联合国 A/CN.9/WG.IV/WP.163

大 会

Distr.: Limited
20 February 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 4 月 6 日至 9 日，纽约

关于使用和跨境承认身份管理和信任服务的条文草案

世界银行提交的文件

秘书处的说明

世界银行提交了一份文件，供委员会第六十届会议审议。现将该文件按秘书处收到的原样转载于本说明的附件。

V.20-01481 (C) 240320 240320

附件

世界银行对 WP.162 号文件的评论意见

在工作组于 2020 年 4 月 6 日至 9 日在纽约举行会议之际，世界银行高兴地就 A/CN.9/WG.IV/WP.162 号文件——“关于使用和跨境承认身份管理和信任服务的条文草案”（“条款草案”）——提交以下评论意见。

一. 一般背景评论和意见

1. 侧重于身份管理：总的来说，世界银行支持第四工作组的工作，特别是身份管理方面的工作。由于世界银行的主要关注点是身份管理，以下评论侧重于条文草案中的身份管理部分。

2. 身份管理系统相对于身份交易：条文草案主要侧重于身份管理系统和身份管理服务提供人，而不是身份交易。鉴于身份交易的重要性——特别是从法律守规和法律承认的角度来看，并且由于电子身份交易可以而且通常是在不使用身份管理系统或身份管理服务提供人的情况下进行的，工作组应考虑进一步处理予身份交易有关的问题。

3. 作用：条文草案主要侧重于身份管理系统和身份管理服务提供人，（除第 5 和第 8 条外，）没有真正涉及依赖方、主体或身份管理系统或交易其他潜在参与方的需要。例如，凡是法律要求依赖方核实身份的，条文草案都没有涉及依赖方使用第三方核实身份的权利。同身份交易问题一样，工作组应考虑更多地侧重于影响身份管理系统作用的问题，而不是影响身份管理服务提供人的问题。

4. 公共部门和私营部门身份管理系统之间的关系：条文草案侧重于私营部门的身份管理系统和私营部门的身份管理服务提供人。从表面上看，条文草案不适用于由公共部门运营的身份管理系统或身份管理服务提供人，如国家身份管理系统。因此，由于许多国家身份管理系统是政府运营的身份管理系统（如印度、爱沙尼亚等），它们都不在条文草案所设想的工作产品的范围之内。

然而，重要的是认识到，公共部门和私营部门的身份管理系统之间可能存在着重大的互动关系。例如，条文草案可能适用于以下情况：政府机构是私营部门身份管理服务提供人的客户（如依赖方或数据主体），或者依赖于私营部门的联合身份系统而不是政府运营的身份管理系统。此外，私营部门身份管理服务提供人所使用的身份核实和认证过程往往依赖于政府系统签发的基本身份证书——通常认为这些证书是权威的和高度可靠的。

因此，工作组应当研究和澄清公共部门和私营部门身份管理系统之间关系的性质，所涉及的问题包括但不限于，何时适合私营部门身份管理系统利用政府提供的基本身份信息和认证程序以及以何种方式利用这种信息和程序合适。例如，这可能包括考虑制定与私营部门身份管理系统有关的规则：

- 使用政府签发的身分证号码或其他身份识别信息
- 使用政府签发的身分凭证
- 访问政府数据库以进行身份核实和身份验证过程，或

- 一般依赖于政府提供的信息或程序

5. 信任框架：条文草案没有涉及单个身份管理系统基于合同的规则的作用，这些规则通常称为信任框架、系统规则或计划规则（此处统称为“信任框架”），以及它们如何与条文草案对接。[1]工作组应考虑修订条文草案，以澄清条文草案与身份管理的信任框架之间的联系，以及条文草案中应涉及哪些问题和详细程度，而不是单个身份管理系统的信任框架。例如，诸如参与方义务、可靠性和保证级等问题经常在单个身份管理系统的独特信任框架中涉及。

同样，工作组应考虑信任框架的条款可在多大程度上修改或否决条文草案中的条款。例如，尽管条文草案中有关于赔偿责任的条款，但各方能否在各自的身份管理特定信任框架中制定自己的赔偿责任规则尚不清楚。

6. 依赖于电子签名法律模式：条文草案中采取的结构和做法在很大程度上是以贸易法委员会的《电子签名示范法》为基础的，因此没有考虑到涉及签名的问题与涉及身份问题所必须处理的问题有很大不同（尽管身份有时是签名的一个组成部分）。因此，虽然在法律上定义了签名要求的单一电子等同形式，但对于核实身份的要求却不容易做到这一点。

这一问题部分源于这样一个事实，即凡是要求签名的法律都要求相同的东西（即签名），而要求识别人的身份的法律往往就身份识别过程规定各种必须满足的不同要求（例如，取决于身份是“基础性的”还是“功能性的”、[2]要求身份识别的目的、所涉及的风险等）。因此，虽然比较容易界定统一签名概念的法律等同形式，但同样办法不一定适用于身份识别方面的各种法律办法。因此，重要的是，工作组不应局限于从电子签名法律中找出一种预定结构，而应独立思考需要在身份方面处理的法律问题。

7. 身份验证方面的选项：任何依赖方验证与其打交道的人的身份都有两个选项，即依赖方可以：

- 自行进行身份验证；或者
- 使用第三方身份管理服务提供人

大多数依赖方使用第一个选项。然而，条文草案只侧重于第二个选项。工作组似宜考虑条文草案是否应对身份问题采取更广泛的做法，并处理这两种情况下的问题。

8. 依赖方的依赖权：理想情况下，条文草案应涉及依赖方的依赖权的相关问题。例如，这可能包括依赖方的下述权利：㈠一般依赖于身份凭证；㈡依赖于第三方凭证以满足规定了识别身份义务的特定法律的具体要求，以及㈢使用第三方身份管理服务提供人以履行其识别某人身份的法定义务。

9. 依赖方使用第三方的权利：与此相关的是，虽然一些规定了身份识别义务的法律明文授权使用第三方服务提供人（如《加利福尼亚消费者隐私法》条例），[3]但许

[1] 虽然“管辖身份管理系统运营的规则”这一术语出现在条文草案第 6 条(c)项、第 6 条(f)项、第10条第 1 款(b)项和第 23 条第 1 款(a)项中，但该术语既未定义也未详细说明。

[2] 例如，见《从业人员指南》（世界银行，2019 年）第 12、13 页（除其他外），可在以下网址查阅：https://id4d.worldbank.org/guide。

[3] 见《加利福尼亚消费者隐私法条例》第 4 条，第 999.323(b)节；可在以下网址查阅：www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?。

多法律在这一点上不置一词（或要求依赖方自行进行身份识别）。这些身份识别问题也应是工作组审议的问题。

二. 逐条评注

1. 第 1 条 定义

(a) **术语不全**：条文草案通篇使用的若干术语未作定义。所使用但未定义的术语包括：

- “电子身份识别因素”，见第 6 条(d)项㈠目
- “电子身份识别机制”，见第 6 条(d)项㈡目、第 8 条(a)项、第 8 条(b)项
- “身份管理”，自始至终用作限定语，但从未定义
- “标识”——见第 1 条(b)项
- “管辖身份管理系统的规则”——见第 6 条(c)项、第 6 条(f)项、第 10 条(b)项、第 23 条(a)项
  - 这一术语可能用以指单个身份管理系统的信任框架，不过按其目前的措辞，可适用于管辖身份管理系统的任何法律或条例。其使用范围应当加以澄清。
- “验证”——见第 6 条(a)项㈡目
  - 对“验证”概念加以澄清可能也很重要，因为这一术语经常导致大量混淆。例如，“身份验证”这一术语在某些情况下常用以指数据主体的识别，而在其他情况下则是指该数据主体的认证。鉴于其使用频度，需仔细澄清这一术语并在全文中正确使用。

(b) **认证**：“认证”和“电子身份识别”这两个术语所指之事基本相同，但认证是在信任服务中使用，而电子身份识别是在身份管理服务中使用。由于概念相同，工作组不妨考虑在这两种情况下使用同一个术语。

(c) **电子身份识别**：以“身份核实”和“电子身份识别”取代单一术语“身份识别”，是澄清和区分身份识别过程两个方面的重要一步。然而，可能令人关切的是，“电子身份识别”这一术语描述了核实身份、签发凭证以及认证凭证数据与个人之间关系的整个过程，或者说容易与这一过程混淆。因此，建议工作组考虑是否可以使用“电子身份识别”以外的其他术语。

此外，这一术语使用“电子”一词，其用意是描述“实现对主体与身份之间绑定的保证的过程”，但可能会对条文草案所涉及的过程、系统和服务的性质造成混淆。同样的问题出现在“身份管理服务”和“身份管理系统”的定义中，这两个定义都要求其为“电子形式”。将绑定过程描述为“电子的”，或者将身份管理服务或身份管理系统描述为“电子形式的”，忽略了这样一个事实，即在某些情况下，该过程的全部或部分可能不是电子的。例如，一些功能可能是以非电子形式执行的，或者依赖于纸质文件，如身份核实。因此，建议工作组考虑承认这样一个事实，即条文草案所涵盖的过程、系统和服务很可能包含各种非电子要素。

(d) **身份**：将身份定义为允许在特定环境下对[主体][人]进行“独特辨别”的一组属性，似乎限制性过强；在许多情况下，身份识别是为了确定属性而非唯一性。例如，身份识别可简单地用来确定某个特定的人是否是特定组群的成员，例如，你超过 21 岁了吗？你是俱乐部会员吗？你是公民吗？等等。想必许多人会拥有这些属性，因此身份不一定是唯一的，但在需要这种限定性身份的情况下，它将充分辨别数据主体。

(e) **身份凭证**：工作组应考虑身份信息传递手段方面的新发展。虽然身份凭证是主张和验证身份的典型方式，但值得注意的是，许多新的身份管理系统并不使用身份凭证本身。因此，尽管该定义不一定不合适，但应注意避免在条文草案中确立一种假设，即始终都将使用身份凭证。此外，注意到该定义局限于“电子形式”。工作组似宜考虑，条文草案是否还应涵盖传统的纸质或面对面的身份识别形式。

(f) **身份核实**：身份核实的过程不需要完全“确定和确认”主体的身份。也就是说，身份核实大概可以包括收集、验证和/或确认一项或多项属性，尽管这些属性本身不足以确定和确认身份，但可以被其他人用来确认身份。因此，工作组可能希望考虑扩大身份核实的定义。

(g) **依赖方**：删除此项定义并代之以术语“订户”，可能不合适。订户的概念意指系统中受规则约束的积极参与方。虽然这可能包括依赖方，但其他个人/实体也有可能订立提供身份管理服务的安排，其中包括主体等。因此，如果不能区分依赖方和主体（或身份管理系统的其他用户），可能会在适用条文草案中的规则时造成混乱。建议工作组考虑保留“依赖方”的定义，以便后面各条中涉及的问题将适当地适用于依赖方或主体。

(h) **主体**：在身份管理服务的环境下，主体是被识别的人或架构，或者是至少参与身份核实过程的人或架构。删除对身份识别的定义会导致该术语泛型，而且可能没有什么帮助。

(i) **订户**：如上所述，订户的概念——“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”——似乎包括面过宽，因其可能包括身份系统中的许多角色以及主体。例如，拟订第 12 条中备选案文 C 的第 3 款是基于订户为依赖方的假设。然而，订户也可能是主体或身份管理系统众多其他角色中的一个，在这种情况下，该条的规定就不合适了。

2. 第 2 条　适用范围

工作组应考虑重新评估条文草案的范围，因为这些条文与身份管理有关。按第 2 条目前的写法，其范围仅限于两个方面：(1)***身份管理系统*的*使用***，(2)***身份管理系统*的*跨境承认***。

工作组可能希望考虑其范围是否还应涉及***身份管理交易***，并且可能还应提及身份管理系统的***运作***和/或身份管理服务的***提供***。

此外，鉴于工作组认识到工作组无权就政府运营的身份管理系统（如国家身份管理系统）起草规则，工作组应考虑修订第 2 条，以澄清其“适用于……***私营部门*的**身份管理系统。”

3. 第 3 条　自愿使用身份管理服务和信任服务

根据第 3 条第 2 款，可以根据一人的行为推断其是否同意使用身份管理系统。然而，工作组应当注意到，在该人身份被盗用的情况下，例如，盗用身份者使用假凭证，或使用发给他人的真凭证，是不宜作这种推断的。在这种情况下，被推断其同意的人并非进行所参照行为的人。

4. 第 4 条　解释

工作组可能希望考虑通过纳入***身份管理系统中性***（或身份交易中性）的概念，确保条文草案不区别对待不同的身份管理系统模式。重要的是，由于有多种不同方式进行在线身份交易（例如，单一身份提供商系统、（多个身份提供商）联合系统、用户控制/以用户为中心系统、中枢系统、分布式分类账技术系统、无凭证系统、身份自主权系统，等等），条文草案不应要求或假定对身份识别和/或认证过程或其执行系统采用一种特定方法。因此，工作组应考虑如何确保条文草案不暗示和/或要求使用某种系统模式。

5. 第 5 条　对身份管理的法律承认

可能需要对第 5 条(a)项进行一些进一步研究和分析。该条规定，不得仅以电子身份识别的电子形式为由而否定其法律效力。我们假设（但未经核实），一些关于使用身份凭证的法律要求以纸质或其他物质形式，而不是以电子形式出示。因此，在取代这类法律之前，我们建议进行一些进一步的研究和分析，以确定这一条款的影响。

6. 第 6 条　身份管理服务提供人的义务

“一刀切”方法的适当性：第 6 条规定了身份管理服务提供人的一系列义务。所列出的义务是适合传统身份管理系统模式的义务，其假设是，身份管理服务提供人执行或负责此类传统身份管理系统的所有功能。然而，身份管理系统的各种模式正在经历各种变化和试验，由此引起的关切是，使用这一义务清单是基于一种旧的模式，它可能不适合较新的身份管理系统，并且/或者可能会不适当地抑制进一步的试验。例如，在许多较新的身份管理系统中，第 6 条中列出的身份管理服务提供人的一些功能或许是各种不同实体（如信任提供人、登记官、注册代理人、凭证服务提供人、管理员、认证商、中枢等）的责任。鉴于身份管理系统模式日益多样化，工作组应考虑的是，在条文草案中对身份管理服务提供人规定一套一刀切的义务是否还合适。

义务的来源：工作组还可能希望考虑一个关键的门槛问题。这就是，是否应在条文草案中载列私营部门身份管理服务提供人（或身份管理系统的任何其他角色）的义务并使之适用于所有身份管理系统，或者是否应由每个私营部门身份管理系统在各自基于合同的信任框架中界定此类义务。如果将每个角色的义务都包括在所适用的身份管理系统的信任框架中，这将允许系统运营人和参与方调整这些义务使之适合特定身份管理系统的目的和用途，并遵守适用的法律。

管辖身份管理系统的规则：最后，应当注意的是，该条所提到的“管辖身份管理系统的规则”并没有加以定义。例如，有一点尚不清楚，即这些规则是指适用于特定身份管理系统的基于合同的信任框架，还是其他什么。

7. 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

应对泄露情况的责任：按目前的写法，第 7 条似乎混淆了身份管理系统和身份管理服务提供人，似乎假设身份管理系统将置于单个身份管理服务提供人的控制之下，由其执行身份管理系统的所有功能。此外，第 7 条规定了此类身份管理服务提供人在凡是“发生”安全违规情形或完整性丧失情形时应承担的责任，而不论身份管理服务提供人是否知道该违规情形或者是否对其负有责任或具有控制。但现实情况是，可能有多方参与身份管理系统，其中许多角色可能对违规所涉服务器/网络/系统、员工或其他人员或设备不负有任何责任或不具有控制。

在身份管理系统采用的许多较新做法中，其中一些功能可由不同的实体（如信任提供人、登记官、注册代理人、凭证服务提供人、管理员、认证商、中枢等）来完成。这样的角色有可能独立地成为违规源，而这种违规情形甚至可能不为身份管理服务提供人所知。

因此，在处理数据泄露问题时，工作组应考虑到*身份管理系统与身份管理服务提供人*之间的区别，以及可能有多个*身份管理服务提供人*（以及多个其他角色）参与单个身份管理系统这一事实。因此，第一个问题可能是确定对于违规所涉事项的责任，以及对于通知义务的责任。

理想情况下，第 7 条规定的违规应对义务（例如，纠正违规情形、吊销凭证、通知有关机构或通知受影响的数据主体和依赖方）应仅限于实际受害方或在其他方面对安全违规情形或完整性丧失情形所涉特定服务器/网络/系统负责的一方。例如，对于涉及包括多个身份管理服务提供人或多个角色的身份管理系统的情形，可能宜规定：㈠实际受害于违规情形且有能力遏制并纠正违规情形的实体有义务纠正违规情形，㈡与各主体有关系的实体有义务通知各主体。

系统级违规：与此相关的是，工作组还应考虑修订第 7 条，以处理在包含多个身份管理服务提供人的身份管理系统中发生的重大系统级违规（例如，根私钥失密）可能危及整个身份管理系统及其所有身份管理服务提供人——具体取决于身份管理系统的类型和结构——的可能性。在这种情况下，违规可能会影响所有身份管理服务提供人，而不论其对实际违规的责任如何。因此，可能需要有不同类型的响应，所有身份管理服务提供人大概都需要承担某些响应义务，即使他们可能对违规没有责任。

对丧失情形的责任：最后，请注意，第 7 条第 1 款(b)项要求身份管理服务提供人“纠正违规情形或*丧失情形*”。虽然要求身份管理服务提供人纠正违规情形（至少是在其控制之下的违规情形）可能是适当的，但工作组应考虑要求身份管理服务提供人还纠正“丧失情形”是否适当。损失可能颇巨，至于身份管理服务提供人是否或在多大程度上应对所发生的损失承担赔偿责任，应当遵从适用的赔偿责任规则——无论这些规则如何确定。

8. 第 8 条　订户的义务

需涉及的角色义务：一般而论，如果要在条文草案中处理身份管理系统各参与方的义务（如第 6、第 7 和第 8 条），工作组可能希望考虑处理**所有**系统参与方的义务——例如，注册代理人、属性提供人、身份管理服务提供人、身份验证提供人、用户、中枢、依赖方、信任提供人、订户等的义务。这对于按照下文第 12 条分配赔偿责任的目的似乎也很重要。

在何处处理义务问题：此外，工作组可能希望考虑在何处处理身份管理服务提供人、订户和身份管理系统其他参与方的义务问题最合适。条文草案第 6、第 7 和第 8 条对处理身份管理服务提供人和订户的义务提供了一刀切的办法。但是，鉴于身份管理系统的多样性，允许或要求每个身份管理系统在根据其具体技术、方法和目的量身制定的信任框架中处理其所有不同角色的义务可能更为合适，而不是利用条文草案将一刀切的做法强加于所有身份管理系统。这在一定程度上是因为，系统角色的类别和定义以及担任这些角色的参与方的义务可能会因身份管理系统的不同而有很大差别。造成这些差异的一个因素是建立特定身份管理系统的目的（例如，是为了便利制药行业内的在线通信，如 SAFE BioPharma 的身份管理系统；是为了便利学术信息交流，如大学使用的 InCommon 身份管理系统；或是为了便利与政府机构的通信，如《电子身份识别和信任服务条例》系统）。

此外，如上文关于第 6 条所述，身份管理系统模式正在进行着各种调试，由此引起的担心是，可能不适合列入一份标准的义务清单，因为这可能会强加一种不适合当前许多身份管理系统的过时的模式并阻碍进一步的试验。

主体订户的义务：第 8 条涉及订户（即订立身份管理服务安排的人）。这大概包括身份管理系统中的多个参与方，如依赖方、单个数据主体，或许还包括身份管理系统中的各种其他角色。该条对订户规定的义务是，不论何时，只要任何订户知道身份管理系统中的任何身份凭证或电子身份识别机制已经失密，或其所知道的情况导致失密可能已经发生的重大风险，即应通知身份管理服务提供人。

如果订户是个人（如数据主体），这可能成为一项繁重和不合理的要求。例如，想必这种情况不在少数，即身份管理系统的单个订户可能意识到表明可能已经发生失密的情况，但只是不理解其重要性。此外，由于这一义务似乎适用于整个身份管理系统（而不是诸如签发给特定个人的单项身份凭证），这一条款似乎给个人（并因此而给系统其他用户）造成重大负担，因为他们可能意识到、但只是不理解某些信息对全系统的重要性。

即使涉及个人身份凭证的损失或失密，对个人规定报告损失的义务也未必总是适当的。就如同信用卡号码被盗，要求当事人报告这些事件可能根本不现实，甚至可能不合适（特别是如果使用人没有经验，或者被盗发生在互联网上或是以使用人可能没有能力察觉的其他方式发生的）。而对于身份管理系统来说，如果这一系统不是基于物理凭证的使用，主体可能根本不知道他或她的凭证数据（如身份号）已经失密。

9. 第 9 条　使用身份管理系统对[主体][人]进行身份识别

取代现行法律的适当性：第 9 条在很大程度上是根据《电子签名示范法》和《联合国国际合同中使用电子通信公约》改拟，似乎具有取代现行法律的效果——这些法律确定对特定情况下身份识别的独特要求。在电子签名法律中，这种取代所有其他签名法律的一般做法行之有效。但是，工作组可能希望评估这种做法对于主体的身份识别是否一定有效。具体而言，由于一些法律要求进行简单的身份识别，而另一些法律则对身份识别的方式和方法有非常具体的规定（包括隐私法、“了解你的客户”法律、公证法等），因此，一项仅仅要求通过满足可靠性标准来表明遵守情况的一般规则可能并不合适。

一般性的身份识别程序，即使是“可靠的”，估计也不大可能满足所有现行法律对身份识别的各种不同要求。此外，就商业交易当事人对身份识别有各自要求而言，一种符合“可靠性”一般标准的电子替代手段可能也不足以满足当事各方的特殊或独特要求。

条款之间的潜在冲突：工作组还应审议第 2 条第 3 款与第 9 条之间似乎存在的潜在冲突。第 2 条第 3 款认识到许多现行法律对私营部门当事方规定了各种身份识别要求，并为此规定，“本文书中的规定概不影响按照法律所界定或规定的程序对[主体][人]进行身份识别的法律要求”。然而，第 9 条的“一刀切”做法似乎与这项规定相抵触。

第 9 条备选案文 A 规定：

> “法律或一方当事人要求对[主体][人]进行身份识别的，就身份管理而言，如果使用了一种可靠[方法][身份管理系统]对该[主体][人]进行电子身份识别，即为满足了这一规则。”

第 9 条备选案文 B 作出类似规定：

> “使用某一可靠方法对[主体][人]进行电子身份识别的，可使用身份管理服务识别该主体的身份。”

鉴于各种法律对身份识别程序的要求多种多样，第 9 条的“一刀切”办法似乎不是可行的办法。这个问题似乎部分在于身份识别是以对待电子签名的同样方式处理的。就电子签名而言，按照《示范法》规定的方式生成电子签名即可满足任何要求签名的法律的要求。但身份识别要求却并非如此。

关于识别某人身份的法律要求因所涉法律、要求身份识别的目的（基础性身份识别还是功能性身份识）以及有关事项的重要性而有很大不同。例如，最近发布的《加利福尼亚消费者隐私法》相关条例规定，在应声称是主体的人的要求发布或删除个人数据之前，必须满足广泛的身份识别要求。[4]同样，金融部门的“了解你的客户”规则规定了各种具体的身份识别要求。因此，工作组可能还希望考虑的是，是否或在何种情况下适合使用一刀切的表述，大意是，使用一种可靠系统即为满足了法律规定的身份识别要求。

[4] 见《加利福尼亚消费者隐私法条例》第 4 条，可在以下网址查阅：www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?。

这些条款相互抵触，表明在试图沿用以前用于电子签名的相同方法建立一套身份规则时面临的问题。

可靠性是相对概念：此外，还有一点考虑很重要，即第 9 条是否充分承认可靠性（同安全性一样）是一个相对概念。某种方法在一种情况下可靠，可能在另一种情况下不可靠。例如，使用 Facebook 或 Google 进行个人电子身份识别，对于简单的网站帐户访问通常是足够可靠的，但对于访问银行帐户和授权从该帐户在线转账资金可能不够。因此，如果要保留取得法律效力的可靠办法，鼓励工作组考虑修改第 9 条的案文，以承认“可靠方法”是一个相对概念。一种可能的办法是，纳入《联合国电子通信公约》中使用的类似于“既适当也可靠”的概念——即：所使用的方法是：㈠从各种情况来看，包括任何相关约定，对于要求进行身份识别的目的既适当也可靠；或㈡事实上已证明足够可靠。

与可靠性有关的多个程序环节：第 9 条仅对用于电子身份识别的方法适用可靠性要求，[5]似乎还忽略了对身份识别的所有其他程序要求，而这些要求也都有可能对结果的可靠性以及可能用于这些程序环节的方法的可靠性产生影响。这些程序环节包括身份核实、入册、凭证安全、认证、电子身份识别、软件、数据安全、雇员，等等。例如，即使对个人电子身份识别使用了客观上可靠的方法，但如果身份核实环节也不够可靠，那就没有价值可言。

10. 第 10 条　与确定可靠性相关的因素

第 10 条仅规定了与确定第 9 条中提到的“电子身份识别……方法”可靠性有关的因素。[6]然而，它没有具体指明在确定身份管理系统所执行的任何其他关键环节（如身份核实）的可靠性时应当加以评估的因素。

第 10 条侧重于以下四类因素：

- 遵守第 6 条规定的义务
- “管辖身份管理系统运营的规则”是否符合包括保证级框架在内的任何公认国际标准和程序
- 就身份管理系统提供的任何监督或核证
- “当事人之间的任何协议。”

然而，虽然所列四类因素侧重于遵守规则或标准、核证和当事人之间的协议，但它们不一定建立可靠性。规则标准、核证或协议的存在并得到遵守并不一定意味着遵守这些规则标准、核证或协议的身份管理系统对于任何特定用途都是可靠的。因此，如果工作组决定处理确定“电子身份识别……方法”可靠性的因素，工作组可能希望考虑哪些具体环节与可靠性有关（例如，身份核实、入册、凭证安全、认证、电子身份识别、软件、数据安全、员工，等等），然后查看哪些规则或标准确立与这些环节中的每一个环节相关的可靠性。

[5] 见条文草案第 1 条(d)项，其中将电子身份识别定义为“用以实现对[主体][人]与身份之间绑定的充分保证的过程。”

[6] 按第 1 条(d)项中的定义，“电子身份识别”限于用以实现对主体/人与身份之间绑定的充分保证的过程。这一定义不包括身份管理系统所必需的许多其他环节。

此外，如上表所示，身份管理系统使用多种不同程序，每一种程序都可以使用一种或数种不同的“方法”来完成，而这些方法可能是可靠的，也可能是不可靠的。此外，确定一种“电子身份识别……方法”是通过可靠方法完成的，并不一定意味着它所依赖的身份核实程序是使用可靠方法完成的。

11. 第 11 条　　指定可靠的身份管理系统

标准和权限：第 11 条赋予国家规定的公共部门或私营部门人员或机构（“**可靠性管理机构**”）指定被认为可靠的身份管理系统的权力。然而，第 11 条并没有就可靠性管理机构作出此种指定的权限规定任何标准。此外，除了要求考虑到所有相关情况——包括第 10 条所列因素，以及笼统要求符合并未具体指明的“确定可靠性的相关公认国际标准和程序”，该条并没有具体指明应使用的程序。由此引起的关切是，不合格的可靠性管理机构可能使用不适当的标准来评估可靠性，这样一来，就有可能将不可靠的身份管理系统指定为可靠的系统。此外，不同国家对可靠的身份管理系统的指定可能大相径庭，即便对同一个身份管理系统也是如此。鉴于此种指定对于第 9 条中的规定的重要性（即第 9 条假定此种被指定的身份管理系统使用的是“可靠方法”并因此而具有法律效力），这可能会导致重大问题。

工作组可能还希望考虑一国将如何指定这样一个可靠性管理机构为主管机构，以及一国将如何确保这样一个可靠性管理机构拥有指定“可靠的”身份管理系统所必需的专门知识、程序和资源。例如，国家规定的可靠性管理机构是否应在被赋予这种权力之前经过一些核证？

系统可靠性相对于交易可靠性：既然可靠性是一个相对概念，可靠性评估可能需要提出的问题是“可靠性是对于什么目的而言？”这就提出了一个门槛问题，即工作组应侧重于身份管理系统的一般可靠性（而不论使用身份管理系统的身份交易是何类型），还是应侧重于身份管理交易的可靠性（这些交易是据以判断可靠性的具体背景）。

身份管理系统的可靠性相对于“电子身份识别……方法”的可靠性：第 11 条侧重于“身份管理系统”的可靠性，而第 9 条则确定基于“电子身份识别……方法”可靠性的身份识别的法律效力。这两种方法似乎不一致，特别是因为电子身份识别方法的可靠性不过是身份管理系统各种功能整体可靠性的一个子集。

实际问题：第 11 条侧重于可靠性管理机构的作用（及其对于获得第 9 条规定的法律效力的重要性），这表明有必要建立一个集中的体制性机制来评估每个国家的身份管理系统，并需要有公共机构的参与，至少要任命可靠性管理机构。我们鼓励工作组考虑这是否可行。

此外，工作组可能希望考虑的是，由于需要获得成为被指定的可靠身份管理系统的益处，是否会对那些无力负担可靠性指定程序费用的身份管理系统产生歧视。工作小组可能希望考虑的其他问题包括：

- 谁适合指定可靠性管理机构？
- 如何确定可靠性管理机构是否有资格和能力？
- （由于是某一时间点上的可靠性评估，）可靠性管理机构指定的可靠性有多可靠？需要多久重复一次评估？

- 国家是否应参与为私营部门的身份管理系统指定可靠性管理机构的事务，或规定某些法律效力取决于取得此种可靠性指定？
- 这是否具有要求所有身份管理系统达到国家和/或可靠性管理机构所选择的标准的实际效果（因为每个人都希望被指定为可靠的系统），从而可能扼杀未来的发展？
- 什么才算是“公认国际标准”？这种“公认”由谁来判断？如果标准变了怎么办？
- 所选择标准的施行和遵守是否可能要求进行可能费用不菲的复杂的核证程序？
- 确定可靠方法的各种因素（第 10 条）与确定可靠身份管理系统的要求（第 11 条）是什么关系？

最后，由于第 11 条规定身份管理系统的指定不考虑地理位置，工作组应考虑这会不会导致身份管理系统实际上需要在其订户将开展业务的每个国家寻求这种指定，以及这是否会抑制跨境交易。

12. 第 12 条　身份管理服务提供人的赔偿责任

关于本草案中的赔偿责任条款，工作组可能希望考虑一些相关的关切问题。

基本假设：第 12 条（至少是备选案文 B 和 C）同第 6 条一样，似乎是基于同样规则可以适用于所有身份系统的假设。但是，鉴于身份管理系统在类型、目的、范围、功能、操作以及参与方角色和责任等方面的差异日渐扩大，第 6 条中规定的规则或第 12 条备选案文 B 或 C 中规定的赔偿责任规则似乎不大可能适合所有情况。人们只需比较传统的基于公钥基础设施的身份系统、基于区块链的身份系统、以用户为中心的身份系统和自我主权身份系统之间的差异，就会发现这些规则并不是所有情况下都适用。由于身份管理系统可能有很大不同，任何标准的赔偿责任分配办法可能都并不能适合所有身份管理系统。因此，工作组可能希望考虑对赔偿责任采取“一刀切”的做法是否适当。

涵盖的角色：第 12 条仅涉及身份管理服务提供人的赔偿责任。如果工作组得出结论认为应在条文草案中处理赔偿责任问题，则可能适宜考虑在所有参与方之间分配赔偿责任。例如，这可能包括身份管理服务提供人、注册代理人、属性提供人、身份提供人、主体、用户、中枢、验证商、信任提供人、依赖方等的赔偿责任。这一点很重要，因为处理一个系统角色的赔偿责任并不能减轻或消除问题可能带来的损害。这不过是将损失转嫁给其他人。赔偿责任的适当分配办法应当考虑谁应适当地承担这一损失。

免除或限制赔偿责任的权利：工作组可能希望考虑身份管理服务提供人（或其他系统参与方）是否应有权通过合同或其他方式免除或限制其赔偿责任。备选案文 A 可允许限责或免责，至少是在适用法律允许的范围内。这大概是承认有许多情形或赔偿责任类型是身份管理服务提供人或其他各方可以合法地寻求免责或限责的，并且至少给适用法律提供的限责和免责选项留有灵活余地。

虽然备选案文 C 确实提供了有限的免责权利，但其范围非常有限，没有留出灵活余地。另外还有一个问题是，备选案文 B 或 C 的规定是否一般禁止身份管理服务提供人完全免除赔偿责任（政府实体通常会这样做）。

此外，如果备选案文 B 和 C 将身份管理服务提供人的赔偿责任限制在其违反第 6 条规定的义务的范围内，那就有一个问题，在发生盗用身份的情况下将如何适用这一限制。也就是说，如果身份管理服务提供人在没有违反第 6 条规定的情况下向身份窃贼签发了凭证或者对其进行了电子身份识别，损失由谁来承担？与身份管理服务提供人可能没有任何互动或合同的身份盗窃的受害人是否应蒙受损失？

备选案文 C 的赔偿责任限制：备选方案 C 第 12 条第 3 款基于这样的假设：(1)可以对特定的身份交易设置目的或价值限制（不过该款未具体说明在何处或如何实施这些限制），以及(2)依赖方在依赖之前可以很容易地知道这些限制。这似乎沿用了一些早期公钥基础设施系统中使用的原始方法，根据这种方法，核证机构签发的证书将包含依赖方在任何依赖之前应审查的目的或金额限制。鉴于当今存在的身份管理系统种类繁多，工作组似宜考虑以交易为基础的责任限制是否可行。例如，该条可加以修改，承认可以在身份管理服务提供人与依赖方的信任框架或合同中、而不是在单项交易中具体规定此类限制。

政府接口：最后，工作组可能还希望考虑与政府的身份管理系统的潜在相互作用。在许多情况下，身份管理服务提供人依赖于第三方提供的属性宣示，例如，国家身份管理系统或其他政府数据库（如“机动车辆部名单”（DMV））。由于政府的身份管理系统通常被认为是权威的，但其通常也不会对差错承担任何赔偿责任，应当考虑确定在政府提供的信息出错的情况下由谁来承担损失。因此，在涉及公共实体的范围内，可能需要采取不同方法。

我们敦促工作组考虑避免试图处理赔偿责任分配问题，特别是考虑到身份管理系统、程序和参与方种类繁多。如果工作组决定处理赔偿责任问题，我们鼓励以可确定赔偿责任的方法，而不是以实际标准、规格或赔偿责任规则本身作为参照。例如，这些方法可能包括提及现行法律（如备选案文 A），或提及身份管理系统所采用、并经当事各方以合同方式商定的基于合同的信任框架。

13. 第 26 条　对身份管理服务和信任服务的跨境承认

- 关于跨境“承认”问题，工作组不妨作出澄清，回答三个基本问题：承认什么？谁来承认？为何目的而承认？
- 承认什么？第 26 条第 1 款似乎回答了这个问题，其侧重于“身份管理系统”以及“身份管理系统”的“法律效力”。然而，并不清楚身份管理系统如何取得法律效力，或者系统可能具有什么法律效力。对于身份管理系统进行的身份核实和/或电子身份识别程序的依赖，估计可能会产生法律效力，但身份管理系统本身如何被视为具有法律效力，这一点并不清楚。

以此类推，各国承认其他国家根据国际民航组织标准签发的护照。每个国家大概都同意国际民航组织标准的有效性，对彼此的护照签发系统是否符合这些标准可能会评估，也可能不评估，但正是凭证——即每个国家的系统所签发的护照——在边境被赋予“法律效力”。

- 谁来承认？可能是对外国身份管理系统给予承认的实体，或是(1)公共实体，如适用相关法律/法律制度的政府或法院（例如，满足验证身份的法律要求或在法庭上组构可采信的证据等方面），或是(2)依赖方（公共或私营部门）。第 26 条草案或许是侧重于第一种选择，因其提到凡是被承认者的“法律效力”。此外，第二种选择不要求适用法律或法律结论，因为依赖方当然可以自行决定是否为其从事的任何交易而承认和/或依赖身份管理系统或身份。
- 为何目的而承认？如果一种“身份管理系统”得到外国法律的承认，这意味着什么？身份管理系统具有法律效力这一概念似乎有点混乱。例如，这是否意味着外国将自动接受由被承认的身份管理系统进行的电子身份识别的结果，还是仅仅意味着将允许被承认的身份管理系统在外国司法管辖区开展业务，但其程序可能需要加以修改，以满足外国司法管辖区对其自己的身份管理系统规定的法律要求？

工作组应当考虑澄清，在[颁布国]以外运营的身份管理系统应在[颁布国]境内具有与在[颁布国]境内运营的身份管理系统相同的法律效力，这种说法是什么意思。

14. 第 27 条　合作

第 27 条的用意并不明确。其侧重点似乎是交流信息、经验和良好做法——这种事肯定是不能反对的，理想情况下还应当予以鼓励，特别是如果交流是自愿的，而且不涉及对非合作方实体具有约束力的协议的谈判。然而，在这种情况下，似乎没有必要要求颁布国指明负责信息交流的实体。此外，似乎没有必要将合作重点放在第 27 条所列明的三个类别上。

如果合作和交流是强制性的，或者作为一国法律承认的基础或作为对非谈判当事方的实体具有约束力的协议的谈判的基础，这似乎会引起各种关切，需要工作组进一步讨论和澄清。

还应注意的是，第 27 条允许（或要求）颁布国指明的主管实体或机构“与外国实体”合作。不清楚“外国实体”一语指的是什么——例如，是指外国政府，还是指恰巧在某一外国运营的身份管理服务提供人，等等？或许，与“外国实体”的这种合作应当限于也被某一外国指明的外国主管实体。