联合国 A/CN.9/WG.IV/WP.162

大 会

Distr.: Limited
28 January 2020
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第六十届会议
2020 年 4 月 6 日至 9 日，纽约

关于使用和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.20-00754 (C) 260220 260220

一. 导言

1. 如 A/CN.9/1005 报告所述，本文件附件所载关于使用和跨境承认身份管理和信任服务的条文修订草案（“本草案”）纳入了工作组第五十九届会议（2019 年 11 月 25 日至 29 日，纽约）的审议情况。在本草案所附脚注中，工作组第五十九届会议所审议的载于 A/CN.9/WG.IV/WP.160 号文件中的条文草案被称为“前一版草案”。

2. 工作组似宜注意到，本草案载有对术语的修改，以解决对潜在不同理解的各种关切。特别是，“认证”一词已改为“电子身份识别”，原来称为“身份识别”的程序现在称为“身份核实”（第 1 条）。因此，身份管理过程现在由两个阶段（或步骤）组成，即“身份核实”和“电子身份识别”。“认证”一词现在专门用于信任服务（第 21 和第 22 条）。

3. 关于第四工作组目前工作的背景资料载于 A/CN.9/WG.IV/WP.161 号文件第 6-18 段。

附件一

关于使用和跨境承认身份管理和信任服务的条文草案[1]

第一章　总则

第 1 条　定义

在本[文书]中：

(a)　“属性”指与[主体][人]关联的一条信息或数据；[2]

(b)　“认证”，在信任服务的范围内，指用以分配架构标识的过程；[3]

(c)　“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；[4]

[1] 文书的形式：在工作组第五十九届会议初步讨论期间，对文书采用示范法形式而不是公约形式表示了强烈倾向（A/CN.9/1005，第 123 段）。本草案中使用“[文书]”一词，尚待工作组将文书转呈委员会通过时就此问题作出决定。

[2] 定义—“属性”：这一定义取自 A/CN.9/WG.IV/WP.150 号文件第 13 段。该术语用于“身份核实”和“身份”的定义以及第 6 和第 7 条。

关于“主体”和“人”的用法，取决于工作组对“主体”定义的审议结果，见脚注 14。

[3] 定义—“认证”：“认证”系新加入的定义，指使用信任服务确认架构身份的过程。工作组似宜结合某些建议审议该项定义，这些建议提出引入一项关于架构认证的一般条文（第 22 条）并将架构排除在身份管理条文的范围之外（第 1 条(k)项，“主体”的定义）。

[4] 定义—“数据电文”：这一定义取自贸易法委员会关于电子商务的现有法规，特别是《贸易法委员会电子商务示范法》《电子商务示范法》（联合国出版物，出售品编号：E.99.V.4）和《联合国国际合同使用电子通信公约》《电子通信公约》（联合国，《条约汇编》，第 2898 卷，第 50525 号，第 3 页）。该术语用于界定第三章所列各种信任服务的要求。如“信任服务”定义中所阐明的，数据电文的这种特质才是每项信任服务的重点。

(d) “电子身份识别”，在身份管理服务的范围内，指用以实现对[主体][人]与身份之间绑定的充分保证的过程；[5,6,7]

(e) “身份”指允许在特定环境下对[主体][人]进行独特辨别的一组属性；[8]

(f) “身份凭证”指[主体][人]为了对其身份进行电子身份识别而可以电子形式出示的数据或数据可驻留的物理架构；[9]

(g) “身份管理服务”指包含对[主体][人]的电子形式的身份核实或电子身份识别进行管理的服务；[10]

(h) “身份管理服务提供人”指提供身份管理服务的人；[11]

---

[5] 定义—“电子身份识别”：如第上文第 2 段所述，本草案使用“电子身份识别”这一术语，而不是“认证”这一术语，以解决对“认证”的多重含义的关切。在工作组第五十九届会议上，就“认证”这一术语的含义以及在使用该术语的不同语境中其是否具有相同含义提出了若干问题（A/CN.9/1005，第 13、84-85、92 段）。工作组请秘书处确保整个文件中术语使用的一致性，并与国际电信联盟（国际电联）所采用的术语保持一致（见 A/CN.9/1005，第 86 段）。

“电子身份识别”的定义取自 A/CN.9/WG.IV/WP.150 号文件第 15 段中“认证”的定义，其又取自国际电联的建议 ITU-T X.1252。定义中使用了“保证”一词，而不是“信任”，其依据是：(a) 本草案使用了“保证”一词；(b)“建议 ITU-T X.1252”在认证的语境中将“保证”等同于“信任”，“保证级”被定义为“对实体与所显示的身份信息之间绑定的信任程度”表明了这一点。

本草案中，“身份凭证”、“身份管理服务”、“身份管理系统”的定义以及第 5、第 6、第 8 和第 9 条都在身份管理方面使用了这样定义的“电子身份识别”概念。

在文书草案中，“认证”这一术语是指使用信任服务来识别架构，这与信任服务“网站认证”的标题是一致的。

[6] 定义—“电子身份识别因素”：工作组似宜审议是否应在文书草案中加入以下定义：“‘电子身份识别因素’，在身份管理服务的范围内，指用以通过电子方式识别主体身份的某条信息或程序”。为此，工作组似宜谨记“电子身份识别”和“身份凭证”的定义。该定义依据的是 A/CN.9/WG.IV/WP.150 号文件第 17 段所载定义。“电子身份识别因素”这一术语仅在第 6 条中使用。

[7] 定义—“电子身份识别机制”：工作组似宜审议是否应在文书草案中加入以下定义：“‘电子身份识别机制’，在身份管理服务的范围内，指主体使用身份凭证进行自我身份识别所借助的机制”。该定义取自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）第 8 条第 3 款(c)项，该条例撤销第 1999/93/EC 号指令（《电子身份识别和信任服务条例》）。为此，工作组似宜谨记“电子身份识别”和“身份凭证”的定义。“电子身份识别机制”这一术语仅在第 6 条中使用。

[8] 定义—“身份”：这一定义取自 A/CN.9/WG.IV/WP.150 号文件第 31 段。在工作组第五十九届会议上，普遍认为应在该定义中列入“独特性”要求（见 A/CN.9/1005，第 108 段）。

[9] 定义—“身份凭证”：这一定义取自 A/CN.9/WG.IV/WP.150 号文件第 21 段。该术语与《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。该定义包含根据《弗吉尼亚电子身份管理法》（《弗吉尼亚法典》第 59.1 篇第 50 章）第 59.1-550 条中的定义的要素。在工作组第五十九届会议上指出，电子身份凭证可以离线使用，因此建议该定义改为提及“电子形式的”（而不是“在网上环境中的”）的身份证书。工作组同意据此对该定义作出修改（A/CN.9/1005，第 110 段）。

[10] 定义—“身份管理服务”：这一定义取自 A/CN.9/WG.IV/WP.150 号文件第 31 段选项(a)。该定义反映了这样的理解，即身份管理包含两个阶段（或步骤）：“身份核实”和“电子身份识别”（以前称“身份识别”和“认证”：A/CN.9/1005，第 84 段）。曾经对身份管理的定义并列提及这些阶段表示了一些关切（A/CN.9/965，第 91 段）。考虑到这一关切，该定义提及“身份核实或电子身份识别”，要注意的是，“或”字不是非此即彼的意思（A/CN.9/1005，第 109 段）。使用“电子形式”的提法，是依照工作组就“身份凭证”的定义商定的意见（见脚注 9）。“身份识别”一词被改为“身份核实”，以反映术语上的变化（见脚注 13）。

[11] 定义—“身份管理服务提供人”：这一定义反映了工作组第五十九届会议商定的意见（A/CN.9/1005，第 111 段）。

(i) “身份管理系统”指对[主体][人]的电子形式的身份核实和电子身份识别进行管理的一套功能和能力；[12]

(j) “身份核实”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][人]身份的过程；[13]

(k) “主体”指人[或架构][14]；

(l) “订户”指与身份管理服务提供人或信任服务提供人订立提供身份管理服务或信任服务安排的人。[15]

(m) “信任服务”指就数据电文的某些品质提供保证的电子服务，包括电子签名、电子印章、电子时间戳、网站认证、电子存档和电子挂号发送服务。[16]

(n) “信任服务提供人”指提供一项或多项信任服务的人。

---

[12] 定义—“身份管理系统”：在工作组第五十九届会议上建议，由于草案提及“身份管理服务”，因此没有必要提及“身份管理系统”。但指出，在文书草案的若干条文中，提及“身份管理系统”更为合适，包括关于不区别对待的第 5 条（A/CN.9/1005，第 86、112 段）以及关于事前确定可靠性的第 11 条（A/CN.9/1005，第 102 段）。因此，工作组决定保留身份管理系统的定义（A/CN.9/1005，第 112 段）。该术语目前的定义反映了工作组商定的意见，即与国际电联的术语保持一致，提及“功能和能力”。在这方面，“建议 ITU-T X.1252”将身份管理定义为用于㈠身份信息的保证；㈡实体身份的保证；以及㈢支持商业和安全应用的“一套功能和能力”。

[13] 定义—“身份核实”：如上文第 2 段所述，针对就“身份识别”的多重含义所表达的关切，本草案改用“身份核实”一词，不再使用“身份识别”一词（参见 A/CN.9/WG.IV/WP.150，第 29 段）。在工作组第五十九届会议上指出，“身份识别”的定义包括身份管理的入册阶段（或步骤），但不包括认证阶段（或步骤），后者在本草案中称为电子身份识别阶段（或步骤）（A/CN.9/1005，第 84 段）。“入册”可定义为“身份管理服务提供人在向某一主体签发凭证之前验明该主体的身份主张的过程”（A/CN.9/WG.IV/WP.150，第 26 段）。

在第 9 条中，“身份识别”一词用于非技术意义。

[14] 定义—“主体”：为使整个条文草案保持一致，对术语“主体”和“人”的使用作了修订。“主体”这一术语仅在身份管理的语境中使用。

如果工作组同意将身份管理方面的条文限于自然人和法人，则可以删除“或架构”一词。在这种情况下，工作组似宜考虑删除“主体”的定义，在整个文书草案中将“主体”一词改为“人”。

[15] 定义—“订户”：“订户”这一术语用于第 8 和 15 条，这两条规定了订户在发生安全违规或服务泄密的情况下的义务。在工作组第五十九届会议上指出，“用户”一词不明确，因其可能指代以下两种人：(a)接受服务的人（例如，被识别身份的人）和与服务提供人有合同关系的人，(b)与服务提供人没有合同关系的依赖方（见 A/CN.9/1005，第 28、39、95 段）。会上表示倾向于使用“订户”一词来指代接受服务的人（A/CN.9/1005，第 43、96 段）。

[16] 定义—“信任服务”：“信任服务”这一术语取自《电子身份识别和信任服务条例》，其中将信任服务定义为“通常为取酬而提供的电子服务”，由《条例》第三章所描述的各种服务中的一项服务组成。因此，《电子身份识别和信任服务条例》并未单独提出“信任服务”的定义。前一版草案试图确立这样一种定义，将其界定为“就数据品质提供一定程度可靠性的电子服务”。在工作组第五十九届会议上指出，这样的定义并没有提供充分指导，应当采用《电子身份识别和信任服务条例》中的办法。同时还指出，一则更“抽象”的定义可以更好地适应未来的发展变化。还指出，信任服务更多地涉及数据的真确性和真实性，而不是其可靠性。目前的定义反映了工作组关于罗列非详尽信任服务的决定（A/CN.9/1005，第 18 段）。

第 2 条　适用范围

1. 本[文书]适用于在商业活动以及与贸易有关的服务中使用和跨境承认身份管理系统和信任服务。[17,18]

2. 本[文书]中的规定概不要求：

(a) 对人进行身份识别；[19]

(b) 使用特定的身份管理服务；或者

(c) 使用特定的信任服务。

3. 本[文书]中的规定概不影响按照法律所界定或规定的程序对[主体][人]进行身份识别的法律要求。

4. 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或信任服务适用任何可适用的法律规则，包括适用于隐私和数据保护的任何法律规则。[20]

第 3 条　自愿使用身份管理服务和信任服务[21]

1. 本[文书]中的规定概不要求某人在其未予同意的情况下使用身份管理服务和信任服务。

2. 就第 1 款而言，可根据该人的行为推断其是否同意。

第 4 条　解释

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。[22]

---

[17] *适用范围—国内和跨境使用身份管理服务和信任服务*：委员会第五十二届会议指出，工作组应努力制定一部既适用于国内使用也适用于跨境使用身份管理服务和信任服务的文书（A/74/17，第 172 段）。

[18] *适用范围—与贸易有关的服务*：工作组第五十九届会议商定，“与贸易有关的服务”这一术语足以涵盖与某些涉及贸易的公共机构的交易，例如，有单一窗口业务的海关，因此没有必要用“政府”一词对该术语加以限定（A/CN.9/1005，第 115 段）。

[19] 工作组还似宜审议该条文与第 3 条第 1 款之间的关系。

[20] 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）。

[21] *自愿使用身份管理服务和信任服务*：第 3 条依据的是《电子通信公约》第 8 条第 2 款。措辞作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 116 段）。按目前的案文，该条文不仅防止对订户规定新的义务，而且也防止对服务提供人和依赖方规定新的义务。工作组第五十七届会议曾审议过自愿使用原则（A/CN.9/965，第 110 段），将其与当事人意思自治原则联系起来。

[22] *统一解释*：贸易法委员会法规通常包含一项确立统一解释义务的条文。工作组第五十九届会议商定，应具体指明所提及的诚信是指“在国际贸易中”的诚信（A/CN.9/1005，第 118 段）。按目前的案文，第 4 条第 1 款反映了《电子通信公约》第 5 条第 1 款。

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，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。[23]

第二章 身份管理

第 5 条 对身份管理的法律承认[24]

不得仅根据下列理由之一而否定[主体][人]的电子身份识别的法律效力、有效性、可执行性或证据可采性：[25]

(a) 身份核实和电子身份识别为电子形式；或者[26]

(b) 身份管理系统不是根据第 11 条指定的身份管理系统。

第 6 条 身份管理服务提供人的义务[27]

身份管理服务提供人[至少]应：

(a) 办理[主体][人]入册，包括以下述方式：

㈠ 登记并收集于身份管理服务相适合的属性；

㈡ 进行身份核实和验证；并且

㈢ 身份凭证与[主体][人]绑定；

(b) 更新属性；

(c) 根据管辖身份管理系统的规则对身份凭证进行管理，包括以下述方式：

---

[23] *一般原则*：工作组第五十九届会议商定，不列出文书所依据的某些一般原则，即不区别对待电子手段的使用的原则、技术中性原则和功能等同原则（A/CN.9/1005，第 118 段）。按目前的案文，第 4 条第 2 款反映了《电子通信公约》第 5 条第 2 款。

[24] *对身份管理的法律承认—概述*：第 5 条第 1 款是基于贸易法委员会现有电子商务法规中的类似规定，例如，《电子商务示范法》第 5 条、《电子通信公约》第 8 条第 1 款，以及《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》）（联合国出版物，出售品编号：E.17.V.5），第 7 条第 1 款。该款在法律上赋权使用身份管理，无论是否存在离线等同方式均予适用（参见第 9 条）。“证据可采性”的提法取自《电子商务示范法》第 9 条。第 1 款(b)项将不区别对待规定延伸到区别事前和事后确定可靠性。第 1 款(b)项仅涉及否定使用非指定的身份管理系统的法律效力，因此不影响第 9 条第 2 款，该款以可推翻的可靠性推定的形式，为事前确定可靠性提供了更大的法律效力。

[25] *对身份管理的法律承认—不区别对待*：工作组第五十九届会议商定，第 5 条第 1 款前导语中确定的不区别对待的目标（即受不区别对待条款所保护的对象）应为“身份的验证”（A/CN.9/1005，第 86 段），在这方面，“验证”与“认证”同义（A/CN.9/1005，第 85 段）。鉴于第 2 款所描述的做法，现在使用“电子身份识别”一词。

[26] *对身份管理的法律承认—禁止提出的理由*：工作组第五十九届会议商定，第 1 款(a)项所列禁止提出的区别对待的理由应当是“身份识别和验证为”电子形式（见 A/CN.9/1005，第 86 段）。鉴于第 2 款所描述的做法，并与第 1 条中“身份管理服务”的定义保持一致，现在使用的术语是“身份核实”和“电子身份识别”。

[27] *身份管理服务提供人的义务*：第 6 条中的义务系根据工作组第五十八届会议的要求（A/CN.9/971，第 67 段）与专家协商拟订。该条文作了修订，以反映工作组第五十九届会议的决定，即修订(a)项㈠目，以体现数据最小化原则（A/CN.9/1005，第 93 段）。

㈠ 签发、交付并激活凭证；

㈡ 暂时取消、吊销并重新激活凭证；并且

㈢ 续订并更换凭证；

(d) 对[主体][人]的电子身份识别进行管理，包括以下述方式：

㈠ 管理电子身份识别因素；并且

㈡ 管理电子身份识别机制；

(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。

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[28]

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情形或完整性丧失情形，身份管理服务提供人应：

(a) 采取一切合理步骤遏制违规情形或丧失情形，包括在适当情况下暂停受影响的服务或吊销受影响的身份凭证；

(b) 纠正违规情形或丧失情形；

(c) 根据适用法律通知违规情形或丧失情形。

2. 如果[主体][人]向身份管理服务提供人通知了违规情形或丧失情形，则身份管理服务提供人应：

(a) 调查潜在的违规情形或丧失情形；并且

(b) 根据第 1 款采取其他任何适当行动。

第 8 条 订户的义务[29]

有下列情况的，订户应通知身份管理服务提供人：

(a) 订户知道相关身份管理系统的身份凭证或电子身份识别机制已经失密；或者

(b) 订户所知道的情况导致身份凭证或电子身份识别机制可能已经失密的重大风险。

---

[28] 身份管理服务提供人在发生数据泄露情况下的义务：第 7 条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 94、第 32 至 36 段）。工作组特别商定，应按照第 14 条第 2 款所载信任服务提供人在**发生**数据泄露情况下的义务的写法，拟订身份管理服务提供人在发生数据泄露情况下的义务。关于这些义务范围的讨论，详见脚注 43、44。

[29] 订户的义务：第 8 条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 94、第 37 至 43 段）。工作组特别商定，身份管理服务订户的义务应与第 15 条所载信任服务订户的义务保持一致。关于这些义务范围的讨论，详见脚注 45、46。

第 9 条　使用身份管理系统对[主体][人]进行身份识别[30]

备选案文 A

1. 法律规则要求或允许对[主体][人]进行身份识别的，就身份管理而言，如果使用了一种可靠方法对该[主体][人]进行电子身份识别，即为满足了这一规则。[31]

备选案文 B

1. 使用某一可靠方法对[主体][人]进行电子身份识别的，可使用身份管理服务识别该主体的身份。[32]

2. 使用根据第 11 条指定的某一身份管理系统的，即推定某一方法为第 1 款之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

(a) 为第 1 款之目的，根据第 10 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的身份管理系统的不可靠性举出证据。[33]

第 10 条 与确定可靠性相关的因素

1. 在为第 9 条之目的而确定方法的可靠性时，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) 管辖身份管理系统运营的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；

㈡ 发布的通知和用户信息；

---

[30] *对身份管理的法律承认—概述*：这一条文旨在在法律上承认为身份识别目的而使用身份管理。现提交两个备选案文供工作组审议。

第 9 条的备选案文 A 作了修订，以反映工作组第五十九届会议的决定（A/CN.91005，第 98、99、101 段）。在该届会议上指出，第 9 条通常适用于当事人同意使用身份管理服务彼此识别身份的情形（A/CN.9/1005，第 97 段）。根据第 2 条第 2 款(b)项，第 9 条并不取代适用法律中关于按照已界定或规定的程序识别主体身份的任何法律要求。

[31] *对身份管理的法律承认—离线等同方式*：第 9 条的备选案文 B 保留了前几版草案的功能等同做法。早先曾指出，基于功能等同的规定要求确定一种离线等同方式（A/CN.9/965，第 66 段）。工作组第五十九届会议商定，如该条的标题所反映的，这种离线等同方式是“对[主体]的身份识别”。

[32] *对身份管理的法律承认*：第 9 条的备选案文 B 旨在在不采用功能等同办法的情况下假定使用电子身份识别的合法性。工作组在审议这一备选案文时似宜铭记第 5 条。

[33] *可靠性推定*：工作组第五十九届会议商定，第 9 条应当按照载列信任服务要求的相应条文（即第 16 至 22 条）的写法重拟（A/CN.9/1005，第 99 段）。据此，插入了第 2 款和第 3 款，这两款依据第 16 条第 2 款和第 3 款，实际上取代了前一版草案第 11 条的第 4 款和第 5 款。

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。

第 11 条 指定可靠的身份管理系统[34]

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 条所指的可靠的身份管理系统。

2. [颁布国指明的主管个人、公共或私人机关或机构]应：

(a) 在指定身份管理系统时考虑到所有相关情况，包括第 10 条所列因素；并且

(b) 发布所指定的身份管理系统清单，包括身份管理服务提供人的详细信息。

3. 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。

4. 在指定某一身份管理系统时，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。

[34] 指定可靠的身份管理系统：第 11 条确立了事前确定可靠的身份管理系统的机制。该条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 102 段），因此，其案文系按照第二章关于事前确定可靠信任服务的相应条文（第 24 条）重拟。关于该条各要素的讨论，详见脚注 63、64。

第 12 条 身份管理服务提供人的赔偿责任[35]

备选案文 A

[应根据适用法律确定身份管理服务提供人的赔偿责任。][36]

备选案文 B

身份管理服务提供人应为其未能遵守[本文书]对其规定的义务而承担法律后果。

备选案文 C

1. 身份管理服务提供人应为由于故意或因疏忽而未遵守[本文书]对其规定的义务而给任何人造成的损害承担赔偿责任。[37]

2. 第 1 款的适用应符合适用法律关于赔偿责任的规则。

3. 虽有第 1 款的规定，身份管理服务提供人不应为使用身份管理系统所产生的损害而对订户承担赔偿责任，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) 身份管理服务提供人已按照适用法律将这些限制通知订户。

第三章 信任服务[38]

第 13 条 对信任服务的法律承认[39]

对于通过使用信任服务或在信任服务支持下[所保证的数据电文的品质][40][所交换、验证或认证的数据]，不得仅根据下列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[41]：

---

[35] 身份管理服务提供人的赔偿责任：工作组第五十九届会议决定不列入在某些条件下排除身份管理服务提供人赔偿责任的安全港条款（A/CN.9/1005，第 104 段）。对于其余部分，工作组同意结合信任服务提供人的赔偿责任重新审议身份管理服务提供人的赔偿责任（A/CN.9/1005，第 106 段）。据此，第 12 条作了修订，对应于第 25 条中提出的备选案文。现提交三个备选案文供工作组审议。

[36] 工作组似宜审议，如果文书草案采用示范法形式，是否应保留这一条文，或者，鉴于这一条文将在一般法律原则的基础上发生法律效力，其是否多余。

[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，以澄清导致赔偿责任的损害的原因。

[38] 信任服务一章载有一则关于对信任服务的法律承认的一般规定（第 13 条）；一项可靠性一般标准，其中的不区别对待地理位置条款可便利跨境承认（第 23 条）；一种用于事前指定可靠信任服务的机制（第 24 条）、一则关于赔偿责任的规定（第 25 条），并列出各项信任服务（第 16-22 条）。

[39] 对信任服务的法律承认—概述：第 13 条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 26 段）。

[40] 建议改用“所保证的数据电文的品质”这种措辞，以使第 13 条更贴近“信任服务”的定义。

[41] 建议插入“或证据可采性”，以使该条文与第 5 条保持一致。

(a) 其为电子形式；或者

(b) 其不为根据第 24 条指定的信任服务所支持。

第 14 条 信任服务提供人的义务

1. 信任服务提供人应：[42]

(a) 应按其就其政策和做法所作的表述行事；并且

(b) 使这些政策和做法便于订户查阅。

2. 如果发生了对信任服务有重大影响的安全违规情形或完整性丧失情形，信任服务提供人应：

(a) 采取一切合理步骤遏制违规情形或丧失情形，包括在适当情况下暂停或吊销受影响的服务；[43]

(b) 纠正违规情形或丧失情形；并且

(c) 根据适用法律通知违规情形或丧失情形。[44]

第 15 条 订户的义务

有下列情况的，订户[45]应通知信任服务提供人：

(a) 订户知道信任服务已经以影响到信任服务的可靠性的方式失密；[46]或者

(b) 订户所知道的情况导致信任服务可能已经以这种方式失密的重大风险；

---

[42] *信任服务提供人的义务—遵守政策和做法*：第 14 条第 1 款作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 31、73 段）。关于第 1 款(b)项，工作组曾商定以下案文：“这些政策和做法应便于订户查阅”，本草案重拟了这段案文，以澄清这是对服务提供人规定的一项义务。工作组似宜审议，这项义务是否应当与第 6 条(f)项规定的身份管理服务提供人的义务相一致，即“提供对管辖身份管理系统的规则的合理访问权”。

[43] *信任服务提供人的义务—遏制安全违规情形*：前一版草案第 14 条第 2 款(a)项规定了暂停受安全违规影响的信任服务的义务，并规定可选目标以违规情形“得到遏制”或签发新的凭证或等同证明来衡量（另见 A/CN.9/WG.IV/WP.154，第 47 段）。工作组认识到，采取其他措施而非全面暂停可能更合适，因此在第五十九届会议上商定，应改为规定信任服务提供人有义务“采取一切合理步骤”（A/CN.9/1005，第 33 段）。本草案第 14 条第 2 款(a)项反映了这一商定意见，并明确规定所采取的措施必须旨在遏制违规情形。工作组似宜审议，“遏制”违规情形这种提法是否反映了信任服务提供人为应对安全违规情形而采取的步骤的预期目标。

[44] *信任服务提供人的义务—通知安全违规情形*：前一版草案第 14 条第 3 款对信任服务提供人规定了通知义务，其中具体指明(a)谁应被通知，以及(b)此种通知的时间。工作组第五十九届会议商定，文书应当在这些事项上遵从适用的法律（A/CN.9/1005，第 36 段）。

[45] *订户的义务—概述*：工作组第五十九届会议商定，文书不应对依赖方规定义务（A/CN.9/1005，第 38 至 40 段、第 95 至 96 段）。

[46] *订户的义务—触发*：第 14 条第 2 款中对信任服务提供人规定的义务是由“安全违规情形或完整性丧失情形”触发的，而第 15 条对订户规定的义务是由信任服务“失密”触发的。在工作组第五十九届会议上建议，第 15 条应提及信任服务的可靠性（A/CN.9/1005，第 37 段）。本草案中增加的语句“以影响到信任服务的可靠性的方式”反映了这一建议。《电子身份识别和信任服务条例》第 10 条第 1 款中有类似的表述。

第 16 条 电子签名

1. 法律规则要求或允许有某人签名的，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：

(a) 识别该人的身份；并且

(b) 指明该人对于该数据电文所包含信息的意图。

2. 使用根据第 24 条指定的电子签名的，即推定某一方法为第 1 款之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

(a) 为第 1 款之目的，根据第 23 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的电子签名的不可靠性举出证据。[47]

第 17 条 电子印章

1. 法律规则要求或允许法人[48]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：

(a) 提供对数据电文发端地的可靠保证；并且

(b) 检测加盖印章之后对该数据电文的任何更改，并允许附加任何签注以及正常通信、存储和显示过程中发生的任何改动。[49]

2. 使用根据第 24 条指定的电子印章的，即推定某一方法为第 1 款之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

(a) 为第 1 款之目的，根据第 23 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的电子印章的不可靠性举出证据。[50]

---

[47] 电子签名—可靠性推定：工作组第五十九届会议商定，根据事前办法（即根据第 24 条）被确定为可靠的信任服务，应当以可推翻的可靠性推定的形式具有更大的法律效力（A/CN.9/1005，第 12）。工作组还商定，这一推定应载于每项载列信任服务要求的条文（即第 16 至 22 条）（A/CN.9/1005，第 51 段）。第 16 条第 2 款和第 3 款反映了这一商定意见，并分别取代前一版草案第 24 条的第 4 款和第 5 款。第 16 条第 3 款系仿照《电子签名示范法》第 6 条第 4 款（联合国出版物，出售品编号：E.02.V.8）。

[48] 电子印章—仅限于法人：工作组第五十九届会议商定，电子印章仅由法人制作，因此，前一版草案第 17 条（本草案第 18 条）应当仅限于作为法人的订户（A/CN.9/1005，第 52、54 段）。

[49] 电子印章—功能：工作组第五十九届会议商定，电子印章的功能是对电子印章关联数据的发端和完整性提供保证（A/CN.9/1005，第 52、54 段）。(a)项就发端地保证作出规定，(b)项就完整性保证作出规定。据建议，发端地保证在功能上等同于识别制作印章的法人（A/CN.9/1005，第 52 段），在这种情况下，可以通过使用电子签名对数据的发端地提供保证。(b)项允许“附加任何签注以及正常通信、存储和显示过程中发生的任何改动”，这反映了工作组商定的意见（A/CN.9/1005，第 56 至 58 段）。

[50] 电子印章—可靠性推定：见脚注 47。

第 18 条 电子时间戳

1. 法律规则要求或允许将某些文件、记录、信息或数据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：

(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关联。[51]

2. 使用根据第 24 条指定的电子时间戳的，即推定某一方法为第 1 款之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

(a) 为第 1 款之目的，根据第 23 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的电子时间戳的不可靠性举出证据。[52]

第 19 条 电子存档

1. 法律规则要求或允许留存某些文件、记录或信息的，如果符合下列条件，就数据电文存档而言，即为满足了该规则：[53]

(a) 数据电文所包含的信息可调取以供日后查询时使用；并且

(b) 采用了一种可靠方法：

㈠ 指明存档的时间和日期，并将该时间和日期与数据电文关联；并且

㈡ 检测该时间和日期之后对该数据电文的任何更改，并允许附加任何签注以及正常通信、存储和显示过程中发生的任何改动。[54]

(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。[55]

2. 使用根据第 24 条指定的电子存档服务的，即推定某一方法为第 1 款(b)项之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

---

[51] *电子时间戳—概述*：第 18 条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 55 段）。

[52] *电子时间戳—可靠性推定*：见脚注 47。

[53] *电子存档服务—概述*：前一版草案提到以“留存数据电文”的方式进行电子存档。为了与信任服务其他条文中的措辞、第 1 款其余部分中的措辞以及工作组第五十九届会议使用的措辞（A/CN.9/1005，第 59 段）保持一致，本草案采用的提法是“数据电文存档”。

[54] *电子存档服务—功能*：工作组第五十九届会议商定，电子存档的一项基本功能是保证数据的完整性（A/CN.9/1005，第 59 段）。根据工作组作出的决定，(b)项㈡目已经重拟，以反映第 17 条第 1 款(b)项载明的完整性评估标准。

[55] 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《电子商务示范法》第 10 条第 2 款。

(a) 为第 1 款之目的，根据第 23 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的电子存档的不可靠性举出证据。[56]

第 20 条 电子挂号发送服务

1. 法律规则要求或允许通过挂号邮件或类似服务发送某些文件、记录或信息的，[57] 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：

(a) 指明收到应发送的数据电文的时间和日期；并且

(b)指明发送数据电文的时间和日期；[58]

2. 使用根据第 24 条指定的电子挂号发送服务的，即推定某一方法为第 1 款之目的是可靠的。

3. 第 2 款不限制任何人在以下方面的能力：

(a) 为第 1 款之目的，根据第 23 条以其他任何方式确证某一方法的可靠性；或者

(b) 就所指定的电子挂号发送服务的不可靠性举出证据。[59]

第 21 条 网站认证

法律规则要求或允许对某一网站进行认证的，如果使用了一种可靠方法识别该网站域名持有人的身份并将该人与该网站关联，即为满足了该规则。[60]

---

[56] *电子存档服务—可靠性推定*：见脚注 47。

[57] *电子挂号发送服务—离线等同方式*：前一版草案提到法律规则要求或允许提供文件等的“发出和收到证据”。在工作组第五十九届会议上建议，可拟订更适当的措辞，侧重于挂号邮件服务与电子挂号发送服务之间的功能等同。据此，第 21 条第 1 款的起首部分作了修订，提及法律规则要求“通过挂号邮件或类似服务发送”文件等。

[58] *电子发送服务—功能*：工作组第五十九届会议商定，电子发送服务的基本功能是对“电子挂号发送服务系统收到应发送的数据电文的时间以及该系统将该数据电文发送给收件人的时间”提供保证（A/CN.9/1005，第 64 段）。本草案第 20 条第 1 款已经据此重拟，不过该款提及“指明”时间，与第 18 条第 1 款中使用的术语一致。工作组似宜审议，这一条文是否应当明确要求电子发送服务保证数据电文的完整性、确认收讫和发送，并识别发件人和（或）收件人的身份。(a)项和(b)项已涵盖这些功能，但仍可商榷。

[59] *电子发送服务—可靠性推定*：见脚注 47。

[60] *网站认证—功能*：工作组第五十九届会议商定，网站认证的基本功能是在网站与被分配或被许可使用其域名的人之间建立关联（A/CN.9/1005，第 66 段）。本草案中，“域名持有人”一词用以涵盖被域名注册机构分配域名或被许可使用域名的人。在迄今为止的讨论中，工作组所侧重的情形是某一方（如网站所有人）同意对网站进行认证的情形，而不是其为了满足“要求”进行此种认证的法律规则而对网站进行认证的情形。就前一种情形而言，该方将是根据“允许”此种认证的法律规则行事。

第 22 条 架构认证

法律规则要求或允许对某一构架进行认证的，如果使用了一种可靠方法对该架构进行认证，即为满足了该规则。[61]

第 23 条 信任服务的可靠性标准[62]

1. 在为第 16 条至第 22 条之目的而确定方法的可靠性时，应考虑到所有相关情况，其中可包括：

(a) 管辖信任服务的任何运营规则，包括为确保连续性而终止活动的任何计划；

(b) 任何适用的公认国际标准和程序；

(c) 任何适用的行业标准；

(d) 硬件和软件的安全性；

(e) 财力和人力资源，包括资产的存在；

(f) 独立机构审计的经常性和范围；

(g) 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

(h) 任何相关协议。

2. 某一方法事实上证明已履行相关信任服务的有关功能的，即被视为可靠方法。

3. 在确定该方法的可靠性时，不得考虑：

(a) 信任服务运营的地理位置；或者

(b) 身份管理服务提供人营业地的地理位置。

第 24 条 指定可靠的信任服务[63]

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 16 条至第 22 条所指的可靠的信任服务。

2. [颁布国指明的主管个人、公共或私人机关或机构]应：

(a) 在指定信任服务时考虑到所有相关情况，包括第 23 条所列因素；并且

---

[61] 架构认证—功能：工作组似宜审议是否应加入第 23 条，以提及对物理架构和数字架构进行身份识别的所有情形。为此，工作组似宜审议所提议的“认证”定义以及对“主体”定义所提议的修订，以便将架构排除在关于身份管理的条文的范围之外。

[62] 可靠性标准：第 23 条作了修订，以反映工作组第五十九届会议的决定（A/CN.91005，第 67、68 段）。

[63] 指定可靠的信任服务—概述：第 24 条确立了事前确定可靠的信任服务的机制。第 1 款和第 4 款（前一版草案第 3 款）作了修订，以反映工作组第五十九届会议的决定，即指定所侧重的是信任服务，而不是信任服务所使用的方法（A/CN.9/1005，第 73 段）。在第五十九届会议讨论期间作出的解释是，这一指定并不涉及信任服务的一般类型或某一具体信任服务提供人提供的所有信任服务，而是涉及由已被确定的服务提供人提供的某项信任服务。

(b) 发布所指定的信任服务清单，包括信任服务提供人的详细信息。[64]

3. 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，包括可靠性框架。

4. 在指定某一信任服务时，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。

第 25 条 信任服务提供人的赔偿责任[65]

备选案文 A

[应根据适用法律确定信任服务提供人的赔偿责任。][66]

备选案文 B

信任服务提供人应为其未能遵守[本文书]对其规定的义务而承担法律后果。

备选案文 C

1. 信任服务提供人应为由于故意或因疏忽而未遵守[本文书]对其规定的义务而给任何人造成的损害承担赔偿责任。

2. 第 1 款的适用应符合适用法律关于赔偿责任的规则。

3. 虽有第 1 款的规定，信任服务提供人不应为使用信任服务所产生的损害而对订户承担赔偿责任，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) 信任服务提供人已按照适用法律将这些限制通知订户。

---

[64] 指定可靠的信任服务—指定机构的义务：增加了新的第 2 款，以反映工作组第五十九届会议决定对指定机构规定两项新的义务（A/CN.9/1005，第 73 段）。第 2 款(a)项的目的是，确保采用事前办法被指定为可靠的信任服务与采用事后办法满足第 23 条中可靠性标准的信任服务这两者之间保持一定程度的一致。第 2 款(b)项的目的是，增进透明度，并让相关信任服务的潜在订户了解情况（A/CN.9/1005，第 70 段）。

[65] 信任服务提供人的赔偿责任：在工作组第五十九届会议上，普遍支持保留一项赔偿责任条文，以提供法律确定性。提出了几点建议。工作组请秘书处重拟第 25 条以反映这些建议，供今后审议。本草案第 25 条已经据此重拟。备选案文 A 采用最低限做法，提醒注意将根据适用法律确定信任服务提供人的赔偿责任，包括任何赔偿责任限制。备选案文 B 采用《电子签名示范法》第 9 条第 2 款中采取的办法。在保留适用法律规定的任何赔偿责任限制的同时，该备选案文还具体规定，信任服务提供人未能遵守文书草案规定的义务将产生一些法律后果。备选案文 C 是在前一版草案第 25 条的基础上拟订的，提供的指导最多。其中包括新的第 2 款，该款是以《电子身份识别和信任服务条例》第 11 条第 4 款为基础。第 2 款作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 76 段）。

[66] 工作组似宜审议，如果文书草案采用示范法形式，是否应保留这一条文，或者，鉴于这一条文将在一般法律原则的基础上发生法律效力，其是否多余。

第四章　国际方面

第 26 条　对身份管理服务和信任服务的跨境承认[67]

1.　在[颁布国]境外运营的身份管理系统或提供的信任服务，如果具有基本等同的[68]可靠度，应在[颁布国]境内具有与在[颁布国]境内运营的身份管理系统或提供的信任服务相同的法律效力。

2.　在确定[身份凭证][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[公认的国际标准]。

第 27 条　合作[69]

[颁布国指明的主管个人、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)　对外国身份管理系统和信任服务的法律效力以单方面准予或相互协定的形式给予承认；

(b)　对身份管理系统和信任服务进行指定；以及

(c)　对身份管理系统的保证级和信任服务的可靠度作出界定。

---

[67] 跨境承认—概述：第 26 条借鉴了《电子签名示范法》第 12 条第 2 款。这一条文的目的是“提供对于跨境承认证书的一般标准，没有这些标准，验证服务供应商将可能面临必须在多个法域中获取许可证的不合理负担。”（见 2001 年《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，第二部分，第 153 段）。第 26 条旨在就文书草案中涉及跨境承认的其他条文的执行提供指导，即：第 10 条第 2 款（地理发端地于确定身份管理方法的可靠性无关）、第 11 条第 4 款（地理发端地于指定可靠的身份管理方法无关）、第 23 条第 3 款（地理发端地于确定信任服务的可靠性无关）以及第 24 条第 4 款（地理发端地于指定可靠的信任服务无关）。第 10 条第 2 款、第 11 条第 4 款、第 23 条第 3 款和第 24 条第 4 款都是依据《电子签名示范法》第 12 第 1 款，其中确立的一般规则是，在确定凭证或电子签名的法律效力时不区别对待（见 2001 年《贸易法委员会电子签名示范法及其颁布指南》，第二部分，第 152 段）。为协助审议这些条款，工作组似宜回顾 A/CN.9/483 号文件第 29-36 段中记载的工作组讨论《电子签名示范法》第 12 条第 1 款与第 12 条第 2 款之间相互作用的情况。

[68] 跨境承认—等同程度：在工作组第五十九届会议上，就跨境法律效力所必需的等同程度发表了不同意见。本草案所依照的是《电子签名示范法》第 12 第 2 款，其中要求具有“基本”等同性。前一版草案中提出的另一种选择是完全等同（即，外国服务必须提供“相同的”可靠度）。

[69] 国际合作：第 27 条作了修订，以反映工作组第五十九届会议的决定（A/CN.9/1005，第 122 段）。