联合国 A/CN.9/WG.IV/WP.154

大 会

Distr.: Limited
12 September 2018
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十七届会议
2018 年 11 月 19 日至 23 日，维也纳

与身份管理和信任服务有关的法律问题

秘书处的说明

目录

V.18-05925 (C) 111018 111018

一. 导言

1. 本说明介绍了工作组所确定的与审议身份管理和信任服务相关法律问题有关的若干专题的某些方面（A/CN.9/936，第 58 段），以便于进一步讨论。本说明尤其力求着重说明某些关键问题并就可能的解决办法提出建议，而无意限制审议更多专题或酌情一并审议某些专题的可能性。A/CN.9/WG.IV/WP.153 号工作文件介绍了由工作组确定的事关其审议身份管理和信任服务相关法律问题的其他专题的某些方面。

2. 关于身份管理和信任服务相关法律问题工作组工作情况的背景资料见 A/CN.9/WG.IV/WP.152 号工作文件，第 6-17 段。更多相关文件的清单见 A/CN.9/WG.IV/WP.152 号工作文件，第 18 段。

二. 身份管理和信任服务所涉法律问题今后工作的相关问题

A. 身份管理和信任服务提供商的核证

3. 核证包括自我核证、资格鉴定和独立审计，可大大有助于建立对身份管理提供商和信任服务提供商的信任。选择最合适的核证形式可能会受到所涉服务的类型、成本以及所寻求保证级的影响。

4. 《电子身份识别和信任服务条例》设想了一种全面的信任服务监管和核证系统。根据其第 17 条，各成员国应指定一个机构负责对合格信任服务提供商执行定期监管任务，并对其他信任服务提供商执行临时任务。第 17 条第(4)款提供了一份清单，列出了由监管机构执行的具体任务。

5. 必须指出的是，根据《电子身份识别和信任服务条例》，监管机构的存在对于信任服务提供商被视为合格的是必要的。特别是，根据第 20 条，合格信任服务提供商必须至少每 24 个月由合规评估机构进行一次审计，由此产生的合规评估报告将提交给监管机构。不遵守监管机构的要求可能会导致信任服务提供商或其任何服务的合格状态被撤销。

6. 反之，根据《电子身份识别和信任服务条例》，只有合格信任服务提供商可以提供与某些法律效力相关的合格信任服务，如推定。例如，根据《电子身份识别和信任服务条例》第 25 条第(2)款，合格的电子签名应具有与手写签名同等的法律效力。简言之，监管机构的存在使得能够提供与法律效力相关的合格信任服务。

7. 关于信任服务，《电子签名示范法》第 10 条(e)和(f)项提到资格鉴定、审计和自我核证的存在是与评估认证服务提供商所使用的系统可信赖性可能有关的一个因素。因此，根据这一办法，监管机构和资格鉴定计划的存在是可选的，则对其存在的评价是裁量性的。

8. 在使用可信赖清单（见 A/CN.9/WG.IV/WP.153，第 61-73、76-79 段）的相互法律承认模式中，核证（包括自我核证）是用以评估使用基于成果标准的身份管理方案的一个必要因素。或许有必要预先制定一套用以进行此种评估的规范概要。

9. 工作组似宜审议，核证的存在——包括自我核证、资格鉴定和独立审计——是否应与某些法律效力关联，如果是，哪些效力，或者更确切地说，应被列为可能与评估身份管理和信任服务提供商的可靠性、可信赖性或其他资质相关的要素。工作

组还似应在审议时说明，核证——包括自我核证、资格鉴定和独立审计——的使用应是强制性的还是选择性的。

B. 保证级

1. 身份管理

10. 保证级是基于所用流程的身份声明可靠性的衡量标准。公共实体和私营实体对保证级有不同的定义。这些定义根据技术和业务流程的发展变化定期更新。鉴于采用了技术中性原则，只考虑以技术中性方式制定的保证级。

11. 美利坚合众国国家标准和技术研究所（NIST）确定了三种不同级别的身份相关保证：身份保证级（IAL）、认证人保证级（AAL）和联合保证级（FAL）。[1]IAL 指身份验证过程，AAL 指认证过程，FAL 指在联合环境中传递认证信息并（在适用情况下）将信息归属于依赖方所使用的辨认规程。

12. 更确切地说，IAL 指的是身份验证过程的牢固性，以自信地确定个人的身份；AAL 指的是认证过程本身的牢固性以及认证元素与特定个人的身份识别特征之间的绑定；FAL 指的是在使用联合身份架构的情况下联盟系统用以传递认证信息并将信息归属于依赖方的辨认规程的牢固性。[2]

13. 每级身份保证各有与特定要求关联的牢固级别。例如，在 IAL-1 级，属性（如有的话）是自我宣称的，或者应当视为自我宣称的。在 IAL-2 级，要求进行远程或面对面的身份验证。IAL-2 级要求面对面验证身份属性，或者至少使用指定程序远程验证身份属性。IAL-3 级要求面对面验证身份，而且身份属性必须由经授权的认证服务提供商代表按照指定程序通过检验物理文档来验证。

14. 《电子身份识别和信任服务条例》第 8 条规定了身份管理的三个保证级：低级、实质级和高级以及各自的标准。特别是，“低级”保证对声称或宣称的个人身份提供有限程度的信任；“实质级”保证对声称或宣称的个人身份提供实质程度的信任；“高级”保证对声称或宣称的个人身份提供的信任程度比“实质级”保证更高。

15. 《电子身份识别和信任服务条例》的一项实施法案[3]规定了最低限技术规格和程序，用以确定登记的可靠性和质量、电子识别手段管理、认证以及跨境身份管理提供商的管理和组织。这些技术规范和程序是以技术中性方式描述的。

16. 鉴于上述情况，工作组似宜审议，保证级概念是否应当用于满足法律要求或确定法律效力的目的。若如此，委员会还不妨特别讨论保证级与法律承认要求和机制之间的关系。工作组还不妨讨论是否以及在何种程度上进行保证级特征的讨论。

---

[1] 美国国家标准和技术研究所特别出版物 800-63-3，*Digital Identity Guidelines*，2017 年 6 月，第 2 节。查阅网址：https://doi.org/10.6028/NIST.SP.800-63-3。

[2] 美国国家标准和技术研究所，Digital Identity Guidelines，前引，第 5.2 节。

[3] 欧盟委员会 2015 年 9 月 8 日第 2015/1502 号执行条例，规定了电子识别手段保证级的最低限技术规格和程序。

2. 信任服务

17. 关于信任服务的一个根本问题是，保证级概念是否也适用于信任服务。一些关于电子签名的国内法律承认电子签名有两个级别。第一级涵盖一切形式的电子签名。第二级将某些法律后果——如来源和完整性推定——与满足某些要求的电子签名关联。这可以被解释为对电子签名引入不同级别的保证。

18. 关于信任服务，《电子身份识别和信任服务条例》第 24 条第(1)款举例说明了在满足签发合格证书的身份识别要求的情况下使用保证级。具体而言，为了满足合格信任服务提供商验证获其所签发合格证书者的身份的要求，《电子身份识别和信任服务条例》允许使用具有“实质级”或“高级”保证的电子识别手段远程进行这种验证。

19. 工作组似宜审议保证级概念是否应适用于信任服务，如果适用，应采用何种方式。

C. 赔偿责任

20. 适用的赔偿责任制度可能对促进身份管理和信任服务用于商业和非商业目的产生重大影响。这方面应当指出的是，虽然一般可获得对商业交易中错误识别的法律补救办法，但如果国内法不要求公共实体承担对这种服务的责任，则纸质文件中基本身份的归属错误可能不会引起赔偿责任。

21. 工作组已经确定了与讨论身份管理和信任服务参与者责任相关的某些问题，即：应承担赔偿责任的实体（发证商、提供商、其他当事方），同时考虑到公共实体的特殊赔偿责任制度；对遵守预定要求的当事方限制赔偿责任的可能性；限制赔偿责任的法定机制，例如，免责或举证责任倒置；以及合同规定的赔偿责任限制（A/CN.9/936，第 85 段）。

22. 在某些情况下，如果对时戳服务使用分布式账本技术，可能不易确定责任实体，例如涉及信任服务所提供的可信赖的属性数据（A/CN.9/936，第 86 段）。在其他情况下，可将基于保险的机制用于商业交易，在这种机制下，对电子身份识别方案或信任服务的错误使用可能导致保险人赔偿。另一种可用机制设想在满足某些条件的情况下自动发放预先约定的赔偿金或定额罚金。

1. 身份管理

23. 《电子身份识别和信任服务条例》第 9 条要求在发送身份管理方案的通知时提交关于适用于电子身份识别手段发证商和适用于认证程序操作方的赔偿责任制度的信息。

24. 《电子身份识别和信任服务条例》第 11 条将由于成员国未能履行其下述义务而造成损失的赔偿责任归于成员国，即未能确保唯一代表相关人的个人身份识别数据归属于相关人，并且未能确保在网上提供用以确认个人身份识别数据的认证信息。该款还将由于未能将电子身份识别手段归属于个人身份识别数据所唯一代表的个人所引起的损失的赔偿责任归于电子身份识别手段发证商。最后，该款将未能确

保正确操作用以确认个人身份识别数据的网上认证程序的赔偿责任归于认证程序操作方。

25. 《电子身份识别和信任服务条例》第 11 条仅适用于跨境交易，并规定未守规必须是有意为之或疏忽。该款根据有关损害定义和举证责任分配等问题的国内法适用，不影响国内法对使用身份管理方案的交易所涉各方规定的额外赔偿责任。

26. 总之，《电子身份识别和信任服务条例》将未能遵守某些指明的义务——如果是故意为之或疏忽——归责于身份管理方案参与方，条件是所涉交易是跨境交易，且不影响国内法下所产生的额外赔偿责任。

27. 贝宁第 2017-20 号法律第 281 条指出，如果损害是故意或疏忽造成的，身份管理系统运营商应对给身份管理方案用户造成的损害负责。

28. 根据《弗吉尼亚电子身份管理法》第 1-552 节，如果签发身份证书或者分配身份属性或信誉标志符合弗吉尼亚联邦技术部长核准的身份管理标准，并且符合任何合同协议以及身份提供商所加入的身份信任框架的任何书面规则和政策，则身份信任框架运营商或身份提供商不承担责任。根据第 1-550 节，信誉标志是“一种机器可读的官方印章、认证特征、核证、许可证或徽标，可由身份信任框架运营商在其身份信任框架范围内向经核证的身份提供商提供，以表明身份提供商遵守身份信任框架的书面规则和政策”。

29. 简言之，《弗吉尼亚电子身份管理法》免除了遵守公共机构制定的标准、合同表述和联盟规则的身份信任框架运营商和身份提供商的责任。独立的第三方核证机构根据明确定义的核证标准提供客观、一致、可审计的合规审查，通过使用这种机构来确定是否遵守弗吉尼亚联邦规定的最低限规格和标准。[4]如果身份信任框架运营商或身份提供商犯有严重疏忽的作为或不作为或犯有故意不当行为，则免责不予适用。

30. 《弗吉尼亚电子身份管理法》第 1-555 节规定，该法的条款，或者与身份管理有关的公共实体的相关作为或不作为，不得解释为放弃该公共实体的主权豁免。

31. 工作组似宜讨论，哪些实体应被追究责任，在哪些责任制度下追究其责任，以及是否应对公共实体实行特别责任制度。

32. 在讨论赔偿责任制度时，工作组似宜审议：(a)对遵守预定要求的当事方限制赔偿责任的可能性，例如，免责或举证责任倒置；(b)不同保证级是否应与不同赔偿责任制度关联；(c)通过合同限制赔偿责任的可能性；(d)是否需要提供描述赔偿责任制度（包括任何责任限制）的元数据。

2. 信任服务

33. 根据《电子身份识别和信任服务条例》第 13 条，信任服务提供商将对由于未能遵守该《条例》规定的义务故意或因疏忽而给任何自然人或法人造成的损害承担责任。换言之，信任服务提供商遵守《条例》规定的义务即可不追究责任。

[4] 弗吉尼亚联邦身份管理标准咨询委员会，Guidance Document 5: Certification of Identity Trust Framework Operators（草案），第 7 节：身份信任框架运营商的核证。

34. 此外，第 13 条就合格信任服务提供商的故意或疏忽引入了一个可推翻的推定，同时要求索赔人证明不合格信任服务提供商的故意或疏忽。这项规定旨在建立用户对合格提供商的信任，因为通过推定有助于在发生损害时寻求补救。最后，第 13 条承认信任服务提供商有可能限制其赔偿责任，前提是客户事先被告知这些限制，并且这些限制可为第三方承认。

35. 《电子签名示范法》载有关于签字人的行为（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）所产生的赔偿责任的条款。这些条款规定了参与电子签名生命周期的每个实体的义务。《电子签名示范法》承认认证服务提供商有可能限制其赔偿责任的范围或程度。

D. 机构合作机制

36. 机构合作机制可能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。这种合作机制可以是私人性质的，也可以公共性质的。

37. 《电子身份识别和信任服务条例》第 12 条提供了机构合作机制的例子，指出成员国应在身份管理方案互操作性和安全性方面进行合作。合作可包括交流信息、经验和良好做法，特别是在技术要求和保证级方面，对身份管理方案进行同行审查，以及审查相关发展。

38. 《电子身份识别和信任服务条例》的一项实施法案提供了关于信息交流和同行审查的更多细节，包括指出，如果披露可能违反公共安全或国家安全事项，或者泄露商业、专业或公司机密，成员国可以不提供所需要的信息。[5]该法案还建立了一个合作网络，以促进合作活动的开展。应当指出的是，虽然对要通知的身份管理方案进行同行审查是自愿的，但在实践中，其结果可能就该方案符合规定标准的可能性提供重要观察，因此是通知机制中的一个重要步骤，而这是《电子身份识别和信任服务条例》机构体系的核心所在。

39. 身份管理系统之间的另一种合作可通过身份管理系统联盟来实现。按照此种模式，身份信息在一身份管理系统内验证后，即以商定和受管理的方式提供给另一不同身份管理系统内为不同目的而需要此种身份信息的多个当事方（另见 A/CN.9/WG.IV/WP.153，第 47 段）。通过使用根据一套系统规则界定的共同技术和法律框架，身份管理系统联盟实现了联盟参与方之间的互通。因此，联盟可有助于增加参与用户及应用程序的数目并抑制身份管理的相关费用。尽管联盟是基于合同协议的，但法定条款仍可以有助于促进联盟（例如，见上文第 28 段《弗吉尼亚电子身份管理法》关于信誉标记的使用）。

E. 透明度

40. 工作组确定透明度原则与今后关于身份管理和信任服务的讨论有关（A/CN.9/936，第 8 段）。为此，工作组强调了与该原则相关的两项义务：披露提供了哪些身份管理和信任服务及其质量的义务；通知泄密事件的义务。

[5] 欧盟委员会 2015 年 2 月 24 日第 2015/296 号决定，该决定确立了成员国之间电子身份识别合作程序安排。

41. 关于所提供的服务及其质量，应当指出，大量信息将由参与联盟或以其他方式获得对其服务核证的身份和信任服务提供商披露。可为其他提供商规定最低限披露义务。例如，《电子签名示范法》第 9 条第(1)款载有认证服务提供商应向依赖方披露的信息清单。

42. 关于通知泄密事件的义务，据指出，泄密通知与数据泄露通知有共同之处，但也有重大区别。补充说，关于在发生泄密时不限于发出通知的机制，已经有一些有用的例子（A/CN.9/936，第 89 段）。其他考虑因素可能涉及可使用网络威胁情报来减轻风险。

43. 《电子身份识别和信任服务条例》第 10 条载有成员国通报影响跨境认证方案可靠性的泄密或损害事件的义务。有关成员国还应立即暂停或撤销已受损的认证或其受损部分。

44. 《电子身份识别和信任服务条例》第 19 条第(2)载有一项类似义务，要求信任服务提供商向监管机构和其他任何相关机构（如数据保护机构）通报对所提供的信任服务或其中保存的个人数据产生重大影响的任何泄密或完整性受损事件。通知应在没有不当延误的情况下发出，任何情况下，通知应在得知泄密或受损事件后 24 小时内发出。

45. 《电子签名示范法》第 8 条第(1)款(b)项提供了一种任择通知机制，签字人可在签名生成数据已泄露或者极有可能已泄露的情况下使用这种机制。

46. 关于披露泄密事件的义务，可拟订一则可能的条文如下：

> 身份提供商和信任服务提供商应毫不拖延地将对所提供的服务、身份证书或认证过程或对其中保存的个人数据有[重大]影响的任何泄密或完整性受损事件通知[监管机构][其受影响的客户和依赖方][，任何情况下，通知应在得知该事件后……天内发出]。
>
> 在发生重大泄密或完整性受损事件时，身份提供商和信任服务提供商应暂停提供受影响的服务[，直至……]。
>
> 身份和信任服务的用户应在身份证书、认证过程或信任服务生成数据已经泄露的情况下，或者在用户所知悉的情况导致身份证书、认证过程或信任服务生成数据有重大泄密风险的情况下，通知服务提供商。

47. 关于必须发出通知的时限规定、确定需通知的当事方，以及确定触发通知义务的服务、身份证书或个人数据受影响程度，该条文草案提供了可选措辞。还可以确立一种义务，规定直至泄密或受损得到控制或者建立起新的认证或类似程序，必须暂停身份管理系统和信任服务。

F. 数据留存

48. 工作组已经强调了跨境贸易数据留存制度协调和互操作的重要性（A/CN.9/936，第 91 段）。为此，工作组着重指出至少两个可能令人感兴趣的方面。第一个方面涉及数据保护。第二个方面涉及数据存储和归档。

49. 数据保护是一个可能引起特别复杂问题的专题。工作组似宜确认，根据贸易法委员会关于电子商务赋权案文不影响实质性条款的一般原则（见 A/CN.9/WG.IV/WP.153，第 48 段），关于数据保护和相关问题（如隐私）的法律仍应完全适用，工作组还应审议，任何补充性具体说明或澄清是否有用。

50. 如《电子商务示范法》第 10 条所指出的，文件存储和归档是一项可通过使用电子手段实现的功能，该条规定了数据电文与纸质文件在留存方面的功能等同要求。保存文件的义务产生于实体法，并且与规范各种行动所需的时间有关。

51. 为数据存储和归档提供服务可能是一项专门信任服务的目标（见下文第 64-65 段）。在信任服务互操作性框架内，工作组似宜讨论与电子档案可移植性有关的事项。

G. 服务提供商的监管

52. 如果工作组确定着眼点应当是身份管理方案和信任服务系统，而不是相关交易（见 A/CN.9/WG.IV/WP.153，第 57-59 段），则建立一个监管机构对于确立对服务提供商和所提供服务的信任或许是有用的，甚至是必要的。不过，设立这样一个机构会带来若干行政和财政方面的影响。而如果使用替代或补充机制，例如第三方核证，则可能有助于实现服务提供商监管工作所追求的目标，同时又可降低相关成本。

53. 佛蒙特州和弗吉尼亚州的立法将身份服务提供商的监管权赋予公共机构。同样，多哥第 2017-07 号法律第 97 条将对信任服务提供商的监管职能赋予国家核证局。根据贝宁第 2017-20 号法律第 283 条，身份服务提供商由公共当局指定。《电子身份识别和信任服务条例》所建立的通知制度中也隐含着对管理和提供身份服务的监管机制。

54. 关于信任服务提供商，一些法律赋予监管机构授予资格或监管第三方如何授予资格的权力。《电子身份识别和信任服务条例》要求成员国指定一个国家监管机构，主管信任服务提供商。

55. 鉴于《电子签名示范法》采用模式中立原则，所以其中作为一个选项提到监管机构的存在，这是因为，如果列入关于存在监管机构的强制性条款，可能会被理解为阻止采用基于自我规范信任服务的市场模式。

H. 信任服务的具体问题

56. 信任服务相关法律问题的工作与身份管理方面的工作密切相关。因此，在功能等同原则（A/CN.9/WG.IV/WP.153，第 36-37 段）、法律承认（A/CN.9/WG.IV/WP.153，第 93-98 段）、保证级（上文第 17-19 段）和赔偿责任（上文第 33-35 段）的范围内，结合对身份管理方面同样问题的审议，提出了与信任服务有关的评论。

57. 然而，法律上如何处理信任服务的问题也可能提出特殊挑战。一个基本问题是，信任服务各不相同，因此提出一套需要考虑的不同问题。此外，还有一个问题是，对于信任服务的法律处理办法是否应考虑一种基于“信任服务”共同定义的信任服务敞开式清单，抑或提供适用于所有信任服务的共同规则和适用于其中每项服务的具体规则。

58. 此外，可能会提及功能等同条款，以类似于贸易法委员会关于电子签名和文件留存的条款的方式，描述使用每项信任服务所追求的功能（见 A/CN.9/WG.IV/WP.153，第 36 段）。大量涉及电子签名立法的存在[6]以及在适用该立法方面积累的经验会有助于考虑这一建议。

59. 《电子身份识别和信任服务条例》提供了一个信任服务全面立法的例子。该《条例》载有关于赔偿责任和举证责任（第 13 条；见上文第 23-26 段）、监管（第 17 条；见上文第 53 段）和安全要求（第 19 条；见上文第 44 段，关于泄密或数据丢失的通知义务）等方面的一般条款。

60. 《电子身份识别和信任服务条例》载有专门一节适用于所有合格信任服务。合格的信任服务是可识别的，因其被列入欧洲联盟成员国所保持的信任名单。在这方面，工作组似宜审议，是否应根据与信任服务关联的保证级来区分信任服务，在这种情况下，应使用哪种机构机制来区分信任服务。

61. 《电子身份识别和信任服务条例》还载有与下列信任服务有关的具体规定:电子签名；电子印章；电子时戳；电子登记交付服务和网站认证。[7]每一种信任服务都可以用特定形式交付。电子签名和电子印章也可用高级形式提供。

62. 布基纳法索第 045-2009/AN 号法律载有一节，其中包含关于适用于所有信任服务提供商的条款以及关于如何获得资格鉴定的条款，其与获得合格信任服务提供商地位相关。该法还载有关于合格电子证书、电子存档、电子时戳和电子登记交付服务的具体规定。其中还有专门一章涉及电子签名。

63. 贝宁第 2017-20 号法律载有一个适用于所有信任服务提供商的一般部分和关于下列信任服务的具体规定：电子签名；电子印章；电子时戳和电子存档。

64. 该法第 301 条指出，“电子存档保证以这种方式储存的文件、数据和信息的真实性和完整性”。该法还载有功能等同规定，类似于《电子商务示范法》第 10 条。

65. 贝宁第 2017-20 号法律第 302 条进一步指出，电子存档的目的是保存文件、数据和信息以供进一步使用，相关数据的结构、索引和存储方式应考虑到保存和迁移（另见上文第 51 段）。无论技术如何演变，都应设置访问可能性。这项规定既适用于源自电子形式的文件，也适用于源自纸面并随后数字化的文件。

66. 多哥第 2017-07 号法律也有一节包含适用于所有信任服务提供商的条款，其中包括获得合格信任服务提供商地位的程序。该法还载有关于电子证书、电子存档、电子时戳和电子登记交付服务的具体规定。其中还有专门一章涉及电子签名。

67. 多哥第 2017-07 号法律由第 2018-062/PR 号法令加以补充，后者进一步规定了所有信任服务提供商的共同义务。这些义务涉及数据安全和保密、赔偿责任、财政资源、可访性、数据保护、透明度和风险管理。此外，该法令载有与第 2017-07 号法律所确定的每项信任服务有关的条款。

[6] 贸发会议全球网络法律跟踪系统显示，145 个国家，即总数的 78%，通过了关于电子交易的法律，其中通常包括关于电子签名的条款。

[7] A/CN.9/WG.IV/WP.150 提供了这些信任服务的定义。

68. 其他已经确定但尚未具体立法处理的信任服务包括电子代管账户和电子在场证明。关于电子遗嘱，已经讨论了后一种信任服务。[8]

69. 工作组似宜审议，对于身份管理和信任服务的法律处理办法应使用相同机制还是不同机制。此外，工作组似宜审议，对于信任服务的法律处理办法是否应考虑一种基于“信任服务”共同定义的信任服务敞开式清单，还是说提供适用于所有信任服务的共同规则和适用于其中每项服务的具体规则。特别是，工作组似应审议，是否应为每项信任服务制定功能等同规则，以及是否也应在信任服务方面提及保证级。

[8] 例如，见全国统一州法律专员会议正在起草的电子遗嘱法草案第 8 节。