



Distr.: Limited
7 September 2021
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第六十二届会议
2021年11月22日至26日，维也纳

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

	页次
一. 导言.....	2
二. 需审议的问题.....	2
A. 术语.....	2
B. 对条文草案的修订	3
C. 赔偿责任.....	4
附件	
关于使用和跨境承认身份管理和信任服务的条文草案	5



一. 导言

1. 如同 [A/CN.9/1051](#) 号文件所述，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”）纳入了工作组第六十一届会议（2021年4月6日至9日）的审议情况。¹
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.169](#) 号文件第4至20段。由工作组第六十一届会议审议的载于 [A/CN.9/WG.IV/WP.167](#) 号文件附件中的条文草案被称作“前一版草案”。

二. 需审议的问题

3. 工作组第六十一届会议的审议侧重于术语、信任服务、赔偿责任和跨境承认等问题。对这些问题的审议取得了长足进展。在本节中，秘书处提出了一些补充意见，以协助工作组继续审议这些问题。

A. 术语

4. 工作组承认，身份管理由两个阶段组成。工作组前几届会议使用了不同的术语来指称这两个阶段。对于究竟使用哪些术语，没有做出任何决定。此外，在某些情况下，尚未决定究竟是以“系统”还是“服务”来指称身份管理：

(a) 在本草案（如同前一版草案）中，第一阶段称作“身份核实”。然而，工作组注意到，在专业术语中，这一阶段可称作“身份识别”。²它也被称作“注册”，³事实上，本草案（如同前一版草案）承认，身份核实是注册的一部分（见第6(a)(i)条）；

(b) 在第二阶段中，本草案（如同前一版草案）使用了“电子身份识别”一语，尽管工作组也使用了“认证”和“核实”两个词句。⁴工作组还建议，应当使用“认证”以指称“身份核实”（即第一阶段）。⁵此外，据指出，在第二阶段中使用“身份识别”以指称对身份的主张（然后需要对其进行“认证”或“核实”）。⁶使得术语上的这类差异更形严重的是，最近区域贸易协定的电子商务章节使用了“电子认证”一语；⁷虽然这类协定并没有赋予该用语统一的含义，但它通常对应于身份管理第二阶段。⁸在工作组第六十一届会议上，与会者

¹ 在本草案随附脚注中，工作组第六十届会议所审议的载于 [A/CN.9/WG.IV/WP.162](#) 号文件中的条文草案被称为“前一版草案”。草案还提到贸易法委员会关于电子商务的其他法规，即《贸易法委员会电子商务示范法》（《电子商务示范法》）、《贸易法委员会电子签名示范法》（《电子签名示范法》）、《联合国国际合同使用电子通信公约》（《电子通信公约》）和《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》）。

² [A/CN.9/1005](#)，第84段。

³ 同上。

⁴ 同上。

⁵ [A/CN.9/1051](#)，第67段。

⁶ 同上。

⁷ 例如见《全面与进步跨太平洋伙伴关系协定》，第14.1条；《美国——墨西哥——加拿大协定》，第19.1条；《区域全面经济伙伴关系》，第12.1(c)条。

⁸ 在一些区域贸易协定中，“认证”一语延伸至确保数据电文的完整性，而这是本草案信任服务述及的一项功能。

广泛支持使用“电子身份识别”来指称第二阶段，同时有一些与会者支持使用“认证”；⁹

(c) 条文草案涉及身份管理系统和身份管理服务。第 1 条对这两个用语均做了界定。在多数情况下，本草案使用了身份管理服务的提法。然而，在有些条文中，本草案使用了身份管理系统的提法，以或者(1)有别于身份管理服务（例如见第 6、7、12 和 25 条），或者(2)以替代身份管理服务的提法（例如见第 5、10 和 11 条，这几条涉及“身份管理系统”和“身份管理服务”的可靠性及其指定）。虽然前几届会议讨论了身份管理系统和身份管理服务之间的互动问题，¹⁰但工作组似宜确认，就后一种提法而言，是否应使用“身份管理系统”一语代替“身份管理服务”，或反之亦然。

B. 对条文草案的修订

5. 已经对文书草案第 16 至 21 条加以改拟，以反映工作组审议情况。特别是：

(a) 法律“允许”的情况下——条文草案不再使用法律规则“允许”相应的纸质做法的提法。条文草案由此恢复使用《贸易法委员会电子商务示范法》（《电子商务示范法》和《联合国国际合同使用电子通信公约》（《电子通信公约》）所使用的行文；¹¹

(b) 可靠性推定——为避免重复，第 22 条合并了前一份草案第 16 条至第 21 条第 2 款和第 3 款所述确证对指定信任服务所用方法的可靠性推定的共同规则；¹²

(c) 可靠性的相对标准——已经对第 22 条中的可靠性要求加以修订，插入第 1(a)款，以承认信任服务使用的某一方法的可靠性是相对的，而并非绝对的。¹³该款基于《电子通信公约》第 9(3)(b)(i)条，据以确定相对于基础数据电文（即电子签名所适用的电子通信）“目的”的可靠性。

对第二章关于身份管理的相应条文（即第 9 条和第 10 条）作了修订，以反映这些修改。

6. 此外，对第三章关于信任服务的条文做了调整，以与第二章关于身份管理的条文保持一致，这些条文所履行的功能是相同的。¹⁴特别是：

(a) 信任服务提供人的义务——第 14(1)(a)条增设了制定操作规则、政策和做法的一条新的义务。该义务基于第 6(a)条所载身份管理服务提供人的义务。已经对第 14(1)(b)条中的现有义务作了修订，以同第 6(b)条中关于身份管理服务提供人的现有义务保持一致。因此，信任服务提供人和身份管理服务提供人现在都有义务按照其操作规则、政策和做法及其就这些规则、政策和做法所做的任

⁹ A/CN.9/1051，第 67 段。

¹⁰ 见 A/CN.9/1045，第 126 段和 A/CN.9/1051，第 59 段。另见 A/CN.9/WG.IV/WP.171 的讨论情况。

¹¹ A/CN.9/1051，第 42-44 段。

¹² 同上，第 31-34 段。

¹³ 同上，第 45 段。

¹⁴ 同上，第 52 段。

何陈述行事。也已经对第 6(d)和(e)条中的现有义务做了修订，以同第 14(1)(c)和(d)条保持一致：

(b) 订户的义务——已经对第 15 条作了修订，以采用第 8 条中关于相应义务的措辞。

C. 赔偿责任

7. 已经对文书草案第 12 至 24 条中的赔偿责任规则加以改拟，以反映工作组第六十一届会议审议情况。¹⁵

8. 本草案保留了上一份草案的“备选案文 B”，与会者广泛认为，该草案中的“备选案文 B”胜过“备选案文 A”。删除了对过错要素（“疏忽”和“故意”）的提及，并用“损失”一词取代了“损害”。¹⁶因此，本草案确立了有别于合同约定的赔偿责任的关于赔偿责任的新依据。¹⁷

9. 各方尚未就赔偿责任规则的实质内容达成共识。与会者在第六十一届会议上提出了工作组在其第六十二届会议上不妨加以进一步审议的若干问题，其中包括：

(a) 与合同的关系¹⁸——根据目前的草案，赔偿责任产生于服务提供者未履行文书草案规定的按照其操作规则、政策和做法行事的义务。这些规则、政策和做法通常会纳入订户和服务提供者之间的合同。因此，根据文书草案和合同法，违约可能会引发服务提供者的赔偿责任。各国的法律反过来又可能会影响服务提供者根据第 12(3)和第 24(3)条限制或免除其赔偿责任的能力。因此，工作组似宜考虑，除第 12(3)和第 24(3)条所述赔偿责任外，服务提供者究竟可以在多大程度上经由合同限制其在文书草案下的赔偿责任；

(b) 其他法律后果——根据目前的草案，就损失承担的赔偿责任并非服务提供者未履行文书草案规定的义务所产生的唯一法律后果。未履行该义务不仅可能损害服务提供者使用的方法的可靠性（见第 10(2)(a)和第 22(2)(a)条），还可能损害服务提供者的指定（见第 11(2)(a)和第 23(2)(a)条）。

10. 工作组第六十一届会议就赔偿责任提出的一个相关问题是文书草案规定的义务与合同约定义务之间的关系。工作组普遍认为，至少就其中某些义务而言，不存在偏离合同的余地。¹⁹工作组还听取了这样的建议，即通过把相关条文表述为确定“最低”要求，即可经由合同补充而非减损这些义务。换言之，条文草案确立了法定下限。工作组似宜进一步审议该事项。

¹⁵ 同上，第 13-29 段。

¹⁶ 同上，第 21 段。

¹⁷ 同上，第 24 段。

¹⁸ 同上，第 16 段。

¹⁹ A/CN.9/1045，第 19 段。

附件

关于使用和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”指与某人关联的一条信息或数据；
- (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) “电子身份识别”[“认证”]，在身份管理服务的范围内，指用以实现对某人与某一身份之间绑定的充分保证的过程；²⁰
- (d) “身份”指允许在特定环境下对某人进行独特辨别的一组属性；
- (e) “身份凭证”指为了进行电子身份识别某人可出示的数据或数据可驻留的物理架构；
- (f) “身份管理服务”指包含对个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；²¹
- (g) “身份管理服务提供者”指提供身份管理服务的人；²²
- (h) “身份管理系统”指对个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；²³
- (i) “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某人身份的过程；
- (j) “订户”指与身份管理服务提供者或信任服务提供者订立提供身份管理服务或信任服务安排的人；
- (k) “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递送服务的创建和管理方法；²⁴
- (l) “信任服务提供者”指提供一项或多项信任服务的人。

²⁰ 见上文第 4 段。

²¹ 工作组似宜考虑，根据“身份核实”和“电子身份识别”的定义，是否可以删除“电子形式个人”一语。

²² 工作组似宜考虑是否应在“身份管理服务”之前插入“任何”一词，以澄清第 6 条所列功能可能并非都事关所有身份管理系统，因此，身份管理服务提供者可能没有履行所列的每一项功能（A/CN.9/I045，第 88 段）。

²³ 见脚注 21。

²⁴ 已经对“信任服务”的定义做了修订，以反映工作组第六十一届会议审议情况（A/CN.9/I051，第 35-36 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和信任服务。
2. 本[文书]中的规定概不要求：²⁵
 - (a) 对个人进行身份识别；
 - (b) 使用特定的身份管理服务；或者
 - (c) 使用特定的信任服务。

[适用法律或当事人协议不要求对个人进行身份识别或使用特定的身份管理服务或特定的信任服务的。]²⁶

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识别某人身份[或使用某一信任服务]的法律要求。²⁷
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关于隐私和数据保护的任何适用法律。²⁸

第 3 条. 自愿使用身份管理服务和信任服务²⁹

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或信任服务[或使用某一特定的身份管理服务或信任服务]。³⁰
2. 就第 1 款而言，可根据该人的行为推断其是否同意。

²⁵ 第 2(2)条旨在维护技术和示范中立，而第 3(1)条款旨在维护当事人意思自治。工作组似宜考虑是否应当把与条文实施有关的第 2 条第 2 款和第 3 款放在第 3 条中。在此情况下，第 2 条将只是厘清文书主题事项的范围。

或者，工作组似宜考虑是否只应将第(2)(b)和(c)款纳入第 3(1)条（见脚注 30）。

²⁶ 置于括号内的案文旨在表明，第 2 款概不影响规定有义务进行识别或使用特定的身份管理服务和信任服务的任何法律或合同约定的协议。

²⁷ 第 2(3)条适用于对身份管理的使用的限制。工作组似宜审议，是否应当将其延伸至限制对信任服务的使用，如果加以延伸，则是否应当插入置于方括号内的案文。《电子商务示范法》及《贸易法委员会电子签名示范法》（《电子签名示范法》）采取了把信任服务的使用限制在一定范围内（例如，电子签名）的不同做法，并为此促使各颁布法域具体指明特定除外情形（包括采用提及特定法律的做法）：见《电子商务示范法》第 7(3)条和《电子签名示范法》第 1 条（随附说明）。

²⁸ 按照现行贸易法委员会示范法（如同 A/CN.9/WG.IV/WP.167 脚注 10 所做的解释），对第 2(4)条进行了修订，以删除对“任何适用的法律规则”的一般保留，同时对适用于数据保护和隐私的法律的具体保留不做改动。

²⁹ 第 3 条基于《电子通信公约》第 8(2)条，后者涉及自愿使用和接受电子通信。工作组一致认为，该条文应当保护订户和依赖方免于被强加使用身份管理或信任服务的任何新的义务（A/CN.9/I005，第 116 段）。为与《电子通信公约》第 8(2)条保持一致，工作组似宜考虑在“使用”一词之后加上“或接受”一词。工作组还似宜考虑将“身份管理服务或信任服务”改为“电子身份识别或信任服务”。

³⁰ 置于括号内的案文旨在落实将第 2(2)(b)和(c)条纳入第 3 条的建议（见脚注 25）。

第 4 条. 解释

1. 在解释本[文书]时，应考虑到其国际渊源以及促进其统一适用和在国际贸易中遵守诚信的需要。
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。³¹

第二章. 身份管理

第 5 条. 对身份管理的法律承认

在不违反第 2 条第 3 款的前提下，不得仅根据下列理由之一而否定电子身份识别的法律效力、有效性、可执行性或证据可采性：

- (a) 身份核实和电子身份识别为电子形式；或者
- (b) 身份管理系统不是依据第 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³²

身份管理服务提供人[至少]应：³³

(a) 制定与身份管理系统的目的³⁴和设计相适合的操作规则、政策和做法，以[至少]³⁵处理以下要求：

- (一) 办理个人入册，包括以下述方式：
 - a. 登记并收集属性；
 - b. 进行身份核实和验证；及
 - c. 身份凭证与该人绑定；
- (二) 更新属性；
- (三) 管理身份凭证，包括以下述方式：
 - a. 签发、交付并激活凭证；
 - b. 暂时取消、吊销并重新激活凭证；及

³¹ 已经对 4(2)条做了修订，以反映工作组第六十一届会议审议情况（A/CN.9/1051，第 56 段）。

³² 见上文第 6(a)段（关于对义务加以调整以同信任服务提供者所持义务相一致）和第 10 段（关于与合同约定义务的关系）。

³³ “至少”一词载于第 6 条起首部分和(a)款。这些词语是在工作组第六十届会议的审议之后插入(a)款的，目的是解决这样一种关切，即该款不然可能会允许身份管理服务提供者放弃履行与本来由分包人（例如，身份管理多方私营部门系统中的一个单独实体）履行的身份管理服务有关的职能的责任（见 A/CN.9/1045，第 90 段）。工作组似宜审议，第 6 条起首句中的“至少”一词是否已经解决了这一关切，并因而是是否可以删除第 6(a)条中的词句。

³⁴ 工作组似宜考虑，鉴于第 10(1)条中使用了基于贸易法委员会既有术语的“功能”和“目的”这两个用语，该条文是否应当使用“功能”而非“目的”的提法。

³⁵ 见脚注 33。

- c. 续订并更换凭证；
- (四) 对个人的电子身份识别进行管理，包括以下述方式：
 - a. 管理电子身份识别因素；及
 - b. 管理电子身份识别机制；
- (b) 根据其操作规则、政策和做法及就此所作的任何陈述行事；
- (c) 确保身份管理系统的在线可用性和正确操作；
- (d) 使其操作规则、政策和做法便于订户和第三方查阅；及
- (e) 依据第 8 条的规定，提供并公开订户可以向身份管理服务提供者通报安全漏洞的手段。

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情形或完整性丧失情形，身份管理服务提供者[根据法律]应：³⁶
 - (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；及
 - (c) [根据法律]通报违规情形或丧失情形。³⁷
2. 如果某人向身份管理服务提供者通报了安全违规情形或完整性丧失情形，则身份管理服务提供者应：
 - (a) 调查潜在的违规情形或丧失情形；及
 - (b) 根据第 1 款采取其他任何适当行动。

第 8 条. 订户的义务³⁸

有下列情况的，订户应利用身份管理服务提供者依据第 6 条提供的手段，或以其他方式使用合理手段，通知身份管理服务提供者：

- (a) 订户知道其身份凭证已经[或可能已经]失密；或者
- [(b) 订户所知道的情况引起订户身份凭证可能已失密的重大风险。]

³⁶ 在工作组第六十届会议上，据指出，第 7 条所列若干行动可能属于数据保护和隐私法律的管辖范围，因此，对所列所有行动而不仅仅是通知，都应“根据适用法律”加以实施（A/CN.9/1045，第 99 段）。工作组似宜考虑是否删除第 7(1)(c)条中的“根据法律”一语，并在方括号中所示第 7(1)条起首部分末尾处插入这些词句。

³⁷ 见脚注 36。

³⁸ 鉴于工作组第六十届会议所做决定，已经对第 8 条做了修订（A/CN.9/1045，第 105 段）。对起首部分作了进一步修订，以强调该项条文主要涉及通知，而不是特定的通知手段。工作组第六十一届会议没有进一步审议该项条文，因此保留了(a)项和(b)项中的方括号。

第 9 条. 使用身份管理对个人进行身份识别³⁹

在不违反第 2 条第 3 款的前提下，法律要求[为某一特定目的]对个人进行身份识别的，⁴⁰或者就未予身份识别的后果做出规定的，就身份管理服务而言，如果使用了某一种方法[为该目的]对个人进行电子身份识别，即为满足了这一要求。

第 10 条. 身份管理[服务][系统]的可靠性要求

1. 在第 9 条中，该方法应当是：
 - (a) 对使用身份管理服务所要达到的目的既是适当的，也是可靠的；或者
 - (b) 事实上证明已经履行了第 9 条所述功能。⁴¹
2. 在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) 身份管理服务提供者遵守第 6 条所列义务的情况；
 - (b) 身份管理服务提供者的操作规则、政策和做法是否符合与提供身份管理服务有关的任何可适用的公认国际标准和程序，包括[保证级框架][保证级框架或为指定身份管理系统信任度提供指导的类似框架]，特别是关于以下方面的规则：⁴²
 - (一) 治理；
 - (二) 发布的通知和用户信息；
 - (三) 信息安全管理；
 - (四) 记账；
 - (五) 设施和工作人员；
 - (六) 技术控制；及
 - (七) 监督和审计；
 - (c) 就身份管理系统提供的任何监督或核证；
 - (d) 使用身份识别所要实现的目的；及
 - (e) 当事人之间的任何相关协议，包括对可能使用身份管理服务的交易的目的或价值的任何限制。
3. 在确定方法的可靠性时，不得考虑：

³⁹ 第 9 条反映了工作组第六十届会议所做决定（A/CN.9/1045，第 117 段）。如同上文第 5 段所做解释，也对其作了进一步修订。

⁴⁰ 见脚注 34。

⁴¹ 工作组似宜考虑是否应保留第 10 条第 1(b)款（及第 22 条中的相应条文），或者可根据第 10 条第 5(a)款予以删除，在所述方法实际上行使该功能时该款可能已经有此效果。

⁴² “保证级框架或就确定对身份管理系统信任度提供指导的类似框架”一语旨在涵括制定这些框架可能采用的各种形式。“保证级”是 A/CN.9/WG.IV/WP.150 号文件中界定的一个术语。工作组似宜确认这些词句是否足以描述“保证级框架”的概念。

- (a) [身份管理系统运行][所提供的身份管理服务]的地理位置；或者
 - (b) 身份管理服务提供者营业地的地理位置。
4. 根据第 11 条指定的身份管理系统[服务]使用的方法被推定为是可靠的。
 5. 第 4 款不限制任何人在以下方面的能力：
 - (a) 以任何其他方式确证某一方法的可靠性；或者
 - (b) 就依据第 11 条指定的身份管理系统所使用的方法的不可靠性举出证据。

第 11 条. 指定可靠的身份管理系统[服务]

1. [颁布法域指明的主管个人、公共或私人机关或机构]可指定被推定可靠的身份管理系统[服务]。⁴³
2. [颁布法域指明的主管个人、公共或私人机关或机构]应：
 - (a) 在指定身份管理系统[服务]时考虑到所有相关情况，包括第 10 条所列因素；及
 - (b) 发布所指定的身份管理系统[服务]清单，包括身份管理服务提供人的详细信息[，或以其他方式告知公众]。⁴⁴
3. 根据第 1 款做出的任何指定均应符合与履行指定程序有关的公认国际标准和程序，包括保证级框架。⁴⁵
4. 在指定某一身份管理系统[服务]时，不得考虑：
 - (a) 身份管理系统运行[所提供的身份管理服务]的地理位置；或者
 - (b) 身份管理服务提供者营业地的地理位置。

第 12 条. 身份管理服务提供人的赔偿责任⁴⁶

1. 身份管理服务提供者应为未遵守[本文书]对其规定的义务而给[任何人]造成的损失承担赔偿责任。
2. 第 1 款的适用应符合法律关于赔偿责任的规则并且不得损害：
 - (a) 法律规定的关于赔偿责任的任何其他依据，包括对不履行合同约定义务的赔偿责任；或者

⁴³ 见上文第 4(c)段。工作组似宜考虑，鉴于第 23 条提及服务的指定，第 11 条是否应提及系统或服务的指定。工作组就此的最新讨论情况见 [A/CN.9/1045](#)，第 126 段。

⁴⁴ 在其第六十届会议上，工作组同意把“以其他方式告知公众”一语置于方括号内以供进一步审议。这些词句意在涵括除发布清单外的告知公众的其他手段的含义。在第六十届会议上，几个代表团坚持认为，虽然可以使用其他手段，但必须保留发布所指定的身份管理系统清单这项义务（[A/CN.9/1045](#)，第 128 段）。工作组第六十一届会议未曾审议这些词句。如果保留这些词句，工作组似宜考虑也将其插入第 23(2)(b)条。

⁴⁵ 将基于对第 10(2)(b)条的审议的结果修订“保证级框架”的提法。

⁴⁶ 见上文第 7 至 10 段。

(b) 身份管理服务提供者未履行[本文书]规定的义务所造成的在[本文书]下的任何其他法律后果。

3. 虽有第 1 款的规定，身份管理服务提供者不应为使用身份管理系统所产生的损失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；
- [b) 这些限制是在身份管理服务提供人和订户之间商定的；]⁴⁷及
- (c) 身份管理服务提供者已根据法律将这些限制通知[告知]⁴⁸订户。

第三章. 信任服务

第 13 条. 对信任服务的法律承认

不得仅根据下列理由之一而否定使用信任服务所产生的结果的法律效力、有效性、可执行性或证据可采性：

- (a) 其为电子形式；或者
- (b) 信任服务并非是依据第 23 条指定的。

第 14 条. 信任服务提供人的义务

1. 信任服务提供者应：⁴⁹

- (a) 制定与信任服务的目的和设计[功能]⁵⁰相适应的操作规则、政策和做法，包括在活动终止时确保连续性的计划；
- (b) 根据其操作规则、政策和做法及就此所作的任何陈述行事；
- (c) 使其操作规则、政策和做法便于订户和第三方查阅；及
- (d) 依据第 15 条的规定，提供并公开订户可以向信任服务提供者通报安全漏洞的手段。

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，信任服务提供者[根据法律]应：⁵¹

- (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；
- (b) 纠正违规情形或丧失情形；及

⁴⁷ 增设了第 12 条第 3(b)款，以反映工作组所持的这样一种理解，即对赔偿责任的限制如果是商定的即可予以承认。

⁴⁸ 第 12 条第 3(c)款无意引入一项新的义务，而只是提及在适用法律下的现有义务。为避免造成疑虑，工作组似宜考虑为此目的，较之于“通知”一词使用“告知”一词是否更为妥当。

⁴⁹ 见上文第 6(a)段（关于对义务加以调整以同身份管理服务提供者所持义务相一致）和第 10 段（关于与合同约定义务的关系）。

⁵⁰ 见脚注 34。

⁵¹ 见脚注 33。

- (c) [根据法律]通报违规情形或丧失情形。⁵²

第 15 条. 订户的义务⁵³

有下列情况的，订户应利用信任服务提供者依据第 14 条第 1 款提供的手段，或以其他方式使用合理手段，通知信任服务提供者：

- (a) 订户知道信任服务已经失密；或者
- (b) 订户所知道的情况引起信任服务可能已失密的重大风险。

第 16 条. 电子签名

法律要求应由某人签名，或者法律规定了不签名的后果的，在数据电文方面，符合下列条件即满足这一要求：

- (a) 识别该人的身份；及
- (b) 指明该人对于该数据电文所包含信息的意图。

第 17 条. 电子印章

法律要求应由某法人加盖公章的，或者法律规定了不加盖公章的后果的，在数据电文方面，符合下列条件即满足这一要求：

- (a) 提供对数据电文发端地的可靠保证；及
- (b) 检测加盖公章的时间[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。

第 18 条. 电子时间戳

法律要求将文件、记录、信息或数据与某一时间和日期关联的，或者就时间和日期缺失的后果做出规定的，在数据电文方面使用了符合下列条件的某种方法即满足这一要求：

- (a) 指明该时间和日期，包括注明时区；及
- (b) 将该时间和日期与该数据电文相关联。

第 19 条. 电子存档

法律要求将文件、记录、或信息留存，或者就未予留存的后果做出规定的，在数据电文方面使用了符合下列条件的某种方法即满足这一要求：

- (a) 数据电文所包含的信息可调取以供日后查询时使用；

⁵² 同上。

⁵³ 见上文第 6(b)段。将根据关于第 8 条的讨论结果对该项条文加以修订。

(b) 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；

(c) 以生成、发送或接收数据电文的格式，或以可显示的其他格式留存该数据电文，以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；及

(d) 留存方便查明数据电文发端地和目的地及数据电文发送或接收日期和时间的任何可能的此种信息。

第 20 条. 电子挂号发送服务

法律要求通过挂号邮件或类似服务发送文件、记录或信息的，或者就未予发送的后果做出规定的，在数据电文方面使用了符合下列条件的某种方法即满足这一要求：

(a) 标明收到有待发送的数据电文的时间和日期以及发送的时间和日期；

(b) 检测除附加任何签注或本条要求的任何信息外以及正常通信、存储和显示过程中出现的任何改动之外，在有待发送的数据电文从收到之日起至发送之日后对数据电文的任何改动；及

(c) 识别发送人和接收人的身份。

第 21 条. 网站认证

法律要求网站认证或者就未进行网站认证的后果做出规定的，使用了符合下列条件的某种方法即满足这一要求：

(a) 识别网站域名持有人的身份；及

(b) 将该人与网站相关联。

第 22 条. 信任服务的可靠性要求

1. 在第 16 至 21 条中，该方法应该是：

(a) 对使用信任服务所要达到的目的既是适当的，也是可靠的；⁵⁴或者

(b) 事实上证明已经履行了本条所述功能。

2. 在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) 信任服务提供者遵守第 14 条所列义务的情况；

(b) 信任服务提供者操作规则、政策和做法与提供信任服务有关的任何可适用公认国际标准和程序相一致的情况；

(c) 任何可适用的行业标准；

(d) 硬件和软件的安全性；

⁵⁴ 见脚注 34。

- (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) 有监督机构、资格鉴定机构或自愿方案就该方法可靠性作出的声明；
 - (h) 使用信任服务所要实现的功能⁵⁵；⁵⁶及
 - (i) 当事人之间的任何相关协议，包括对可能使用信任服务的交易的目的或价值的任何限制。
3. 在确定方法的可靠性时，不得考虑：
- (a) 信任服务运营的地理位置；或者
 - (b) 信任服务提供者营业地的地理位置。
4. 依据第 23 条指定的信任服务所使用的方法被推定为是可靠的。
5. 第 4 款不限制任何人在以下方面的能力：
- (a) 以任何其他方式确证某一方法的可靠性；或者
 - (b) 就依据第 23 条指定的信任服务所使用的方法的不可靠性举出证据。

第 23 条. 指定可靠的信任服务

1. [颁布法域指明的主管个人、公共或私人机关或机构]可指定被推定可靠的信任服务。
2. [颁布法域指明的主管个人、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 22 条所列因素；及
 - (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。
3. 依据第 1 款做出的任何指定均应符合与履行指定程序有关的公认国际标准和程序。
4. 在指定一项信任服务时，不得考虑：
- (a) 提供信任服务的地理位置；或者
 - (b) 信任服务提供者营业地的地理位置。

第 24 条. 信任服务提供人的赔偿责任

1. 信任服务提供者应为未遵守[本文书]对其规定的义务而[给任何人]造成的损失承担赔偿责任。
2. 第 1 款的适用应符合法律关于赔偿责任的规则并且不得损害：

⁵⁵ 见脚注 34。

⁵⁶ 第 22(1)(h)条反映了工作组第六十届会议所做决定 (A/CN.9/I045, 第 56 段)。工作组似宜注意到，这一因素不同于第 10(2)(d)条所列因素。

(a) 法律规定的关于赔偿责任的任何其他依据，包括对不履行合同约定义务的赔偿责任；或者

(b) 信任服务提供者未履行[本文书]规定的义务所造成的在[本文书]下的任何其他法律后果。

3. 虽有第 1 款的规定，信任服务提供者不应为使用信任服务所产生的损失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；

(b) 这些限制是在信任服务提供者和订户之间商定的；⁵⁷及

(c) 信任服务提供者已按照法律将这些限制通知⁵⁸订户。

第四章. 国际方面

第 25 条. 跨境承认⁵⁹

1. 在[颁布法域]境外运营的身份管理系统、签发的身份凭证或提供的身份管理服务或信任服务，如果具有[基本等同的][至少是等同的]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、签发的身份凭证或提供的身份管理服务或信任服务相同的法律效力。

2. 在确定身份管理系统、身份管理服务或身份凭证是否酌情提供或信任服务是否提供[基本等同的][至少是等同的]可靠度时，应考虑到公认的国际标准。

[3.如果[颁布法域依据第 11 条和第 23 条指明的个人、机关或机构]为本款之目的确定了等同性，即应推定具有等同性。]⁶⁰

第 26 条. 合作

[颁布法域指明的主管个人、机关或机构][应][可]与外国实体合作，交换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给予承认——以单方面准予或相互协定的形式；

(b) 指定身份管理系统和信任服务；及

(c) 对身份管理系统的保证级和信任服务的可靠度做出界定。

⁵⁷ 见脚注 47。

⁵⁸ 见脚注 48。

⁵⁹ 已经对第 25 条第 1 和 2 款做了修订，以反映工作组第六十一届会议审议情况（A/CN.9/1051，第 60 和 61 段）。

⁶⁰ 工作组第六十一届会议对第 25 条第 3 款进行了审议（A/CN.9/1051，第 63-66 段）。工作组商定保留该款以供进一步审议，但须稍作修改，以更正提及指定机构的内容（同上，第 66 段）。