联合国 A/CN.9/WG.IV/WP.141

大 会

Distr.: Limited
30 January 2017
Chinese
Original: Russian

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

与身份管理和信任服务有关的法律问题

秘书处的说明

俄罗斯联邦向秘书处提交了一份文件，供本工作组第五十五届会议。现将秘书处收到的案文原样转载于本说明的附件。

V.17-00119 (C) 200217 200217

附件

俄罗斯联邦提出的建议

通过使用跨境电子交易跨界信任环境和共用信任基础设施来改进身份管理系统

导言

亚洲及太平洋经济社会委员会（亚太经社会）第二十七届会议于 2016 年 5 月 24 日通过了《亚洲及太平洋跨境无纸贸易便利化框架协定》。

该《框架协定》的宗旨是“通过促进电子形式的贸易数据和文件的交换和互认，推动国家和次区域单一窗口和（或）其他无纸贸易系统之间的兼容性，促进跨境无纸贸易，从而提高国际贸易的效率和透明度，并营造有利于遵守法律规制的环境。”

《框架协定》第五条确定“改善跨界信任环境”（第一款第㈦项）为《协定》须遵循的总体原则之一。

本文件目的是继续推动改进电子商务跨界信任环境这项工作，这是亚太经社会和联合国国际贸易法委员会（贸易法委员会）一个重要议程项目。

本建议的先前版本载于 A/CN.9/WG.III/WP.136，已提交贸易法委员会第三工作组（网上争议解决）供其在维也纳举行的第三十二届会议（2015 年 11 月 30 日至 12 月 4 日）审议。按照该工作组与会者提出的建议，已将该文件转交第四工作组（电子商务）审议，因为该文件与第四工作组的议程相关。主要关注领域是旨在加强亚洲太平洋区域电子商务跨界信任环境的技术、组织和法律机制。在第四工作组第五十三届会议上，俄罗斯联邦代表团表示有意提交一份关于身份管理的建议供该工作组下届会议审议，但须由委员会确认将在工作组下届会议议程中列入身份管理议题。工作组请各代表团提交关于身份管理的信息，以期促进这一议题的审议。

确保跨境交换电子文件的安全性是全球和区域宣言都曾强调的一个高度相关问题，特别是：

- “促进研究与合作，促成有效使用数据和软件特别是电子文件，以及促成交易包括电子认证手段，并改进安全方法。(“信息社会世界首脑会议十周年关于 2015 年后信息社会世界首脑会议的愿景。C5。建设使用信通技术的信心和安全，”(f)段)；
- “[……]通过鼓励信息包括电子文件的安全跨境流动，在全球范围内促进对电子环境的信心和信任[，并促进]旨在扩展和加强亚洲太平洋信息基础设施并建设使用信通技术的信心和安全的各种努力”(《符拉迪沃斯托克宣言》

（2012 年亚洲太平洋经济合作组织（亚太经合组织）领导人宣言）：“融合谋发展，创新促繁荣”）。

在世界范围内，目前有几个处理这一问题的良好做法实例：

- 欧盟委员会：基于欧洲议会和欧洲联盟理事会关于内部市场电子交易的电子身份认证和信托服务的第 910/2014 号条例（eIDAS 条例）；[1]
- 欧亚经济联盟：基于《欧亚经济联盟条约》以及国家间信息互动使用服务和有法律意义电子文件的框架；[2]
- 亚洲太平洋区域：基于泛亚洲电子商务联盟。[3]

全球经济的发展，尤其是在危机时期，要求加强经济和社会各领域的融合进程，包括通过创新性地使用现有信息和通信技术（信通技术）。

跨境贸易产生的主要问题之一是通过互联网传输的信息的安全和保密。身份管理系统即用来解决这一问题。身份管理是用于下述各个方面的一整套功能和能力（例如，行政、管理和维护、发现、沟通交流、关联和约束、政策执行、认证和断言）：

- 对身份信息（例如身份标识、证书、属性）的保证；
- 对实体（例如：用户/订阅者、团体、用户装置、组织、网络和服务提供商、网络内容和物体和虚拟物体）身份的保证；以及
- 支持商业和安全应用。[4]

身份管理的目标是：

- 访问控制（应当只能由经过授权的使用者为所有者预期的目的访问硬件）；
- 访问的保密；
- 身份管理系统的完整性。

为实现这些目标，身份管理系统应当：

- 确保系统有必要的性能，连同规定的复原力指标；
- 确保身份识别数据管理功能（创建、修改、冻结、存档或删除身份识别信息）；
- 确保对身份识别数据的保护；

[1] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond。

[2] www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713。

[3] www.paa.net/。

[4] https://www.itu.int/rec/T-REC-X.1252-201004-I/en。

- 确保使用安全的身份识别和认证机制（如电子签名、两步密码保护和生物认证）；
- 确保所使用的安全解决方案的互操作性；
- 确保身份管理系统和身份识别信息的完整性。

身份管理系统有两种：即以应用为中心的系统和以用户为中心的系统。[5]

在大型身份管理系统中，以应用为中心的身份管理系统意指身份服务和政策是为满足身份提供商的要求而设计的，并按照具体应用的要求进行了优化，例如管理用户账户信息。在以应用为中心的身份管理系统中有身份提供商和依赖方。为用户提供身份服务时，身份交换通常发生在这两个实体之间。“身份”应理解为以一个或多个信息要素的形式对一个主体的表述，这些信息因素使实体足以在具体背景下被区分出来。就身份管理而言，“身份”一词理解为具体背景下的身份（属性子集），即属性的种类由实体存在和互动所在的具有界定边界条件的框架（具体背景）作了限制。以往，身份和访问管理技术主要侧重于对联合访问各种应用和服务的最终用户的认证（在联合访问模式下，有多个身份提供商可供用户信任，它们在必要时可管理用户的部分身份信息。每个身份提供商掌握的用户身份信息可以共享。这样一来，安全要求限于其应用域的范围之内。

以用户为中心的身份管理系统主要将重点放在最终用户上，按照这些最终用户的要求进行了优化。这意味着身份管理系统的主要目标是为用户提供便利和全面的身份服务。主要特征是使用户可以充分控制其身份。传播用户身份信息时，必须先经过用户，使用户有机会执行必要的隐私政策；例如，选择对保密或个人授权的个人偏好。在以用户为中心的身份管理系统中，与身份管理服务器互动以检索身份信息的客户程序必须安装在用户的计算环境中。这样，就需要简单而全面的安全准则，以指导用户安全地安装和部署任何相关软件。该软件必须对用户与安全有关的一些信息进行管理。以用户为中心区别于其他模式身份管理之处在于它强调用户而非管理机关对如何创建、传播、更新和终止用户身份属性保持控制。这意味着用户对其身份的整个寿命周期拥有全部权力。控制的等级可由用户的隐私要求来确定。

2006 年，首次在国际电信联盟（国际电联）及其电信标准化部门的框架内审议身份管理问题，当时处理电信和信通技术安全问题的电信标准化部门第 17 研究组设立了身份管理焦点小组。该焦点小组的目标是审议电信和信通技术中的身份管理问题和共同原则。该焦点小组的活动逐步演变成于 2008 年实施的一项国际电联全球身份管理举措。国际电联第 2、9、11、13、16 和 17 研究组就该举措相互合作。自 2009 年，由第 17 研究组牵头身份管理联合协调活动。通过该协调活动，制定了身份管理标准路线图，其中纳入了下列组织提供的相关投入：电信行业解决方案联盟、欧洲电信标准研究所、互联网工程任务组、国际标准化组织/国际电

[5] https://www.itu.int/rec/T-REC-X.1253-201109-I/en。

工委员会、国际电联、美国国际标准和技术协会、结构化信息标准促进组织、Kantara 举措和第三代合作伙伴项目（国际电联和这些组织发布的身份管理活动和标准描述见国际电联网站：http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx）。

建立电子商务领域跨界信任环境将有助于简化程序和发展国际贸易，并使得有可能简化各参与国的身份识别过程和身份管理。在安全方面，“信任”一词可理解为意指对于信息可靠性和真实性或对于一个实体在特定情况下能够且愿意适当行事的确定性。因此，在国家之间创建信任环境将有助于使用安全机制方面的协调统一（例如，所有国家使用相同办法挑选电子签名和两步密码保护等机制），还有可能提高电子商务参与方之间的信任级别（对于某人或某事的信誉、能力、有效性或真实性的持续的可衡量的信心）。

提出电子商务跨界信任环境一语，意指联合国相关专门机构和各国际组织为确保对进行电子商务的电子互动当事方（实体）之间国际交换电子文件和数据的信任而建议的法律、组织和技术条件的组合。主要目的是在身份管理系统帮助下，在用户电子互动过程中向其提供各种等级的信任服务（基本、中等和高等）。这将有可能在由用户斟酌决定的情况下赋予电子互动以法律意义，而不管用户的地理位置和法域如何。这方面最重要的研究领域之一是分析可能的身份管理机制。

提议电子商务中“电子互动当事方（实体）”一语理解为意指在源于形成、发送、传送、接收、储存和使用电子文件和数据的关系的框架内互动的所有公共当局及自然人和法人。

这些提议意在查明在联合国相关组织制定一套关于跨界信任环境的组建和运作的建议（电子商务跨界信任环境建议）时应当讨论的方法和问题。目的是促进为实际落实电子商务跨界信任环境建议而构建技术、机构和法律基础设施，尤其是简化着眼于电子商务交易安全的身份管理系统。

设计思路

1. 提议电子商务跨界信任环境建议应重点保障属于联合国会员国管辖的公民和组织在利用互联网和其他大规模使用的开放式信通技术系统进行有法律意义的电子形式信息交易时的权利和合法权益。

2. 将在从事下列活动的专业运营商的商业活动的框架内提供上述机构保障：

- 向用户提供一套信通技术信任服务以便实施身份管理；
- 在既定法律制度框架内运营，这些法律制度包括但不限于对于处理个人数据的限制。

3. 建议对下述可能的不同法律制度作出描述：

- 基于国际协定（公约）和（或）可直接适用的国际监管的法律制度；

- 基于商业协定和（或）行业惯例的法律制度；
- 不受特定国际监管约束的法律制度。

传统机构（政府当局、司法解决机构、保险机构、公证机构和其他）通过互认经由信通技术信任服务认证的电子文件，可为各种法律制度提供额外支持。

既定法律制度也可作出规定，就对于专业运营商商业活动的物质和资金支持提出特殊要求，以防它们对用户造成损害，包括个人数据遭到损害的情况。

建议在贸易法委员会一份单独的建议中述及跨界信任环境区域群组和全球群组的组建和运作以及这些群组框架内提供的功能服务所涉及的机构保证以及法律制度相关问题。

建议按照各种功能性应用的重要性等级描述可能作为基础设施提供的各种信通技术信任服务。这方面最重要的研究领域之一是分析可能的身份管理机制。信通技术服务以及这些服务当前的信任级别可由功能性信息系统运营商（在一个信息系统中组织和（或）进行身份数据储存和处理，以及界定利用该信息系统中的身份数据实施的目标和行动（业务）的运营商）依据威胁、风险、法律制度和用户需求而确定。为确保所要求的信任级别，身份管理运营商可在特定法律制度所界定的中性国际环境中开展业务。建议描述建立和维持中性国际环境所必需的组织结构。

可在联合国贸易便利化和电子商务中心（电子商务中心）和欧洲经济委员会（欧洲经委会）共同发布的“关于确保有法律意义可信跨界电子互动的建议”的框架内考虑关于组建和运作电子商务跨界信任环境区域群组和全球群组、这些群组框架内提供的功能服务以及作为基础设施的各种信通技术信任服务的共同条款。

身份管理的实施和具体信通技术信任服务的描述可作为国际电联、标准化组织/电工委员会第 1 联合技术委员会、欧洲电信标准研究所和其他机构的技术标准和建议的主题。

5. 用于身份管理的各种属性应由管辖专门从事身份识别工作的运营商和功能性运营商的商业活动的法律制度界定，并可由适当的信通技术信任服务来支持。运营商的活动可由除其他外关于个人数据保护的组织和技术方面的专门要求来规范。

用于身份管理的各种属性和身份识别程序本身可作为确定身份识别系统信任级别的基础。此种信任级别可能对于规范不同信任群组之间的互动至关重要（见第 9 节）。

6. 建议描述特定国家及其国际联盟在组建电子商务共同跨界信任环境的框架内与其他国际机构的互动：

6.1. 在加入旨在向电子互动实体提供机构保障的现有法律制度的基础上：

- 一国在国际条约和（或）可直接适用的国际监管基础上完全加入现有法律制度，在此框架内设想或规定组建区域电子商务跨界信任环境，包括该电子商务跨界信任环境内提供的功能服务。

- 一国在国际条约和(或)可直接适用的国际监管基础上部分加入现有法律制度，办法是通过与建立区域和（或）功能性电子商务跨界信任环境的具体条款；

6.2. 在不同国际联盟之间互动的基础上：

- 在第一阶段，若干国家创建独立的区域电子商务跨界信任环境群组，包括在此跨界信任环境框架内提供的功能性电子商务跨界信任环境服务，对电子互动主体提供这些国家指定法律制度所规定的机构保障，并确保电子商务交易的安全；

- 在第二阶段，具体制定与其他国际联盟可信互动、涉及相互承认不同法律制度的议定书和机制。这种相互承认应考虑与每个国际机构有关的机构保障和信息安全要求，也许以特定法律制度下运作的对身份管理负责的信息安全网关为基础；

6.3. 在一国与其他国家或国际联盟互动的基础上：

- 在第一阶段，一国创建在该国指定的国家法律制度下运作的独立的电子商务跨界信任环境国家群组；

- 在第二阶段，具体制定与其他国家和（或）国际联盟可信互动、涉及相互承认不同法律制度的议定书。这种相互承认应考虑与这些国家和国际机构有关的机构保障和信息安全要求，也许以特定法律制度下运作的对身份管理负责的信息安全网关为基础。

7. 建议基于商业协议和（或）行业惯例描述针对各种法律制度的群组组建机制，与第 6 节的描述类似。

8. 建议在将不同群组融合为依下述参数化输入信息组建的单一矩阵的基础上描述全球电子商务跨界信任环境的组建机制：

- 功能服务的类别和区域范围；

- 法律制度的类别及其变式。

9. 建议描述组建几类信息安全网关的办法，信息安全网关是建设全球电子商务跨界信任环境矩阵，以确保电子商务交易安全的关键因素。

创建此类信息安全网关的目的之一是确保全球电子商务跨界信任环境不同群组之间互动的条件得到满足，并且这种互动是安全的。在组建信息安全网关时可以考虑所有必要的技术、组织和法律方面。

组建一般的信息安全网关的办法应当考虑到不同电子商务跨界信任环境群组之间存在着可能不同层面的互动。例如，组建进行身份管理的信息安全网关既可以只涉及法律和组织层面，也可以涉及复合层面，即法律、组织和技术层面。

组建一般的信息安全网关的办法应当考虑到使用转换轮廓图，描述并界定自一个群组到另一个群组的转换。这类转换轮廓图可以考虑互动的各群组内部使用的身份识别办法的信任级别（见第 5 节）。

可在国际电联和第一联合技术委员会的技术标准和建议中对几类信息安全网关作出描述。

借助统一的信任基础设施建设电子商务跨界信任环境

如上所述，建设电子商务跨界信任环境的主要目的是在身份管理系统帮助下，在用户电子互动过程中向其提供各种级别的信任服务（基本、中等和高等）。

电子商务跨界信任环境是一个基础性的易扩缩平台，利用身份管理提供对电子信任服务的统一的安全访问。由于考虑到了现有的电子身份管理系统和机制，对这些系统和机制进行升级以便将其纳入电子商务跨界信任环境的要求可望降到最低。

在开发电子商务跨界信任环境系统的过程中，提出了共用信任基础设施（信任设施）体系结构，描述了其不同组成部分的相互关系及其与用户的互动，正在同时就三个方面开展工作：技术、组织和法律方面。通过分析实际实施的各种选项和以及使用信任设施的场景，得以创建详尽说明该系统所必需的文件清单。信任设施体系结构的设计使其能够容易地按比例进行调整。通过添加新的组成部分，可以在任何层面容易地扩展，如新的法律制度、新的超国家参与方或信任和身份数据服务方面新的运营商。

信任设施的技术方面

提供身份管理和信任服务可能有多种技术机制。对信任设施各要素的主要要求是它们确保互操作性。拟在可信电子数据交换监管机构协调理事会(数据交换监管机构理事会)的文件中提供的各种标准和说明将为这一层面的监管提供便利。在跨界电子互动中使用电子签名等身份管理机制即是信任服务技术运作的一个实例。为比较起见，给出实施信任设施的两种选择：分散性办法，信息互动参与方之间为名义上较低的信任级别（见图 1），以及集中化办法，参与方之间为中等信任级别（见图 2）。

表一列示信任设施分散性办法和集中化办法的特征。表 2 描述信任设施两种实施办法使用电子签名作为身份管理系统机制的程序。

表 1

信任设施中使用身份管理机制进行信息互动，信任级别为低等和中等

低等信任级别（图 3）	中等信任级别（图 4）
1. 加签服务由本国加签服务运营商提供。这些运营商也可能提供其他身份管理服务。 2. 不涉及国际组织（运营商和监管机构）。 3. 国家监管机构之间直接互动，交换安全证书。 4. 国家监管机构确保属于其管辖的信任服务国家运营商就其证书和其他法域国家监管机构的证书开展业务。	1. 加签服务由加签服务国际运营商提供。这些运营商也可能提供其他身份管理服务。 2. 涉及国际组织：信任设施国际监管机构和信任服务国际运营商。 3. 信任设施国家监管机构只通过信任设施超国家监管机构实现互动。信任服务国家运营商也只通过各自的国际运营商进行沟通。 4. 信任设施国际监管机构集中向信任服务国家运营商和信任设施国家监管机构提供证书。 5. 国家监管机构确保属于其管辖的信任服务国家运营商就其证书和国际监管机构的证书开展业务。

表 2

低等和中等信任级别办法中使用电子签名作为身份管理系统机制的程序

低等信任级别（图 3）	中等信任级别（图 4）
1. 自然人/法人 I 在法域 J 发附送有电子签名的文件，同时选择信任设施提供的必要的信任级别（基本、中等或高等）。 2. 向属于法域 Q 的加签服务国家运营商发送要求核实法域 J 的附有电子签名文件的请求。 3. 向属于法域 J 的加签服务国家运营商转发要求核实的请求。 4. 在法域 J 对电子签名进行数学认证。 5/6. 向属于法域 J 的加签服务国家运营商发送关于证书状况的请求/答复。 7. 法域 Q 的加签服务国家运营商收到关于法域 J 的电子签名正确无误的确认。 8. 法域 Q 的加签服务国家运营商对请求作证明，并将其转发给自然人/法人 2。	1. 自然人/法人 I 在法域 J 发送附有电子签名的文件，同时选择信任设施提供的必要的信任级别（基本、中等或高等）。 2. 向加签服务国际运营商 I-J-Q 发送要求核实法域 J 附有电子签名文件的请求。 3. 在法域 J 对电子签名进行数学认证。 4/5. 向属于法域 J 的签名服务国家运营商发送关于证书状况的请求/答复。 6. 加签服务国际运营商 I-J-Q 对请求作证明，并将其转发给自然人/法人 2。

图 1

“低等”信任级别跨界信任环境框架内的电子签名核实（分散性办法）

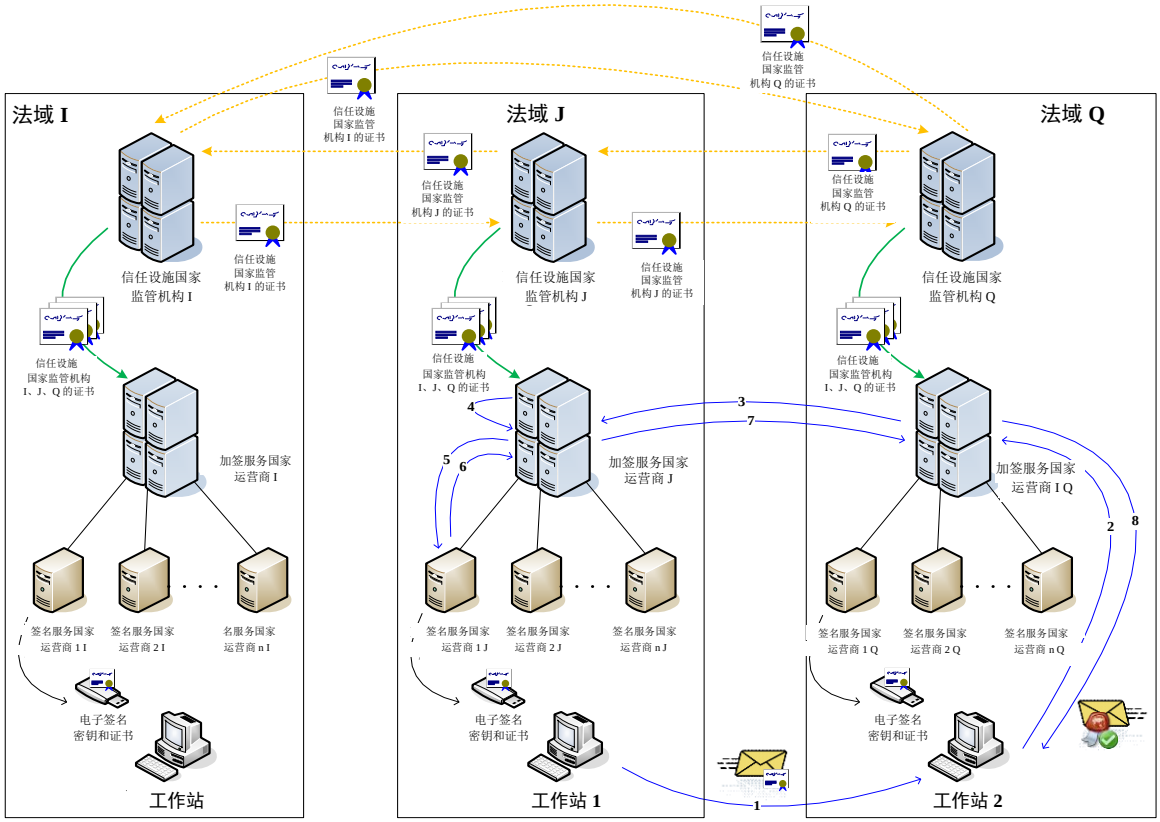
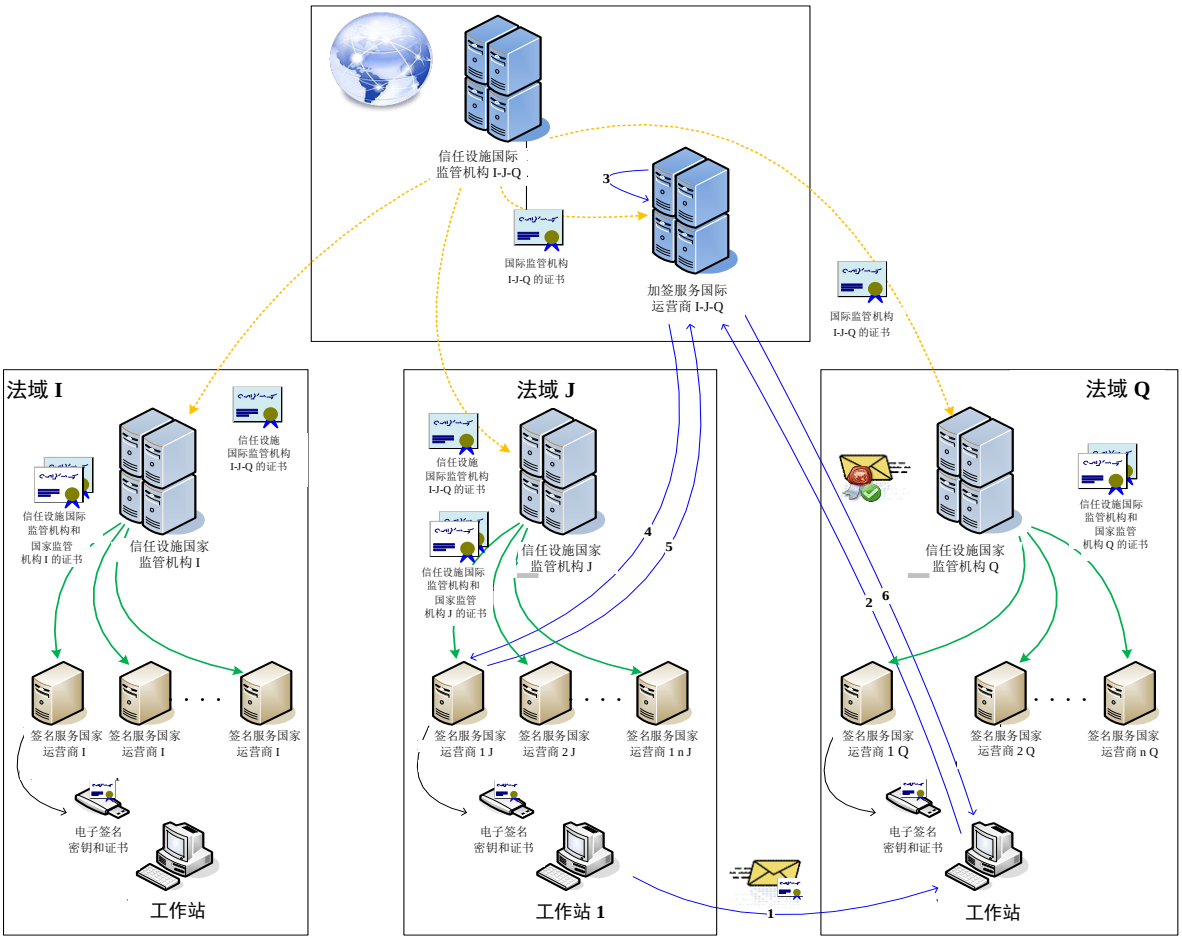


图 2

“中等”信任级别跨界信任环境框架内的电子签名核实（分散性办法）



组织方面

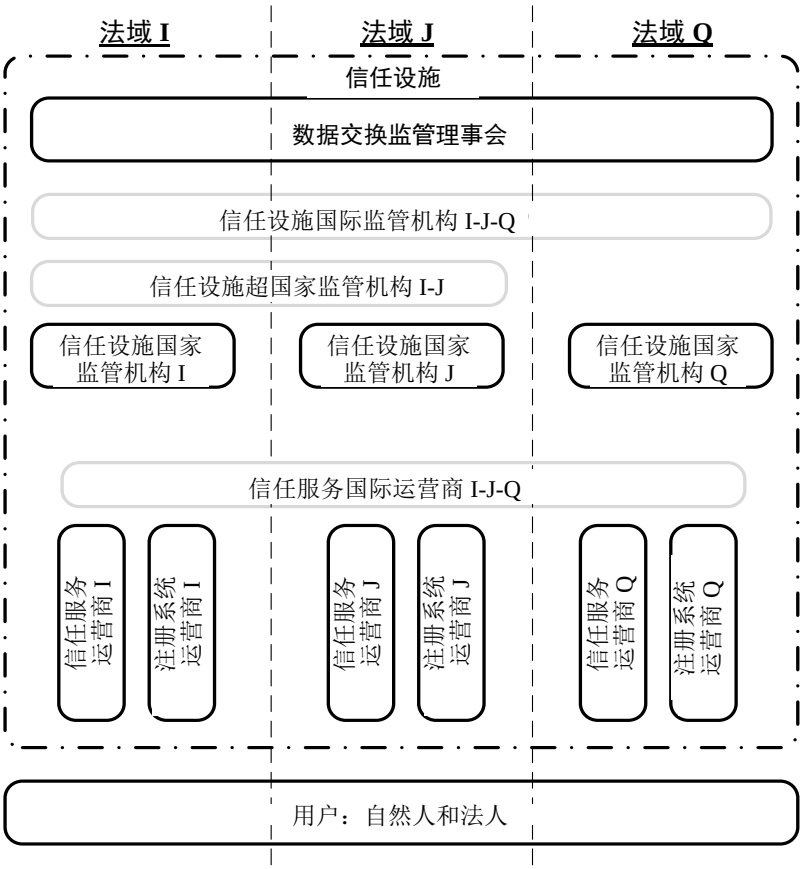
对不同国家法域下提供的身份管理和信任服务的相互承认将通过可信电子数据交换监管机构协调理事会（下称“数据交换监管机构理事会”）的设立和运作得以实现。此类协调理事会的活动由其章程来规范，其章程将由得到授权的所有成员——即首先由信任设施国家监管机构所代表的负责监管电子数据交换的机构——予以承认和签署。

下图对组织监管加以举例说明（见图 3）：

图 3

跨界信任环境的组织监管

（灰色文字框表示可选内容）



协调理事会将发布一系列文件，其章程赋予其此种权力：

- 对协调理事会成员的要求，遵守这些要求是成为协调理事会正式成员的前提条件；
- 关于为获准加入理事会而进行初步的“影子”监管和定期互审以保留自愿会员资格的准则；
- 信任设施服务运营商及身份管理和信任服务运营商的合规标准，以及这些标准的适用方法；
- 评估/核查信任设施服务运营商及身份管理和信任服务运营商遵守这些标准情况的系统。

在电子商务跨界信任环境中，每一个法律制度都由一个信任设施国家监管机构来代表（见图 3，信任设施国家监管机构 I、J 和 Q），该监管机构监管其法域内信任服务和身份管理运营商的活动。

紧密一体化的国家集团（如欧亚经济共同体或欧洲联盟）有可能设立一个信任设施超国家监管机构（见图 3，“信任设施超国家监管机构 I-J”）。这样一来，一个信任设施超国家监管机构 I-J 取代两个信任设施国家监管机构 I 和 J。

协调理事会接纳新成员程序（新的法律制度和超国家参与方），以及对信任设施服务运营商和身份管理运营商是否满足数据交换监管理事会发布的标准进行核查的制度（新的身份管理和信任服务运营商）使信任设施具有自然可扩缩性。

如果协调理事会成员（见下文）达到名义上的“中等”信任级别，它们可以着手创建信任设施国际监管机构以及身份管理和信任服务国际运营商（见图 3，“信任设施国际监管机构 I-J-Q”和“信任服务国际运营商 I-J-Q”）。信任设施国际监管机构将协调信任服务国际运营商、信任设施国家监管机构（根据协调理事会章程）和（或）信任设施超国家监管机构之间的互动。

要想成为信任服务国家运营商或注册系统运营商，相应服务的提供商必须通过本国信任设施国家监管机构获得认证。信任服务国际运营商需要通过信任设施国际监管机构获得认证。对信任服务运营商和注册系统运营商的认证要求，以及对其活动的要求，将由协调理事会发布的合规标准并可能由相应的监管机构发布的国家补充标准来规范。

自然人和法人均可以成为电子商务跨界信任环境框架内电子服务的用户。用户斟酌决定或通过协议选择必要的信任服务级别。

这些服务将由相应的信任服务提供商/运营商提供。有些情况下，服务也可由注册系统运营商提供。信任服务运营商和注册系统运营商将由一个信任设施联系在一起。

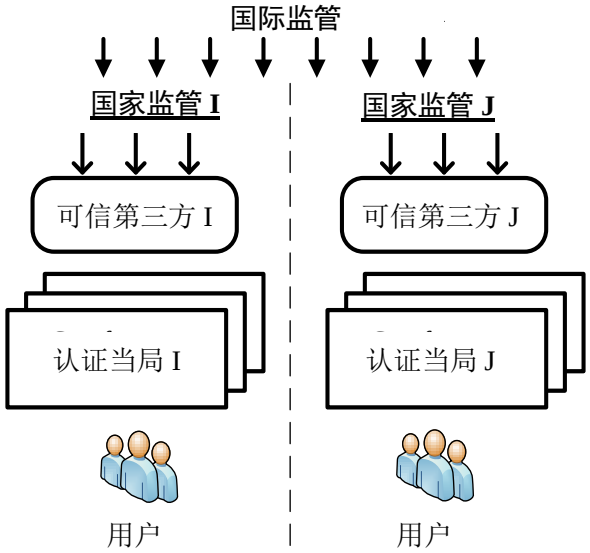
如何实施构成电子商务跨界信任环境组成部分的信任服务可能有不同的选择，视信息互动参与方之间的信任级别而定。例如，若协调理事会成员之间有名义上的高等和中等互信级别，即可有效地使用按照商定标准提供的集中化国际服务。在名义上低等信任级别的情况下，将按照分散性原则组织信任服务的提供，即在每个国家提供本国服务的基础上。

法律方面

电子商务跨界信任环境可在单域或多域基础上创建。从法律和组织方面看，多域基础是较复杂的选择。多域办法要求使用可信第三方的技术资源。图 4 给出法律监管的总示意图。

图 4

跨界信任环境的法律监管



跨界信息互动的法律监管可以分为两个部分：国际部分和国内部分。 国际法律监管基于以下几类文件进行：

- 国际条约/协定；
- 不同国际组织的文书；
- 国际标准和规则；
- 跨界信息互动参与方就特定问题达成的协定；
- 示范立法。

与此类似，国家法律监管建立在每个具体法律制度特有的一套监管文书的基础之上。

摘要

上述材料表明，建立电子商务跨境信任环境可以最佳地加强身份管理系统，理由如下：

- 建立国家、区域和国际信任群组将确保电子签名等身份管理机制实现更大程度的互操作性；
- 在法律上相互承认不同国家法域内提供的身份管理和信任服务使得有可能制定一项实现身份管理系统标准化的共同办法；
- 就使用跨界信任环境通过国际条约和协定及国际标准和条例使得有可能增强电子商务参与方之间的信任级别，这样又有可能简化身份管理的实施；

- 协调理事会（数据交换监管机构理事会）的活动使得有可能制定身份管理运营商和信任服务运营商须遵守的统一的合规标准，以及这些标准的适用方法。

身份管理系统的改进反过来将为跨界国际商业活动创造安全条件。建立电子商务跨界信任环境要求落实一些与系统有关的措施，即：

- 实施技术方面的解决方案，确保信息的安全性和保密性；
- 通过建立一个协调机构，实施组织方面的解决方案；
- 通过起草关于使用电子商务跨界信任环境的国际条例，实施法律和监管方面的解决方案。

电子商务跨界信任环境的组织工作还要求其工作涉及身份管理和跨境贸易相关问题的各组织之间进行协调（包括标准化组织、国际电联、电子商务中心、欧洲经委会、贸易法委员会、亚太经合组织），以便就以下两个方面制定一种共同办法，其一是作为一种身份管理机制使用电子商务跨界信任环境的标准化，其二是将电子商务跨界信任环境用于跨界电子互动和商业活动。

为推动这项工作，下一步将是讨论有志于促进、简化跨界电子服务并同时赋予其法律效力的不同合作伙伴（专家和组织）所积累的经验和知识。

此类相关合作伙伴可能首先是政治和经济组织。[6]已经部分参与本领域工作的政治机构既包括超国家组织（如独立国家联合体（独联体）、亚太经合组织、欧洲联盟和上海合作组织），也包括在某些国家双边关系框架内设立的机构。有志于实现这一目标的经济机构包括相关的联合国机构，如电子商务中心、欧洲经委会、贸易法委员会（第三和第四工作组）、欧洲经委会、欧洲经济区和欧亚经济共同体。可以假设，由于世界各区域特有的自然特征（包括历史、文化、政治、经济和技术特征），由国家组成的各国际组织或区域组织将建立自己的协调机构（不同的可信电子数据交换监管机构协调理事会）和信任设施体系结构，视每个具体安排下的信任级别和上述特征而定。

因此，我们认为，在本项目实施的最初阶段，不会有单个的全球性“信任域”（例如在联合国某组织层面），而是会有区域级别甚至国家级别的若干个“信任域”。[7]尽管如此，考虑到需要确保各信任域之间的互操作性，即使建立分散的信任域也将改进身份管理系统。

一旦确定了（相关信任域内）信任设施的体系结构，就可着手起草经由协调委员会框架内谈判达成的一套组织、监管和技术文件。因此，必须确保相关信任域框架内的互操作性。

---

[6] 其他人道主义组织也可能对这种产品感兴趣，例如，在法律领域有海牙国际私法会议，以及在药品和教育领域；然而，我们认为，这类组织更有可能使用已建立的跨界信任环境，而不是支持开发新的产品。

[7] 使用相同的信任设施的信息和法律环境。

（相关信任域内）协调理事会成员通过这套文件将有助于转入最后阶段，即实际实施有法律意义跨界电子互动系统的阶段。

提请贸易法委员会第四工作组（电子商务）各位专家注意的意见

确保电子商务中各实体和对象安全性和身份识别的问题可通过所提议模式解决（建立和运作矩阵形式的电子商务跨界信任环境的模式，该矩阵在相互关联、其中包括在该电子商务跨界信任环境框架内提供的功能服务的区域和全球群组基础上组建），具体方式如下：

- 建立一个专门用于创建跨界电子商务交易相关身份管理信任域的功能性电子商务跨界信任环境群组；
- 就地域而言，该群组可纳入联合国所有会员国；
- 将通过一家专业运营商或一组相关运营商的商业活动确保该群组的运作；
- 基于电子商务平台框架内采用的一套身份识别办法提供成套的身份管理信任服务可能是专业运营商商业活动的一个方面；
- 将通过与各电子商务平台的协议确立管辖专业运营商商业活动的法律制度。