联合国 A/CN.9/WG.IV/WP.171

大 会

Distr.: Limited
10 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

关于使用与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

V.21-06687 (C) 270921 270921

一. 导言

1. 工作组第六十一届会议请秘书处将解释性材料草案连同订正条文草案一并提交工作组第六十二届会议审议。这些材料见载于附件的解释性说明。

2. 该解释性说明由秘书处编写，以供工作组发表意见并最终予以通过。它记录了向贸法会报告的工作组审议情况以及与工作组任务有关的补充背景资料。它提及A/CN.9/WG.IV/WP.170 号文件所载条文草案，对这些条文草案将加以修订以反映工作组第六十二届会议商定的对这些条文的任何修订——和发表的任何意见。解释性说明还可协助工作组最后审定条文草案。

附件

关于使用与跨境承认身份管理和信任服务的条文草案的解释性说明

一. 导言

A. 本解释性说明的目的

1. [待补。]

B. 目标

2. 在过去二十年里，线上商业活动（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）的价值呈指数级增长。全球电子商务从 1999 年的 640 亿美元增长到 2017 年的 29 万亿美元。[1]这一增长与个人和企业对互联网的使用的增加相吻合。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. 这种增长以信任为基础，并且需要有对网上环境的信任感的支持。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，由此开发了用于创设与管理自然人和法人数字身份的各种系统、方法、技术和设备。在全球一级处理身份管理所涉法律问题，不仅有可能将这些不同的解决方案联系起来，而且可以促进加强各身份管理系统之间的互操作性，而不论所涉系统由私人或政府运行。

4. 在拓宽对身份管理和信任服务的利用方面存在若干障碍。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)法律上针对身份管理的做法各不相同，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；及(4)缺乏对身份管理和信任服务进行跨境法律承认的机制。[3]

5. [文书草案]的主要目标是通过制定统一的法律规则来消除这些障碍。这些规则有这样一些目的：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；并通过协调一致的解决方案为弥合数字鸿沟做出贡献。

6. [文书草案]通过这种方式协助执行“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

---

[1] 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，《2019 年数字经济报告：价值创造和获取：对发展中国家的影响》，联合国文件，UNCTAD/DER/2019，第 15 页。

[2] 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：www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx。

[3] A/CN.9/965，第 52 段。

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 是相吻合的。

C. 范围

7. [待补。]

D. 结构

8. 文书草案由四个章节组成，分别涉及总则、身份管理、信任服务和国际方面。第一章和第四章同时适用于身份管理和信任服务。此外，第二章和第三章的结构和内容十分相似。因此，如有条文重合，对第二章条文的解释也可适用于第三章的相应条文。这分别在第 5、6、7、8、10、11 和 12 条方面特别适用于第 13、14、15、22、23 和 24 条。

9. 第一章载有[文书草案]中使用的某些术语的定义；适用范围的划定；关于自愿使用身份管理和信任服务包括特定服务的规定；关于[文书草案]与其他法律之间关系的规定，包括确定或使用特定信任服务的要求；及根据其统一性和国际渊源包括为填补空白的目的对[文书草案]进行自主解释的规定。

10. 第二章确立了适用于身份管理的法律制度的基本要素，列出了身份管理服务提供人和订户的某些核心义务，并制定了关于身份管理服务提供人所负赔偿责任的规则。第 5 条确立了对电子身份识别给予法律承认和对身份管理不予歧视的原则。第 6 条列出了身份管理服务提供人的核心义务；并就此确定了身份管理生命周期中的主要步骤。第 7 条涉及身份管理提供人在数据泄露情况下的义务，第 8 条就订户在身份凭证失密情况下的义务做了补充规定。第 9 条载有关于按规定必须使用可靠方法的线下身份识别和电子身份识别功能等同的规则。对方法的可靠性评估是基于第 10 条所列情况事后确定的或根据第 11 条予以事前指定的。此外，如果该方法实际上已经履行其功能，则不需要确定其可靠性。最后，第 12 条涉及身份管理服务提供人的赔偿责任。

11. 第三章确立了适用于使用信任服务的法律制度的基本要素。第 13 条载有对信任服务法律效力不予歧视的一般规则。第 14 条规定了信任服务提供人的义务，第 15 条涉及信任服务订户在信任服务已失密情况下的义务。第 16 至 21 条描述了使用某些具名信任服务（电子签名；电子印章；电子时间戳；电子存档；电子挂号发送服务；网站认证）履行的功能及其相关要求，包括对可靠方法的使用。所草拟的关于具名信任服务的规定多数是功能等同规则。但是，由于信任服务可能没有其纸质等同形式，因此不一定需要有一条功能等同规则。第 22 条就事后确定信任服务所用方法的可靠性提供了指导，第 23 条就事前指定提供了指导。最后，第 24 条载有关于信任服务提供人赔偿责任的规则。

12. 第四章涉及为系[文书草案]主要目标之一的对身份管理和信任服务的跨境承认创造便利条件。[文书草案]未考虑设立一个负责在法律上承认身份管理和信任服务的专门机构，但设想了几个基于分权做法的机制。除了第 25 条和第 26 条之外，直接有关的还有第 10(3)条、第 11(4)条、第 22(3)条和第 23(4)条，这几条中的条文专门

涉及禁止在确定身份管理和信任服务的可靠性以及在指定可靠的身份管理和信任服务方面的地域歧视。合同协议也可能与便利跨境使用身份管理和信任服务有关。

E. 背景

1. 起草的历史情况

13. [见 A/CN.9/WG.IV/WP.169 第 4-20 段]。

14. [待补。]

2. 与贸易法委员会早先法规的关系

15. 贸易法委员会早先的法规并未载有关于信任服务的条文。但是，它们确实含有可能事关某些信任服务的功能等同规则。特别是，《电子商务示范法》第 7 条、《电子签名示范法》第 6 条、《电子通信公约》第 9(3)条和《电子可转让记录示范法》第 9 条规定了电子签名为在功能上等同于纸质签名而必须遵守的要求。[文书草案]第 16 条以《电子可转让记录示范法》第 9 条为基础。同样，《电子商务示范法》第 10 条载有信息留存功能等同的要求。[文书草案]第 19 条以《电子商务示范法》第 10(1)条为基础。

16. [文书草案]第 16 至 21 条提及旨在为数据电文的某些品质提供保证的信任服务。然而，这些条文涵盖的信任服务并非都有等同的纸质概念。此外，可能没有必要使用[文书草案]中指明的信任服务来满足贸易法委员会早先的法规中所载功能等同规则。

F. 关键概念和原则

17. 本节对[文书草案]所依赖的几个关键概念和原则进行了解释。对[文书草案]中使用的已界定术语的进一步解释载于下文关于第 1 条的评注，而与身份管理和信任服务有关的范围更广的术语和概念清单则是根据在国际上商定的法律和技术案文所载定义汇集的，该清单载于 A/CN.9/WG.IV/WP.150 号文件。如同该文件所示，这些案文可能对同一概念使用不同的术语来加以界定，或对同一术语做出不同的界定。

1. 基本原则

18. 如同贸易法委员会早先的法规，[文书草案]在可做调整的前提下基于当事人意思自治、技术中性、功能等同和不歧视使用电子手段的原则。[4]虽然[文书草案]未加明确指明，但这些一般原则构成了该案文的关键条文。例如，适用于身份管理和信任服务的不歧视原则分别体现在第 5 条和第 13 条中，而功能等同原则体现在第 9 条和第 16-21 条中。

19. 功能等同做法的预设前提是，存在直接或间接规定某种有形或纸质活动的法律要求，例如使用纸质凭证对个人进行身份识别或使用纸质通信对事实或事物进行认

[4] A/CN.9/902，第 52 段和第 63 段。

证，然后对这些要求的目的和功能展开分析，以确定如何通过电子手段实现这些目的或功能。然而，正如数字技术便利开展没有纸质等同形式的一系列活动，[文书草案]所涵身份管理和信任服务中的有些这类服务可能没有纸质等同形式。

2. 身份管理

20. 身份识别是经由参考个人相关信息（即属性）来区分该人的过程。该信息可以通过收集或观察的方式得到。身份识别对于建立网上交易信任度尤为重要。身份识别的核心内容是，核实所收集的或观察到的属性是否与早先给待识别的人确立的“身份”相匹配。从这个意义上讲，身份识别通常是为了回应对某种特定身份的主张和展示属性以供核实而进行的。

21. 因此，根据[文书草案]，身份管理涉及两个不同的阶段（或步骤）——第一，签发身份凭证，即可以出示以供电子识别的数据；第二，经由电子手段提交和核实这些凭证：

(a) 身份管理的第一阶段涉及收集可能构成个人“基本身份”的属性（即在关于自然人的民事登记和人口动态统计系统中以及在关于法人的公司和企业登记册中由政府机构记录的属性）。这些属性可以以经颁发机构核实由政府颁发的凭证（例如注册证书）的形式呈现。该项工作可以基于当面出示的物理凭证“线下”实施，在工作结束后可向该人颁发凭证；

(b) 身份管理第二阶段涉及经由电子手段提交这些凭证，并经由电子手段核实凭证提交人即为在第一阶段时被颁发凭证的人。

22. 身份管理系统用于管理与这些阶段中各阶段有关的身份识别流程，以及对已收集的属性、颁发的凭证及核实所用手段实施管理。身份管理系统可能涉及执行身份管理每个阶段所涉所有流程的单个实体，或者执行这些流程的多个实体。此外，一些身份管理系统可能会根据当事人（即寻求识别的当事人和寻求被识别的当事人）的需要提供不同的身份管理“服务”。

23. 身份管理系统用于提供身份管理服务。身份管理系统可以由公共或私人实体运营，并可提供多项身份管理服务。在实务中，公共身份管理系统通常对应于单个身份管理服务，而私营身份管理系统可能对应于具有不同级可靠性的多项身份管理服务。对身份管理系统的另一个分类是按照其为集中式系统或分布式系统进行分类。[文书草案]在技术和模式上是中性的，因此可适用于所有各类身份管理系统和服务。

24. 身份管理服务提供人、订户、依赖方及其他相关实体可商定按照系统规则所述兼容的政策、标准和技术运营，以便参与运营的所有各依赖方都能理解和信任由参与运营的各身份管理服务提供人提供的凭证。这种安排可称作“身份联盟”，而具有契约性质的系统规则可称作“信任框架”。身份联盟可能有助于增加共享相同身份管理服务的用户和应用程序的数量，并进而可能有助于控制成本和确保长期可持续性。

3. 信任服务

25. 信任服务在建立对使用电子交易的信任方面同样至关重要。就其核心内容而言，信任服务是为数据电文的某些品质提供保证，例如来源、完整性和数据处理时间。虽然[文书草案]确定了某些常用的信任服务，但它承认可能存在其他一些信任服务，或在今后可以开发其他某些信任服务。

26. [文书草案]中的信任服务概念涉及服务的交付，而不仅仅涉及服务。例如，它涉及的是给电子签名创建和管理方法而不仅仅是给电子签名提供支持的服务。

4. 可靠性的确定

27. 如同贸易法委员会早先的法规，[文书草案]若干条文提及对可靠方法的使用。[文书草案]设想有两种方法可靠性评估机制：第 10 条和第 22 条载有确定可靠性相关因素的指示性清单；第 11 条和第 23 条就可靠方法指定机制做了规定。该做法是建立在《电子签名示范法》第 6 条和第 7 条的基础之上的。

28. [文书草案]兼有确定和指定两种机制，并不厚此薄彼，而是力图各取所长，同时尽量避其所短，并最终促成各方当事人选择其赞同的解决方案。

29. 涉及信任服务的贸易法委员会法规并非都载有颁布事前确定的做法和事后确定的做法的条文。然而，事前确定的做法和事后确定的做法通常被认为是兼容和互补的。

(a) 可靠性的事后确定

30. 可靠性的确定只适用于存有争议的情况，因此是在所涉方法使用之后（事后）。[文书草案]经此方式通常让身份管理交易成为可能，并把对确定所用方法可靠性的需求限定在因一方当事人或多方当事人的身份未获识别或未获充分识别而对交易有效性产生争议的范围内。

31. 事后确定的做法的好处是，它给当事人选择技术和做法提供了最大的灵活性。此外，它可以进行分权化管理，不需要建立一个体制机制并从而能避免产生相关费用。

32. 另一方面，事后确定的做法的缺点是，无助于提前提高法律确定性，从而让当事人无法预测所用方法的有效性，因此在所用方法被视为不可靠的情况下，可能会让他们承受更多风险。此外，它将方法可靠性的确定交由第三方进行裁断，这可能既费时，又致使所做决定前后不相一致。

(b) 事先指定可靠服务

33. 可靠服务的指定是在使用可靠方法之前（事前）按照预定条件清单笼统进行，而并非参照某一特定的交易。对[文书草案]所述条件的进一步确定不应导致强行规定特定技术要求。

34. 指定所涉及的并非通类身份管理和信任服务，也并非由身份管理服务提供人或信任服务提供人提供的所有各种身份管理和信任服务，而只是由某一特定服务提供人提供的某一特定服务。

35. 较之于事后确定的做法，事前确定的做法可在包括跨境使用等情况下提高身份管理和信任服务法律效力的清晰度和可预测性。然而，这方面的管理应当能够根据技术演进迅速做出调整以避免阻碍创新。否则，它可能会歧视虽然可加利用而且基于可靠方法但却未获指定的身份管理和信任服务。

36. 颁布法域必须确定可以是私营或公共机构的指定事务负责实体。可根据适用于产品、工艺和服务认证机构的技术标准对指定实体进行认证。认证（包括自我认证）也有助于使用基于成果的标准对服务进行评估，因此可能事关服务的指定。

37. 实施事前确定的做法所需体制机制需要有一个通常集中管理的专门的指定机制。该机制应列有诸如服务评估标准、决策评估工作详细情况和筹资来源等各种要素。取决于包括体制安排在内的若干因素，该许可证制度的治理工作可能情况复杂并且耗费昂贵。为此原因，指定这一方式可能更适宜于保证度和可靠性更高的服务，并因此可能更加适用于价值更高的交易。对于希望实施事前确定的做法的颁布法域，[文书草案]以已有必要的体制机制为预设前提，并未就这类机制的建立或管理预做规定。

5. 国际方面

38. 从法律上允许跨境使用身份管理和信任服务是[文书草案]所追求的主要目标之一。该目标是经由技术中性和禁止地域歧视原则的适用来实现的。这些原则贯穿于[文书草案]第 10(3)条、第 11(4)条、第 22(3)条和第 23(4)条。此外，第四章（第 25 和 26 条）专门处理跨境承认问题。

39. [文书草案]不要求跨境法律承认需要建立正式的体制安排。然而，在区域和双边各级均有这种安排的实例。颁布法域不妨将[文书草案]用作包括在专门协议下与国际伙伴建立体制安排的模板。

40. [文书草案]还可有助于落实自由贸易协定或数字经济专门协定中所载关于在法律上相互承认的条文。

二. 逐条评注

A. 第一章——总则（第 1 至 4 条）

1. 第 1 条. 定义

41. 第 1 条载有[文书草案]中所用术语的定义。[5]

[5] 编制了基于国际商定的法律和技术文本所载定义汇集的身份管理和信任服务相关术语和概念清单，以作为对[文书草案]编制工作的支持，该清单载于 A/CN.9/WG.IV/WP.150 号文件。

“属性”

42. “属性”指与某人关联的一条信息或数据。自然人属性的实例包括姓名、地址、年龄和电子地址，以及诸如网络活动和所用设备等数据。法人属性的实例包括公司名称、主要办公地址、注册名称、注册管辖权。对身份的定义使用了属性的概念。

43. 属性可能包含如何处理属于数据隐私和保护法律客体的个人数据。[文书草案]不涉及数据隐私和保护，并明确保留对该项法律的适用。

参考文献

A/CN.9/WG.IV/WP.150，第 13 段。

“数据电文”

44. “数据电文”的定义载于贸易法委员会关于电子商务的所有现行法规。该术语是界定关于信任服务的各项要求的主要参考，其原因是，适用信任服务的结果就是保证数据电文的品质。

参考文献

A/CN.9/1045，第 40 段。

“电子身份识别”[“认证”]

45. “电子身份识别”一语是指对所称的身份和出示的凭证进行绑定加以核实，它是身份管理工作的第二阶段。使用“电子身份识别”而不是“认证”一语，是为了消除对赋予“认证”一语多重含义所持的关切。就其技术上的用法而言，“认证”一词是指出示身份证据。

46. 第 9 条是从非技术层面的意义上使用不带限定词的“身份识别”一语的。

参考文献

A/CN.9/1005，第 13 段、第 84-86 段、第 92 段；A/CN.9/1045，第 134 段和第 136 段；A/CN.9/1051，第 67 段。

“身份”

47. “身份”的定义是身份管理概念的核心所在，是指在特定背景下独一区分自然人或法人的能力。因此，它是一个在特定背景下的相对概念。该定义取自建议 ITU-T X.1252 第 6.40 条所载定义。

参考文献

A/CN.9/WG.IV/WP.150，第 31 段；A/CN.9/1005，第 108 段。

“身份凭证”

48. “身份凭证”是包含为身份核实而出示的数据在内的数据或实物。数字凭证的实例包括用户名、智能卡、移动身份和数字证书、生物特征护照和电子身份证。根据身份管理系统的特点，电子形式的身份凭证可以线上或线下使用。从广义上讲，“身份凭证”一语与区域和国家立法中使用的“电子身份识别手段”一词（例如见《电子身份识别和信任服务条例》第 3(2)条）具有相同的含义。

参考文献

A/CN.9/1005，第 110 段；A/CN.9/1045，第 137 段。

“身份管理服务”

49. “身份管理服务”的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”。身份管理服务的定义是指与其中一个或两个阶段有关的服务，因为该定义中“或”一词的使用并非是不连贯的。关于身份管理服务提供人核心义务的第 6(a)条描述了提供身份管理服务所包含的各个阶段和步骤。

参考文献

A/CN.9/1005，第 84 段和第 109 段。

“身份管理服务提供人”

50. 身份管理服务提供人是通过直接或经由分包人履行第 6 条所列功能而提供身份管理服务的自然人或法人。但是，并非该条所列所有功能都与所有身份管理系统有关，因此身份管理服务提供人不需要执行所列出的每一项功能。

参考文献

A/CN.9/971，第 97 段；A/CN.9/1005，第 111 段；A/CN.9/1045，第 88 段。

“身份管理系统”

51. “身份管理系统”的定义描述了通过身份核实和电子身份识别来进行身份管理的管理系统。它使用了与国际电联的术语保持一致的“功能和能力”的提法，即建议 ITU-T X.1252，第 6.43 条。不同于“身份管理服务”的定义，“身份管理系统”的定义必然包括两个阶段，即使每一个阶段涉及不同的服务提供人。

参考文献

A/CN.9/1005，第 112 段。

“身份核实”

52. “身份核实”一语是指包括入册在内的身份管理第一阶段，该阶段是身份管理服务提供人在向某一主体签发凭证之前核实该主体的身份主张的过程。将“身份识别”一词改为“身份核实”，是为了消除对“身份识别”具有多重含义所持的关切。

参考文献

A/CN.9/1005，第 84 段。

“订户”

53. “订户”一语是指得到所提供的服务的人，并且不包括依赖方。它以服务提供人和订户之间订有合同为预设前提。举例说，电子签名的签名人属于“订户”这一定义的范围之内。

参考文献

A/CN.9/1005，第 43 段和第 96 段；A/CN.9/1045，第 18 段和第 22 段。

“信任服务”

54. “信任服务”的定义既有对使用侧重于保证诸如真确性和真实性等数据品质服务的信任服务执行相关功能的抽象描述，也有列出[文书草案]列明的各项信任服务的非详尽清单。采用非详尽清单有助于对今后各类信任服务适用关于信任服务的一般规则。

55. “创建和管理方法”的提法澄清“信任服务”的概念是指所提供的服务，而并非指使用这些服务所产生的结果。举例说，信任服务不是电子签名本身（即对签名人进行身份识别并表明其对基础数据电文所含信息的意图的数据），而是给电子签名提供支持的服务（即为签名人提供创建电子签名的方法并确保履行电子签名所要求的功能的服务）。

参考文献

A/CN.9/965，第 101-106 段；A/CN.9/971，第 110-111 段；A/CN.9/1005，第 14-18 段；A/CN.9/1051，第 35-40 段。

“信任服务提供人”

56. 信任服务提供人是提供信任服务的自然人或法人。《电子签名示范法》含义内的认证服务提供人即为体现电子签名方面信任服务提供人的一个实例。不同于身份管理服务提供人（第 6 条），[文书草案]没有确定拟由信任服务提供人履行的功能。

57. [文书草案]没有要求把利用第三方信任服务提供人作为给予法律承认的一个先决条件。如果没有利用第三方信任服务提供人，则同一实体可能发挥信任服务提供人和订户的角色。

参考文献

[待补。]

2. 第 2 条. 适用范围

58. 第 2 条划定了[文书草案]的适用范围，提及在商业活动和贸易相关服务中使用并跨境承认身份管理系统和信任服务。“贸易相关服务”一词旨在涵盖与贸易密切有关但非商业性的交易。这些交易可能涉及诸如一站式办理进出口手续的海关部门等公共实体。

59. 由于使用身份管理和信任服务的影响超出了商业交易，颁布法域可以将[文书草案]的范围扩大至所有各类交易。

60. 按照贸易法委员会关于电子商务的法规所依据的主张避免或尽量减少对现有实体法的修改的一般原则，第 2(a)款澄清，[文书草案]没有引入任何新的身份识别义务。

61. 表示[文书草案]不要求使用任何特定的身份管理或信任服务的第 2(b)和(c)款，贯彻了技术中性原则，包括有关模型和系统中性的原则。

62. 第 3 款保留了要求使用某种身份识别程序或使用具体指明的信任服务的法律要求。此种典型的监管要求例如包括要求提供特定身份证件（如护照）或具有与相关属性相对应的某些特征的身份证件（如带有持证人照片和出生日期的身份证）。身份识别要求也可要求由履行特定功能的某个人进行身份识别。如果电子身份识别获得允许的话，相关监管机构通常要求使用具体指明的身份管理程序或诸如由公共机构签发的身份凭证之类信任服务。

63. 鉴于其赋能性质，[文书草案]不影响对身份管理和信任服务适用可规范其活动或规范使用身份和信任服务进行交易的某些实质性方面的其他法律，一如现有的贸易法委员会示范法。第 4 款载明了关于数据隐私和保护法律的这一原则，这项原则因其关联性而被专门提及。该项条文没有提及其他情况下的隐私。

参考文献

A/74/17，第 172 段；A/CN.9/936，第 52 段；A/CN.9/965，第 125 段；A/CN.9/971，第 23 段；A/CN.9/1005，第 115 段；A/CN.9/1045，第 76-78 段。

3. 第 3 条. 自愿使用身份管理服务和信任服务

64. 第 3 条指出，[文书草案]没有强行规定不同意使用身份管理或信任服务的人必须使用身份管理或信任服务。然而，此种同意可以从一方当事人的行为中推断出来，例如从选择使用由身份管理和信任服务提供支持的特定电子商务软件或电子通信系统即可做出此种推断。

65. 自愿使用身份管理和信任服务的原则与当事人意思自治原则是有关联的，因为这两项原则都是建立在意愿的基础之上。同意使用身份管理和信任服务与同意根据数据隐私和保护法律处理个人信息可能不尽一致。

66. 基于《电子通信公约》第 8(2)条的第 3 条，防止给订户、服务提供人和依赖方规定使用身份管理和信任服务的任何新的义务。这与不打算对实体法做任何修订的一般规则是相吻合的。

67. 其他法律可能订有使用身份管理和信任服务的义务。在与公共实体的交易中或在涉及遵守监管义务的交易中可能会规定此种义务。

参考文献

A/CN.9/965，第 22 段和第 110 段；A/CN.9/1005，第 116 段；A/CN.9/1045，第 79 段。

4. 第 4 条. 解释

68. 第 4 条基于贸易法委员会早先几项条约和示范法所载条文，包括关于电子商务的条文（《电子商务示范法》第 3 条；《电子签名示范法》第 4 条；《电子通信公约》第 5 条；《电子可转让记录示范法》第 3 条）。

69. 第 1 款旨在促进各颁布法域的统一解释。为此，它提请法官和其他裁决机构注意这样一个事实，即对[文书草案]的国内法律制定应根据其国际渊源和统一适用的需要来加以解释。因此，鼓励裁决机构在裁决案件时考虑来自外国法域的裁决，目的是协助巩固跨国统一解释的趋势。

70. 第 2 款旨在确保统一解释和适用为执行[文书草案]而制定的法律，要求未予明确解决的问题应根据[文书草案]所依据的一般原则而不是国内法所载原则予以解决。

71. 类似于贸易法委员会关于电子商务的其他立法案文，[文书草案]没有明文确定它所依据的一般原则。不歧视使用电子手段、技术中性、功能等同和当事人意思自治等原则通常是贸易法委员会关于电子商务的立法案文的依据，并已被确定为经做调整也与[文书草案]有关。例如，虽然当事人意思自治是商法的一项基本原则，但该原则的适用必须遵守强制性法律所述限制，包括当事人不得减损的[文书草案]中的条文。此外，如同上文所述（第 20 段），没有线下要求的，功能等同原则可能就无法适用。

参考文献

A/CN.9/936，第 67 段和第 72 段；A/CN.9/1005，第 117-118 段；A/CN.9/1051，第 53-56 段。

B. 第二章——身份管理（第 5 条至第 12 条）

1. 第 5 条. 对身份管理的法律承认

72. 第 5 条从法律上承认身份管理，指出身份核实和电子身份识别的电子形式本身不应妨碍其作为证据的法律效力、有效性、可执行性或可采性。因此，第 1 款贯彻了在身份管理方面不歧视使用电子手段的一般原则。无论是否有线下等同形式，该原则都将适用。

73. 第 5 条禁止歧视作为身份管理工作所获成果的电子身份识别。其标题采用“法律承认”而不是“不歧视”的提法，是为了与贸易法委员会现有法规相应条文的标题保持一致。

74. (b)项明确指出，身份管理服务并非指定服务的事实不妨碍其得到法律承认。换言之，(b)项在法律上对指定的和未指定的身份管理服务给予同等的承认，从而确保了所选择的可靠性评估做法是中性的。然而，(b)项并不意味着任何身份管理服务均使用可靠的方法并因而为电子身份识别提供了充足的保证：为了实现这一结果，需要酌情根据第 10 条和第 11 条评估所用方法的可靠性。

75. 第 5 条起首部分提及第 2 条第 3 款，强调第 5 条不影响按照法律界定或规定的程序对个人进行身份识别的任何法律要求。第 2 条第 3 款不仅对第 5 条而且还对[文书草案]所有其他条文做了限定。

参考文献

A/CN.9/965，第 107-108 段；A/CN.9/1005，第 79-86 段；A/CN.9/1045，第 17 段和第 82-84 段。

2. 第 6 条. 身份管理服务提供人的义务

76. 第 6 条列出了身份管理服务提供人的义务。所列出的这些义务是身份管理服务提供人的基本义务，可以经由法律规定的或合同约定的其他义务对其加以补充。不履行这些义务可能会产生第 12 条所述赔偿责任，并影响包括指定服务在内的身份管理服务的可靠性。

77. 此外，第 6 条旨在确保身份管理服务提供人仍然负责向订户提供全套身份管理服务，不过某些功能可以由诸如私营部门多方身份管理系统中的分包人或单独的身份管理服务提供人等其他实体执行。第 6 条不妨碍身份管理服务提供人对任何功能进行外包或在其分包人或其他业务合作伙伴之间分配风险。

78. 身份管理系统的目的和设计以及所提供的服务可能都有很大的不同。身份管理系统的设计进而也可能取决于所选择的模型。因此，第 6 条列出的所有各项义务并非都可适用于所有身份管理服务提供人：相反，身份管理系统的设计和所提供的身份管理服务的类型将决定究竟哪些义务适用于特定的身份管理服务提供人。身份管理系统设计做法的此种灵活性体现在“与目的和设计相适合”的词句上。

79. 对这些义务是以技术中性方式描述的，因为身份管理方面技术中性原则的落实所需要的身份管理系统最低要求指涉的是系统属性而并非特定技术。

80. 在商业实务中，第 6 条列出的各项功能通常必须遵守合同约定的运营规则，特别如果涉及私营部门的身份管理服务提供人的话。就运营方式提供指导的这些规则，以政策为基础，经由实务予以落实，并在合同协议中得到体现。“制定操作规则、政策和做法”的义务是对该商业实务的认可。由于其在法律和实务上的重要性，(d)项要求操作规则、政策和做法应便于订户和第三方查阅。

81. 服务提供人应受其所做陈述和承诺约束的原则载于《电子签名示范法》第 9(a)条，该条确立了认证服务提供人“按其所作出的关于其政策和做法的表述行事”的义务。

参考文献

A/CN.9/936，第 69 段；A/CN.9/1045，第 85-95 段。

3. 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

82. 第 7 条确立了在发生对身份管理系统具有重大影响的数据泄露情况下身份管理服务提供人所持的基本义务。无论身份管理系统的目的和设计如何，第 7 条所述义务都将适用，不得经由合同包括其操作规则加以变更。安全违规可能会影响身份管理系统和身份管理服务，也可能会影响身份管理系统中管理的属性。

83. “数据泄露”的概念是指导致所传输、存储或以其他方式处理的数据的意外或非法销毁、丢失、更改、未经授权的泄露或访问的安全违规情况。可以在数据隐私和保护法律中对这一概念加以界定。

84. 区域[6]和国家法律中使用了“重大影响”的概念。有几个因素可能有助于影响评估。违规事件通知表为协助进行影响评估而要求说明所涉事件的持续时间、数据类型和受影响订户的百分比及其他相关信息。还将提供事件报告技术准则和安全事件年度报告。

85. 第 7 条认识到可能适宜采取其他措施而非全面暂停，它要求身份管理服务提供人“采取一切合理阶段”以应对和遏制安全违规情形。

86. 第 1(c)款确立了属于透明度原则一个方面的安全违规情形通知义务。适当的安全违规情形通知机制对改进身份管理和信任服务工作情况及提升信心度具有重要意义。

87. 对第 7 条所载义务的某些方面，例如识别被通知违规情形的当事人的身份、发送通知的时间和通知的内容及披露违规情形及其技术细节，均可在各国法律、合同协议以及身份管理服务提供人的操作规则、政策和做法中加以具体规定。

88. 第 7 条确立的义务可能与数据隐私和保护法律规定的义务相吻合。在这种情况下，对所列出的所有各种行动，而不仅仅是通知，都应根据可适用的数据隐私和保护法律加以落实。

89. 第 7 条与数据隐私和保护法律以及适用于特定事件的任何其他法律同时一并适用。例如，数据泄露通知与安全违规通知有共同之处，但也有重大区别。

参考文献

A/CN.9/971，第 84-87 段；A/CN.9/1005，第 32-36 段和第 94 段；A/CN.9/1045，第 96-101 段。

[6] 欧洲议会和理事会 2014 年 7 月 23 日关于内部市场内电子交易的电子身份识别和信任服务并废除第 1999/93/EC 号指令的第 910/2014 号条例（欧盟）第 19(2)条（《电子身份识别和信任服务条例》）。

4. 第 8 条. 订户的义务

90. 第 8 条规定了订户在身份凭证失密或有失密风险方面的通知义务。这些义务是对身份管理服务提供人所持的这样一些义务的补充，即提供关于安全违规情形的通知手段（第 6(e)条）和对安全违规情形或完整性丧失情形做出反应（第 7 条）。

91. 身份凭证失密或者存在或许失密的一定的可能性即可触发订户对数据泄露所持义务。因此，该事件不同于确立身份管理服务提供人对数据泄露所持义务的事件，数据泄露是指发生了对身份管理服务具有重大影响的安全违规情形或完整性丧失情形。

92. 提及身份凭证可能已失密的可能性，旨在确保不会对订户的技术专业水平抱持不合理的过高期望。通知义务只应在用户已知的会引起对身份凭证是否使用适当持有合理怀疑的情况下产生。

93. 订户和身份管理服务提供人之间的合同可能载有对订户的额外义务。该合同还可载有关于如何履行第 8 条所载通知义务的补充信息。

94. “以其他方式使用合理手段”的提法表明，订户不限于使用身份管理服务提供人提供的沟通渠道。

95. “已失密的身份凭证”的概念是指未经授权访问身份凭证的情况。

96. (b)款旨在述及订户对失密实际并不知情但有理由相信可能已经发生失密的情况。它受到《电子签名示范法》载有签名人类似义务的第 8(1)(b)㈡条的启发。

参考文献

A/CN.9/936，第 68 段；A/CN.9/971，第 88-96 段；A/CN.9/1005，第 37-43 段和第 95-96 段；A/CN.9/1045，第 102-105 段。

5. 第 9 条. 使用身份管理对个人进行身份识别

97. 在贸易法委员会关于电子商务的法规中，功能等同规则规定了电子记录、方法或流程为履行纸质法律要求而必须满足的条件。第 9 条载有关于法律要求必须进行身份识别或当事人商定相互识别对方身份的功能等同规则。由于这项条文的目标是确立线下和线上身份识别具有等同性的条件，因此第 9 条仅在有线下身份识别等同形式的情况下方可适用。不过，第 9 条是建立身份管理法律制度的核心条文。

98. 按照贸易法委员会法规中的既有原则，该功能等同规则是对第 5 条所述法律承认规则的补充。然而，虽然第 5 条适用于所有各种形式的电子身份识别，而无论是否存在线下身份识别等同形式，但第 9 条的目的是，将电子身份识别作为线下身份识别的功能等同形式，因此第 9 条的适用只能参照纸质等同形式。

99. 该条提及对身份管理服务的利用是为了表明，使用身份凭证而不是使用身份管理系统或身份本身即可满足等同性要求。

100. 第 9 条不影响第 2(3)条所述根据某一特定方法或程序进行身份识别的要求。这些要求可能与诸如由银行和反洗钱条例规定的要求等监管合规性要求有关（见上文第 62 段）。

101. 按照基于物理实体的身份识别的要求，可使用电子身份识别来满足核实诸如年龄或住所等个人身份特定属性的要求。在这方面，由于“身份”的概念是参照“背景”来界定的，而“背景”又决定了身份识别所需属性，因此基于第 9 条顺利识别个人的身份包括了核实所需的属性。核实相关属性的需要也反映在“为此目的”一词中。第 10 条所载关于可靠性的条文不涉及对特定属性的核实，因为这些条文涉及的是身份凭证的管理过程，而不是身份凭证所包含的属性。

102. [文书草案]第 9 条和第 16 至 21 条提及法律要求采取行动或对不采取行动所造成的后果做出规定的情况。所草拟的在《电子通信公约》第 9 条中使用的表述是为了在法律不要求采取行动但是给某些行动赋予法律后果的情况下顾及功能等同规则，也涵盖了法律允许采取某些行动的情况（见《电子可转让记录示范法》第 9 条）。

参考文献

A/CN.9/965，第 62-85 段；A/CN.9/971，第 24-49 段；A/CN.9/1005，第 97-100 段；A/CN.9/1045，第 106-117 段；A/CN.9/1051，第 42-44 段。

6. 第 10 条. 身份管理服务的可靠性要求

103. 第 10 条就方法使用后确定第 9 条中身份识别所用方法（事后确定的做法)的可靠性提供指导。

104. 第 1(a)款贯彻了事后确定的做法，采用了使用一种“对于所正在使用的身份管理服务的目的而言是可靠和适宜的”方法的提法。这项条文反映了对可靠性属于相对概念的理解。然而，不同于可能履行多种功能的某些信任服务，电子身份识别只履行一种功能，即使用电子手段进行可靠的身份识别。可以为不同的目的履行该功能，而每一目的都与不同的可靠度相关联。

105. 第 1(b)款载有一项旨在防止在身份管理服务实际上已经履行其功能情况下拒绝接受该服务的条款。拒绝接受发生于主体宣称未执行某项行动之时。第 1(b)款所载机制发挥作用的先决条件是，该方法无论可靠与否，都必须事实上履行了身份识别的功能，即把寻求身份识别的人与身份凭证相关联。该项条文基于《电子通信公约》第 9(3)(b)㈡条。

106.第 2 款载有一份以技术中性术语描述的情况清单，这些情况可能对裁定人确定可靠性有所帮助。由于该清单是说明性的，并非详尽无遗，因此可能还存在其他与此有关的情况。而且，所列出的情况并非都与需要确定可靠性的所有各种情况有关联。特别是，当事人协议的相关性可能区别很大，这取决于相关法域对在身份识别领域当事人意思自治的承认程度。此外，合同协议可能不会影响第三方，因此，当涉及第三方时，这种情况不具关联性。

107. 第 3 款规定，提供身份管理服务的地点和身份管理服务提供人的营业地本身无关可靠性的确定。这项规定旨在便利对身份管理服务的跨境承认，并受到《电子签名示范法》第 12(1)条的启发，该条规定了在确定证书或电子签名的法律效力时不

予歧视的一般规则。关于《电子签名示范法》第 12(1)条和第 12(2)条之间的相互关系的讨论，见 A/CN.9/483，第 28-36 段。

108. 第 4 款规定，根据第 11 条指定可靠的身份管理服务即为推定指定的身份管理服务所用方法是可靠的。这是指定和非指定身份管理服务之间的唯一区别。而且，根据第 5(b)款，对赋予指定的可靠性推定可加以反驳。

109. 第 5 款澄清了第 10 条和第 11 条之间的关系，它明确规定，指定机制的存在并不排除对方法的可靠性可以事后加以确定。该项条文受到《电子签名示范法》第 6(4)条的启发。

(a) 保证级框架

110. 第 10 条和第 11 条提及“保证级”或以其他方式指明的类似框架的概念。保证级就其对身份核实和电子身份识别过程的信任度以及这些过程是否足以实现特定目的向依赖方提供指导。[文书草案]既没有界定保证级，也没有对界定或使用保证级提出要求。

111. 保证级框架预见存在与不同需求相关联的不同的保证级。换言之，保证级框架描述了身份管理系统和服务为确保其可靠性具有某种保证级而必须满足的要求。应当笼统描述保证级以保持技术中性。

112. 而对所用身份可靠性的某种保证级的要求可以参照保证级框架所述级别来加以表述。然后可以对照所需保证级的要求列明特定的身份管理系统和服务。如果能在身份管理服务和与该保证级相关要求之间顺利匹配，就有可能对某一特定类别的交易使用该身份管理服务。

(b) 核证和监督

113. 第 10 条在可能相关的情况中列出了“就身份管理服务提供的任何监督或核证”。核证和监督可能大大有助于建立对身份管理服务提供人及其包括为确定所用方法可靠性而提供的服务的信任，因为这类服务在评估所用方法可靠性时具有一定程度的客观性。这已得到《电子可转让记录示范法》第 12(a)㈥条和《电子签名示范法》第 10(f)条的承认。

114. 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；以及公共实体的核证。选择最合适的核证形式可能会受到所涉服务类型、成本以及所寻求的保证级的影响。在企业对企业的环境中，业务合作伙伴应该能够选择最适合其需求的选项，并认识到每个选项都会产生不同的效果。

115. 有身份管理系统和服务的监督机制可被视为给建立对身份管理的信任是有益的或甚至是必要的。然而，建立监督机构会造成在行政和财政方面可能代价高昂的后果。[文书草案]没有对建立监督制度提供授权或便利。

116. 让公共机构参与核证和监督是颁布法域的一项政策决定，在这方面的做法各不相同。[文书草案]所持做法基于模式中性，提及核证和监督并没有把自我核证制度排除在外。当公共实体既是核证机构或监管机构又是身份管理服务提供人时，核证和监管职能可区别于身份管理服务的提供。

117. 在某些情况下，例如当使用某些类型的分布式分类账技术时，以某种核证、认证或监督中央机构为预设前提的解决办法可能都不合适，因为在确定能够申请认证、接受评估并负责采取纠正和强制措施的实体等方面存在挑战。

参考文献

A/CN.9/965，第 40-55 段和第 112-115 段；A/CN.9/971，第 50-61 段；A/CN.9/1005，第 101 段；A/CN.9/1045，第 118-124 段；A/CN.9/1051，第 47-49 段；A/CN.9/WG.IV/WP.153，第 74-75 段。

7. 第 11 条. 指定可靠的身份管理服务系统[和服务]

118. 第 11 条是对第 10 条的补充，该条提供了指定身份管理系统[和服务]的可能性。更准确地说，它列出了身份管理服务系统[或服务]列入指定身份管理服务系统[和服务]清单所必须满足的条件。

119. 使用可靠方法指定身份管理系统[和服务]是基于所有相关情况，包括第 10 条中列出的用于确定方法可靠性的情况。提及第 10 条所列情况确保了事先指定的可靠方法与事后确定的可靠方法存在某种程度的一致性。而且，指定应“符合与施行指定程序有关的公认国际标准和程序”，以促进跨境法律承认和互操作性。

120. 关于指定的身份管理系统[和服务]的信息对让潜在订户了解其存在至关重要。指定实体有义务例如在其网站上公布指定的身份管理系统[和服务]清单，包括身份管理服务提供人的详细信息，或以其他方式将指定告知公众。广为使用的技术标准也承认清单在确保身份管理服务指定工作透明度方面的相关性，包括在跨境情况下。

121. 第 2(a)款提及与确定可靠性有关的标准和程序，目的是确保对可靠性的事前和事后评估在结果上存在某种统一性。另一方面，第 3 款明确提及事前确定做法所特有的指定相关标准和程序，例如合格评估和审计。

122. 类似于第 10(3)条，第 4 款明确规定，提供身份管理系统[或服务]的地点和身份管理服务提供人的营业地本身无关可靠服务的指定。因此，第 4 款也是基于《电子签名示范法》第 12(1)条，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予区别对待。在实务中，该项条文允许外国身份管理服务提供人向颁布法域主管机构提出关于指定身份管理系统[或服务]的请求，这也见于第 25(3)条。

参考文献

A/CN.9/965，第 40-55 段；A/CN.9/971，第 68-76 段；A/CN.9/1005，第 102 段和第 105 段；A/CN.9/1045，第 125-129 段。

8. 第 12 条. 身份管理服务提供人的赔偿责任

123. 赔偿责任制度对促进使用身份管理和信任服务可能会有重大影响，并且是[文书草案]的一项核心要素。第 12 条确立了身份管理服务提供人对订户的统一的赔偿责任制度，该制度所依据的原则是，身份管理服务提供人未能提供法律要求的和合同约定的服务，应对所造成的后果承担赔偿责任。

124. 第 12 条基于三个要素：(a)它不影响强制性法律的适用，包括身份管理服务提供人在[文书草案]下的强制性义务；(b)它确定了身份管理服务提供人对违反其强制性义务所承担的赔偿责任，而无论这些义务是否也有合同约定的依据；(c)它承认在某些条件下是可以对赔偿责任加以限制的。

125. 第 12 条下的赔偿责任具有法定性，因此，它区别于合同法下的赔偿责任。其目标是承认，服务提供人可能因未履行[文书草案]规定的义务承担赔偿责任，而不论这些义务是否也具有合同约定的依据。无论身份管理服务提供人在性质上是公营或私营的，该项条文均为适用。

126. 身份管理服务提供人的赔偿责任可能源于对指定的和非指定的身份管理服务的使用。然而，这并不是绝对的。例如，如果损失因在凭证失密之时使用了订户知道或本应知道的服务造成，身份管理服务提供人对订户可能不会承担赔偿责任。

127. 与赔偿责任有关并且在第 12 条中未予涉及的事项将留待条文草案范围以外的适用法律处理。这些事项包括注意的标准和过错程度、举证责任、损害赔偿和补偿数额的确定等。

128. 第 12 条承认，在某些条件下是可以对赔偿责任加以限制的，即存在对使用身份管理服务的交易目的或价值的限制，并且已将该限制告知订户。

129. 除其他外，限制赔偿责任可能为控制保险费用所必需。赔偿责任限制在服务提供人和订户之间的合同中约定。在实务中，它们通常见于服务提供人的操作规则、政策和做法。

130. 身份管理服务提供人能够在多大程度上给其赔偿责任设限将由适用法律决定。[文书草案]不影响限制服务提供人对其赔偿责任设限的权利或给这类设限拟订先决条件的任何法律的适用。

131. 第 3(b)款无意引入新的告知义务，而是表明该项条文并不凌驾于适用法律下更严格的通知要求之上。该法律将决定诸如通知或明确批准之类在提供信息上所可适用的任何要求。

132. 第 12 条只涉及身份管理服务提供人对订户的赔偿责任。因使用身份管理服务而遭受损失的第三方可以根据现有赔偿责任规则向服务提供人或订户寻求补救。在后一种情况下，订户可以随之向身份管理服务提供人索赔。

133. 第 12 条对服务提供人根据其他法律就对第三方的赔偿责任设限的能力不做限制。第 6(d)条要求服务提供人也应使其操作规则、政策和做法方便第三方查阅。然而，[文书草案]并未具体要求服务提供人者将对赔偿责任的限制告知第三方依赖人，因为事先识别这些第三方的身份可能是有难度的。

134. 无论身份管理服务提供人在性质上是公营或私营的，第 12 条均为适用。颁布法域可能需要根据关于公共实体赔偿责任的任何特别规则而对该项条文加以调整。第 12 条不适用于履行监督职能和管理可能提供基本身份凭证的民事记录和人口动态统计的公共实体。

参考文献

A/CN.9/936，第 83-86 段；A/CN.9/965，第 116-118 段；A/CN.9/971，第 98-107 段；A/CN.9/1005，第 76 段；A/CN.9/1045，第 130-131 段；A/CN.9/1051，第 13-29 段。

C. 第三章——信任服务（第 13 至 24 条）

1. 第 13 条. 对信任服务的法律承认

135. 第 13 条确立了一项关于不歧视使用信任服务所产生的对数据电文某些品质所提主张这一结果的一般规则。提及使用信任服务所产生的结果使其同第 5 条采取的做法相一致，后者从法律上承认使用身份管理进行的电子身份识别。

136. 第 13 条适用于信任服务，而无论所涉服务是否在[文书草案]中指明，也无论服务的运营是否独立于功能等同规则的存在。

参考文献

A/CN.9/971，第 112-115 段；A/CN.9/1005，第 19-26 段；A/CN.9/1045，第 16-17 段。

2. 第 14 条. 信任服务提供人的义务

137. 第 14 条规定了信任服务提供人的核心义务，而无论是否指明了信任服务。合同协议可以对这些核心义务加以明确规定和补充，但不得予以偏离。该做法类似于关于身份管理服务提供人的义务的第 6 条和第 7 条所持做法。

138. “对于信任服务的目的和设计而言是适宜的”操作规则、政策和做法的提法承认，信任服务提供人的义务因每项信任服务的设计和功能的多样性而有所不同。

139. 按照自愿使用信任服务的原则（第 2(2)(c)条和第 3(1)条），使政策和做法也能够为第三方所查阅的义务反映了承认此类信息有助于依赖方决定是否接受因使用信任服务而产生的结果的现行做法。

140. 对可能使用信任服务的交易目的或价值的限制通常见于信任服务操作规则，其中也包括信任服务提供人的政策和做法。因此，第 1(c)款还旨在履行就可适用的合同限制对第三方承担的透明度义务。类似条文见《电子签名示范法》第 9(1)(d)㈡条。

参考文献

A/CN.9/971，第 152-153 段；A/CN.9/1005，第 28-36 段和第 73 段；A/CN.9/1045，第 18-21 段、第 57 段。

3. 第 15 条. 订户的义务

141. 第 15 条规定了订户在信任服务失密情况下的义务。[文书草案]没有确定订户在使用信任服务方面的额外义务。这种义务的一个实例见《电子签名示范法》第 8(1)(a)和(c)条。

142. 第 15 条规定了订户在发生信任服务失密情况下的义务，而第 14(2)条规定了信任服务提供人在发生数据泄露情况下的义务。“失密的信任服务”这一概念是指未经授权访问信任服务的情况。因此，第 15 条以发生了影响信任服务可靠性的事件为预设前提，而第 14 条则以发生了对信任服务有重大影响的安全违规事件或完整性丧失事件为预设前提。

143. 信任服务提供人和订户之间订立的合同通常会提供关于如何遵守第 15 条所列义务的详细情况。此种合同协议通常指涉信任服务提供人的政策和做法。

144. [文书草案]不含有关于订户人的赔偿责任规则。因此，订户的赔偿责任将由可能会具体规定订户额外义务的合同条文和一般赔偿责任规则决定。

145. 不同于贸易法委员会早先法规中的某些条文（见《电子签名示范法》第 11 条），第 15 条没有规定第三方的义务，根据其他法律，第三方可能负有赔偿责任。

参考文献

A/CN.9/1005，第 37-43 段；A/CN.9/1045，第 22-26 段。

4. 第 16 条. 电子签名

146. 第 16 条涉及电子签名。贸易法委员会关于电子商务的所有立法案文都载有关于使用可由自然人和法人附加的电子签名的条文。第 16 条的行文受到《电子可转让记录示范法》第 9 条的行文的启发，而该条又顾及《电子通信公约》第 9(3)条的行文。

147. 使用一种方法来识别数据电文签名人的身份并表明签名人对所签名的数据电文的意图，即为满足纸质签名的要求。使用“关于数据电文所含信息”的方法的提法一并适用于识别该人的身份和表明该人的意图。

148. 电子签名可用于实现各种目的，例如识别电文发件人的身份以及与电文内容的联系。有几种可以满足电子签名要求的技术和方法。在商业环境中，当事人可以根据成本、所寻求的安全度、风险分配及其他考虑确定最合适的电子签名技术和方法。贸易法委员会早先的法规已就电子签名的目的和方法进行了深入讨论（《电子签名示范法颁布指南》，第 29-62 段；《增进信心》，第 24-66 段）。

参考文献

A/CN.9/971，第 116-119 段；A/CN.9/1005，第 44-51 段；A/CN.9/1045，第 34 段；A/CN.9/1051，第 50 段。

5. 第 17 条. 电子印章

149. 电子印章给源自法人的数据电文的来源和完整性提供保证。在实务中，它们兼有一般的电子签名在来源方面的功能和通常基于使用加密密钥的某些类型的签名在完整性方面的功能。这种电子签名的存在见《电子签名示范法》第 6(3)(d)条。因此，对第 17 条所载完整性要求的描述基于《电子签名示范法》第 6(3)(d)条。

150. 第 17 条受到区域性法规的启发，根据该法规，“除了对法人签发的文件进行认证外，电子印章还可用于对诸如软件代码或服务器之类法人的任何数字资产进行认证。”（《电子身份识别和信任服务条例》，陈述部分 65）。

151. 对数据电文来源的保证可以通过确定其出处来实现，而这又要求识别作为数据电文发件人的法人的身份。识别加盖印章的法人身份所用方法与识别签名人身份所用方法相同，已颁布的贸易法委员会关于电子签名的条文通常适用于自然人和法人。

152. 此外，贸易法委员会法规所载条文要求要求保持完整性，以实现与纸质“原件”概念的功能等同。《电子签名示范法》第 6(3)(d)条尤其提及“完整性”概念，据此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。

153. 鉴于上述情况，已就贸易法委员会关于电子签名的条文制订提供完整性保证的法域可能不会对使用电子签名所追求的功能与使用电子印章所追求的功能进行区分。这也可能反映了使用兼具电子签名和电子印章的混合方法的商业做法。

完整性

154. 完整性是电子印章和电子存档的一个基本组成部分，也可能是其他信任服务的一个可选组成部分。在贸易法委员会早先的法规中，完整性是实现与纸质“原件”概念功能等同的一项要求（《电子商务示范法》第 8 条）。第 17 条和第 19 条受到《电子商务示范法》关于确保完整性要求的第 8(3)条的启发。

参考文献

A/CN.9/971，第 124-128 段；A/CN.9/1005，第 52-54 段和第 58 段；A/CN.9/1045，第 35-36 段和第 56-58 段。

6. 第 18 条. 电子时间戳

155. 电子时间戳提供了时间戳与数据绑定的日期和时间的证据。法律通常对某一事件的发生日期和时间无法提供具有充分可信度的证明这一事实附加后果。例如，可能需要向第三方提供关于合同订立日期的证明。

156. 附加时间戳通常是针对某些相关的行动，例如生成最终形式的电子记录、电子通信的签名、发送和接收等。具体说明时区的要求可以但不需要参照协调世界时来予以满足。

157. 第 18 条载有除提及“文件、记录、信息”外还提及“数据”的说法。该说法旨在涵盖时间戳与未载于文档或记录并且未作为信息有组织地加以展示的数据相关联的情况。

参考文献

A/CN.9/971，第 129-34 段；A/CN.9/1005，第 55 段。

7. 第 19 条. 电子存档

158. 第 19 条涉及电子存档服务，该项服务给所留存的电子记录的有效性提供了法律确定性。电子存档所用方法还可为存档的电子记录的完整性以及存档日期和时间提供保证。而且，根据与“书面”纸质概念功能等同的要求（《电子商务示范法》第 6(1)条），所存档的信息应当具有可及性。

159. 除其他外，第 19 条受到关于数据电文留存的《电子商务示范法》第 10 条的启发。然而，《电子商务示范法》第 10 条之所以提及数据电文的“留存”，是因为它涉及满足留存文件的纸质法律要求，而第 19 条之所以提及“存档”，是因为它涉及为满足该要求而提供的信任服务（即电子存档）。

160. 存档的数据电文不需要是已经发送或接收的，并且可以由发件人留存。

161. 由于技术原因，数据电文的传输和留存可能需要对数据电文进行不改变其完整性的增补和修改。只要数据电文的内容仍然是完整的并且未做改动，就应当允许进行这类增补和修改。特别是，(a)㈡款考虑到了属于数据留存普通做法一部分的文档迁移和格式更改。其行文基于《电子商务示范法》第 8(3)(a)条。

162.第 19 条不涉及存档的电子记录是否应当能够迁移以便虽技术过时但仍能查阅的问题。由此可以将技术中性原则和功能等同要求适用于“完整性”的概念，以便在需要提交信息时，该信息能够向被提交人展示（《电子商务示范法》第 8(1)(b)条）。

参考文献

A/CN.9/971，第 135-138 段；A/CN.9/1005，第 56-61 段；A/CN.9/1045，第 37-41 段。

8. 第 20 条. 电子挂号发送服务

163. 第 20 条给发送人发送电子通信和收件人接收电子通信、发送和接收的时间、所交换的数据的完整性以及发送人和接收人的身份提供了保证。

164. 电子挂号发送服务等同于挂号邮件服务，因为这两类服务都被用来给通信的传输提供证明。为了确保电子交换的安全性和隐私性，在获准访问电子通信之前首先应当识别接收人的身份。

165. 第 20 条没有使用贸易法委员会早先法规中使用的诸如“发送”和“接收”等概念（见《电子通信公约》第 10 条），因为草拟该条时所侧重的是挂号邮件服务和电子挂号发送服务之间的功能等同，而并非其基本概念。

参考文献

A/CN.9/971，第 139-141 段；A/CN.9/1005，第 62-64 段；A/CN.9/1045，第 42-44 段。

9. 第 21 条. 网站认证

166. 第 21 条涉及网站认证，其基本功能是，将网站与被分配域名或被许可使用域名的人相关联，以确认网站的可信度。因此，网站认证包括两个要素：网站域名持有人的身份识别和该人与网站的关联性。网站认证并非是为了对网站进行识别。

167. 第 21 条并非功能等同规则，因为网站仅以电子形式存在，所以网站认证没有线下的等同形式。

168. “域名持有人”一词是指被域名注册机构分配域名或被许可使用域名的人。该人不需要是网站的“所有人”、内容提供人或运营人。

169. 如果发生使用域名的平台是托管由不同的人创建和管理的网页的情况，就可能需要有额外的保护措施。例如，平台运营人可能需要根据维护网站认证的某种程序对所涉人员进行身份识别。

参考文献

A/CN.9/971，第 142-144 段；A/CN.9/1005，第 65-66 段；A/CN.9/1045，第 47-48 段。

10. 第 22 条. 信任服务的可靠性要求

170. 第 22 条载有可能事关根据事后确定的做法确定所用方法可靠性情况的非详尽清单。该清单受到《电子签名示范法》第 10 条和《电子可转让记录示范法》第 12 条所载清单的启发。

171. 类似于身份管理服务所用可靠方法的概念（见上文第二十段），信任服务所用可靠方法的概念是相对的，并根据所追求的目的而有所不同。可靠性的相对性质反映在第 1(a)款中，即根据贸易法委员会既定用法旨在更好反映信任服务各种用途的“既适当又可靠”一词中，并且还反映在“对于使用信任服务的目的而言”的提法中。

可靠度

172. 《电子签名示范法》和若干关于电子签名的国内法律基于信任服务具有的可靠度对信任服务进行区分。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赋予了更大的法律效力。而且，某些法律可能要求只能指定可靠度更高的电子签名。[文书草案]未遵行该做法，可指定任何可靠度的信任服务。

173. 由于提供高保证级的身份凭证可以用于具有不同可靠度的信任服务，因此在身份管理服务的保证级和信任服务的可靠性级之间没有任何直接的相关性。

参考文献

A/CN.9/965，第 106 段；A/CN.9/971，第 120-121 段；A/CN.9/1005，第 67-68 段和第 73 段；A/CN.9/1045，第 18-21 段、第 27-29 段、第 52-57 段和第 61 段；A/CN.9/1051，第 45-46 段。

11. 第 23 条. 指定可靠的信任服务

174. 第 23 条是对第 22 条的补充，它允许按照事前确定的做法指定信任服务。更准确地说，它列出了身份管理服务为列入就第 16 至 21 条的目的而言被推定为可靠的指定身份管理服务清单而必须满足的条件。

175. 第 23 条侧重于信任服务的指定，其所持理解是，指定信任服务的过程必然涉及对这些方法的评估。类似于对身份管理服务的指定，使用可靠方法对所推定的信任服务的指定所涉及的并非一般类型的信任服务，也并非由特定信任服务提供人提供的所有各种信任服务，而是属于由被确定身份的服务提供人提供的特定信任服务。

176. 由于指定的唯一法律效力是对所用方法可靠性的推定，使用已获指定但又已经失去此种指定的信任服务，会妨碍相关当事人利用此种推定，但不会对方法可靠性的确定造成后果。

177. 第 23 条要求指定机构公布所指定的信任服务清单，包括信任服务提供人的详细情况。这种义务的目的是，增进透明度，并让潜在订户了解信任服务。颁布法域似宜考虑如何大体按照现有区域实例汇总这些清单以便能在超国家集中存储库查找这类信息。

参考文献

A/CN.9/971，第 150-152 段；A/CN.9/1005，第 69-73 段；A/CN.9/1045，第 30-33 段和第 58-61 段。

12. 第 24 条. 信任服务提供人的赔偿责任

178. 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。包括所提供的信任服务类型等若干因素将共同决定该赔偿责任的范围。至于[文书草案]的其他条文，第 24 条不影响对未遵守[文书草案]范围以外产生的义务所承担的赔偿责任。

179. 在某些情况下，对信任服务提供人进行身份识别可能具有挑战性或无法做到（例如，与分布式分类账技术结合使用的时间戳服务），因此可能无法分配赔偿责任。在这些情况下，该系统可以以其他方式来建立对使用信任服务的信任度。

180. 关于贸易法委员会早先的法规，《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）所产生的法律后果的条文。这些条文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对其赔偿责任的范围或程度设限。

参考文献

A/CN.9/1005，第 74-76 段；A/CN.9/1045，第 62-66 段。

D. 第四章——国际方面（第 25 和 26 条）

1. 第 25 条. 跨境法律承认

181. 第 25 条建立了对身份管理和信任服务的跨境法律承认制度，其制度基于在法律上同等对待国内外身份管理系统、身份凭证、身份管理服务和信任服务。它所依据的是禁止地域歧视的原则。

182. 第 25 条的一个目标是，减少服务提供人根据第 23 条申请在多个法域得到指定的需要。这在依赖于使用同外国技术标准可能不尽相同的本国技术标准的法域可能特别有益。在可能情况下相互承认认证可在实施该条文上发挥重要作用。

183. 第 25 条中“可靠度”的提法同时包含了保证级和可靠度的概念，前者是评估身份管理服务的专用术语，后者是评估信任服务的专用术语。这些概念又进而可能事关根据第二章和第三章确定服务的可靠性或指定可靠的服务。

184. [文书草案]由于在商定全球公认的定义方面存在的挑战而没有为身份管理系统建立一套共同的保证级以及为信任服务建立一套共同的可靠度。而且，不同法域在确定这些定义方面各有不同的法律和商业惯例，特别是在中央主管机构相对于合同协议的作用方面。

185. 另一方面，确定身份管理服务保证级和信任服务可靠度是一项耗费时间和资源的工作，并非所有法域都拥有足够的资源。这些法域可能尤其获益于有可能通过依赖外国所做的确定和指定而承认外国身份管理和信任服务。

186. 提及“视情况而定的身份管理系统、身份管理服务或身份凭证”旨在涵盖与跨境承认有关的所有可能的方面。在实务中，最好侧重于每一项身份管理服务，以避免把得到身份管理系统支持的所有各项身份管理服务视为同等可靠，即使其中一项或多项服务的可靠度可能较低。此外，对身份凭证的承认应避免虽然用于签发凭证的身份管理服务已经失密但其仍然未做改动的身份凭证。

187. 对外国身份管理和信任服务的承认可能需要服务提供人调整其服务条款。例如，给予承认的法域的强制性法律可能会影响服务提供人对赔偿责任设限的能力。

188. 第 1 款就所需可靠度的等同性提出了两种备选办法。第一种办法要求至少同样的可靠度；第二种办法提供了基本等同的可靠度。“至少等同的可靠度”的提法包括了高于必需可靠度的可靠度。

189. “基本等同的可靠度”的概念旨在涵盖不同法域所界定的可靠度并不完全匹配的情况，鉴于普遍同意的具体可靠度定义的缺失，这是一种有可能出现的情况。这一概念所可处理的另一个问题涉及因要求遵守严格的技术要求而可能产生的贸易障碍。

190. 如果系统、服务或凭证提供了基本等同的可靠度，则适用第 10 条和第 22 条的情况所确定的其可靠度将同样是等同的。“基本等同的可靠度”包括了高于必需可靠度的可靠度。“基本等同的可靠度”的概念取自《电子签名示范法》第 12(2)条。

191. 第 3 款对指定机构是如何指定外国身份管理和信任服务的情况做了进一步的澄清。它展开论述了第 11(4)条和第 23(4)条所述机制，就禁止指定过程中的地域歧

视做了规定，引入了颁布法域指定机构依赖外国指定机构对身份管理和信任服务所做指定的可能性。

192. 在通过实施条例时，颁布法域可决定第 3 款究竟应在自动承认基础上发挥作用（例如，由外国主管机构指定的身份管理和信任服务将自动享有颁布法域指定的法律地位），还是应当以推定形式发挥作用（例如，由外国主管机构指定的身份管理和信任服务将被推定为在颁布法域是可靠的，但如果指定机构不采取进一步行动，则不享有该法域指定的法律地位）。

193. 基于第 25(3)条的机制可以取代建立在订立监督机构间临时相互承认协议基础之上的安排。

参考文献

A/CN.9/936，第 75-77 段；A/CN.9/1005，第 120 段；A/CN.9/1045，第 67-74 段；A/CN.9/1051，第 57-66 段。

2. 第 26 条. 合作

194. 机构合作机制可大大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。这种机制以不同的形式存在，可以是私有的，也可以是公共的。合作可包括交流信息、经验和良好做法，特别是在包括保证级和可靠度等技术要求方面。

195. 此外，第 26 条可便利就包括保证级和可靠度等技术标准做出给确定等同性提供支持的共同定义。

参考文献

A/CN.9/965，第 119-120 段；A/CN.9/1005，第 122 段；A/CN.9/1045，第 75 段；A/CN.9/WG.IV/WP.153，第 95-98 段。