联合国 A/CN.9/WG.IV/WP.165

大 会

Distr.: Limited
30 September 2020
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第六十届会议
2020 年 10 月 19 日至 23 日，维也纳（线上）

重新考虑对身份管理和信任服务的方法

美利坚合众国提交的文件

秘书处的说明

美利坚合众国提交了一份文件，供工作组第六十届会议审议。现将该文件按秘书处收到的原样转载于本说明附件。

V.20-05627 (C) 141020 141020

附件

重新考虑对身份管理和信任服务的方法

1. 美国谨就第四工作组关于身份管理系统和信任服务的当前项目提交本文件。本表分三个部分：本文件第一部分提供了下面各节的概述和执行摘要。第二部分提供身份管理系统及其运作规则的背景情况。最后，第三部分概述所有身份管理系统运作通常依据的法律框架，以及关于工作组如何调整 WP.162 号文件以有效处理私营部门身份管理系统的概念框架。

2. 就本文件而言，美国仅侧重于身份管理系统以及工作组如何有效地处理身份管理系统。尽管如此，美国欢迎工作组就 WP.162 文件中的信任服务部分进行类似讨论，因为我们认为这一部分提出的许多问题与下文概述的关于身份管理条文的概念问题是相同的。

一. 概述和执行摘要

3. 总体而言，对于 WP.162 所反映的工作组目前对身份管理系统采取的做法，美国有一些根本性的关切（见附录），认为工作组有必要在概念层面上进行讨论以解决这些关切。

4. 贸易法委员会的任务应是提供一个能够帮助各国就私营部门身份管理系统可能出现的法律问题提供指引的框架，特别是在管辖各个身份管理系统的基于合同的具体运营规则无法涵盖的领域。这可以包括修订现行国内法以消除现有法律中的障碍和不确定性，填补与身份管理系统相关的现有法律中无法通过合同解决的空白，或者处理可促进私营部门身份识别系统发展的新问题。然而，WP.162 采取了一种显著不同的方法，在美国看来，这种方法是不可行的。

A. 何为身份管理系统？

5. **身份管理**涉及一组允许对个人或实体进行身份识别（即你是谁？）并对该身份进行认证（你如何证明这一身份？）的政策、流程和程序。如下文第二节所做的更为全面的描述，**身份交易**是一种以证实身份信息与主体之间关系的方式向依赖方提供关于该主体的某些身份信息的通信。这种**身份交易**借助身份管理系统。**身份管理系统**是涉及将参与实体、流程和技术组成一体的复杂安排，其中每个参与方根据一组预定义的具有法律约束力的流程、政策和程序履行一项或多项预定义角色的职责，目的是促成将允许个人使之与多个非附属性实体相关联的身份交易。

6. 要做到这一点，每个身份管理系统需要一套可强制执行的操作规则。如下文第二节所做的更为全面的描述，操作规则涉及各个身份管理系统的操作，其中具体规定如何进行其身份管理程序和相应的身份交易，以及如何安排各方的权利和职责。由于每个身份管理系统都不同，因此每个系统都需要一套具体适合其目的、结构、参与方基群和风险概况的独特操作规则。

7. 在涉及公共部门的身份管理系统时，操作规则通常是在法规或条例中载明的，因此通过法律对参与方具有约束力。在涉及私营部门的身份管理系统时，操作规则是在系统运营人（或某些其他人或实体）编写的文件中载明的，并通过合约对参与方具有约束力。

B. 贸易法委员会的文书应涉及哪些方面？

8. 贸易法委员会针对私营部门身份管理系统制定的任何文书都应考虑到现行的国内法和各个身份管理系统所使用的基于合约的不同操作规则。具体而言，贸易法委员会文书应处理与现行国内法适用于私营部门身份管理系统有关的问题，这些问题㈠无法通过各个身份管理系统所采用的基于合约的具体操作规则来解决，或㈡在其他方面给所有私营部门的身份管理系统带来问题。因此，贸易法委员会文书中要涉及的领域包括：对私营部门身份管理系统身份交易的法律承认、关于确定私营部门身份交易是否满足某人身份识别的适用法律要求的规定、以及不能以身份管理系统操作规则加以修改的法律的适用性，例如，关于使用政府身份识别特征的法律、消费者保护法和侵权法。

9. 这种做法是基于这样一种认识，即私营部门的身份管理系统有三层法律管辖框架，上层是现行国内法（第 1 级），下层是基于合约的各个身份管理系统操作规则（第 3 级）。这一法律框架的中层（第 2 级）将在第 1 级和第 3 级之间提供桥梁。贸易法委员会的目标应当是制定一部文书，就第 2 级法律将包含的内容向各国提供指导。下文第三节对这一法律框架做了更全面的描述（包括图 1，其中提供了这三层法律及其相互关系的图示）。第三节还提供了贸易法委员会可如何思考此类文书内容的详细路线图。

10. WP.162 没有承认这一法律框架，而是采取了一种根本不同的方法，在我们看来，这种方法是不可行的。虽然该文件处理了一些理应由第 2 级文书涵盖的问题，但其将这些问题与许多更适合由基于合约的各个身份管理系统操作规则（第 3 级）来处理的问题结合并混为一谈。结果是，该文件频繁采用“一刀切”的做法来处理在各种基于合约的管辖各个身份管理系统的操作规则之间存在极大差异的问题。随着就案文草案的谈判取得进展，越来越清楚的是，这并非一种可行的方法。

11. WP.162 号文件使用公共部门身份管理系统的操作规则（即《电子身份识别和信任服务条例》）作为概念模式，并寻求将这一模式全面扩展到所有身份管理系统。《电子身份识别和信任服务条例》的确是身份管理系统规范方面的一种高度创新方法，对全世界了解身份管理系统如何运作以及如何对公共部门使用这种系统进行规范做出了显著贡献。然而，问题在于，《电子身份识别和信任服务条例》是（由欧盟国家各种不同身份提供人组成）单一公共部门身份管理系统的一套独特操作规则。因此，在公共部门中，它相当于管辖特定私营部门身份管理系统的基于合约的操作规则。试图对其他所有身份管理系统规定这些操作规则是不合适的。

12. 换言之，《电子身份识别和信任服务条例》是管辖单一个身份管理系统的一套操作规则（第 3 级），而贸易法委员会应制定一部将适用于所有身份管理系统的文书（第 2 级）。《电子身份识别和信任服务条例》是面向公共部门身份管理

系统的一套操作规则（即规范公共部门使用的身份交易），而贸易法委员会应制定一部适用于私营部门身份管理系统的文书。具体而言，贸易法委员会的文书应在管辖各个私营部门身份管理系统的基于合约的操作规则（第 3 级）与现行国内法（第 1 级）中对所有身份管理系统有不利影响、但不能由各个身份管理系统操作规则解决的那些方面（如身份交易的法律承认或侵权责任）之间架起一座桥梁。[1]

13. 相反，WP.162 号文件所载明的规则涉及通常由各个身份管理系统的基于合约的操作规则处理的若干问题。这包括诸如身份管理服务提供人的义务（第 6 条）、违规情况下的义务（第 7 条）、订户的义务（第 8 条）或身份管理服务提供人的赔偿责任（第 12 条）等问题。同时，WP.162 号文件未能清楚地界定合同当事人在哪些情况下可以在这些问题上偏离现行法律，以及在哪些情况下必须遵守现行法律。

14. 此外，虽然 WP.162 号文件所依据的《电子身份识别和信任服务条例》框架依赖于一个对身份管理系统进行监管、制定标准和认证的集中机制，但并不存在这样一个全球范围的集中机制来支撑诸如 WP.162 号文件这样的贸易法委员会文书。WP.162 号文件则完全以存在这样一个全球机制为前提。在没有这种全球机制的情况下，WP.162 号文件中关于跨境承认和可靠性标准的条文提出了一些未决问题，需要工作组进一步讨论。事实上，《电子身份识别和信任服务条例》规定，只有在欧盟与第三国之间订有特定类型协议的情况下才承认欧盟以外提供人的信任服务（《电子身份识别和信任服务条例》第 14.1 条）。

15. 除了与《电子身份识别和信任服务条例》模式不吻合之外，WP.162 号文件以《贸易法委员会电子签名示范法》作为一种依赖模式也不合适。电子签名相对简单和标准化，而身份管理系统则更为复杂和多层次。例如，电子签名通常涉及两方，而身份管理系统通常涉及多方。身份管理系统根本用不上《电子签名示范法》中的规则。

16. 这些都是根本性问题，由此提出了非常基本但关键的问题：WP.162 号文件所反映的办法一旦通过，对各国有何用处？在没有一个集中机制对身份管理系统或信任服务进行监管或认证的情况下，该文本将如何实现其设定的目标，例如，在跨境承认或可靠性标准方面的目标？按照美国的理解，如果打算让 WP.162 号文件适用于私营部门的身份管理系统，那么该文件中规定的规则与管辖身份管理系统的合同各方所规定的操作规则是何关系？

17. 美国先前对秘书处的问卷模板作了答复，并提供了对最新案文的书面回复，本文件附录载有对 WP.162 号文件的逐条分析。然而，美国认为，在推进 WP.162 号文件之前，工作组应首先进行概念性讨论，以澄清 WP.162 号文件将如何切合管辖身份管理系统的总体法律框架。虽然美国赞赏为拟定 WP.162 号文件做了大量工作并且为就该文件达成协商一致做出了努力，但工作组如果继续推进一部对成员国或私营部门身份管理系统用处不大的文书，将是令人遗憾的。

[1] 虽然可以说《电子身份识别和信任服务条例》包括了针对同意加入欧盟单一框架的欧盟国家各种身份提供人的第 2 级和第 3 级要素，但我们认为，贸易法委员会应完全侧重于制定一部适用于所有私营部门身份管理服务提供人的第 2 级文书。此外，《电子身份识别和信任服务条例》是供公共部门使用的身份管理系统，而贸易法委员会的任务是制定一部适用于私营部门身份管理系统的文书。

18. 如本文件所反映的，在一些方面，WP.162 号文件所处理的问题与身份管理系统的问题密切相关，但方法不可行，工作组或许能够在这些方面以 WP.162 号文件为基础，将概念上的变化纳入现有条文。至于其他方面，可能需要进行比较大的调整或删改。

19. 美国在下文第三部分中提供的框架可作为路线图，以指导进行将有助于规划前进道路的概念性讨论。

二. 关于身份管理系统的背景情况

20. 我们认为，这个项目的目标应当是确立一个支持并鼓励发展强大身份生态系统的法律框架，在这个生态系统中，私营部门各种类型的多个身份管理系统得以蓬勃发展，并支持国内和全球商业。这需要把重点放在找出现有国内法中需要解决的任何障碍或差距。此外，为了鼓励开发新的、不同的身份管理系统，工作组务必避免对应当通过各个身份管理系统制定的基于合同的独特操作规则来解决的问题和疑难采取“一刀切”的解决方案。

21. 为了找出身份管理法律框架中需要解决的障碍和差距，我们首先需要做以下工作：

- 审查身份交易和身份管理系统的概念；
- 审查管辖各个私营部门身份管理系统运作的操作规则的必要性和作用；以及
- 了解管辖身份管理系统的总体法律框架，以及一部贸易法委员会的文书以何种方式可有助于/切合哪些方面。

22. 在了解这一背景后，工作组就可以确定哪些法律问题无法由作为身份管理系统组成部分的基于合约的独特操作规则来解决，因而需要使用贸易法委员会制定的法律文书通过增补和修改国内法来解决这些法律问题。

A. 身份交易

23. 身份交易是依赖方籍以接收关于某一个人[2]的一些身份信息（身份识别），同时验证声称是该个人的人确实是该个人（认证）的通信。这样做通常是为了以下目的：(1)与主体进行某种交易（例如，订立合同、提供利益、交流信息等），或(2)授予主体对某种数字或物理设施（例如，网站、数据库、建筑物等）的访问权。

24. 身份交易通常要求：(1)收集和验证关于个人数据主体的信息（属性）（身份识别过程），(2)签发包含其中一项或多项属性的凭证（凭证签发过程），以及(3)将凭证中的身份属性与特定个人相关联，该个人通常远在他地（即认证过程）。身份交易旨在通过这些流程验证个人身份并认证该身份与特定个人的关系。

[2] 身份交易的主体可以是个人、实体、设备或数字对象。本文件将侧重于个人，因为这是工作组迄今讨论的重点。

25. 因此，举例来说，在边境出示某人的护照以获准进入一个国家就是一种身份交易。在这种情况下，向依赖方（边境检查人员）提供（护照中注明的）关于个人的先前经过验证的身份属性，同时通过一种方法验证出示护照的人是护照中指明的个人（即通过嵌入护照中的照片或指纹数据）。同样，使用用户名和密码登录在线网络以访问数据库的过程也是一种身份交易。这一过程涉及（根据用户名）将先前经过验证的个人身份属性（通过密码）与声称是该个人的人（即输入用户名的人）相关联。

B. 身份管理系统是旨在促进身份交易的多方系统

26. **身份管理系统**是由参与实体、流程和技术组合起来的整体，其中每个参与方为促成身份交易而根据一组预定义的具有法律约束力的流程、政策和程序履行一项或多项预定义角色的职责。[3]

27. 身份管理系统是复杂的多方系统。这些系统涉及多个参与方担任各种角色，如登记机构、身份核实人、属性提供人、信任提供人、身份提供人、凭证提供人、验证提供人、中枢等。他们协调为收集和验证个人数据主体的身份（属性）而必需开展的工作，签发包含其中一项或多项属性的凭证，并在身份交易的情况下对特定个人的这些身份属性进行认证。这些参与方共同努力促进多个依赖方的身份交易。

28. 就结构的复杂性而言，身份管理系统类似于为便利信贷交易而建立的信用卡系统（如万事达卡或威士信用卡），或为便利支付交易而建立的电子支付系统（如环球银行间金融电信协会（SWIFT）或非洲信息交换所（ACH））。虽然这些类型系统中每一种系统都使用不同结构、为不同目的而设计，但它们都是为便利特定类型的经济交易（如信用卡、支付或身份交易）而设计的多方系统。

29. 身份管理系统的结构可能大相径庭。例如，身份管理系统可以是集中式的（为单个身份提供人，以便利多个依赖方的身份交易），可以是联合式的（由一组有限的身份提供人集中存储和提供用户身份信息，以便利与一个或多个依赖方的身份交易），也可以是分布式的（由多个身份提供人对用户在本地存储的身份信息进行认证，以便利与多个依赖方的身份交易）。身份管理系统结构的这种多样性是工作组正在拟订的文书不能对众多问题采取一刀切办法的主要原因之一。

C. 身份管理系统需要具有法律约束力的操作规则

30. 由于身份管理系统是复杂的多方系统，各参与实体的协调与合作对于实现预期目标至关重要。因此，身份管理系统需要一个有组织、有目的的结构，该结构由相互关联和相互依赖的参与实体组成，这些实体扮演各种角色，执行一套详细的流程，并遵循一套政策和程序，所有这些都旨在实现特定目标——即便利身份交易。

[3] 例如，这种角色可以包括登记机构、身份核实人、身份提供人、经纪人、中枢、属性提供人、依赖方等。

31. 此外，由于身份管理系统涉及多个可能相互交互以执行一系列复杂交易的独立参与实体，因此身份管理系统不会自动独立运行。每个参与方都必须遵循一套规则或指示，以确定其特定角色的行为方式。这样的规则一般必须是法律上可强制执行的，以确保所有参与方遵守适用于他们的要求，并能够依赖所有其他参与方遵守规则并产生可信赖的结果。

32. 因此，每个身份管理系统都需要一套法律上可强制执行的**操作规则**来管理其运作。[4]这些操作规则有三个重要功能：

- 操作规则确保身份管理系统**正常运作**，即，操作规则具体规定系统运作的政策、程序和流程，从而使身份管理系统按其应有的方式“工作”；
- 操作规则界定每个参与方角色的**职责和义务**（例如，以便每个参与方知道要做什么），以及各自的法律责任，(适当情况下）还界定并公平分配责任风险；以及
- 操作规则还规定有助于使身份管理系统为其预期目的而“**值得信赖**”的其他要求——这些要求超出了仅仅确保身份管理系统正常运作的范围，同时实施额外步骤以确保参与方对据此进行的身份交易抱有信心并愿意依赖这些交易。

33. 为实现这些目标，操作规则的设计通常着眼于特定身份管理系统操作中出现的具体业务、技术和法律问题。例如，这可能包括以下问题：参与要求、角色定义和责任、关于数据主体注册、身份核实、凭证签发和身份认证的流程和程序、技术规格和标准、数据安全要求、保证、责任分配、争议解决程序、终止权。操作规则还涉及对身份管理系统的管理，如参与资格、规则执行和规则修订。操作规则构成了身份管理系统的管理框架。此外，由于每个身份管理系统的结构、技术和目的可能不同，因此各个身份管理系统的操作规则可能有很大差异。

34. 为确保身份管理系统操作规则具有法律约束力和可执行性，操作规则可以采取规约或条例形式，也可以采取合同形式。

35. 就**公共部门**身份管理系统而言，操作规则通常采用详细**法规**或条例的形式。例如，印度的《阿达尔法》、[5]爱沙尼亚的《身份证件法》[6]和欧盟的《电子身份识别和信任服务条例》。[7]不过，一些公共部门的身份管理系统已经使用了合同，如 GOV.UK.Verify 身份管理系统。[8]

36. 就**私营部门**的身份管理系统而言，操作规则采用对系统参与方有约束力的**合同**形式（正如信用卡系统或支付系统参与方通过合同同意各自角色所适用的

[4] 操作规则还经常使用各种其他称谓，如管理框架、信任框架、方案规则和系统规则。

[5] 《阿达尔法》（有针对性地提供财政和其他补贴、福利和服务），2016 年，https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf。

[6] 《身份证件法》，1999 年 2 月 15 日通过，RT I 1999, 25, 365，2000 年 1 月 1 日生效，www.riigiteataja.ee/en/eli/ee/504112013003/consolide。

[7] 2014 年 7 月 23 日通过的关于内部市场电子交易的电子身份识别和信任服务第 910/2014 号条例（欧盟）（《电子身份识别和信任服务条例》）提供了一个可预测的监管环境，以支持企业、公民和公共当局之间安全和无缝电子互动；可查：https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014。

[8] www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify。

操作规则的条款一样）。私营部门身份管理系统操作规则的例子包括 SAFE Identity Trust Framework、[9]Sovrin Governance Framework、[10]Pan-Canadian Trust Framework。[11]另见《信任框架和互操作性指南》。[12]

D. 操作规则对于每个身份管理系统都是独特的

37. 由于每个身份管理系统都各不相同，因此每个系统都需要一套具体适合其结构、技术、目的、市场和风险概况的独特操作规则。

38. 私营部门的身份管理系统采用各种各样的结构和技术，每种**结构和技术**都要求以不同方法制定操作规则。如果试图将一套统一的、一刀切的此类规则强加于所有系统，将会阻碍此类私营部门身份管理系统的发展。

- 2016 年世界经济论坛[13]确定了不同的身份管理**系统结构**，例子包括内部身份管理系统、外部认证身份管理系统、集中式身份管理系统、联合式身份管理系统和分布式身份管理系统。最近部署的其他身份管理系统结构包括基于中枢的身份管理系统和自主身份管理系统，以及正在开发的使用移动电话的身份管理系统。每一种结构都要求以不同方法制定操作规则，并将因试图对所有系统上规定一套统一的此类规则而受到影响。

- 不同的身份管理**系统技术**的例子包括基于公钥基础设施的身份管理系统、区块链身份管理系统，以及使用 OAuth（“开放授权”）和 OpenID Connect（“开放身份连接”）标准的系统，每种系统都需要以不同方法制定操作规则，并将因试图对所有系统上规定一套统一的此类规则而受到影响。

39. 私营部门的身份管理系统一般也是为各种不同**目的和/或市场**而设计的，这就要求在其操作规则中采用各种不同方法、信任要求和风险分配办法。如果试图将一套统一的、一刀切的此类规则强加于所有系统，将会阻碍此种身份管理系统的发展。

- 为各种不同**目的和市场**设计的身份管理系统的例子包括：为教育用途（如大学和学生）设计的 InCommon 身份管理系统；为制药业设计的 SAFE BioPharma 身份管理系统；为国际航空航天工业设计的 CertiPath 身份管理系统；为识别网站运营商设计的 CA Browser Forum 身份管理系统；为移动身份设计的 Zenkey；以及为低风险网站访问而设计的轻量级 Google、LinkedIn 和 Facebook 身份管理系统。

---

[9] www.globenewswire.com/news-release/2020/05/19/2035512/0/en/SAFE-Identity-Announces-Revamped-SAFE-Biopharma-Trust-Framework-and-New-Services-to-Expand-and-Evolve-Digital-Trust-in-Healthcare-Sector.html。

[10] https://sovrin.org/library/sovrin-governance-framework。

[11] https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view。

[12] Open Identity Exchange，“A Guide to Trust Frameworks and Interoperability”，可查：https://openidentityexchange.org/guide-trust-frameworks-interoperability。

[13] 见世界经济论坛，“数字身份蓝图”，2016 年 8 月，可查：http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf。

40. 由于这些规则的设计着眼于特定身份管理系统的独特要求，因此此类操作规则涉及的事项不应在工作组正在制定的文书的范围之内。

41. 由于私营部门身份管理系统的操作规则以合约为基础，并与特定身份管理系统的独特要求挂钩，重要的是，贸易法委员会制定的任何文书都不应试图以适用于所有身份管理系统的一刀切办法复制这些操作规则。因此，工作组面临的挑战是，它制定的文书既不限制也不妨碍私营部门身份管理系统制定各自操作规则的需要或能力，同时明确规定基于合约的操作规则必须遵守的法律要求。

三. 管辖私营部门身份管理系统的法律框架和一部贸易法委员会可能制定的文书

A. 总体法律框架

42. 我们认为，作为制定 WP.162 号文件所设想的文书的一项先决条件，工作组需要考虑关于私营部门身份管理系统的总体法律框架的结构。具体而言，工作组应考虑㈠各种私营部门身份管理系统的各个操作规则和㈡拟议的贸易法委员会文书如何切合这一框架。这对于确定贸易法委员会文书中应处理哪些问题非常重要。

43. 同大多数多方商业交易系统一样，私营部门的身份管理系统通常由一个法律框架管辖，这一框架由㈠政府制定的法律和㈡参与实体的合同协议组成。**政府制定的法律**包括由立法机关作为法规颁布的规则、由政府机构作为条例通过的规则、或者通过司法裁决确定的规则组成。**基于合约的法律**由一个或多个参与方或身份管理系统的理事机构起草的规则——即身份管理系统的操作规则——组成，这些规则通过合同对身份管理系统的参与方具有约束力。

44. 任何私营部门身份管理系统运作的法律框架通常由最多三层（或级）法律组成，每级向下对身份管理系统的规定越来越具体。下文说明法律框架的这三个层级（并在接下来的一页以图表列示）：

- **（第 1 级）现行法律**：最高一级是最基本的法律，只有**现行国家法律**。这些是政府制定的法律，包括成文法、条例和司法裁决。这类法律管辖所有类型的商业活动，不是专门为身份管理系统系统拟定的，在某些情况下可能已有数百年历史。尽管如此，这类法律经常适用于私营部门身份管理系统的活动。这包括一般合同法、侵权法、隐私法、出口管制法、担保法、消费者保护法、竞争法、银行法等。

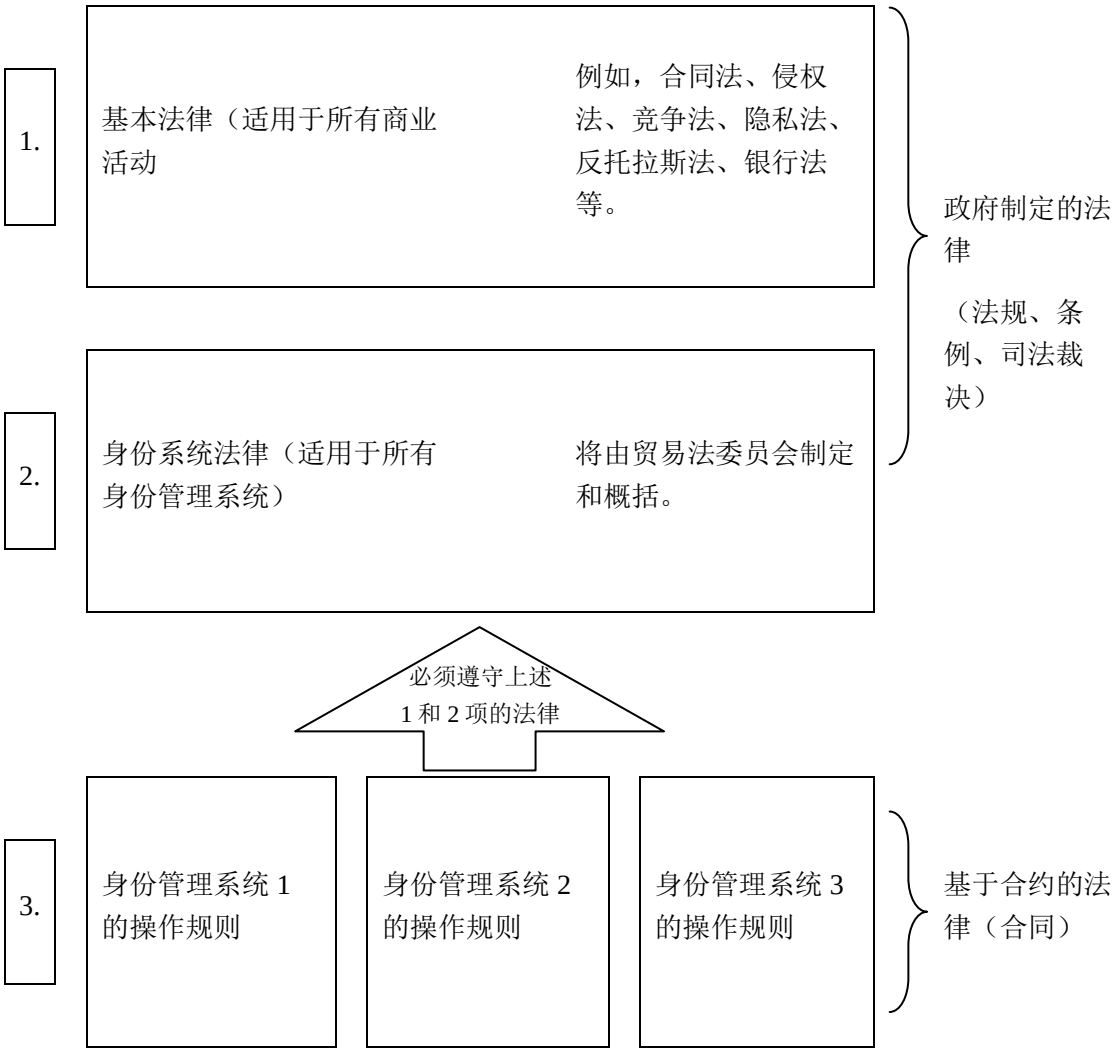
- **（第 2 级）身份系统法律**：第二级法律管辖私营部门的**身份管理系统**，可称之为身份系统法律。这类法律是专门为管辖所有私营部门的身份管理系统而拟订的，无论其类型、结构、技术或目的如何。第 2 级身份系统法律也是政府制定的法律，旨在处理第一级现行法律给所有身份管理系统造成的问题，并可以填补第一级法律留下的一些空白。第 2 级法律应切合在第 1 级的现行法律和第 3 级的各个身份管理系统基于合约的操作规则之间。

- **（第 3 级）各个身份管理系统的操作规则：**第三级法律管辖私营部门的身份管理系统，由专为每个私营部门身份管理系统管理各自环境而拟订的基于合约的操作规则组成。与适用于所有身份管理系统的第 2 级身份系统法律不同的是，第 3 级的操作规则着眼于特定身份管理系统的独特要求。[14]这些操作规则可能非常详细，但必须符合第 1 级和第 2 级的法律。

45. 工作组的任务是制定一部概括第 2 级法律要素的文书。

图一

私营部门身份管理系统的法律框架：三级法律



B. 贸易法委员会的文书应涉及哪些方面？

46. 为避免采取“一刀切”的做法，妨碍私营部门身份管理系统的发展以及相关的商业活动，工作组制定的文书应仅涉及各个身份管理系统的操作规则无法解决的问题。此外，文书对第 1 级现行国家法律的修改和/或补充应仅限于鼓励

[14] 注意，在涉及公共部门身份管理系统的情况下，如国民身份系统，特定系统的操作规则体现在法规或条例中。因此，第 2 级和第 3 级法律合并在一起。

和促进发展私营部门身份管理系统以支持网上商业活动所必需的范围。为此，涉及第 2 级法律的文书的设计应：

- 消除第 1 级现行法律中妨碍私营部门身份管理系统发展的障碍并根除其中的不确定因素；
- 填补第 1 级现行法律中对私营部门身份管理系统的成功有重要影响、但无法通过合同解决的空白；并且
- 处理新的普遍适用的问题，以促进所有私营部门身份管理系统的发展。

47. 此外，鉴于身份管理系统性质各异，每个系统有独特需要，工作组制定的任何涉及第 2 级法律的文书都应坚持技术中性和身份系统中性的原则。特别是，鉴于如上所述私营部门身份管理系统所使用的结构和技术以及目的和市场多种多样，身份系统的中性至关重要。

48. 对比之下，WP.162 号文件的拟订反而规定了以下方面的规则：*身份管理服务提供人的义务*（第 6 条）、*身份管理服务提供人在发生数据泄露情况下的义务*（第 7 条）、*订户的义务*（第 8 条），*或身份管理服务提供人的赔偿责任*（第 12 条）。私营部门身份管理系统需要在各自的身份管理系统操作规则中处理这些问题。对于其中的每一个问题都需要采取独特的方法，根据所涉及的特定身份管理系统的结构、技术、目的和市场量身制定。任何处理上述等问题的尝试都难以成功，因为每一种身份管理系统处理这些问题的方法很可能大相径庭，如果对身份管理系统规定一刀切的方法，只会导致阻碍私营部门身份管理系统的发展。

C. 贸易法委员会文书纲要

49. 相反，工作组可处理的问题分为以下几类：[15]

- 明确承认操作规则对于身份管理系统管理的作用
- 第 1 级现行法律中未处理的问题，其性质决定无法通过基于合约的操作规则来解决。例子包括：
  - 对身份管理的法律承认[16]
  - 关于确定一项身份交易何时满足适用法律对识别某人身份的要求的规定[17]
  - 是否应评估私营部门身份管理系统的可靠性（如果是，如何评估）[18]
- 第 1 级现行法律在一定程度上解决了的问题，但对身份管理系统的适用性不确定，因此造成模棱两可的情况，可能成为身份管理系统的一

[15] 拟作为涉及第 2 级法律的文书将处理的潜在问题初步清单，但有待工作组展开并推敲，同时除其他要素外应以各种现有国家一级制度的需要为依据。

[16] WP.162 号文件，第 5 条试图处理这一问题。见附录中美国对第 5 条现草案的问题的评论意见。

[17] WP.162 号文件，第 9 条试图处理这一问题。见附录中美国对第 9 条现草案的问题的评论意见。

[18] WP.162 号文件，第 11 条试图处理这一问题。见附录中美国对第 11 条现草案的问题的评论意见。

个问题，因为这些问题难以在以合约为基础的操作规则中解决。例子包括：

- 现行侵权法对身份管理系统参与方的适用性；
- 关于过失性虚假陈述法律的适用性；
- 关于默示担保的现行法律的适用性

- 可能需要补充到现有法律中的问题，例如涉及：
  - 身份管理系统使用来自政府身份管理系统的信息的权利；
  - 身份管理系统使用政府签发的标识符（例如，社会保险号、国民身份证号等）的权利。
- 由于公共政策考虑，所有身份管理系统都应以同样方式处理的问题，无论这些问题是否可以通过基于合约的操作规则来处理，例如：
  - 是否以及（如果是）如何提供跨境承认[19]
  - 是否以及（如果是）如何从法律角度处理可靠性问题[20]

50. 一部包含这些要素的贸易法委员会文书将有助于各国制定第 2 级身份系统法律，这种法律旨在：(1)鼓励发展私营部门身份管理系统，(2)消除此种发展的障碍，(3)尽可能尊重和支持每个私营部门身份管理系统对于制定各自操作规则的需要。

[19] WP.162 号文件，第 10 和第 11 条试图处理这一问题。见附录中美国对第 10 和第 11 条现草案的问题的评论意见。

[20] WP.162 号文件，第 10 和第 11 条试图处理这一问题。见附录中美国对第 10 和第 11 条现草案的问题的评论意见。

Appendix[21]

Article-by Article Analysis of WP.162

In this appendix to our comments, we provide a detailed article-by-article commentary on WP 162. We reiterate, though, that we do not believe that a simple set of revisions to the text of WP 162 will result in a viable instrument. To achieve this, we believe the Working Group must make the conceptual and structural changes required to address the current reality of IdM systems that we set forth in Sections II and III of our comments.

Before turning to the article-by-article analysis, here is a summary of the U.S. concerns with WP.162:

(a) The definitions in WP 162 are both incomplete and based on a static model for IdM that is not reflective of the wide variety of actual IdM systems;

(b) WP.162 does not provide a basis for determining how and when the instrument would accede to or supersede existing laws that require identification in a specific form. The failure to provide guidance on this issue is compounded by the fact that articles 2, 5 and 9 contradict one another;

(c) The articles on obligations (art. 6–8) and liability (art 12) do not reflect the wide variations among types of IdM systems nor the multiple types of roles that may make up any specific IdM system. These one-size-fits all provisions do not accurately reflect the rights and obligations that different IdM system roles may have or expect in various IdM systems;

(d) We do not believe the provisions on cross-border recognition are workable without an enacting jurisdiction having some basis for assuming the reliability of a system in another jurisdiction. We do not believe this obligation is realistic.

Draft Article 1: Definitions

We believe the Working Group should revisit the definitions after the articles in the rest of the draft are concluded. Base on the current draft,[22] we make the following observations for consideration by the Working Group.

The term “electronic identification” may describe or be easily confused with the entire process of identity proofing, credential issuance, and authenticating the relationship between the credential data and an individual. Thus, we recommended that the Working Group consider whether there is an alternative term to “electronic identification” that could be used for the authentication process.

All the stages of the IdM process might collectively be defined as “identity verification.” The modifier “electronic” should not be used in this definition, however, since all or part of the stages of the IdM process might not be done electronically.

“Authentication” is used only in terms of trust services; it has the same meaning as “electronic identification”. We believe it could be misleading to have two terms for the same concept and would recommend using the same term for this concept throughout the draft. As noted above, however, we believe the term “electronic identification” itself may be misleading.

[21] The Appendix has been provided to Member States in English only. However, significant portions of the substance of the Appendix are a reproduction of the U.S. response to the Secretariat’s questionnaire for A/CN.9/WG.IV/WP.162, which has been circulated in all official languages as A/CN.9/WG.IV/WP.164 and Add.1.

[22] A/CN.9/WG.IV/WP.162.

As to the secretariat's inquiry whether there should be a definition of levels of assurance, we believe such a definition is unnecessary. We note the secretariat's proposed language provides that "identification factors are those factors that are necessary to make an electronic identification" In other words, the proposed definition does not provide any guidance; it simply restates the obvious. Moreover, we believe this proposed language could cause confusion, as it implies that there are specific factors that an IdM service provider must manage. Depending on the nature of the identity system involved, there could be numerous such factors. The relevant factors, however, will vary from IdM system to IdM system, and the responsibility for managing these factors will vary from system role to system role.[23] We note also that the proposed definition appears to combine two very different concepts: identity attributes (that vary depending on purpose for which identity is used), and identity processes that are used for identity proofing, credential issuance, or authentication processes.

Draft Article 2: Scope of application

The draft instrument provides that it "applies to the use and cross border recognition of IdM systems and trust services in the context of commercial activities and trade related services." As we discuss below, we believe the Working Group needs to closely examine how the draft instrument will apply to cross-border transactions, and how the rules in this instrument relate to existing legal requirements regarding identification and authentication.

Draft article 2(3) provides that "[n]othing in this [instrument] affects a legal requirement that a [subject][person] be identified in accordance with a procedure defined or prescribed by law." We understand this exclusion as being necessary as most if not all jurisdictions have some mandatory requirements for the form in which identification is to be made.

The question then is whether this section can be reconciled with articles 5(a), which provides that "The electronic identification of a [subject][person] shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that …[t]he identity proofing and electronic identification are in electronic form" and article 9(1) option A, which provides that " Where a rule of law requires or permits the identification of a [subject][person], that rule is satisfied with respect to IdM if a reliable method is used for the electronic identification of the [subject][person]."

We believe article 2(3) and article 5(a) might be reconciled by expressly clarifying these two sections to indicate that article 5(a) is not intended to overrule any other law, but is only intended to provide that, as between the parties, the law will not block the choice of the parties to use an electronic means of identification if the law would otherwise allow this under freedom of contract. This reading would appear to narrow the scope of article 5, and if the Working Group intended article 5 to have this limited meaning, this needs to be clarified in the text and comments.

We do find a more serious problem reconciling draft article 2(3) with draft article 9(1) Option A. These two sections, we believe, cannot be reconciled. Were the instrument intended to supersede all laws that may require a specific mode of identification, the instrument would risk being non-enactable. In addition, this interpretation would expressly contradict the language of draft article 2(3). In our view, the draft instrument provides contradictory rules: electronic identification meets the requirements of other legal identification requirements, and the instrument does not displace any other legal identification requirements. These conflicting rules

[23] This potential confusion raises the issue of whether draft article 6 may itself create minimum obligations that should not necessarily apply to all IDM service providers. In other words, article 6 may assume a one size fits all IDM service provider that does not reflect the multitude of existing and developing models.

cannot co-exist if the draft instrument. We view Option B of draft article 9 as essentially restating the rule of Option A. We believe the Working Group must re-examine these draft articles and reformulate them to express a non-contradictory policy that respects the existing legal requirements that are recognized in draft article 2(3).

Draft Article 3: Voluntary use of IdM and trust services

We believe both the current text of the draft[24] as well as the proposed new language by the secretariat[25] shows confusion on the role of consent. We suggest the Working Group examine the rule on consent to determine which parties are required to consent and the relationship between article 3 on consent and how it works with both article 2 and 5 on freedom or lack of freedom to choose the mode of identity management.

Draft Article 4: Interpretation

Although we appreciate that this language has appeared in prior model laws,[26] we note this language was drawn from the United Nations Convention on Contracts for the International Sale of Goods,[27] and it is language specifically tailored for an international convention. As such, we are not sure that it is appropriate for a model law that is drafted for domestic legislation.

Thus, for example, we are not clear on what the "international character" of the draft model law refers to. As the draft instrument is neither derived from international instrument nor intended to be used primarily in international transactions, we do not know what constitutes the instrument's "international character".

Moreover, although uniformity of interpretation is a useful admonition for an international convention,[28] the utility of this interpretive rule is not clear in an instrument designed for domestic legislation. When, as with an international convention, an autonomous interpretation is useful to create a universal understanding that parties can rely upon in international commercial transactions, the application of this rule is unclear and probably redundant for a domestic law.

As for the rule that the instrument should be interpreted on the general principles on which it is based,[29] we suggest that either the draft provide the guidance of what these principles are[30] or this rule should be removed. To do otherwise creates the risk of vagueness and uncertainty in the text.[31]

---

[24] A/CN.9/WG.IV/WP.162, draft article 3.

[25] "There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state that "Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person's][relying party's] consent. "?".

[26] UNCITRAL Model Law on Electronic Commerce (1996), article 3; UNCITRAL Model Law on Electronic Signatures (2001), article 4.

[27] United Nations Convention on Contracts for the International Sale of Goods (1980), article 7.

[28] We note this language is also derived from the CISG.

[29] A/CN.9/WG.IV/WP.162, footnote 23.

[30] We note that a statement of underlying principles was removed from the last draft.

[31] The Working Group may want to consider the comments of the World Bank in WP.163 to ensure that the Draft Provisions do not discriminate among IdM system models by including the concept of IdM system neutrality (or identity transaction neutrality). Because there are many different ways of conducting online identity transactions (e.g., single identity provider

Draft Article 5: Legal recognition of IdM

As we discussed above in our analysis of draft Article 2, we believe the Working Group needs to clarify how this rule is intended to work with identifications that are required to be in a specific form such as a driver's license or passport.

Draft Article 6: Obligations of IdM service providers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

As noted in the World Bank's comments,[32] the obligations set out in draft article 6 for IdM service providers assume a model where the IdM service provider provides all the services. This may not always be the case. There could be several parties that contribute to or provide part of an IdM service (e.g., trust providers, registrars, enrolment agents, credential service providers, stewards, authentication providers, hubs, etc.). Given the increasing diversity of IdM system models, the Working Group should consider whether it is still appropriate to restrict the definition of the roles or to impose a one-size-fits-all set of IdM service provider obligations. We believe the Working Group needs to address article 6 to consider the potential multiple parties that may contribute to the IdM service, and to consider whether it is still appropriate to impose a one-size-fits-all set of IdM service provider obligations.

Draft Article 7: Obligation of IdM service providers where there is a breach

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems. We agree that there should be some obligations by an IdM service provider where there has been a breach of security. As we noted note our comments to draft article 6, however, there may be multiple parties involved in the IdM service provider process.[33] For this reason, we believe the Working Group should reconsider the language of draft article 7 to reflect the various parties that may be involved in IdM process and accordingly fix the obligations based on the respective nature and status of these parties consistent with which party is best placed to respond to the breach.

Draft article 7 is limited to breaches that have "a significant impact". We do not understand what "significant impact "means in this context. In addition to being a

(IdP) systems, federated (multiple IdP) systems, user controlled/user centric systems, hub systems, DLT systems, systems without credentials, self-sovereign identity systems, etc.), it is important that these Draft Provisions do not require or assume a particular approach to the identification and/or authentication processes, or the system that delivers them. Thus, the Working Group should consider ways to ensure that these Draft Provisions do not imply and/or require a certain system model.

[32] A/CN.9/WG.IV/WP.163.

[33] We agree with the comments by the World Bank in WP.163 that the current draft compresses and confuses the distinction between and the respective roles of IdM systems and IDM service providers.

vague standard, we are not sure why a "breach" is not enough in and of itself to justify some remedial action by the entity that bore the risk the breach.

We are not sure what "remedies" are or should be available where there has been a breach of security.[34] We believe the Working Group should clarify this issue.

We do not know what "applicable law" refers to in 7(1)(c). If it refers to a notification obligation from the draft instrument, this obligation should be referred to. If this refers to law outside of the instrument, it is not clear what law would impose an obligation of notification.

Draft Article 8: Obligation of subscribers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We agree with the comments by the World Bank that the duties imposed on subscribers (particularly individuals, such as data subjects) in Article 8 may not be reasonable in all circumstances.[35] For example, there may be situations where an individual subscriber may be aware of circumstances indicating there may have been a compromise, but simply does not understand their significance.

We believe Article 8 should be clarified that it is not intended to impose these duties on relying third parties that have no contractual relationship with the issuing IdM service provider but who may nonetheless rely on a credential because:

(a) it would be difficult to enforce as it will likely be hard to identify such relying third parties;

(b) it imposes an undue burden on relying third parties to police identity system credentials for an IdM service provider with whom they have no relationship; especially when their use of and reliance on such credentials may be sporadic at best; and

(c) it is not currently required by law applicable to paper-based credentials (e.g., the bartender who refuses entry to a person because he determines that the person has presented a false driver's license or someone else's driver's license is not required to report that to the issuing authority).[36]

The requirement to notify in cases of a "substantial" risk seems problematic, as subscribers will likely have no way of knowing (and in most cases will not even be qualified to determine) what constitutes a substantial risk as opposed to some lesser risk.

Draft Article 9: Identification of a person using IdM

We address our concerns on draft article 9 in our discussion of draft article 2 above.

---

[34] See Draft article 7(1)(b).

[35] A/CN.9/WG.IV/WP.163.

[36] We also agree with the comments by the World Bank in WP.163 that if the draft is going to raise issues about third parties, more clarification would be useful as to which third parties are envisaged. We also note that if there is going to be a notification requirement on non-contracting parties, there needs to be some sanction for failure to notify, as otherwise the requirement is meaningless.

Draft Article 10: Factors relevant in determining reliability

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

Draft article 10 provides an illustrative list of factors to determine the reliability of an IdM service. If article 10 only applies to systems governed by contractual rules, it is not clear what the purpose of the list of possible considerations serve. This list is not useful to explain and interpret an otherwise applicable contractual agreement. If draft article 10 is intended to provide a minimal standard of reliability for IdM systems, then it is not clear how an illustrative and not a mandatory list would operate.

Moreover, it is not clear how this would override, if at all, otherwise agreed to contractual standards.

Moreover, in any given situation, there are numerous factors that may affect reliability. We question whether attempting to list them in these rules is appropriate in any event.

Draft Article 11: Designation of reliable IdM systems

Although this provision is made optional, as we note in our analysis of draft article 24, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

In addition, we believe this provision, as presently drafted, rests on the flawed assumptions that there are “recognized international standards and procedures” for determining the reliability of a IdM service, and that there is a centralized body that can make these determinations.

Draft Article 12: Liability of IdM service providers

As noted in Section III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We do not believe any of the three options in the current draft are sufficient. Both Options A and B state, albeit unartfully, that an IdM service provider will be legally responsible under otherwise applicable law outside of this instrument. If liability rules are to be included in this instrument, some guidance would be necessary. The term “applicable law” is vague. Does this refer to contract law, tort law, privacy law, data security law, etc. or all of them? If the answer is it could apply to any law otherwise deemed to be appropriate, then no function is served by this provision. Likewise, we have no idea what type of guidance is intended by the phrase “legal consequences”.

The word “damage” in option 3 we assume means “harm”, but as with all the options in the current draft, we fear no real guidance or standards are provided.

We suggest that the rules governing liability should likely vary depending upon the nature of the identity system, and will most likely to be determined by the applicable trust framework (subject, of course, to any existing law that cannot be varied by agreement).

At a minimum, we believe a further discussion is warranted on what type of liability the rules of the draft would invoke. We think a discussion of liability should go beyond service providers and consider liability for all parties that may come within the scope of the draft. We also believe that a discussion on contractual waivers to liability should be included in any discussion on liability. Further, as noted above, we do not believe that a universal one-size-fits-all approach to liability is appropriate in any event, as identity systems, their purposes, and their participants will vary widely.

Draft Article 13: Legal recognition of trust services

As we have noted, we believe trust services should be addressed in a separate instrument.

This provision states that a trust service may be provided in electronic form. As the purpose of a trust service is, in fact, to verify electronic data, this provision would appear to be tautological and unnecessary. If the intent of draft article 13 is to make clear that a third party may provide a trust service, that should be clarified.

Draft Article 14: Obligations of trust service providers

As a conceptual matter, this draft provision raises two questions. First, how does this provision interact with contractual obligations that a trust service provider may have to remedy a breach of loss of integrity? If the intent of Article 14(2) is to impose obligations for breaches or losses of integrity that are not covered by contract (i.e., because it refers to impact on the trust service itself), this should be made clear.

If the intent is to impose some minimal obligation on trust service providers below which the parties cannot contract, this should be expressly stated. If that is the intent, we believe the Working Group should address the question of mandatory rules and their relationship to freedom of contract.

A second question unexamined in this draft provision is the question of the consequence for failing to meet the obligations set out in Article 14? If a trust service provider fails to fulfil a contractual obligation owed to a customer, then customer/other party to the contract could pursue a contract claim. Article 14 does not appear to impose any consequences or sanction for failure to fulfil the obligations set out therein, assuming they are distinct from contractual obligations.

Draft Article 15: Obligations of trust service providers

This draft article, as with draft article 14, purports to impose obligations without any corresponding sanctions. As we mentioned in our comments to draft article 12, we believe the Working Group needs to examine fully the question of liability throughout the draft instrument.

Draft Articles 16–20: Various trust services

Articles 16–20 address the issue of the validity of a data message (such as an e-signature) and not the use of a trust service to validate the data message. In some cases, such as with e-signature, there is already existing law that governs the validity of the data message itself (this was the subject of the United Nations

Convention on the Use of Electronic Communications in International Contracts and the UNCITRAL Model Law on Electronic Signatures). But in any event, because these provisions are not concerned with trust services, they do not belong in this instrument.

Draft Article 21: Website authentication

As drafted, article 21 appears to confuse the authenticity of the website, which is the true concern, with the owner of the domain, which does not prove the authenticity of website itself. We believe the Working Group should reconsider this draft article to provide a rule that achieves its intended purpose.

Draft Article 22: Identification of objects

We do not believe the identification of objects should be covered in the draft. We also note that given the limited scope of trust services in the draft, that being to verify information (data messages), the identification of objects is more appropriately covered in the provisions on identity management and not trust services.

Draft Article 23: Reliability standards for trust service providers

While Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact with contractual agreements. As contract underlies trust service relationships, we believe this is an essential clarification that the Working Group should explore.

Draft Article 24: Designation of reliable trust services

Although this provision is made optional, as we have noted in our analysis of draft article 11, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

As we noted with our analysis of draft article 11, this provision ought to be reconsidered as it rests on flawed assumptions. These assumptions include, for example, that there are “recognized international standards and procedures” for determining the reliability of a trust service, and that there is a centralized body that can make these determinations. Moreover, while Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact altogether with contractual agreements.

Draft Article 25: Liability for trust service providers

We think this section needs to be reconsidered. Option A, which leaves liability to otherwise applicable law, should be clarified to state whether it includes both contact and torts, and if it includes contractual liability, the extent to which, if at all, the liability may be excluded. As with our concerns with Option A, we believe Option B is too vague because we are not sure what the scope of “legal consequences” entails. Option C provides tort liability but leaves open the question

of contract responsibility. This should be clarified. We note we expressed similar concerns with the current drat of Article 12.

Draft Article 26(1): International aspects of the draft law

Given that modern commercial transactions often transcend national borders, we believe cross- border recognition is an admirable and hopefully achievable goal in this and any commercial law instrument. We are concerned, however, that the current draft does not provide adequate standards and guidance to achieve this goal.

Draft article 26(1) provides that: "An IdM system operated or a trust service provided outside [the enacting State] shall have the same legal effect in [the enacting State] as an IdM system operated or a trust service provided in [the enacting State] if it offers a substantially equivalent level of reliability." We believe this raises two issues that we believe deserve consideration by the Working Group.

First, the language of draft article 26(1) is derived from article 12 of the UNCITRAL Model Law on Electronic Signatures.[37] However these two articles serve significantly different functions. Article 12 of the MLES provides for non-discrimination of a certification service provider that verifies the public key of a PKI transaction. This quite limited function allows parties to choose a third-party certification provider to verify the authenticity of a signature between two parties who have chosen the third-party certifying provider. This is a simple application of freedom of contract.

Unlike article 12 of the MLES, draft Model Law article 26 would impose an obligation on all parties who rely on IDM systems and trust service providers that reside in other jurisdictions without these relying parties necessarily having the ability to choose the providers and therefore evaluate the risks attendant to the choice of a specific provider. These third parties in reliance on the IDM and trust services systems would not normally have any power to choose the providers and therefore would have to rely on assurances of providers outside the jurisdiction of the enacting state.

It is this broader scope of application of draft article 26 that suggests that article 12 of the MLES may not be the appropriate rule for IDM and trust services.

The second concern we have is whether the standard of "substantial equivalent level of reliability" (also taken from article 12 of the MLES) is either meaningful or realistic. The language itself is vague, but more importantly this standard raises a fact question that would be burdensome and expensive to prove or disprove. To meet the standard, a party would have to show both the level of reliability of the domestic system as well as the level of reliability the non-domestic system and then make some qualitative judgment on substantial equivalence. This, we believe would be unduly burdensome for parties.

We note that, for example, the recognition of foreign IDM and trust service providers under eIDAS requires an extensive and complex verification process in which each respective country in the European Union participates. This provides a level of reliability and certainty that minimizes the risks for parties relying on a non-domestic system. Thus, under the eIDAS, the "substantial equivalence" has already been established for parties relying on any respective system within the European Union. Outside such a closed system such as eIDAS, the burden on parties to prove or disprove "substantial equivalence" would itself be substantial. We think it is important to note that this is not primarily a legal but is a factual and technological question that is not easily resolved by a vague legal mandate.

This issue of "substantial equivalence" is further complicated, we believe, because what parties that use IDM and trust service systems understand about the systems is

[37] UNCITRAL Model Law on Electronic Signatures (2001), article 12.

often quite different from the underlying technological structure of those systems. Most parties who must rely on IDM and trust services are not in a position to evaluate the reliability of the systems, and therefore the parties must assume reliability with the knowledge that if the systems are certified and responsible under the domestic law, the parties will have recourse under the domestic law in the case of failure. But where the domestic law, as in draft article 26 only provides protection to parties if the parties can show "substantial equivalence" of a foreign system.

Draft Article 26(2): International aspects of the draft law

Draft article 26(2) provides that "recognized international standards' shall be used to determine "substantial equivalence". We appreciate the aspirational nature of this provision. We believe, however, before adopting this provision, which was borrowed from article 12(4) of the MLES, this provision should be further discussed by the working group to determine its applicability to the draft law. We see two points which should be discussed. First, we are not certain at this time that there are generally recognized international standards in this evolving area of the law and technology. At best, we believe that the rule should also provide for evolving standards as a basis for determining equivalence. Guidance would be most useful in how these standards should be determined. Moreover, irrespective of the standard, we note that this involves a factual issue of technological reliability that creates a substantial burden on parties to prove what "international standards" are.

Draft article 27: International Aspects of the Draft Law

We find article 27 an admirable but possibly impractical rule as may place a burden on the enacting states of significant obligations to coordinate and cooperate with foreign entities. We would not want to discourage this cooperation, but merely to ensure that it is optional and not mandatory. Legislation that creates a significant financial burden on the state often creates an impediment to adoption. This section risks posing a financial burden on the governments of jurisdictions that adopt this law that go shifts the risks of using foreign IDM and trust services providers on the respective governments instead of the private parties that choose to use these systems.

Although this may be a useful and possibly mandatory provision in a law that is designed to provide government created or recognized IDM or trust services that may be used in cross-border transactions, we are not convinced that this burden on governments is not excessive for the draft law that is designed for privates users and private providers.

We suggest that if this provision is retained, it be placed in brackets with commentary that explains fully the obligations this article would impose on the enacting jurisdiction. We suggest this article be optional for those states that have or would be willing to develop the cooperative framework necessary to implement this article.