



大 会

Distr.: Limited
30 January 2017
Chinese
Original: English/French

联合国国际贸易法委员会

第四工作组（电子商务）

第五十五届会议

2017 年 4 月 24 日至 28 日，纽约

电子商务领域的工作——与电子身份管理和信任服务有关的法律问题

奥地利、比利时、法国、意大利、联合王国和欧洲联盟的建议

秘书处的说明

比利时、法国、意大利和大不列颠及北爱尔兰联合王国政府以及奥地利代表团和欧洲联盟向秘书处提交了一份文件，供工作组第五十五届会议审议。现将秘书处收到的案文照原样转载于本说明的附件。



附件

奥地利、比利时、法国、意大利、联合王国和欧洲联盟的建议

日期：2017 年 1 月 26 日

比利时、法国、意大利和大不列颠及北爱尔兰联合王国政府以及奥地利代表团和欧洲联盟的建议：电子商务领域的工作——与电子身份管理和信任服务有关的法律问题

一. 导言

1. 根据委员会 2011 年第四十四届会议期间的任务授权，关于电子商务的第四工作组（下称第四工作组）开展了电子可转让记录方面的工作。¹在委员会第四十九届会议期间，第四工作组报告了其第五十二和第五十三届会议期间开展工作的情况。电子可转让记录示范法草案条文的工作正在进行最后审定。

2. 委员会 2011 年第四十四届会议还注意到，对于将身份管理方面的法律问题作为可能在第四工作组任务授权范围内处理的议题也表示了一定支持。²委员会 2015 年第四十八届会议上指示秘书处就身份管理和信任服务、云计算和移动商务进行准备工作，包括为此举办学术讨论会和专家组会议，以便今后在关于电子可转让记录的目前工作完成之后在工作组级别进行讨论。委员会还请秘书处向第四工作组呈报这一准备工作的成果，以期征求关于准确范围、可能方法和优先事项的建议，供委员会第四十九届会议审议。³

3. 根据这一要求，在其第四十九届会议上，秘书处向委员会提交了一份关于身份管理和信任服务方面法律问题的说明，其中概述了学术讨论会以及其他相关会议上就这一主题举行的讨论。⁴

4. 委员会 2016 年第四十九届会议确认了赋予第四工作组的任务授权是完成电子可转让记录示范法草案及其随附解释说明的拟订工作，并在完成示范法草案的工作之后审议身份管理和信任服务主题以及云计算主题。⁵

¹ 联合国国际贸易法委员会第四十四届会议报告（2011 年 6 月 27 日至 7 月 8 日）——[A/66/17](#)，第 238 段。

² 同上，第 236 段。

³ 联合国国际贸易法委员会第四十八届会议（2015 年）工作报告，联合国第 [A/70/17](#) 号文件，第 358 段。

⁴ 第 [A/CN.9/891](#) 号文件。

⁵ 联合国国际贸易法委员会第四十九届会议（2016 年）工作报告，联合国第 [A/71/17](#) 号文件，第 353 段。

5. 根据这一经重申的任务授权，第四工作组第五十四届会议期间对电子可转让记录示范法草案进行了最后审定，并启动了身份管理和信任服务方面的工作。在对后一个主题进行富有成果的讨论之后，⁶第四工作组决定，下届会议将特别专注于以下几个方面：澄清身份管理和信任服务项目的目标，着重说明其范围，确定适用的一般原则，列出拟界定的概念，并拟订这些概念的定义初步草案。⁷

6. 为此，本建议的目的是就上述要素向第四工作组建言，以期支持第五十五届会议期间进行的讨论，同时对旨在促进讨论的进一步建议持开放态度。

二. 项目背景、范围和目标

7. 拟议在身份管理和信任服务方面开展的工作与第四工作组下述方面的工作直接相关：(1)以往工作（特别涉及《电子商务示范法》、《电子签名示范法》和《国际合同使用电子通信公约》），(2)当前工作（电子可转让记录方面的工作），(3)今后工作，关于已经讨论过的其他主题，如云计算或者移动支付。

8. 事实上，身份管理是第四工作组已经（或者正在）开展的大多数工作所涉及的一项基本要求。此外，如果使用信任服务提供商提供的一种或多种信任服务，是会有利于实现贸易法委员会法规所规定的诸多适用于电子商务的要求的。“信任服务”可包括确保文件来源和完整性的电子签名和电子印章，可提供文件具体时间的电子时间戳，各方（电子登记交付服务）之间的安全通信，或者网站认证。

9. 由于网上交易的重要性和敏感性日渐增加，可靠的身份管理以及使用可靠的可信赖服务已成为电子商务活动的基本要求。

10. 在许多互联网交易中都需要核实网站主的身份，以确保网站属于声称拥有网站的法人且由其进行有效管理。同样，各方在开始网上互动时表明身份，往往也很重要。此外，最后协议上的电子签名也可能要求辨明不同签名人的身份，以确保签名人对一项将保持其完整性的内容表示同意，并给文件加上标明其具体日期和时间的印章。最后一点，在某些情形下，文件必须通过安全渠道传输给对方，该渠道要确保记录文件的发出和接收日期。

11. 身份认证和信任服务大大有助于无纸化商业环境，因为公共行政部门和企业的日常运作可以更快，更高效，费用也更低。在这方面，许多公共和私营实体开发（或者希望开发）可提供或者利用身份管理和信任服务的经济模式。

12. 如今，无论在国家还是区域范围，身份管理和（或）信任服务领域的思考和倡议举不胜数，现已达到成熟程度。虽然这些思考和倡议有时采取相互矛盾的做法，但它们有助于确定相关问题，并且为在国际层面进行关于适当法律框架设计的讨论，从而有可能将其植入现行不同法律制度提供指导。

⁶ 关于电子商务的第四工作组第五十四届会议的报告（2016 年 11 月 16 日）的报告，[A/CN.9/897](#)，第 107 至 123 段。

⁷ 同上，第 120 段。

13. 身份管理和信任服务领域工作的目的是：

- 促进国际贸易法发展，并着眼于为经济参与者提供工具以确保其电子交易法律确定性的需要。
- 针对目前在国家或国际一级从深层处理这些问题的项目，促进协调统一其中正在出现的各种法律问题。目标是提供一个同时适用于身份管理和信任服务的总体法律框架，包括为促进国际跨境法律和技术互通而作出适当规定。
- 提高公共行政部门和企业的认识——它们并非总是很了解所涉及的法律问题，以期促进对电子商务和交易的信任。
- 完成贸易法委员会制定的现有文件并提供切实可行的解决办法。更具体而言，这一领域的工作将着眼于拟订法律条文，以期使上述贸易法委员会法规中制定的“抽象”要求更为“具体和可操作”。因此，企业将利用明确的法律规则更好地管理国际电子商务中的风险并以简单、高效方式确保其交易的法律确定性。

14. 鉴于身份管理与信任服务两者之间的密切关系，这项工作从一开始就应把重点同时放在这两个主题上。因此，对工作范围和概念的界定应当包括这两个密切相关的主题。这一方针不妨碍在以后阶段就这些专题依次展开工作。

三. 确定适用的一般原则和可能方向

15. 应当以贸易法委员会法规所依据的基本原则来指导身份管理和信任服务方面的工作。这些原则包括：

- 当事人意思自治原则。对所提供工具的使用应当是任择性的，充分尊重当事人意思自治。当事人还应能自由决定拟使用保证/安全的级别。服务商应能自由提供一项或多项身份管理和信任服务，其中包括提供一个或多个保证/安全级别。总之，这套法律规则应被视为交由市场参与人支配的“法律工具箱”。
- 技术中性和经济模式中性原则。提供法律框架决不能因为引入倾向于某种技术解决方案或者某种经济模式的严格规则而阻碍创新和商业机会。
- 不歧视原则。对于电子身份识别（eID）或者信任服务的法律效力以及在法律程序中作为证据采信，不应仅以此种服务为电子形式或其不符合保证/安全级别的要求为由而加以否定。
- 功能等同原则旨在确保相当的法律功能，无论我们是在实体环境下还是在电子环境下行事。

16. 以下是就身份管理和信任服务拟订法律条文时应当处理的问题：

(a) 根据客观标准界定不同保证/安全级别：身份管理和信任服务的保证/安全级别通常是一个关键要素。在某些情况下，保证/安全级别的界定和衡量可能至关重要。什么是身份服务或管理系统或者信任服务的保证/安全？没有客观证据来判断一项服务的实际质量和保证，可能是给各相关方提出的一个重大问题，作为其风险管理政策的一部分尤其如此。以一种灵活模式针对身份管理和（或）信任服务以及身份和（或）信任服务商规定不同级别的要求，将能尊重世界各地不同制度的多样性。

(b) 法律效力的差异与保证级别相关：应当对电子身份识别和认证的法律效力以及一些信任服务的法律效力加以界定。目的是根据每一界定的保证级别来确定电子身份识别和信托服务所产生的法律效力。因此，各相关方能够通过选择符合其需要的最合适保证级别和法律效力，对其法律风险进行有效管理。为了界定这些不同法律效力，可以特别考虑到不歧视原则、同化原则、相互承认原则，以及关于倒置举证责任的特别推定和（或）机制，视情况而定。保证级别越高，法律效力对服务使用者越有利。

(c) 根据保证级别建立赔偿责任制度：界定对于电子身份识别系统和信任服务提供人的赔偿责任制度，以促进实现必要的明确性和可预测性。这一制度将因所提供的保证级别而相异。

17. 以下是身份管理服务应当特别依循的准则：

- 网上服务提供人可以通过适用当事人意思自治原则，决定是否要求为利用其服务而进行电子身份识别和认证以及所要求的保证级别。
- 对保证级别相当于或者高于规定的网上访问保证级别的电子身份识别手段的跨境相互承认。这项原则将以不同保证级别的电子身份识别手段的定义为基础。每级都将适用统一的客观标准。
- 为了确定应在我们工作中考虑哪些身份管理系统，首先应当确定使用电子身份识别手段的宗旨/目的，即这种手段是否全部或部分用于商业交易，然后了解由谁签发电子身份识别手段（公共部门或者私营部门，或者这两个部门）。由于使用电子身份识别手段的目的可能是商业性的，所有电子身份识别手段都应纳入我们的工作中审议，即使是那些完全或者部分由公共部门签发的电子身份识别手段。
- 我们的工作应当首先侧重于确定自然人和法人，初期阶段暂不审议确定物质对象（如服务器，智能手机，终端等）问题或者确定数字对象（软件……）问题。既然我们需要确定法律规则，就应优先考虑确定法律主体（自然人或者法人）及其权利和义务以及所承担的赔偿责任（如网站，版权或者服务器拥有人）。物质对象或者数字对象将始终与自然人或者法人相关联。对象的确定基本上是一个技术和安全问题，不是法律问题。

- 由权威来源签发/管理的个人身份识别数据至少应当配置级别更高的电子身份识别手段。
 - 为了实现更高级别的保证，应当规定电子身份识别手段提供人有义务通知任何违反电子身份识别系统事宜并在必要时暂停其运行。提供人应依照本国法律的规定发出通知，并视跨境情形将该信息公诸于众。
 - 可以建立这样的推定：如果提供人符合国际机构确定的技术标准，即应当尊重界定保证级别的客观标准以及法律要求。
18. 身份管理的三个保证级别可设定为：(a)低、(b)基本、(c)高。
- 保证级别将以与之相关的技术规格、标准和程序为依据。
 - 可以设想在合作机制和互通性框架中界定保证级别所依据的标准并交换与电子身份识别手段及其保证级别有关的信息。
 - 将设想针对具有（自基本级别起）等同（或更高）安全级别的这些电子身份识别手段制定一项跨境相互承认原则。
19. 以下是信任服务应当依循的准则：
- 为了确定和统一信任服务的安全级别，至少应分为两个层面：
 1. 不合格信任服务；
 2. 合格信任服务。
 - 法律效力根据信任服务的安全级别而不同：
 1. 如果信任服务不合格：法律效力限于不歧视条款。
 2. 如果信托服务合格：法律效力将包括同化、推定、举证责任倒置。
 - 将确定对于具有等同安全级别信任服务的跨境相互承认原则。
 - 将设定对于所有（合格或不合格）提供人的与风险程度相称的一般安全要求。
 - 将规定对合格信任服务提供人和对其提供的合格信任服务的具体要求，以确保高级别可靠性/安全性。
 - 赔偿责任制度将取决于信任服务提供人是否合格。
 - 可以确定对所有信托服务提供人（至少是合格者）通知任何违反信任服务系统事宜并在必要时暂停其运行的要求。提供人应依照本国法律规定发出通知，并视跨境情形将该信息公诸于众。
 - 可以建立这样的推定：如果提供人符合国际机构确定的技术标准，即应当尊重界定安全级别的客观标准以及法律要求。

四. 确定概念和提议的定义草案

20. 鉴于即将就身份管理和信任服务进行的讨论，以下提出概念和定义清单（非穷尽）：

- **电子身份识别**指使用唯一代表自然人或法人或者代表作为法人的自然人的电子形式个人身份识别数据的过程；
- **电子身份识别手段**指包含个人身份识别数据并用于网上服务认证的物质装置和/或非物质装置；
- **个人身份识别数据**指使得能够确定自然人或法人身份或者作为法人的自然人身份的一套数据；
- **电子身份识别办法**指向自然人或法人或者作为法人的自然人签发电子身份识别手段的电子身份识别系统；
- **认证**指一种使得能够对自然人或法人或者电子形式数据来源和完整性的电子身份识别加以确认的电子进程；
- **权威来源**指为了提供可用于证明身份的准确数据、信息和（或）证据而能够依赖的任何来源，其形式不予考虑；
- **信任服务**指（通常为付酬而提供的）一种电子服务，其中包括：
 1. 电子签名、电子印章或电子时间戳、电子登记交付服务以及与这些服务有关的证书的生成、核实和验证，或者
 2. 网站认证证书的生成、核实和验证；或者
 3. 电子签名、电子印章或者与这些服务有关的证书的保全；
- **合格信任服务**指满足本案文[公约、示范法]规定的相关要求的信任服务；
- **电子签名**指附于电子形式的其他数据或与之有逻辑联系，并由签名人用以签署的电子形式数据；
- **签名人**指生成电子签名的自然人；
- **电子印章**指附于电子形式的其他数据或与之有逻辑联系，以确保这些其他数据的来源和完整性的电子形式数据；
- **电子时间戳**指将电子形式的其他数据与某一特定时间连接，从而确立可证明这些特定数据在该时间存在的证据的电子形式数据；
- **电子登记交付服务**指使得能够通过电子手段在第三方之间传输数据并提供与处理被传输数据相关证据的服务，这种服务保护被传输数据免于丢失、盗窃、损毁或任何未经授权更改的风险；

- **网站认证证书**指使得能够对网站进行认证、并将网站与被签发证书的自然人或法人相连接的证明；
- **电子文件**指以电子形式存储的任何内容，特别是文本或音频、视像或视听录制；
- **验证**指核实和确认电子签名或印章有效的过程；
- **依赖方**指依靠于电子身份识别或信任服务的自然人或法人。

五. 联系实际

为了更好地了解工作范围、各种概念和与实际的联系，第四工作组届会期间可以提出在不同国家或区域设立的具体项目。不妨介绍欧洲连通设施（CEF）的电子身份识别（eID）数字服务基础设施（DSI）以及《电子身份识别和信任服务条例》（eIDAS）节点，以说明其如何运作以及欧盟成员国如何实行。
