联合国 A/CN.9/1112

大会

Distr.: General
21 February 2022
Chinese
Original: English

联合国国际贸易法委员会
第五十五届会议
2022 年 6 月 27 日至 7 月 15 日，纽约

关于使用和跨境承认身份管理和信任服务的示范法草案

秘书处的说明

1. 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）完成了其对关于使用和跨境承认身份管理和信任服务的条文草案及其解释性说明的三读。

2. 在该届会议上，工作组请秘书处对条文草案和解释性说明加以修订，以反映其审议情况和决定，并将修订后案文以示范法形式提交 2022 年贸法会第五十五届会议审议。工作组还请秘书处将修订后案文分发给各国政府和相关国际组织征求意见，并将所收到的意见汇总以供贸法会审议（A/CN.9/1087，第 11 段）。

3. 经修订的示范文本载于本文件附件一，经修订的解释性说明载于本文件附件二。修订本纳入了 A/CN.9/1087 号文件所述工作组第六十二届会议的审议情况。

附件一

关于使用和跨境承认身份管理和信任服务的示范法草案

第一章. 总则

第 1 条. 定义

在本法中：

(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；

(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”指对身份核实或电子身份识别进行管理的服务；

(g) “身份管理服务提供人”是指与订户订立提供身份管理服务安排的人；

(h) “身份管理系统”指对身份核实和电子身份识别进行管理的一套功能和能力；

(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) “依赖方”是指根据身份管理服务或信任服务的结果行事的人；

(k) “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；

(l) “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；

(m) “信任服务提供人”是指与订户订立提供一项或多项信任服务安排的人。

第 2 条. 适用范围

1. 本法律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. 本法律概不要求对个人进行身份识别。

3. 本法律概不影响按照法律所界定或规定的程序识别个人身份或使用某一信任服务的法律要求。

4. 除本法律另有规定外，本法律概不影响对身份管理服务或信任服务适用关于数据保护和隐私的任何适用法律。

第 3 条. 自愿使用身份管理服务和信任服务

1. 本法律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。

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. 在解释本法律时，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. 与本法所管辖事项有关的问题，在本法中未明确解决的，应按照它所依据的一般原则加以解决。

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) 身份管理系统并非是依据第 11 条指定的。

第 6 条. 身份管理服务提供人的义务

身份管理服务提供人至少应：

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

㈠ 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；

㈡ 更新属性；

㈢ 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

c 续订并更换凭证；

㈣ 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；

(e) 提供方便可及的手段，以使依赖方能够酌情确定：

㈠ 对可使用身份管理服务的目的或价值的任何限制；及

㈡ 对身份管理服务提供人规定的赔偿责任范围或程度上的任何限制；及

(f) 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人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对由该系统管理的属性具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根据法律应：

(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；及

(c) 通报违规情形或丧失情形；

2. 如果某人向身份管理服务提供人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人应：

(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

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

(a) 订户知道其身份凭证已经失密；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。

第 9 条. 使用身份管理对个人进行身份识别

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，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。

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) 身份管理服务提供人遵守第 6 条所列义务的情况；

(b) 身份管理服务提供人操作规则、政策和做法与提供身份管理服务有关的任何可适用公认国际标准和程序包括与保证级框架特别是下述方面的规则相一致的情况；

㈠ 治理；

㈡ 发布的通知和用户信息；

㈢ 信息安全管理；

㈣ 记账；

㈤ 设施和工作人员；

㈥ 技术控制；及

㈦ 监督和审计；

(c) 就身份管理服务提供的任何监督或核证；

(d) 所用方法的任何相关可靠度；

(e) 使用身份识别所要实现的目的；及

(f) 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：

(a) 提供身份管理服务的地理位置；或者

(b) 身份管理服务提供人营业地的地理位置。

4. 根据第 11 条指定的身份管理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 条指定的身份管理服务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) 在指定身份管理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服务清单，包括身份管理服务提供人的详细信息。

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。

4. 在指定某一身份管理服务时，不得考虑：

(a) 提供身份管理服务的地理位置；或者

(b) 身份管理服务提供人营业地的地理位置。

第 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当为未遵守第 6 条和第 7 条对其规定的义务而给订户或依赖方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

(b) 身份管理服务提供人因未履行本法律对其规定的义务所造成的任何其他法律后果。

3. 虽有第 1 款的规定，但身份管理服务提供人不应对订户因使用身份管理服务而遭受的损失承担赔偿责任，前提是：

(a) 此种使用超出了对使用身份管理服务的交易目的或价值的限制；及

(b) 这些限制载于身份管理服务提供人和订户间的安排。

4. 虽有第 1 款的规定，但身份管理服务提供人不应对依赖方因使用身份管理服务而遭受的损失承担赔偿责任，前提是：

(a) 此种使用超出了对使用身份管理服务的交易目的或价值的限制；及

(b) 身份管理服务提供人履行了其在第 6 条(e)项下对该交易的义务。

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. 信任服务提供人至少应：

(a) 制定与信任服务的目的和设计相适应的操作规则、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；

(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人通报安全漏洞的手段；及

(e) 提供方便可及的手段，以使依赖方能够酌情确定：

㈠ 对可使用信任服务的目的或价值的任何限制；及

㈡ 对信任服务提供人规定的赔偿责任范围或程度上的任何限制。

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，信任服务提供人根据法律应：

(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；

(b) 纠正违规情形或丧失情形；及

(c) 通报违规情形或丧失情形。

第 15 条. 订户的义务

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

(a) 订户知道订户用于访问和使用信任服务的数据或手段已经失密；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. 电子封条

法律要求应由某法人加盖印章的，或者法律规定了不加盖印章的后果的，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) 检测加盖印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；

(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；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) 信任服务提供人遵守第 14 条所列义务的情况；

(b) 信任服务提供人操作规则、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) 所用方法的任何相关可靠度；

(d) 任何可适用的行业标准；

(e) 硬件和软件的安全性；

(f) 财力和人力资源，包括资产的存在；

(g) 独立机构审计的经常性和范围；

(h) 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；

(i) 使用信任服务所要实现的目的；及

(j) 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) 信任服务提供人营业地的地理位置。

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) 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 24 条. 信任服务提供人的赔偿责任

1. 信任服务提供人应当为未遵守第 14 条对其规定的义务而给订户或依赖方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

(b) 信任服务提供人因未履行本法律对其规定的义务所造成的任何其他法律后果。

3. 虽有第 1 款的规定，但信任服务提供人不应对订户因使用信任服务而遭受的损失承担赔偿责任，前提是：

(a) 此种使用超出了对使用信任服务的交易目的或价值的限制；及

(b) 这些限制载于信任服务提供人和订户间的安排。

4. 虽有第 1 款的规定，但信任服务提供人不应对依赖方因使用信任服务而遭受的损失承担赔偿责任，前提是：

(a) 此种使用超出了对使用信任服务的交易目的或价值的限制；及

(b) 信任服务提供人履行了其在第 14 条第 1 款(e)项下对该交易的义务。

第四章. 国际方面

第 25 条. 对电子身份识别的跨境承认

1. 如果身份管理系统、身份管理服务或身份凭证所使用的方法酌情提供至少是同等水平的可靠度，则在[颁布法域]外提供的电子身份识别在[颁布法域]内的法律效力一如在颁布法域内提供的电子身份识别。

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至少是等同的可靠度时，应考虑到公认的国际标准。

3. 就第 1 款而言，如果[颁布法域依照第 11 条指明的个人、机关或主管机构]在考虑到第 10 条第 2 款所列情形的情况下确定了此种等同性，则应推定身份管理系统、身份管理服务或身份凭证至少提供了等同的可靠度。

第 26 条. 对使用信任服务的结果的跨境承认

1. 使用在[颁布法域]境外提供的信任服务所得结果，应在[颁布法域]境内具有与使用在[颁布法域]境内提供的信任服务所得结果相同的法律效力，前提是信任服务所用方法至少具有等同的可靠度。

2. 在确定信任服务是否提供至少等同的可靠度时，应考虑到公认的国际标准。

3. 就第 1 款而言，如果[颁布法域依照第 23 条指明的个人、机关或主管机构]在考虑到第 22 条第 2 款所列情形的情况下确定了此种等同性，则应推定信任服务至少提供了等同的可靠度。

第 27 条. 合作

[颁布法域指明的主管个人、机关或机构]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作出界定。

附件二

关于使用与跨境承认身份管理和信任服务的示范法草案的解释性说明

一. 导言

A. 本解释性说明的目的

1. 联合国国际贸易法委员会（贸易法委员会）在编写和通过《贸易法委员会关于使用与跨境承认身份管理和信任服务的示范法》（以下简称《示范法》）时，认为《示范法》如果附有背景和解释性资料，将能更有效协调立法工作并使之现代化。

2. 本解释性说明摘自《示范法》准备工作文件，旨在为诸如决策者、立法机构、学者、从业人员、法官和仲裁员、商业运营人及身份管理和信任服务用户等对《示范法》的通过、使用和统一解释感兴趣者提供帮助。例如，在颁布《示范法》时，这类资料可助力各法域就《示范法》的条文与身份管理和信任服务监管制度间的相互关系，根据自身需要对《示范法》进行调整。

B. 目标

3. 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。这种增长因减轻 COVID-19 大流行病的影响的需要而进一步加快，[1]伴随而来的是数据交易量出现类似的增长，从而就需要有一个适当的法律和技术框架。

4. 电子环境下的线上商业活动的增长以信任为基础，并且需要以信任感的持续存在为支撑。该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。“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，包括电子形式的法律身份。在数字经济中，这将成为一项对数字身份的权利。

5. 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。

6. 在线信任的另一个重要组成部分是能够足够自信地依赖数据交换赖以进行的数据质量。对诸如来源、完整性和处理某一相关行动的时间等数据电文质量提供保证的信任服务，已成为提供该信心的解决办法。

7. 影响更广泛使用身份管理和信任服务的障碍可能具有不同的性质。例如，由于费用、认识不足和技术上的制约，获得身份管理和信任服务的机会可

[1] 贸发会议，《数字经济报告：跨境数据流动和发展：数据为谁流动》，联合国文件。UNCTAD/DER/2021，第 16 至 17 页。

能有限。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。[2]

8. 示范法的主要目标是通过制定服务于若干目的的统一的法律规则来消除这些障碍。统一规则可经推动各系统认可实施身份管理和信任服务的结果而提高效率；经便利履行监管要求而降低交易成本；在使用跨境承认机制等做法共同处理相关问题的基础上提高电子交易的法律可预测性和确定性；并通过便利提供共同解决办法协助弥合数字鸿沟。

9. 特别是，身份管理和信任服务方面的法律框架将促进安全可靠地落实数字身份和数据交易。通过促进对网上环境的信任，这一框架还将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

10. 《示范法》适用于在商业活动以及与贸易有关的服务中使用与跨境承认身份管理和信任服务。颁布法域可决定将《示范法》的适用范围扩大到非商业性活动。

11. 许多不同的法规都可能事关数据交换。《示范法》并非意在影响现有法律，即适用于数据隐私和保护的法律。它也没有引入使用身份管理和信任服务或任何特定身份管理或信任服务的新的义务，并且不影响任何此种现有要求（见下文第 102-104 段）。

12. 《示范法》的身份管理条文适用于对自然人和法人的身份识别。关于信任服务的条文适用于以数据电文为形式的所有信息。不论服务提供人、订户和依赖方属于私营或公营的性质，这两套条文均为适用。

D. 结构

13. 《示范法》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，对第二章所载条文的解释可能事关第三章的相应条文。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。

14. 第一章载有《示范法》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《示范法》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示范法进行自主解释的规定。

15. 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

[2] A/CN.9/965，第 52 段。

偿责任的规则。第 5 条确立了对身份管理予以法律承认和不歧视电子身份识别的原则。第 6 条列出了身份管理服务提供人的核心义务。在此过程中，它确定了身份管理服务提供人的核心义务，这些义务与身份管理系统基本组成部分和身份管理生命周期主要步骤相对应。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。

16. 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；电子封条；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。

17. 第四章涉及为系《示范法》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《示范法》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、26 和 27 条之外，与此有关的还有第 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

18. 《示范法》源自贸法会 2015 年第四十八届会议提出的一项请求。在该届会议上，贸法会请秘书处就身份管理和信任服务所涉法律问题进行准备工作，包括为此举办学术讨论会和专家组会议，以便今后在工作组级别进行讨论，[3] 并向第四工作组呈报这类准备工作的成果，以期征求关于准确范围、可能方法和优先事项的建议，以供贸法会审议。[4]

19. 针对这项请求，贸法会 2016 年第四十九届会议收到了秘书处关于身份管理和信任服务所涉法律问题的说明（A/CN.9/891），其中概述了 2016 年 4 月 21 日至 22 日在维也纳举行的贸易法委员会关于身份管理和信任服务所涉法律问题专题讨论会期间的讨论情况。[5]贸法会一致认为，工作组工作议程应保留身份管理和信任服务这一专题。[6]

---

[3] 《大会正式记录，第七十届会议，补编第 17 号》（A/70/17），第 354 至 355 段、第 358 段。

[4] 同上，第 358 段。

[5] 同上，《第七十一届会议，补编第 17 号》（A/71/17），第 228 段。

[6] 同上，第 235-236 段。

20. 工作组收到贸法会的授权后，在其第五十四届会议（2016 年 10 月 31 日至 11 月 4 日，维也纳）上就这一专题进行了初步讨论。工作组一致认为，今后在身份管理和信任服务方面的工作应当限于为商业目的而使用身份管理系统，这一工作应当一并考虑私营和公营的身份管理服务提供人。工作组还一致认为，虽然身份管理方面的工作可以先于信任服务方面的工作进行，但鉴于身份管理和信任服务这两者之间关系密切，应当同时对这两方面的相关术语加以确定和界定。工作组还一致认为，应当侧重于多方当事人的身份管理制度以及对自然人和法人的身份识别，工作组应当继续其工作，进一步澄清项目目标，具体说明项目的范围，确定所可适用的一般原则，并草拟必要的定义（A/CN.9/897，第 118-120 段和第 122 段）。

21. 按照其先前的决定，工作组第五十五届会议（2017 年 4 月 24 日至 28 日，纽约）除其他议题外讨论了身份管理和信任服务方面工作的目标、一般原则和范围（A/CN.9/902，第 29-85 段）。

22. 贸法会重申其 2017 年第五十届会议赋予工作组的任务授权（见上文第 19 段），并请秘书处考虑召开专家组会议。贸法会邀请各国和国际组织分享其专门知识。[7]秘书处由此于 2017 年 11 月 23 日和 24 日在维也纳召开了一次关于身份管理和信任服务所涉法律问题的专家组会议。

23. 还基于专家组会议所获成果，在其第五十六届会议（2018 年 4 月 16 日至 20 日，纽约）上，工作组确定了与讨论身份管理和信任服务所涉法律问题有关的下列议题：工作范围总则；定义相互承认要求和机制；身份管理和信任服务的核证；身份管理和信任服务的保证级别；赔偿责任；机构间合作机制；透明度；身份识别义务；数据留存；对服务提供人的监督（A/CN.9/936，第 61-94 段）。

24. 在其 2018 年第五十一届会议上，经工作组提议（A/CN.9/936，第 95 段），贸法会请工作组开展工作，以期基于这些原则以及工作组所确定的议题，拟订一个旨在便利跨境承认身份管理和信任服务的案文（见上文第 23 段）。[8]

25. 因此，工作组继续审议其第五十七届会议（2018 年 11 月 19 至 23 日，维也纳）所确定的问题（A/CN.9/965，第 10-129 段）。

26. 提交了关于跨境承认身份管理和信任服务的第一套条文草案（A/CN.9/WG.IV/WP.157），并附有解释性说明（A/CN.9/WG.IV/WP.158），以供工作组第五十八届会议（2019 年 4 月 8 日至 12 日，纽约）审议。工作组审议了关于适用范围、身份管理系统和信任服务的承认和可靠性、拟涵盖的信任服务类型以及身份管理和信任服务提供人的义务和责任的条文草案（A/CN.9/971，第 13-153 段）。

27. 在该届会议上，工作组请秘书处与专家协商，就与身份管理系统可靠性有关的事项提出具体建议（A/CN.9/971，第 67 段）。根据这一请求，秘书处于 2019 年 7 月 22 日至 23 日在维也纳召开了一次专家组会议，讨论对身份管理系

[7] 同上，《第七十二届会议，补编第 17 号》（A/72/17），第 127 段。

[8] 同上，《第七十三届会议，补编第 17 号》（A/73/17），第 159 段。

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。

28. 贸法会对工作组在 2019 年第五十二届会议上取得的进展表示满意。[9]它指出，工作组应致力于拟订一部既适用于国内使用也适用于跨境使用身份管理和信任服务的文书，并指出这项工作的结果对商业交易以外的事项有影响。[10]

29. 工作组第五十九届会议（2019 年 11 月 25 日至 29 日，维也纳）审议了一套条文草案修订本（A/CN.9/WG.IV/WP.160），其中纳入了秘书处与专家磋商的结果（见上文第 27 段）。工作组对条文草案进行了全面通读，重点是与信任服务有关的条文（A/CN.9/1005，第 10-122 段）。它还就文书的形式进行了初步讨论，会上表示强烈倾向于文书采用示范法形式，而不是公约形式（同上，第 123 段）。

30. 贸法会对工作组在 2020 年第五十三届会议上取得的进展表示满意。[11]

31. 工作组第六十届会议（2020 年 10 月 19 日至 23 日，维也纳）收到了第二套条文草案修订本（A/CN.9/WG.IV/WP.162），对这些条文（A/CN.9/1045，第 16-138 段）进行了全面阅读。它还商定可以举行非正式协商以讨论未决议题。

32. 2021 年 3 月 15 日至 17 日，与各国代表和观察员举行了远程非正式协商，就赔偿责任、条文草案与贸易法委员会现有法规的关系、跨境承认、定义及其他术语问题进行了讨论。

33. 向工作组第六十一届会议（2021 年 4 月 6 日至 9 日，纽约）通报了非正式协商的结果。鉴于届会以混合方式举行所产生的限制（包括减少开会时间），在审议第三套修订条文草案（A/CN.9/WG.IV/WP.167）时，工作组将重点审议协商期间讨论的问题（A/CN.9/1051，第 13-67 段）。

34. 贸法会 2021 年举行的第五十四届会议获悉，尽管开会时间缩短，但工作组在完成该文书方面取得重大进展。贸法会对已经取得的进展表示满意，鼓励工作组最后完成其工作，并将其提交贸法会 2022 年第五十五届会议审议。[12]

35. 工作组第六十二届会议（2021 年 11 月 22 日至 26 日，维也纳）基于附有解释性说明（A/CN.9/WG.IV/WP.171）的修订本（A/CN.9/WG.IV/WP.170）对条文草案进行了另外一次阅读（A/CN.9/1087，第 12-114 段）。工作组请秘书处对条文草案和解释性说明加以修订，以反映其审议情况和决定，并将修订后案文以示范法形式提交贸法会第五十五届会议审议。工作组请秘书处将修订后案文分发给各国政府和相关国际组织征求意见，并将所收到的意见汇总以供贸法会审议（A/CN.9/1087，第 11 段）。

36. [待补。]

---

[9] 同上，《第七十四届会议，补编第 17 号》（A/74/17），第 175 段。

[10] 同上，第 172 段。

[11] 同上，《第七十五届会议，补编第 17 号》（A/75/17），第二部分，第 41、51(d)段。

[12] 同上，《第七十六届会议，补编第 17 号》（A/76/17），第九章。

2. 与贸易法委员会早先法规的关系

37. 贸易法委员会早先的法规中没有关于信任服务的规定。但是，这些案文载有可能事关某些信任服务的功能等同规则。《贸易法委员会电子商务示范法》（《电子商务示范法》）[13]第 7 条、《贸易法委员会电子签名示范法》（《电子签名示范法》）[14]第 6 条、《联合国国际合同使用电子通信公约》（《电子通信公约》）[15]第 9(3)条和《电子可转让记录示范法》[16]第 9 条列有电子签名为在功能上等同于纸质签名而必须遵守的要求。这些条文要求识别签字人的身份，而这可能涉及对电子身份识别并推而广之可能涉及对身份管理的使用。示范法第 16 条以《电子可转让记录示范法》第 9 条为基础。

38. 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。《示范法》第 19 条以《电子商务示范法》第 10(1)条为基础。已用作《示范法》各项条款渊源的贸易法委员会其他条文列在相应条款的评述中。此外，可能没有必要使用示范法中指明的信任服务以满足贸易法委员会早先法规中所载功能等同规则。

39. 关于在国际上使用电子签名的一份指导文件详细讨论了与《示范法》有关的若干事项，例如可靠性评估、赔偿责任和跨境承认机制。[17]

F. 关键概念和原则

40. 本节对《示范法》所依赖的几个关键概念和原则进行了解释。对《示范法》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

41. 如同贸易法委员会早先的法规，示范法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。[18]

42. 当事人意思自治原则允许合同当事人在强制性法律的限制下选择适用规则。它基于这样一种认识，即这些当事人可能最有能力为既有交易确定最适当规则。

---

[13] 贸易法委员会，《电子商务示范法及颁布指南》，1996 年，1998 年通过的附加第 5 条之二（1999 年），联合国出版物，出售品编号 E.99.V.4。

[14] 《贸易法委员会电子签名示范法及颁布指南》（2002 年），联合国出版物，出售品编号：E.02.V.8。

[15] 联合国，《条约汇编》，第 2898 卷，第 3 页。

[16] 《贸易法委员会电子可转让记录示范法》，（2018 年），联合国出版物，出售品编号：E.17.V.5。

[17] 贸易法委员会秘书处，《促进对电子商务的信任：在国际范围内使用电子核证和签名方法的法律问题》，2007 年，联合国出版物，出售品编号 E.09.V.4。

[18] A/CN.9/902，第 52 和 63 段。

43. 首先见于《电子商务示范法》第 5 条并且也称作法律承认原则的不歧视原则，确保不会仅仅因信息为电子形式而不承认其法律效力、有效性或可执行性。

44. 技术中性原则确保法律不强制或不赞成使用任何特定的技术或方法，从而使法律能够面向未来。技术中性是实现互操作性的必要条件，而互操作性给数据流提供了有效支持。该原则的法律基础是首见于《电子商务示范法》第 2(a)条的“数据电文”的涉面广泛的定义，该定义旨在涵盖现在和今后的所有各项技术。

45. 功能等同原则载述了据以认为电子交易满足适用于纸质文件形式要求的标准，例如文件应当采用书面形式、为原件或附有签名。它以存在例如使用纸质凭证对个人进行身份识别等直接或间接规定若干物理或纸质活动的法律要求为预设前提。它随之对这些要求的目的和功能展开分析，以确定如何经由电子手段实现这些目的或功能。

46. 虽然《示范法》没有明确确定这些一般原则，但这些原则构成了本案文的关键条文。当事人意思自治原则载于第 3 条，适用于身份管理和信任服务的不歧视原则分别载于第 5 条和第 13 条。此外，关于电子身份识别的第 9 条和关于指定信任服务的第 16-21 条贯穿了功能等同原则。然而，《示范法》所涵盖的某些信任服务可能没有其纸质等同物，因此功能等同原则将不适用于这些服务。

2. 身份管理

47. 身份识别是经由参考个人相关信息（即属性）来将该人与他人区分开的过程。该信息可以通过收集或观察的方式得到。身份识别涉及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某人对某种特定身份的主张和展示其属性以供核实而进行的。

48. 因此，根据《示范法》，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。

49. 身份管理系统用于管理与这两阶段中每一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，身份管理系统可以提供不同的身份管理服务。各方当事人（即寻求识别的一方当事人和寻求被识别的一方当事人）可以根据需要选择合适的身份管理服务。

50. 身份管理系统可以由公营或私营实体运营。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。在适用技术中性原则时（见上文第 44 段），《示范法》不以使用任何技术或模式为预设前提，因此可适用于所有各类身份管理系统和服务。

51. 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，并进而可降低成本并从而确保长期可持续性。

3. 信任服务

52. 信任服务是为诸如来源、完整性和数据处理时间等数据电文的某些品质提供保证的在线服务。保证数据质量是建立对数据交换的信任的关键，而数据交换是数字贸易的支柱。《示范法》确定了某些常用的信任服务，并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。

53. 《示范法》中的信任服务概念涉及服务的提供，而不仅仅涉及该服务本身。例如，可以通过利用以创建和管理电子签名的方法提供的服务来附加电子签名。为避免产生疑虑，《示范法》各项条文就它究竟是涉及提供电子签名服务所用方法还是应用该服务所产生的电子签名做出了具体规定。

4. 对可靠性的评估

54. 如同贸易法委员会早先的法规，《示范法》若干条文提及对提供身份管理和信任服务的可靠方法的使用。《示范法》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。

(a) 事先指定可靠性

55. 在评估服务可靠性上的一种可能的做法是，在使用可靠方法之前（事前）评估按照预定条件清单笼统进行，而并非参照某一特定的交易。《示范法》将该做法称作对可靠性的指定，并在第 11 条（适用于身份管理服务）和第 23 条（适用于信任服务）中列出了关于该指定的要求，其中包括与确定可靠性有关的相同情形。

56. 指定的对象并非是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。

57. 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，对其的管理是以存在一个有能力管理指定过程的实体这样一个体制机制为预设前提的。

58. 希望执行事前确定做法的颁布法域必须确定可以是私营或公共机构的负责指定事务的实体。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）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。

59. 《示范法》以存在实施事先做法所需体制机制为预设前提，但未就这类机制的设立或管理作出规定。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。

60. 指定机制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并且基于可靠方法但却仍然未获指定的身份管理和信任服务。而且，对指定所涉先决条件的进一步确定不应导致强行规定特定技术要求。

(b) 对可靠性的事后确定

61. 关于方法可靠性的另一种可能的评估做法是，将这种评估延后至在就可靠性出现争议之时。因此，唯有在使用该方法之后方才进行评估（“事后确定”）。《示范法》将这种做法称做对可靠性的确定，并在第 10 条（适用于身份管理服务）和第 22 条（适用于信任服务）中列出了确定可靠性的要求，包括列举相关情形的不完整清单。

62. 事后确定做法一般允许在没有事先评估可靠性的情况下进行身份管理交易，并将评估可靠性的需要限定于实际发生争议的情况。它还为各方当事人对技术和方法的选择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。

63. 另一方面，事后确定做法可能无法在实际使用前对所用方法的有效性提供更高程度的可预测性，从而使当事人承受了该方法可能会被视为不可靠的风险。此外，它将对该方法可靠性的确定留待第三方裁决程序裁定，而这可能会耗费时间并导致所做裁定不相一致。

(c) 混合做法

64. 《示范法》兼顾确定和指定两种做法，从而既允许承认任何身份管理和信任服务，同时又就究竟哪些身份管理和信任服务在可靠性方面提供了更高的信任度提供了指导（“双重”做法）。《示范法》在对待两机制方面并不厚此薄彼，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所赞同的解决方案。

65. 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。《示范法》采用的综合做法是建立在《电子签名示范法》第 6 条和第 7 条的基础之上的

5. 赔偿责任问题

66. 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《示范法》的一项核心要素。从历史上看，立法机构采取了不同的解决办法，其中包括不设专门的赔偿责任制度；采纳涉及仅适用于服务提供人或适用于所有相关当事人（服务提供人、订户和依赖方）的行为标准和赔偿责任规则的条文。[19]《电子签名示范法》采用了后一种做法。[20]

67. 与身份管理和信任服务有关的赔偿责任分配主要是经由合同协议或法规的方式进行。后一种做法对确保不致在合同中选择对某些条款不予适用上可能更为可取。此外，法定规则也可在就依赖方未有合同约定的情况下予以适用。

68. 第 12 和 24 条确立了服务提供人对订户和依赖方的统一的赔偿责任制度，该制度所依据的原则是，服务提供人未能提供法律要求的服务，则应对所造成的后果承担赔偿责任。因此，第 12 和 24 条引入了与合同约定的赔偿责任和非合同约定的赔偿责任一并适用的赔偿责任法定依据。此外，《示范法》允许服务提供人限制对订户和依赖方的赔偿责任。

69. 《示范法》既不涉及追究赔偿责任所需的过失程度，也不涉及可以追回的损害赔偿的类型和数额。[21]因此，如果在《示范法》颁布之时未曾通过适用于身份管理和信任服务提供人的特别规则，颁布法域的普通规则将适用于这类问题。

6. 国际方面

70. 国际方面对使用身份管理和信任服务并乃至对电子交易都至关重要。然而，存在可能会阻碍此种使用的两类障碍：导致缺乏互操作性的技术上的不兼容，以及影响跨境承认的法律障碍。[22]

71. 法律障碍可能来自互有冲突的国家做法，特别是在法律授权或支持某一特定技术、方法或产品之时。在这种情况下，国内的法律要求可能会妨碍对不合规的各类身份管理和信任服务的认可。此外，国家技术标准的问世——当这些标准与法律推定有关时也可能产生于“双重”做法——可能会导致出现也具有阻碍跨境使用影响的各种混杂拼凑的要求。

---

[19] 促进对电子商务的信心，第 175 段。

[20] 详细情况见《电子签名示范法》，解释性说明，第 77-81 段。

[21] 关于这些问题，见促进对电子商务的信心，第 177-至 193 段（赔偿责任的依据：一般过失、推定过失和严格的赔偿责任)及第 194-201 段（损害赔偿权利人和可追回损害赔偿的范围）。

[22] 促进对电子商务的信心，第 137-152 段。

72. 从法律上允许跨境使用身份管理和信任服务是《示范法》所追求的主要目标之一。为此，适用了贯穿于《示范法》第10(3)条、第11(4)条、第22(3)条和第23(4)条的技术中性原则和禁止地域歧视原则。[23]此外，第四章专门处理跨境承认事项。因此，《示范法》非但不鼓励通过针对具体技术的法律，而且还鼓励包括经由合作等方法制定可互操作的技术标准。

73. 《示范法》与贸易法委员会先前法规所持做法是相一致的，不只是把来源地称作对外国身份管理和信任服务给予法律承认的一个相关因素。更准确地说，它要求在用于类似国内身份管理和信任服务的相同情况基础上，事后确定外国身份管理和信任服务的可靠性。它还提供了在用于类似国内身份管理和信任服务的相同情况基础上指定外国身份管理和信任服务可靠性的机制。简而言之，决定是否给予法律承认的应该是技术可靠性，而并非来源地。

74. 《示范法》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《示范法》用作包括在专门协议下与国际伙伴建立体制安排的模板。

75. 自由贸易协议关于电子商务的章节通常载有关于电子签名或通常称作“认证方法”的其他形式的电子身份识别的条文，这类条文日益要求对电子身份识别方法给予相互承认。此外，数字经济协议列有旨在实现跨境互操作性的专门针对数字身份的模块。《示范法》的颁布可有助于执行自由贸易和数字经济协议的这些条文。

二. 逐条评注

A. 第一章－总则（第 1 至 4 条）

1. 第 1 条. 定义

76. 第一条载有《示范法》中使用的某些术语的定义；

“属性”

77. “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。

78. 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。《示范法》不涉及数据隐私和保护，并明确保留对该项法律的适用。

[23] 关于促进对电子商务的信心的文件第 149 段已经把在对外国签名和服务采取技术中性和非歧视性做法确定为支持就跨境承认电子签名的法律机制逐步形成共识的基本原则。

参考文献

A/CN.9/WG.IV/WP.150，第 13 段。

“数据电文”

79. “数据电文”的定义可见于利用该定义以落实技术中性原则（见上文第 44 段）的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”]

80. “电子身份识别”一语是指对自然人或法人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。

81. 在对其他属性加以核实即可的情况下可能没有必要为满足电子身份识别的要求而披露自然人或法人的姓名。这与贸易法委员会先前法规即《电子签名示范法》所持做法是相一致的，根据这种做法，“就根据《示范法》界定‘电子签名’而言，‘身份识别’一语的范围可能广于仅仅按姓名对签字人进行身份识别”[24]。

82. 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”

83. “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。

[24] 《电子签名示范法》，解释性说明，第 117 段。

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”

84. “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。[25]

参考文献

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

“身份管理服务”

85. “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；A/CN.9/1087，第 19 段。

“身份管理服务提供人”

86. 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。提及与订户之间的安排提醒人们，身份管理服务提供人对所提供的全部服务负责，而无论相关功能是由其直接履行还是承包给第三方当事人的。

[25] 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（欧盟）第 910/2014 号条例（欧盟）（《电子身份识别和信任服务条例》）。

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；A/CN.9/1087，第 22 段。

“身份管理系统”

87. “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；A/CN.9/1087，第 19 段。

“身份核实”

88. “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。主体可以是自然人，也可以是法人。将“身份识别”一语改为“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。

“依赖方”

89. “依赖方”这一用语是指事实上根据身份管理服务或信任服务的结果行事的自然人或法人。例如，依赖方是根据电子签名而不是根据用于创建电子签名的信任服务行事的人。该定义是建立在《电子签名示范法》第 2 条(f)款所载定义基础之上的。

参考文献

A/CN.9/1087，第 55 段和第 72 段。

“订户”

90. “订户”一语是指得到所提供的服务的人，并且不包括依赖方。它以服务提供人与订户之间存在可能是合同约定的或其他性质的（例如，法律规定的）某种关系为预设前提。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；A/CN.9/1087，第 23 段。

信任服务

91. “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，也有列出示范法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。

92. “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，故乡 14-18 段；A/CN.9/1051，第 35-40 段。

“信任服务提供人”

93. 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），《示范法》没有确定拟由信任服务提供人履行的功能。提及存在与订户间的安排提醒人们，信任服务提供人对所提供的全部服务负责，而无论相关功能是由其直接履行还是承包给第三方当事人的。

94. 《示范法》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

A/CN.9/1087，第 22 段。

2. 第 2 条. 适用范围

95. 第 2 条参照在商业活动和贸易相关服务中使用与跨境承认身份管理服务和信任服务的提法划定了《示范法》的适用范围。“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。

96. 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《示范法》的范围扩大至涉及企业、政府和消费者的所有各类电子交易。

97. 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，《示范法》没有引入任何新的身份识别义务。

98. 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，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。

99. 鉴于其赋能性质，《示范法》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关于电子商务的立法文本。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；A/CN.9/1087，第 27 段。

3. 第 3 条. 自愿使用身份管理服务和信任服务

100. 第 3 条指出，《示范法》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。

101. 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一定一致。

102. 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。

103. 而且，第 3 条表示《示范法》不要求使用任何特定的身份管理或信任服务，从而贯彻了技术中性原则，包括有关模型和系统中性的原则。

104. 使用身份管理和信任服务或特定身份管理或信任服务的义务可能存在于其他法律中。例如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；A/CN.9/1087，第 28 段。

4. 第 4 条. 解释

105. 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）。

106. 第 1 款旨在促进所有各颁布法域的统一解释，它提请法官及其他裁决机构注意，对《示范法》的国内法规应当根据其国际渊源和统一适用的需要来进行解释。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。

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

108. 类似于贸易法委员会关于电子商务的其他立法案文，《示范法》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《示范法》有关（见上文第 41-45 段）。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[示范法]中的条文。此外，如同（上文第 46 段）所述，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

109. 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，它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。

110. 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。

111. (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。

112. 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《示范法》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

113. 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。第 6 条前导句中的“至少”一词表明，身份管理服务提供人不得减损对这些核心义务的履行，而且它在利用承包商提供服务之时，仍对订户和依赖方负有赔偿责任。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。

114. 对第 6 条所载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。

115. 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。因此，(a)项中“至少”一词表明，身份管理服务提供人必须拟订述及履行所列功能要求的规则、政策和惯例。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。

116. 服务提供人应受其所做陈述和承诺约束的原则已经载于《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。

117. 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。

118. 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。(e)项中也有便于获取的提法，目的是便利可能不太熟悉技术事项的当事人如微型或小型企业等获取信息。

119. (e)项规定了为了给其对依赖方的赔偿责任设限身份管理服务提供人所必须履行的义务，从而对第 12 条做了补充。该机制旨在防止因要求事先识别依赖方的身份而出现的挑战。

120. 同样，(f)项是对第 8 条的补充，它规定了身份管理服务提供人在通报订户安全违规情形时所必须履行的义务。

参考文献

A/CN.9/936，第 69 段；A/CN.9/1045，第 85-95 段；A/CN.9/1087，第 30-33 段及第 55 和 61 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

121. 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。

122. “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。也可以在数据隐私和保护法律中对这一概念加以界定。

123. 区域和国家法律中使用了“重大影响”的概念。[26]评估这种影响可考虑若干因素。违规事件通知表可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。数据隐私和保护机构还将提供事件报告技术准则和安全事件年度报告。

124. 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。

125. 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。

126. 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。

127. 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，均可在其他法律——即数据隐私和保护法律——、合同协议以及身份管理服务提供人的

[26] 《电子身份识别和信任服务条例》第 19(2)条。

操作规则、政策和做法中加以具体规定。在这种情况下，对所列出的所有各种行动，而不仅仅是通知，都应根据可适用法律加以落实。

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；A/CN.9/1087，第 35 段。

4. 第 8 条. 订户的义务

128. 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）。

129. 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。订户未履行第 8 条对其规定的义务并不一定能免除身份管理服务提供人的赔偿责任。

130. 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。

131. “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。“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。

132. (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，并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。

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；A/CN.9/1087，第 36-37 段。

5. 第 9 条. 使用身份管理对个人进行身份识别

133. 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。

134. 用于履行第九条所述规则的方法必须符合第十条第一款的规定，即对于使用身份管理服务的目的而言既是适当的也是可靠的，或者事实上证明已经履行了使用该方法所追求的功能。

135. 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。

136. 第 9 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。

137. 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 98 段）。

138. 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。

139. 《示范法》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但允许采取行动不过给某些行动赋予法律后果的情况下顾及功能等同规则。

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；A/CN.9/1087，第 38 段。

6. 第 10 条. 身份管理服务的可靠性要求

140. 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。它指涉身份管理服务所用方法，而并非身份管理系统所用方法，因为单个的身份管理系统可以给所用方法可靠度各不相同的多项身份管理服务提供支持。

141. 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。

142. 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。

143. 《示范法》一般要求使用可靠的方法，第1(b)款无意促进使用不可靠的方法，也无意验证对这些方法的使用。相反，它承认，从技术角度来看功能（在第 9 条中即为身份识别）和可靠性是两个独立的属性，并澄清，根据《示范法》，身份识别事实上可以实现或可经使用可靠方法予以实现。换言之，身份识别的实现事实上即预先排除了确定所用方法可靠性的需要。

144. 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。

145. 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。[27]

146. 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 款(b)项，对赋予指定的可靠性推定可加以反驳。

147. 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

148. 第 10 条和第 11 条提及“保证级框架”或以其他方式指明的类似框架的概念。保证级框架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。《示范法》既没有界定保证级，也没有对界定或使用保证级提出要求。

149. 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。

150. 可利用保证级框架述及在就所提供的身份管理服务可信赖程度提供指导方面的市场需求。身份管理服务提供人如果在其操作规则、政策和做法中不提及保证级，就有可能会被视为所提供的服务保证级极低。然而，可能尚未商定得到全球认可的保证级框架的定义，可能必须使用不同国家或区域的定义。

[27] 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。

151. 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

152. 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。

153. 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。

154. 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。

155. 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。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。

156. 《示范法》没有对建立监督制度提供授权或便利。《示范法》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。

157. 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的实体、接受评估的实体及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.9/1087，第 42-46 段和第 105-106 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

158. 第 11 条是对第 10 条的补充，该条提供了指定身份管理的可能性。更准确地说，它列出了身份管理服务列入指定身份管理服务清单所必须满足的条件。如同第 10 条，第 11 条指涉身份管理服务所用方法，而并非身份管理系统所用方法，因为一个单一的身份管理系统可以给可靠度不尽相同的多项身份管理服务提供支持，并因而可以被指定或不被指定。

159. 使用可靠方法指定身份管理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。

160. 传播被指定身份管理服务的信息是让潜在用户意识到这类服务存在的关键所在。指定实体有义务例如在其网站上公布指定的身份管理服务清单，包括身份管理服务提供人的详细信息。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。可以使用其他方法向公众告知指定的身份管理服务，但此类方法应当是对公布名单的补充而非取代。

161. 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。

162. 类似于第 10(3)条，第 4 款明确规定，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服务的指定。第 4 款是基于《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服务的请求。

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；A/CN.9/1087，第 47-49 段。

8. 第 12 条. 信任服务提供人的赔偿责任

163.如前所述（上文第 68 段），基于身份管理服务提供人应当对未能向订户和依赖方提供服务所造成的后果承担责任的原则，第 12 条确立了统一的赔偿责任制度。其目标是承认，服务提供人可能因未履行示范法规定的义务承担赔偿责任，而不论这些义务是否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。

164. 第 12 条基于三项要素：(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《示范法》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具有合同约定的依据；及(c)它承认在某些条件下是可以对赔偿责任加以限制的。

165. 第 12 条下的赔偿责任具有法定性，因此，它是按照合同约定的赔偿责任和非合同约定的赔偿责任一并适用的。因此，如同第 2(a)款所示，国内法中与身份管理服务提供人有关的合同约定的赔偿责任和非合同约定的赔偿责任条款的落实不受第 12 条的影响。

166. 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。

167. 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。

168. 第 12 条还承认在某些条件下是可以对赔偿责任加以限制的。赔偿责任限制可能是控制保险费用等所必需的，并且通常见于服务提供人的操作规则、政策和做法。第 12 条还承认身份管理服务提供人根据当事人（即订户或依赖方）及服务类型（例如交易价值的高低）而对其赔偿责任做出不同限制的做法。这并不影响身份管理服务提供人依赖其他法律落实赔偿责任限额的能力，先决条件是，它遵行《示范法》给其规定的义务，包括与赔偿责任限制有关的义务。

169. 关于订户，第 3 款允许在两项条件下限制身份管理服务提供人的赔偿责任。第一项条件是，身份管理服务的使用超出了对交易目的或价值的限制以及对适用于使用身份管理服务的交易的赔偿责任数额所做的限制。第二项条件是，这些限制载于管理服务提供人和订户间的安排。根据“订户”的定义，“安排”的提法意在涵盖身份管理服务提供人与订户之间属于合同或其他性质关系的所有各类关系。

170. 同样，第 4 款允许在两个条件下限制身份管理服务提供人对依赖方的赔偿责任。第一个条件是，对身份管理服务的使用超出了对交易目的或价值的限制，也超出了对适用于使用身份管理服务交易在赔偿责任数额上的限制。第二个条件是，身份管理服务提供人遵行了第 6(e)条给其规定的方便依赖方了解在特定交易方面各种限制的义务。

171. 第 12 条只涉及身份管理服务提供人对订户和依赖方的赔偿责任。因使用身份管理服务而遭受损失的另一方当事人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。

172. 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；A/CN.9/1087，第 52-73 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

173. 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。

174. 第 13 条适用于信任服务，而无论所涉服务是否在《示范法》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

175. 第 14 条规定了信任服务提供人的核心义务，而无论是否指明了所提供的信任服务。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。类似于第 7(1)条，第 14(2)条所列的所有义务都应根据任何可能的适用法律予以履行。

176. “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可以有所不同。

177. 按照自愿使用信任服务的原则（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。

178. 第(1)款(e)项建立了让依赖方了解对可使用信任服务的目的或价值所做限制以及对赔偿责任范围或程度的限制的机制，该机制一如第 6 条(e)项所载机制，是对第 24 条的补充。

179. 第 2 款创立了信任服务提供人在发生数据泄露情况下的义务。它以发生了对信任服务具有重大影响的安全违规情形或完整性丧失情形为预设前提。

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 段和第 57 段；A/CN.9/1087，第 74-76 段。

3. 第 15 条. 订户的义务

180. 第 15 条确立了订户在信任服务失密情况下的义务。“失密的信任服务”这一基本概念是指未经授权访问信任服务的情况，并且以发生了影响信任服务可靠性的事件为预设前提。

181. 第 15 条承认，订户不太可能立即知悉影响整个信任服务的问题，订户可能会意识到可见信息的泄露，但也可能意识到诸如私钥等并非为订户直接可见的信息所涉风险。由于这个原因，(a)款和(b)款有两个不同的目的。

182. 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。此种合同约定的协议通常指信任服务提供人的操作规则、政策和做法。

183. 《示范法》没有确定订户在使用信任服务方面的额外义务。此种义务的一个实例见《电子签名示范法》第 8(1)(a)和(c)条。

184. 《示范法》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。

185. 不同于《电子签名示范法》第 11 条，第 15 条没有确立依赖方的义务，根据其他法律，依赖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；A/CN.9/1087，第 77-78 段。

4. 第 16 条. 电子签名

186. 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。[28]第 16 条的行文受《电子可转让记录示范法》第 9 条的启发，而后者又顾及《电子通信公约》第 9(3)条的措词，并确立了手写签名和电子签名功能等同的要求。因此，对第 16 条中的“身份识别”一语应按照贸易法委员会类似条文和为执行这些条文而制定的法律中的既有含义来进行解释。

187. 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。

188. 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。[29]

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；A/CN.9/1087，第 82-84 段。

[28] 另笼统见促进对电子商务的信心的文件。

[29] 《电子签名示范法》，《颁布指南》，第 29-62 段；促进对电子商务的信心，第 24-66 段。

5. 第 17 条. 电子封条

189. 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。

190. 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）。

191. 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。

192. 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。

193. 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

194. 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；A/CN.9/1087，第 85-86 段。

6. 第 18 条. 电子时间戳

195. 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。通常情况下，法律对关于某一事件的日期和时间的举证可能不具充分可信度的事实会附加后果。例如，可能需要向第三方提供关于合同订立日期的证明。

196. 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。

197. 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 129-134 段；A/CN.9/1005，第 55 段。

7. 第 19 条. 电子存档

198. 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。

199. 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）。

200. 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。

201. 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。(c)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。

202. 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

203. 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。

204. 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。

205. 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

206. 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。

207. 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。

208. “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。

209. 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

210. 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。

211. 类似于身份管理服务所用可靠方法的概念（见上文第 141 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

212. 《电子签名示范法》和若干关于电子签名的区域和国家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。《示范法》未遵行该做法，可指定具有任何可靠度的信任服务。

213. 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；A/CN.9/1087，第 87 段和第 105-106 段。

11. 第 23 条. 指定可靠的信任服务

214. 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，它列出了信任服务为列入就第 16 至 21 条的目的而言被推定为可靠的指定信任服务清单而必须满足的条件。

215. 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。

216. 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事后确定造成后果。

217. 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

218. 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。

219. 第 24 条的草拟方式类似于关于身份管理服务提供人赔偿责任的第 12 条，因此，根据第 12 条所作的考虑可能也适用于第 24 条。特别是，如同第 12 条，第 24 条确立了与合同约定赔偿责任和非合同约定赔偿责任一并适用的赔偿责任法定依据，如同第 2(a)款所示，事关信任服务提供人的合同约定赔偿责任和非合同约定赔偿责任的国内法条文的实施不受第 24 条影响。

220. 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。

221. 在贸易法委员会早先的法规中，《电子签名示范法》载有关于签名人的行为（第 8 条）、认证服务提供人的行为（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》承认认证服务提供人有可能对其赔偿责任的范围或程度设限。[30]

参考文献

A/CN.9/1005，第 74-76 段；A/CN.9/1045，第 62-66 段；A/CN.9/1087，第 89 段。

D. 第四章－国际方面（第 25 至 27 条）

1. 第 25 条. 对电子身份识别的跨境承认

222.第 25 条建立了电子身份识别跨境法律承认机制，该机制意图在法律上同等对待国内和外国身份管理系统、身份管理服务和身份凭证。它所依据的是禁止地域歧视原则，并侧重于使用身份管理系统、身份管理服务和身份凭证进行的电子身份识别。

223. 第 25 条的一个目标是，减少服务提供人根据第 23 条在多个法域提出指定申请的需要。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。

224. 不同法域界定的可靠度可能无法完全匹配。鉴于对具体的可靠度没有普遍商定的定义，是有可能出现此种不匹配的情况的。为解决此种不匹配给跨境承认带来的难题，第 25 条采用了“至少等同的可靠度”的概念的提法，其中包括了等同于或高于各种必需的可靠度。不应当把这一概念解释为要求遵守严格的技术要求，因为这可能会阻碍相互承认并最终阻碍贸易的进行。

225. “视情况而定的身份管理系统、身份管理服务或身份凭证”的提法旨在涵盖与跨境承认电子身份识别有关的所有可能的方面。在实务中，最好侧重于具体的身份管理服务，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所可提供的可靠度较低。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。

226. 对外国身份管理系统、服务和身份凭证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。

[30] 关于对公钥基础设施框架中具体赔偿责任情况的讨论，见促进对电子商务的信心，第 211-232 段。

227. 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)条所述机制，该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所做指定及把身份管理系统和凭证列作可能的指定对象的可能性。因此，第 3 款实施了事前确定的做法。

228. 在确定等同性时，主管机构应当考虑载于第 10(2)条的与确定身份管理服务所用方法可靠性有关的情况清单，以确保对可靠性的确定前后一致。

229. 确定身份管理服务、身份管理系统或身份凭证的可靠度是一项耗费时间和资源的工作，并非所有法域都可能拥有足够的资源。资源较少的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服务和系统及身份凭证。利用第 3 款的机制也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。

230. 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）。

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；A/CN.9/1087，第 90-101 段。

2. 第 26 条. 对使用信任服务的结果的跨境承认

231. 第 26 条引入了跨境承认使用信任服务结果的机制，一如第 25 条就电子身份识别所确立的机制。因此，在第 25 条下所做考虑可能适用于第 26 条。

232. 第 26 条与诸如公钥基础设施间交叉承认和交叉验证等对跨境承认使用信任服务结果现有机制的使用是大体一致的。[31]

参考文献

A/CN.9/1087，第 90-101 段。

3. 第 27 条. 合作

233. 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，可以是私营的，也可以是公营的。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。

[31] 关于交叉承认和交叉核证的更多信息，见促进对电子商务的信心，第 163-172 段。

234. 此外，第 26 条可有助于商定在包括保证级和可靠度等技术标准方面做出给确定等同性提供支持的共同定义。在商业实务中，保证级和可靠度的概念分别被用作评估身份管理和信任服务的专门技术术语。示范法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。

235. 合作应在自愿的基础上进行，并且应当遵照所可适用的国家法律和条例。“外国实体”的提法旨在涵盖可能有助于实现预期目标的所有各类实体，而无论其法律性质如何。

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；A/CN.9/1087，第 108-109 段。