方以后可以验证该意图的方式”的字样，以考虑到电子签名的“长久化”功能（以第三方以后可以验证该意图的方式——见 A/CN.9/971，第 122 段）。同样还提出，没有必要加入这些词语，因为日后进行验证的能力乃是电子签名的一种必要特质（同上）。

[55] 该条文反映了工作组商定的意见，即加入一个关于电子印章的独立条文（A/CN.9/971，第 128 段）。本着脚注 41 中解释的精简办法，工作组似宜审议，是否有必要制定一个独立条文，或者是否可以通过（在身份识别方面）使用电子签名以及（在检测变更情况方面）保证完整性来实现使用电子印章所寻求的同样功能。

第 18 条 电子时间戳

法律规则要求或允许将[某些文件、记录、信息或数据[56]]与某一时间和日期关联的，如果使用了一种可靠方法进行以下操作，[就一项数据电文而言，]即为满足了该规则的要求：

(a) 指明该时间和日期，包括注明时区；并且

(b) 将该时间和日期与该数据电文相关联。[57]

第 19 条 完整性保证[58]

法律规则要求或允许为[文件、记录、信息或数据]的完整性提供保证的，[无论是通过保留该文件的原件形式、存档抑或其他方式，]就一项数据电文而言，除附加任何签注以及正常通信、存储和显示过程中出现的任何改动之外，如果使用了一种可靠方法检测该数据电文创建后对其的任何更改，即为满足了该规则的要求。[59]

第 20 条 电子存档[60]

法律规则要求或允许留存[某些文件、记录或信息]的，通过留存数据电文即为满足了该规则的要求，前提是：

(a) 其中包含的信息可调取以供日后查询时使用；

(b) 数据电文是以下述格式留存的：

㈠ 以生成、发送或接收数据电文的格式；或者

㈡ 以能够被证明可准确重现所生成、发送或接收信息的格式；并且

(c) 任何此种信息的留存可支持查明数据电文的发端地和目的地以及数据电文的发送或接收日期和时间。[61]

---

[56] 加入“数据”一词反映了工作组商定的意见（A/CN.9/971，第 130 段）。

[57] 加入“包括注明时区”这一短语反映了工作组商定的意见（A/CN.9/971，第 132 段）。

[58] 加入该条文是为了引入一条关于数据电文完整性的一般规则。这条规则提供了对纸质环境中“原件”概念的功能等同。该条文是作为关于电子存档的第 20 条的备选案文提交工作组的。按照该规则的这种表述，信任服务是有明显标志的（即提供可靠的方法检测更改情况）。

[59] 工作组似宜审议是否列入一项要求，即数据电文中包含的信息是“可调取以供日后查询时使用的”（另见条文 20(a)草案）。

[60] 如果保留第 19 条草案，工作组似宜审议，是否应删除多余的第 20 条草案。

[61] 此项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。

第 21 条 电子登记交付服务

法律规则要求或允许提供[某一文件、记录或信息]的发出和收到证据的，[就一项数据电文而言，]如果使用了一种可靠方法提供[该数据电文]已离开或进入某一信息系统的保证，即为满足了该规则的要求。[62]

第 22 条 网站认证[63]

法律规则要求或允许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，即为满足了该规则的要求。

第 23 条 信任服务可靠性标准[64]

1. 在第[16 至 22]条中，

(a) 从所有相关情形来看，所指的方法对于使用该方法所要实现的功能既应适当，也应可靠，相关情形可包括：

㈠ 管辖信任服务的运营规则；

㈡ 任何适用的行业标准；

㈢ 硬件和软件的安全性；

㈣ 财力和人力资源，包括资产的存在；

㈤ 独立机构审计的经常性和范围；

㈥ 监督机构、资格鉴定机构或自愿方案就该方法可靠性作出的声明；和

㈦ 任何相关协议；或者

(b) 该方法事实上证明已履行相关信任服务的有关功能。

2. 在确定第[16 至 22]条所指的方法的可靠性时，不应考虑：

(a) 信任服务运营的地理位置；或者

(b) 信任服务提供人营业地的地理位置。[65]

---

[62] 这一案文反映了工作组商定的意见，即在该条文草案中纳入《联合国国际合同使用电子通信公约》第 10 条的内容（A/CN.9/971，第 141 段）。

[63] 本着脚注 41 中解释的精简办法，工作组似宜审议，是否可以通过使用电子签名识别数字对象（包括网站）来实现网站认证所寻求的功能。

[64] 第 1 款(a)项下所列要素借鉴了《电子签名示范法》第 10 条和《贸易法委员会电子可转让记录示范法》第 12 条(a)项，其中规定了对所用方法的可靠性一般标准。

[65] 这是一项基于《电子签名示范法》第 12 条的不区别对待地理位置的条文，其预期效果是支持跨境承认信任服务。

第 24 条 可靠的信任服务的指定[66,67]

1. [颁布国指明的个人、公共或私人机关或机构]可指定第[16 至 22]条所指的可靠[方法][信任服务]。

2. 根据第 1 款作出的任何指定应符合与确定信任服务可靠性相关的公认国际标准和程序，包括可靠度框架。[68]

3. 在指定一种[方法][信任服务]时，不得考虑：

(a) 信任服务运营的地理位置；或者

(b) 信任服务提供人营业地的地理位置。[69]

4. 使用根据第 1 款指定的一项信任服务，应被承认是[该信任服务的相关数据品质]的可靠证明。

5. 第 4 款不限制任何人在以下方面的能力：

(a) 以其他任何方式确证第[16 至 22]条所指的[方法][信任服务]的可靠性；或者

(b)就依据第 1 款指定的[方法][信任服务]的不可靠性举出证据。

第 25 条 信任服务提供人的赔偿责任

1. 信任服务提供人应对由于故意或因疏忽而未遵守其[因提供信任服务而产生的][在[本文书][第 14 条]之下的]义务而给任何人造成的损害承担赔偿责任。

2. 虽有第 1 款的规定，信任服务提供人不应对由于使用信任服务而造成的损害承担赔偿责任，但限于以下情况：

(a) 这种使用超出[对可能使用信任服务的交易的目的或价值的]限制；并且

(b) 信任服务提供人提供了合理可及的手段，使[[用户[70]或] 第三方][71]能够确认这些限制。[72]

---

[66] 工作组似宜澄清，第 23 条草案所列要素是否以及如何适用于根据第 24 条草案指定可靠的信任服务（即，是否要求指定人、机关或机构考虑到第 23 条第 1 款(a)项所列的情况）。

[67] 该条文草案使得能够对信任服务的可靠性进行事前评估。

[68] 该条文作了修订，以反映工作组第五十八届会议商定的修改意见（A/CN.9/971，第 76 段）。

[69] 这是一项基于《电子签名示范法》第 12 条的不区别对待地理位置的条文，其预期效果是支持跨境承认信任服务。

[70] 如果使用该词，工作组似宜考虑界定“用户”一词。

[71] 工作组似宜审议，是否应当在该条草案中指明应当能够确认这些限制的当事人，如果是这样的话，这些当事人是否应当对应于信任服务提供人可能对其承担赔偿责任的当事人。

[72] 该条文草案是基于《电子签名示范法》第 9 条第(1)款(d)项㈡目。

第四章　国际方面

第 26 条　身份管理和信任服务的跨境承认[73]

1.　在[颁布法域]境外[运营的身份管理系统][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[运营的身份管理系统][签发的身份证书]或提供的信任服务相同的法律效力。[74,75]

2.　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]。

第 27 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；并且

(b)　界定身份管理系统的保证级和信任服务的可靠度。

---

[73] 该条文取自 A/CN.9/WG.IV/WP.157 号文件第 19 条草案第 2 和 3 款。工作组似宜审议，鉴于在第 10、11、23 和 24 条中插入了关于不区别对待地理位置的条款，是否还应保留该条文。

[74] 该条文借鉴了《电子签名示范法》第 12 条第 2 款。因此，该条文草案中使用的“可靠度”一词不一定具有文书其他条文草案中的同样含义。

[75] 工作组似宜审议，该条文是否意味着对外国身份管理或信任服务适用颁布法域的一切法律规则，包括本文书的规定以及法规或合同中关于赔偿责任限制的规则。