



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

各国政府和国际组织意见汇编

目录

	页次
二. 意见汇编.....	2
F. 金融与贸易银行家协会.....	2
G. 多民族玻利维亚国.....	4
H. 伊朗伊斯兰共和国.....	4
I. 保加利亚.....	8
J. 新加坡.....	9



二. 意见汇编

F. 金融与贸易银行家协会

[原件：英文]

[2022年5月27日]

1. 金融与贸易银行家协会感谢有机会就“关于使用和跨境承认身份管理和信任服务的示范法草案”发表意见。
2. 金融与贸易银行家协会是一个国际金融服务行业协会，其成员包括全球多个金融机构和金融科技公司。作为一个在国际金融服务方面展开分析、讨论和宣传的全球论坛，金融与贸易银行家协会近 300 个成员在维护全球金融体系的安全和高效运营方面发挥着领导作用。金融与贸易银行家协会的成员机构将国际贸易金融的数字视为行业主要优先事项，而身份管理是数字化取得进展的一个关键组成部分。
3. 建立身份管理的需要贯穿国际交易银行业务的许多方面，包括贸易融资、供应链融资、支付以及诸如了解您的客户和反洗钱等合规领域。因此，金融与贸易银行家协会完全赞同贸易法委员会在拟订示范法草案方面所做努力。
4. 在全球交易银行业务中，有力求给该业务提供完全数字化生态系统的几条行动路线。数字化大有可为；然而，迄今所获成就和采纳方面的速度不能说是令人满意的。很明显，数字化不会以“大爆炸”方式突然发生，而是将通过相辅相成的举措稳步推进。
5. 市场需要有明确的规则，以便能够在日常运营中推进数字化。在这方面，国际商会、亚洲开发银行和新加坡政府启动了数字标准倡议¹，以处理同各平台的标准和互操作性以及与金融科技的关系有关的问题。在法律支持方面，它制定了旨在鼓励各国政府就《贸易法委员会电子可转让记录示范法》²（《电子可转让记录示范法》）所倡导的数字业务颁布具体法律的路线图。金融与贸易银行家协会参与了推动全球采用《电子可转让记录示范法》的努力。除了法律框架外，该行业还在努力制定互操作性标准。2020年8月，金融与贸易银行家协会发布了“分布式分类账支付承诺——行业最佳实践”，³就在分布式分类账上执行的互操作支付承诺制定行业指南。
6. 现有的示范法草案为身份管理和信任服务提供了总体框架；但是避免遵循甚至最低限度的规范性做法。它明确指出，“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。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。”
7. 示范法草案预期身份管理服务将具有第 10 条所要求的可靠性要求，但没有规定应如何制定保证级框架。示范法草案确认，国际层面是使用身份管理和信任服务

¹ 国际商会数字标准倡议，2020年3月。

² 《贸易法委员会电子可转让记录示范法》（《电子可转让记录示范法》），2017年7月。

³ 金融与贸易银行家协会：分布式账本支付承诺，2020年5月。

及乃至于使用电子服务的关键。然而，该案文确认，存在两类障碍：(一)导致缺乏互操作性的技术上的不兼容，及(二)影响跨境承认的法律障碍。

8. 特别是为了给克服这两个障碍指明方向，金融与贸易银行家协会将支持示范法草案直接提及全球法人机构识别编码基金会⁴在实施法定电子身份识别特征方面所做的大量工作和取得的进展。全球法人机构识别编码系统是一个得到监管机构认可的系统，它为法律实体提供了得到全球认可和信任的电子身份识别机制。法人实体识别编码是一种联结得以清晰独一无二识别法律实体的关键参考信息的全球标准（ISO 17442）。2011年在G20国集团的建议下，金融稳定委员会成立了瑞士非营利基金会全球法人识别编码基金会。其活动由来自50多个国家的65名监管者和监管监督委员会的19名观察员负责监督。

9. 公开可用的法人实体识别编码数据池可以被视为大大提升在全球市场中透明度的一个全球目录。法人实体识别编码是一种涉面广泛的公共物品，应对此善加利用以确保国家和国际层面的技术兼容性。

10. 示范法草案旨在经由立法协调统一相关规则。这种方法将导致存在多种国家技术标准，而这意味着，既没有互操作性，又消耗了试图解析和理解异构数据的各种资源。使用繁杂多样的身份识别编码及其所依据的国家技术标准会妨碍以可靠、同质和可比方式识别电子交易中各方当事人的能力。因此，虽然贸易法委员会可能希望避免有任何技术上的偏好并保持其技术中立的立场，但它应考虑把法人实体识别编码作为基本的身份识别特征纳入案文草案，以便利跨境识别和核实法律实体。全球法人实体识别编码系统并非某种技术上的选择。它是20国集团设想的由金融稳定委员会加以实现一种公共产品。

11. 考虑到身份识别编码参考数据已经列入关于实体的本地登记编号、地址信息、对数据最近一次更新的时间戳及对数据字段进行更新的信息，它有可能在全球推动实体数据的一致性。

12. 示范法草案已经承认，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；经由便利遵守监管要求降低交易成本；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方案为弥合数字鸿沟做出贡献。

13. 如果有互不相同的做法，第27条建议，可以展开合作以促进就技术标准的共同定义包括就保证级和可靠度达成一致。然而，互有竞争的国家利益可能会阻碍或至少会延误就所需技术标准及其他基本数据优质框架达成协议。贸易法委员会率先将身份识别编码设定为法律实体身份识别的主要识别编码，可以加快跨境电子身份识别实施工作的进度，并利用监管机构为克服国家/区域/私人身份识别方案的缺陷而建立的系统。作为一个成熟的功能系统，身份识别编码提供了一个互操作并且技术上独立的解决方案。

14. 全球交易银行业务的数字化转型能够降低成本、提高效率、改善监管控制、降低风险，并为全球经济中的利益相关方带来合作的机会。身份管理的创设和调整是在数字化进程中迈出的关键的第一步。身份识别编码是关于法律身份识别的唯一的全球标准，这就是金融与贸易银行家协会赞同将其列入示范法草案案文的原因所在。

⁴ GLEIF（全球法人识别编码基金）（www.gleif.org）。

G. 多民族玻利维亚国

[原件：西班牙文]
[2022年5月27日]

多民族玻利维亚国电信和运输管理局提交了以下关于示范法草案的评论和意见以供审议。

第6条. 身份管理服务提供人的义务

评论/意见：

建议将确保电子身份或电子签名验证系统的在线可用性和正确运行视为一项义务，经由该系统得以有可能核实签名人身份和来源国授权认证实体信任链的有效性。

第16条. 电子签名

评论/意见：

建议考虑建立检测对数据电文的任何改动并确保数据电文真实性、完整性和不可否认性的机制。

第17条. 电子印章

评论/意见：

对于数据电文真实性、完整性和不可否认性，以及其法律有效性和证据有效性，应根据身份管理服务提供商所在国的法规予以确保。

H. 伊朗伊斯兰共和国

[原件：英文]
[2022年5月30日]

1. 适用范围

使用和跨境承认身份管理和信任服务

1. **问题：**根据贸易法委员会关于协调统一国际贸易法并使之现代化的任务授权，并鉴于赋予第四工作组的消除国际电子商务障碍的任务，伊朗伊斯兰共和国认为，示范法的适用范围很广，需要仅限于涉及外国事实要素的国际领域和情形。换言之，根据我们的理解，在国内使用和承认身份管理和信任服务的情况下，如果不包括任何外国要素，并且身份管理和信任服务的生命周期中涉及的所有参与者都在同一个国家，则对此种情况及国内事务，都应由各国国内法管辖。

拟议解决方案

2. 建议将示范法的范围局限于身份管理和信任服务的跨境使用和承认，并澄清本文书的目的并非是干预与身份管理有关的国家基础设施和在成员国建立的信任服务，也不是凌驾于管辖其国内事务的国内法之上。与此同时，我们注意到，如果颁布国愿意的话，则仍有颁行管辖权以将该文书适用范围延伸扩大至其国内事务的余地。

与贸易有关的服务

3. **问题：**关于第2条中的“与贸易有关的服务”这一术语，应当指出的是，尽管在解释性文件第95段中对此作了解释，但根据我们的理解，这一术语仍然模糊不清，不容易为用户所识别，对其的解释可能超出示范法所述范围，或者可能不当涵盖一国在身份管理和信任服务领域中与贸易不一定有关的所有现行系统。

拟议解决方案

4. 建议示范法侧重于商业活动中遇到的情形。尽管如此，解释性说明可以澄清，“示范法中的规定概不妨碍颁布国将示范法的范围延伸扩大至涵盖贸易相关服务中对身份管理和信任服务的使用和跨境承认”。

2. 保护国家主权和公共政策

5. **问题：**我国代表团就该示范法对其国民或企业系跨境身份管理和信任服务用户的国家的主权问题的隐含影响表示关切。足以理解此种关切的做法是，从发展中国家角度审视市场现实情况及这些国家所有相关部门被在数字方面领先的若干国家向全世界用户提供服务的全球数字公司所支配的情况。此外，数字服务提供商在身份管理服务领域的参与，在其事先没有受相关政府委托从事这项任务时，特别是在其收集的属性与个人基本身份密切相关时，则不仅可能是不合理的并且造成不可信的结果，而且鉴于国家对本国公民整个生命周期身份管理享有专属权限，这种情况可能会导致对国家行使其主权职能的干涉。这种现象还可能导致发展中国家失去数据、技术和网络主权，以及强制性法律无法对其公民提供保护。如果人们看到发展中国家的从属地位及其在全球贸易论坛上所面临的选择加入由聚集了多数大型数字公司的少数国家主导的全球数字经济模式的巨大压力，此种做法的有害后果就变得更加明显。因此，伊朗伊斯兰共和国坚定地认为，如果发展中国家要获益于国际组织的工作，它们首先就应该能够维护本国的主权和公共政策。在此背景下，我们认为示范法关于使用和跨境承认身份管理和信任服务的条文没有明确提及保护国家主权、平等和不干涉完全属于其国内管辖权范围内的事务。

6. 维护颁布国的公共政策同样重要。如今，跨境数据流动和外国服务提供商获取其他国家国民和企业的数据，已成为许多发展中国家所关切的重大公共政策问题。不同于贸易法委员会先前的法规（例如《电子可转让记录示范法》第6、7、8、11、12、15和17条），本示范法未设有必要时限制文书范围或对其任何条款的效力加以限定的程序，特别是为了颁布国公共政策的目的是。我们认为，由于本示范法的适用可能涉及本应由每个国家自行处理的各种公共政策问题，因此应允许有一定程度的灵活性，从而让颁布国的法院或负责适用示范法的主管机构能够基于包括其公共政

策理由在内的强制性理由，拒不承认或取消使用外国身份管理或信任服务所产生的法律效力。

拟议解决方案

7. 该文书应明确澄清，示范法的实施应尊重国家主权、平等和不干涉其内政。此外，本文书不得授权外国身份管理/信任服务提供商履行属于主权性质的职能，这些职能根据其国内法完全属于国家的权限范围。同样，预计将在解释性说明 F 节把该事实称之为一般原则和关键概念。

8. 为了回应就公共政策所持关切，并为了与贸易法委员会在其先前法规中所持传统立场保持一致，似宜考虑以下三种选项：

第一选项：在示范法中列入一些规定，允许颁布法域对违背其公共政策的情况排除适用本文书的某些条文或排除其效力（在贸易法委员会先前法规中有这方面的若干先例）。

第二选项：有可能允许某些条款的措辞有一定程度的灵活性，从而减少其绝对适用性。例如，在第 10 条第 3 项和第 22 条中添加大意如下的一句话：“在确定方法的可靠性时，除非裁决机构认为有必要，否则不应考虑……”。同样，可对第 11 条第 4 款和第 23 条修改如下：“在指定身份管理/信任服务时，除非[颁布法域指定的主管个人、公共或私人机关或机构]认为有必要，否则不应考虑……”。此外，将第 25 条和第 26 条中的“应”改为“可”，不仅可以让所引用条款的措辞为了顾及公共政策方面的关切而具有灵活性，而且鉴于 25(2)条和第 26(2)条中的国际公认标准不明确，似乎也更加明智。

第三选项：如果上述两种选项都不可行，则有必要在示范法中提供一条一般性规则，提及公共政策例外，并将细节留给各颁布法域在其法律中具体规定。

3. 压倒一切的强制性法律

9. **问题：**如今，身份管理/信任服务提供商正在向其他国家的国民和企业提供服务。虽然此种现象不可避免，是全球电子商务的一个不可或缺的因素，但应采取预防措施，确保服务提供商遵守相关的压倒一切的强制性法律，而不允许有任何减损。

10. 伊朗伊斯兰共和国意识到该文书事实上并不影响在其规定范围内可能产生的任何强制性法律的适用，并且还意识到示范法无意干涉国际私法规则的运作。尽管如此，我们仍然坚定地认为，需要在本文中列入一项落实身份管理或信任服务提供商国或接收国强制性法律的具体规定。之所以要采取这种做法，有这样几个原因。第一个原因与服务提供商获取所述国家公民、企业和组织的数据有关。考虑到数据是一个宝贵的来源，如果属于域外服务的情况，则可能会落入外国服务提供商的手中，我们认为，如果将数据置于服务被提供国或服务接受国保护制度和强制性法律之下，数据所有者将处于最有利的地位。第二个原因是国际私法中没有一条具体规定适用法律和保护电子商务服务用户的压倒一切的强制性规则的明确规则。虽然在消费者合同中就保护消费者的适用法律似乎存在普遍共识，但在与数字服务提供商签订的合同中，在保护用户方面可能会出现模糊不清的情况，因为这可能不属于消费者保护法的范畴。第三个原因涉及合同对用户和服务提供商之间的规定有欠平

衡。当涉及在数字环境中订立合同并同意其适用的操作规则、政策和惯例时，用户往往处于不对称的地位。我们认为，用户和服务提供商之间的合同所纳入的条款大多是未经谈判的，通常包含适用法律或诉讼地选择条款，这些条款对服务提供商更为有利，而对用户不利。如果根本不提及或不执行根据本示范法被提供服务或接受服务的国家的法律，则用户将得不到他们有权得到的必要保护。

拟议解决方案

11. 寻找适当保障措施和解决方案以应对上述关切要求在多数时候是跨境服务接受方的发展中国家的充分参与下加强国际合作和政策对话。尽管如此，以下是我们提出的一些建议：

- “身份管理/信任服务提供商的业务规则、政策和做法符合其服务被提供地或服务接收地的强制性法律”应是身份管理/信任服务提供商在第 6 条和第 14 条中应遵守的义务，也是在确定第 10(2)条、第 22(2)条中的方法（事后）的可靠性以及在第 11(2)(a)条和第 23(2)(a)条中指定可靠服务（事前）时应予考虑的一个因素，也是第 25 条和第 26 条所载在申请跨境服务时申请授予法律效力的一个标准。
- 为了落实服务被提供地或服务接受地的强制性法律，需要在第 6 条和第 14 条中给服务提供商规定进一步的义务，这可以在解释性说明第 113 和 175 段中加以进一步阐述。例如，服务提供商与服务被提供国或服务接受国的执法机构展开合作（例如，对数据保护事项或关于包括对犯罪的刑事预防、调查、侦查或起诉等可能导致侵权或刑事责任的情况），并为此目的在该国设立办事处或指定相关代表，根据服务被提供地或服务接受地的强制性法律修改服务条款和服务提供商的政策等等。我们认为，违反这些义务构成根据第 12 条和第 24 条确定身份管理/信任服务相关责任的依据。
- 遵守上述义务可有助于实现第 25 条和第 26 条中关于相互承认的目标。因此，颁布法域经由第 27 条中的信息交流规定其强制性法律的要求是非常可取的。此种信息可以让希望在域外提供服务的外国服务提供商提前根据相关规章修改其服务条款和政策。对此种合作的细节可以在解释性说明第 234 段中加以进一步阐述。

4. 自愿使用身份管理服务和信任服务

12. **问题：**伊朗伊斯兰共和国对示范法第 3 条第(2)款中根据一人的行为推断其同意表示关切。虽然这是贸易法委员会先前法规中的一项既有规则，但我们强烈认为，对于技术知识贫乏的人来说，这是不公平的，他们不一定意识到这样一个事实，即注册一项服务或使用一种特定的电子商务软件，即意味着他们允许使用由该软件提供支持的身份管理或信任服务。此外，如果人们看到用户在缔结数字合同时所持的“要么接受要么放弃”的立场，以及有时他们盲目接受给他们规定的条款和条件，那么这种情况就可能会产生更多的负面影响，这些条款和条件就可以推定他们已表示同意合同条款和条件的情况作了具体的规定。我们想提请贸法会注意这样一个事实，即尽管欧洲消费者通过不公平合同条款指令（93/13/EEC）而免受不公平标准合同条款的侵害，但在我们看来，欧洲以往的其他国家普遍没有这方面的法律。

拟议解决方案

13. 我们建议对经由行为推断一人同意使用身份管理/信任服务给予一定的灵活性，并强调对此种默示同意应以更清晰、更可预测的方式加以确定。因此，成员国适宜就该问题展开更详细的讨论，并就如何更好满足数字环境下合同的这一要求找到解决方案。我们认为，适宜对当事人的默示同意采取一种稍后可予以反驳的推定形式。

5. 电子存档

14. **问题：**我们注意到示范法并不影响适用于数据隐私和保护的法律。尽管如此，由于该法律领域与电子存档密切相关，我们认为需要根据第 19 条强调，在电子存档方面，必须适当考虑数据隐私和保护方面的强制性法律。关于与本案相关的强制性法律，应注意跨境身份管理/信任服务提供商的职能及其对其他国家公民、企业和组织的数据的密切依赖。鉴于此类数据的跨境传输构成重大公共政策问题，并可能剥夺用户有权享有的数据保护制度，我们认为，本示范法应当有赋予服务被提供国或服务接收国和用户接收此类服务国数据保护法以法律效力的空间。伊朗伊斯兰共和国希望提请贸法会注意这样一个事实，即虽然欧洲的数据主体在《欧洲一般数据保护规章》所涉广柔地域范围内得到保护，但其他地方特别是在第三世界国家可能没有类似的涉面广泛的规章，这些规章对外国服务提供商具有强制性，并且可能会迫使他们遵守服务被提供地或接受地的保护法。

拟议解决方案

15. 在第 19 条下明确重申：“第 19 条对文件、记录或信息的保存应遵守数据隐私和保护法方面的适当保障措施”。为了回应上述第二个问题，我们建议插入内容大致如下的一段，即电子存档不会剥夺跨境身份管理/信任服务的用户或服务接收地有权享有的数据保护制度。

6. 缺失的项目

16. 为了编写在许多方面更加全面的案文，应考虑在示范法中列入一些缺失的项目。例如，第 1 条中“保证级”、“可靠度”和“依赖方”等术语的定义，描述依赖方的权利和义务，并对用户权利采取明确和更全面的做法。

I. 保加利亚

[原件：英文]

[2022 年 6 月 8 日]

1. 保加利亚国家和欧洲联盟（欧盟）关于电子身份和信任（认证）服务的法律是基于有关内部市场内电子识别和信任服务及废除欧盟第 1999/93 号指令的电子交易信任服务的欧盟第 910/2014 号条例。《电子文件和电子认证服务法》第 32 条界定了监管委员会的权力，根据该法律，监管委员会是电子认证服务领域的国家监管机构，负责执行上述欧盟条例的规定。

2. 欧盟第 910/2014 号条例为在欧盟成员国使用认证服务建立了一个共同的法律框架，该条例第 14 条就承认来自欧盟以外国家的认证服务作了规定。根据《欧洲联盟运作条约》第 218 条，在欧盟与相关第三国或国际组织缔结协定的情况下，此类服务可得到承认。

3. 鉴于上述情况，保加利亚监管委员会认为所提交的由贸易法委员会编拟的示范法草案符合欧盟第 910/2014 号条例所述主要目标和原则。

J. 新加坡

[原件：英文]

[2022 年 6 月 13 日]

1. 新加坡赞赏第四工作组就使用和跨境承认身份管理和信任服务的示范法草案而开展的工作。

2. 我们希望提请委员会注意示范法草案（载于 A/CN.9/1112）中值得认真考虑的三个方面，其内容概述如下。

(a) 第一个方面涉及需要：

(一) 更明确地表述第 9 条和第 10(1)条（身份管理服务）之间的关系，在第 9 条中插入“根据第 10(1)条”一语，做此修改后第 9 条中该短语的内容是：“如果为此目的就对个人进行电子身份识别使用了第 10(1)条规定的方法”；及

(二) 更明确地表述第 16 至 21 条中每一条与第 22(1)条（信任服务）之间的关系，在第 16 至 21 条中的每一条中插入“根据第 22(1)条”的字样，做此修改后的第 16 至 21 条中相应短语的内容为“如果使用第 22(1)条规定的方法……”。

（见下文第 3 和第 4 段的详细讨论）

(b) 第二个方面涉及保留第 10(1)(b)条（关于身份管理服务的可靠性）和第 22(1)(b)条（关于信任服务的可靠性）所体现的“安全条款”的重要性。这些安全条款反映了 2007 年《联合国国际合同使用电子通信公约》⁵第 9(3)(b)(c)条和 2017 年《贸易法委员会电子可转让记录示范法》第 12(b)条的条款，力求避免虚假的法律质疑（即所用方法在理论上既不当也不可靠），规定一种方法在事实上证明已经实现第 9 条所述功能或第 16 条至第 21 条所述相应功能（即事实上的可靠性）的情况下即满足第 9 条或第 16 条至第 21 条的要求，这可以由其本身或连同进一步证据加以证明。我们认为，第 10(1)(b)条和第 22(1)(b)条是防范此类虚假质疑的重要保障，应当以同样的形式予以保留。此外，删除（或移动）第 10(1)(b)条和第 22(1)(b)条将使示范法草案与《电子通信公约》和《电子可转让记录示范法》不相一致。在此种情况下，贸法会将需要(a)就加入《电子通信公约》或已颁布《电子可转让记录示范法》的国家应如何处理不相一致的问题发表意见；和(b)决定贸法会是否将继续向考虑加入《电子通信公约》或执行《电子可转让记录示范法》的国家推荐《电子

⁵ 《电子通信公约》第 9(3)(b)条规定了用于制作电子签名的方法的可靠性要求，与第 10(1)条规定了用于电子身份识别的方法的可靠性要求类似。

通信公约》和《电子可转让记录示范法》(其条文不相一致)。我们建议对解释性说明草案第 142 和 143 段进行修订,以便更准确地描述第 10(1)(b)条草案的目的和效力。

(见下文第 5 至 16 段的详细讨论)

(c) 第三个方面涉及第 25 条和第 26 条中“至少同等可靠度”一语。我们认为,要求把可靠度完全等同作为交叉承认外国身份管理服务或信任服务的先决条件是不可行的。对可靠度无法精准确定,要求完全等同必然会给跨境承认带来实际困难。“基本等同或更高层次的可靠度”一语⁶在多边环境下更为合适。

(见下文第 17 至 19 段的详细讨论)

一. 第 9 条与第 10(1)条的关系以及第 16 至 21 条与第 22(1)条的关系

3. 示范法草案的结构如下:

(a) 第 9 条规定了对个人使用身份管理服务识别身份的功能等同规则,而第 10(1)条规定了第 9 条中的身份识别方法必须符合的可靠性要求。

(b) 同样,第 16 条至第 21 条规定了电子签名(第 16 条)、电子印章(第 17 条)、电子时间戳(第 18 条)、电子存档(第 19 条)、电子挂号递送服务(第 20 条)和网站认证(第 21 条)的功能等同规则,而第 22(1)条规定了第 16 条至第 21 条提及的每种方法都必须符合的可靠性要求。

4. 我们认为,第 9 条和第 10(1)条之间的关系以及第 16 条至第 21 条中的每一条款和第 22(1)条之间的关系应当更加明确,在第 9 条“如果一种方法”之后紧接着插入“根据第 10(1)条”,并在第 16 条至第 21 条中每一条之后紧接着插入“根据第 22(1)条”的词句。这就明确说明如果使用第 10(1)条或第 22(1)条所述方法来履行职能,即满足了要求,从而避免暗示任何方法均已足够。这些条款修订稿载于下文附录。

二. 第 10(1)(b)条和第 22(1)(b)条

A. 防止虚假的法律质疑

5. 示范法草案第 10(1)条规定如下:

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。

6. 示范法草案第 22(1)条具有类似的结构,规定如下:

⁶ 工作组第六十三届会议审议了这一术语。

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
- (b) 事实上证明已经履行了本条所述功能。

7. 有关的“安全条款”载于第 10(1)(b)条和第 22(1)(b)条。它们反映了《电子通信公约》第 9(3)(b)(二)条和《电子可转让记录示范法》第 12(b)条的相同目的, 即防止对有效性的虚假法律质疑。

(a) 《电子通信公约》第 9(3)条载有关于电子签名的功能等同规则, 其内容如下:

3. 凡法律要求一项通信或一项合同应当由当事人签字的, 或法律规定了没有签字的后果的, 对于一项电子通信而言, 在下列情况下, 即满足了该项要求:

(a) 使用了一种方法来鉴别该当事人的身份和表明该当事人对电子通信所含信息的意图; 以及

(b) 所使用的这种方法:

(一) 从各种情况来看, 包括根据任何相关的约定, 对于生成或者传递电子通信所要达到的目的既是适当的, 也是可靠的; 或者

(二) 其本身或连同进一步证据证明事实上已完成了以上(a)项所述的职能。

《电子通信公约》第 9(3)(b)(二)条旨在处理的问题是对电子签名的有效性提出虚假法律质疑的可能性, 该质疑所持理由并非是所称签名人没有签名或已签名文件遭到篡改, 而仅仅是所用签名方法在当时的情况下既不可靠, 也不合适(即原则/理论上的可靠性在当时的情况下并不合适)。⁷第 9(3)(b)(二)条规定, 经证明所用方法符合第 9(3)(a)条所述功能, 也就是说, 经显示所用方法事实上是可靠的, 即可挫败此种虚假的法律质疑。

⁷ 对《电子通信公约》的解释性说明第 164 段就此做了详细的解释(转载如下):

“164. 不过, 贸易法委员会认为, 公约不应允许一方当事人在其实际身份及实际意图可以被证明的情况下仍然借助‘可靠性检验’来否认其签字。电子签字必须‘既是适当的, 也是可靠的’这一要求不应使法院或事实检验者即便在对签字人的身份或签字这一事实没有任何争议, 即电子签字的真实性没有任何问题的情况下, 仍以电子签字并不**适当**可靠为由判定整个合同无效。这种结果将非常令人遗憾, 因为这将允许一桩需要签字的交易的当事人以否认其签字(或另一当事人的签字)有效的方式来设法逃避承担其义务, 其所持的理由并不是所称的签字人未予签字或所签字的文件遭到篡改, 而只是所使用的签字方法在这些情形中**既不可靠也不适当**。为了避免出现这种情况, 第 3(b)款规定, 所用的签字方法无论原则上是否可靠, 只要事实上被证明已经鉴别了签字人的身份并表明了该签字人对电子通信所含信息的意图, 即应认为该签字方法有效。”

[粗体强调]

(b) 出于同样的原因,《可转让记录示范法》第 12 条(b)款载有类似的“安全条款”。⁸

8. 首先应当指出的是,第 10(1)(a)条和第 22(1)(a)条使用了“既可靠又适当”一语,其原因是,所用方法可靠性是否适当取决于考虑到所有相关情况下的相关服务的使用目的,其中可能包括第 10(2)条和第 22(2)条提及的情况。一个尤其相关的情况是当事人就所用方法达成的任何一致意见。换言之,特定交易中所用方法的可靠性是否适当取决于该交易的具体情形,第 10(1)(a)条和第 22(1)(a)条提及的是相对的可靠度,而并非某种单一的一成不变的可靠度。

9. 如同《电子通信公约》第 9(3)(b)(c)条和《电子可转让记录示范法》第 12(b)条,第 10(1)(b)条和第 22(1)(b)条寻求避免基于所用方法可靠性在理论上是否适当(理论上的可靠性)而提出的虚假法律质疑,规定如果事实上证明该方法已符合该条所述功能(事实上的可靠性),则该方法即满足第 9 条或第 16 至 21 条的要求,这既可以由其本身也可结合进一步的证据予以证明。

10. 删除第 10(1)(b)条和第 22(1)(b)条将为提出虚假的法律质疑敞开大门。而这是不可取的。

(a) 如果没有第 10(1)(b)条,出于投机目的行事的行动方(例如在涉及电子识别的交易中想要逃避其义务的一方当事人或甚至从电子识别失效中获益的第三方当事人)可能会受到鼓励,从而对由此产生的识别的有效性提出质疑——该质疑所持理由并非是未曾进行过身份识别,而是所用电子身份识别方法在当时的情况下“既不可靠,也不适当”(缠讼);

(b) 同样的分析也适用于信任服务。以电子签字为例,我们看到,如果没有第 22(1)(b)条,使用电子签字的交易的一方当事人可能会被鼓励经由否认其本人签字(或对方签字)的有效性来试图逃避其义务,其所持理由并非是所称签字人未曾签字或其签署的文件遭到篡改,而是因为所用签字方法在当时的情况下既不“可靠也不适当”(缠讼)。对声称交易无效感兴趣的第三方当事人也可以会被激励去做同样的尝试。

11. 有人可能会争辩说,仅第 10(1)(a)条和第 22(1)(a)条的存在就足以避免上述不可取的结果——因为法院或对事实的审理者可以经事后认定交易所用方法就第 9 条(身份识别)或第 16 至 21 条(信任服务)所述服务用途而言是“既可靠又适当”的而拒不承认出于投机目的而提出的法律质疑。然而,我们认为这种做法有两个问题。第一个问题是,即使出于投机目的提出的法律质疑最终未获成功,但这种法律质疑仍然代表着在电子商务交易中提出不必要的诉讼。而这是不可取的。

⁸ 见《可转让记录示范法》解释性说明第 136 和 137 段(转载如下):

“136. (b)项提供了一个“安全条款”,其目的是防止出现缠讼情形,为此可使事实上已实现其功能的方法具有效力,而不考虑对其可靠性的任何评价。该款提及在有争议的具体情况下履行功能,而非着眼于根据该方法以往运作情况预测今后的可靠性。对于借助电子可转让记录寻求实现的任何功能均可运用这条规定。关于电子签名的功能等同,《电子通信公约》第 9 条第 3 款(b)项(c)目载有类似机制。

137. 实际上,所使用的方法实现了使用这种方法所寻求实现的功能,这一事实将防止根据(a)项就评价该方法可靠性进行任何讨论。”

[粗体强调]

12. 删除第 10(1)(b)条和第 22(1)(b)条中的安全条款，从而使根据颁布示范法的国内立法进行的所有电子交易面临提出虚假法律质疑的可能性，其中可能涉及电子识别（第 9 条）、或电子签名（第 16 条）、电子印章（第 17 条）、电子时间戳（第 18 条）、电子存档（第 19 条）、电子挂号递送（第 20 条）或网站认证（第 21 条），第二个也是更重要的问题是，这给双方同意的商业交易造成了不确定性。此种做法可用下面的例子来加以说明。

(a) 假设在 2023 年（某些法域已将示范法颁布为国内法律），双方当事人同意使用 SHA2-256 散列法（生成 256 位散列法）的数字签名签署一份合同；

(b) 对双方已签署了合同并无争议。也不存在合同有任何改动的指控；

(c) 然而，如果没有安全条款，甲方（例如，他想否定他与乙方签署的合同，因为这是一笔不划算的交易）就可以通过声称散列算法既不是“适当的，也不是可靠的”来质疑用于签署合同的数字签名的有效性，因为应该使用 SHA3-512 来代替并非适当可靠的 SHA2-256。

此种情况是令人遗憾的。我们认为，虽然“既可靠又适当”的标准是一个足够灵活的标准，但有必要解决以所用方法可靠性的理论是否适当为由提出法律质疑的可能性。就业务确定性而言，仅仅依赖“既是可靠又是适当”的标准是不合适的。企业（如上述例子中的乙方）如何相信他们在 2023 年进行的电子交易今后不会受到虚假的法律质疑？示范法草案第 10(1)(b)条和第 22(1)(b)条所载安全条款力求确保此种情况不会发生。

B. 使示范法草案与《电子通信公约》和《电子可转让记录示范法》保持一致

13. 以同样的形式保留第 10(1)(b)条和第 22(1)(b)条还将使示范法草案与《电子通信公约》保持一致，该公约是贸易法委员会关于电子交易的最新文书。至关重要的是，示范法草案应与《电子通信公约》第 9(3)(b)(二)条保持一致。许多国家（包括新加坡在内）是《电子通信公约》的缔约国，因此不能颁布任何与《电子通信公约》不相一致的法律。还有一些国家并非《电子通信公约》的缔约国，但根据《电子通信公约》颁布了关于电子交易的法律，包括一项安全条款。⁹删除第 10(1)(b)条和第 22(1)(b)条（特别是第 22(1)(b)条）将导致示范法草案与《电子通信公约》第 9(3)(b)条不相一致。这也将是《电子通信公约》今后的缔约国所应关切的问题。

⁹ 举例说，澳大利亚 1999 年《电子交易法》第 10(b)(二)节沿用了《电子通信公约》第 9(3)(b)(二)条。澳大利亚第 10(b)(二)节规定如下：如果根据英联邦的法律，要求某个人签名，则就一项电子通信而言，在下列情况下，该要求即被视为已得到满足：

(a) 在所有情况下——使用了一种方法来鉴别该当事人的身份和表明该当事人对所传送的信息的意图；以及

(b) 在所有情况下——使用的方法为：

(一) 从各种情况来看，包括根据任何相关的约定，对于生成或者传递电子通信所要达到的目的既是适当的，也是可靠的；或者

(二) **其本身或连同进一步证据证明事实上已完成了(a)款所述的职能……**

[粗体强调]

14. 已经在国内法律中颁布或打算颁布《电子可转让记录示范法》的国家也会对从示范法草案中删除第 10(1)(b)条和第 22(1)(b)条感到关切,因为这将导致示范法草案与《电子可转让记录示范法》不相一致。

15. 如果第 10(1)(b)条和第 22(1)(b)条没有以同样的形式予以保留,贸法会将需要 (a)就《电子通信公约》的缔约国或已颁布《电子可转让记录示范法》的国家应就如何处理不相一致的问题发表意见; (b)就贸法会是否将继续向考虑加入《电子通信公约》或实施《电子可转让记录示范法》的国家推荐《电子通信公约》和《电子可转让记录示范法》(条文不相一致)做出决定。

C. 对解释性说明草案加以修订,以澄清第 10(1)(b)条和第 22(1)(b)条的目的

16. 为了正确理解第 10(1)(b)条和第 22(1)(b)条中“安全条款”的目的,应当对解释性说明草案第 142 和 143 段做如下修订:

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,该方法无论可靠或适当与否,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)(二)条。

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(就第 9 条而言即为身份识别)和可靠性是两个独立的属性,并澄清说规定,根据示范法,该方法应当既适合使用身份管理服务的目的,也应当是可靠的,或者可以证明已经实现了身份识别事实上可以实现的或经使用可靠方法所实现的目的。换言之,在实现身份识别上的证据事实上排除了确定所用方法可靠性是否适当的需要。

三. 第 25 条和第 26 条

17. 第 25 条和第 26 条分别载有促进对身份管理和信任服务跨境承认的规定。作为交叉承认在颁布法域外提供的电子身份识别及使用信任服务所产生的结果的一个先决条件,第 25 和 26 条草案目前要求身份识别管理服务所用方法与信任服务所用方法必须分别提供“至少等同的可靠度”。

18. 我们认为,“至少等同的可靠度”这一门槛标准是有问题的,因为它是单向运作的,在许多不同国家颁布相同示范法的多边环境中是行不通的。此外,所用方法的可靠度是取决于法律、技术和工艺因素,属于定性标准,而非定量标准。这就意味着,寻求其服务得到交叉承认的国家(A 国)很难将其服务的可靠度完全等同于承认国(B 国)法律规定的服务可靠度。这就产生了更多的问题。我们请贸法会考虑以下假设场景:

(a) 假设 A 国希望其身份管理服务在 B 国得到认可,其可靠度/保证级定为“1 级”。A 国的“1 级”基本上相当于 B 国定为“高”的最高可靠度/保证级。但是,由于 B 国的法律要求服务的可靠度/保证级在可靠性/保证方面必须在完全等同或更高级上得到交叉承认,来自 A 国的身份管理服务不能在 B 国得到交叉承认,除

非 A 国修改其法律和技术标准，从而使其“1 级”的可靠度性/保证级与完全等同于或高于 B 国“高”的定级。

(b) 在此种情况下，A 国的“1 级”增强可靠度/保证级很可能会高于 B 国可靠度/保证级上“高”的定级（因为可靠性不能像精准科学一般衡量，所以 A 国很可能在提高可靠度/保证级时将确保其“1 级”的增强可靠度/保证级的层面更高，以确保顺利获得跨境承认）。

(c) 由于 A 国所做的修改，来自 A 国的“1 级”身份管理服务随后将具有与 B 国“高”标准的身份管理服务可靠度/保证级“至少等同的可靠度”，并且这将使身份管理服务能够在 B 国被交叉承认为具有“高”的定级。然而，这反过来又意味着，B 国定级为高的可靠度/保证级的身份管理服务根据 A 国的法律将无法被交叉承认为等同于“1 级”的服务，因为 B 国定级为“高”的服务如今将被视为与 A 国“1 级”相比可靠度/保证级（尽管它可能实质上是等同的）均较低。

19. 这种状况是不可取的，并且造成几乎无法实现相互间的跨境承认。这会使多个法域在多边基础上的跨境承认变得更加不可行。在此种情况下，第 25 条和第 26 条使用“基本等同或更高的可靠度”标准将更为合适。要求“基本等同或更高的可靠度”将允许在两个法域之间进行双向跨境承认，而不要求完全等同。这将使定级为“1 级”的 A 国服务和定级为“高级”的 B 国服务能够得到相互承认，只要两者的可靠度/保证级基本等同。

附录

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**根据第 10(1)条**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 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，**根据第 22(1)条**使用了符合下列条件的某种方法，即满足这一要求：[……]

第 17 条. 电子印章

法律要求应由法人加盖公章的，或者法律规定了不加盖公章的后果的，在数据电文方面，**根据第 22(1)条**使用了符合下列条件的某种方法，即满足这一要求：[……]

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**根据第 22(1)条**使用了符合下列条件的某种方法即满足这一要求：[……]

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，在数据电文方面根据第 22(1)条使用了符合下列条件的某种方法即满足这一要求：[……]

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，在数据电文方面根据第 22 条使用了符合下列条件的某种可靠方法即满足这一要求：[……]

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，根据第 22(1)条使用了符合下列条件的某种方法即满足这一要求：[……]
