联合国 A/CN.9/WG.III/WP.136*

大 会

Distr.: Limited
2 September 2015
Chinese
Original: English

联合国国际贸易法委员会
第三工作组（网上争议解决）
第三十二届会议
2015 年 11 月 30 日至 12 月 4 日，维也纳

跨境电子商务交易网上争议解决

俄罗斯联邦提交的材料

秘书处的说明

俄罗斯联邦政府向秘书处提交一份文件，其中载有关于跨境电子商务交易网上争议解决的构想和设计思路。该文件在第三工作组（网上争议解决）上一届会议之前已提交秘书处，但现将其交予工作组。秘书处收到的案文按秘书处收到时的原样转载于本说明的附件。

* 因技术原因于 2015 年 11 月 4 日重新印发。

V.15-06244 (C) GH 201015 201015

附件

关于联合国专门机构和相关国际组织拟订跨界信任空间建立和运作系列建议的构想和设计思路

导言

提出“跨界信任空间”（下称“信任空间”）一语，意指联合国相关专门机构（部门）和国际组织为确保对电子互动当事方（主体）之间国际交换电子文件和数据的信任（相信真实性）而建议的法律、组织和技术条件的组合。

提出“电子互动当事方（主体）”一语，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之内互动的公共当局、自然人和法人组成的整体。

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空间的组建和运作的建议（信任空间建议）时应当讨论的方法和问题。目的是促进为实际落实信任空间建议而构建技术、机构和法律方面的基础设施。

欢迎来自国家机构和企业界的相关代表参与本讨论。

世贸组织对信任空间可能发挥的作用和可能作出的贡献。建立信任空间将有助于实现国际贸易的便利化和发展，世贸组织关注信任空间问题将有助于动员政府和企业界支持其实际实施。令人关切的另一个方面是就电子标准和相关问题开展工作的许多国际和区域组织（例如标准化组织、国际电联、联合国欧洲经委会电子商务中心、贸易法委员会、亚太经合组织等等）之间缺乏工作协调（其最终产出往往缺乏互操作性）。让世贸组织在这一过程中发挥协调作用将使该领域的国际标准化工作更有效率、更有成效。

设计思路

1. 提出信任空间建议的目的是提供保障，确保属于联合国会员国管辖框架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息和通信技术（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. 建议在从事下列活动的专业运营商的业务活动内确保提供上述机构保障：

- 向用户提供一套信通技术信任服务；
- 在既定法律制度内运营，这些法律制度包括但不限于因处理个人数据而给予的限制。

3. 建议对下述可能建立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）通过相互承

认经由信通技术信任服务获得的电子文件，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，就专业运营商业务活动的物质和资金支持提出特殊要求，以防对用户造成损害，包括损害个人数据的情况。

建议在贸易法委员会一份单独的建议中考虑组建和运作信任空间区域组和全球组以及这些组别框架内所提供功能服务所涉及的机构保证和法律制度问题。

4. 建议结合各种功能性应用的重要性描述可能作为基础设施提供的各种信通技术信任服务。这些服务及其得到的信任级别可由功能性信息系统运营商依据威胁、风险、商定法律制度和用户需求而确定。为确保所要求的信任级别，功能性信息系统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方面的基础设施。

可在欧洲经委会——联合国电子商务中心“关于确保有法律意义信托跨界电子互动的建议”中考虑关于组建和运作信任空间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。

可在国际电联、第一联合技术委员会、欧洲电信标准研究所和其他机构的技术标准和建议中就单一信通技术信任服务作出描述。

5. 各种身份识别属性可由管辖专门从事身份识别的运营商和功能性运营商的业务活动的法律制度界定，并利用相关信通技术信任服务来维护。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。

各种身份识别属性和身份识别程序本身可作为确定身份识别办法信任级别的基础。身份识别办法的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（见项目 9）。

6. 建议描述特定国家及其国际联盟在组建共同信任空间的框架内与其他国际论坛的互动机制。

6.1. 在加入旨在确保向电子互动主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，该框架内组建区域信任空间的任务已经确定或解决，包括在该信任空间框架内提供的功能服务；
- 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，这些国际条约和国际监管的部分条款涉及组建区域和（或）功能性信任空间；

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信任空间区域群组，包括在此信任空间框架内提供的功能性信任空间服务，确保对这些国家所指定法律制度内电子互动主体的机构保障；
- 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。这种相互承认应考虑到每个国际论坛的机构保障和信

息安全要求，也许以特定法律制度框架内实行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，一国创建在本国指定的国家法律制度框架内运作的独立的信任空间国家群组；
- 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到这些国家和国际论坛的机构保障和信息安全要求，也许以特定法律制度框架内实行的信息安全网关为基础。

7. 建议描述针对基于商业协议和（或）行业惯例的法律制度而言各群组的组建机制，与项目 6 类似。

8. 建议在将不同群组融合为按照下述特点组建的一个矩阵的基础上描述全球信任空间的组建机制：

- 功能服务和区域范围，
- 不同法律制度及其变式。

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信任空间矩阵的关键因素。

创建此类网关的目的是促成全球信任空间不同群组之间的互动。网关组建可以考虑所有必要的方面：法律、组织和技术方面。

组建典型的信息安全网关的办法可以考虑到不同信任空间群组之间存在着可能不同层面的互动。尤其是，网关组建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。

组建典型的信息安全网关的办法可以考虑使用转换轮廓图，描述并配置自一个群组到另一个群组的转换。这些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。

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若干类别的信息安全网关加以描述。

摘要

跨界电子文件交换问题是热门议题，在全球和区域文件中均曾提到，例如：

- 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（有关 2015 年之后的信息社会世界峰会的 WSIS+10 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，努力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，在全球范围内促

进对电子环境的信心和信任（2012 年亚太经合组织领导人宣言，《符拉迪沃斯托克宣言——融合谋发展，创新促繁荣》）

目前世界上有几种解决这项任务的良好做法：

- 欧盟委员会——基于欧洲议会和欧洲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条例（项目 eIDAS[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构想；[2]
- 亚洲太平洋区域——基于泛亚洲电子商务联盟。[3]

全球经济发展需要，尤其是在危机期间，要求启动不同经济和社会领域的融合进程，包括籍由在创新基础上利用现代信通技术。这些正是提议拟订的信任空间系列建议旨在解决的任务。

提请贸易法委员会第三工作组（网上争议解决）的专家注意的意见

网上解决中原告和被告的身份识别问题可在上文所提议模式的范围内（该模式是，组建和运作作为一个矩阵的跨界信任空间，该矩阵由相互关联的区域群组和全球群组组成，其中包括在该信任空间框架内提供的功能服务）以如下方式解决：

- 一方组织专门支持跨界电子商务交易网上解决程序的功能性信任空间群组；
- 所有联合国会员国可参与该群组的布局；
- 该群组的运作通过一家专业运营商或一组相关运营商的业务活动得以维持；
- 专业运营商业务活动的内容可以是基于电子贸易平台框架采用的一组身份识别办法提供成套身份识别信任服务；
- 管辖专业运营商业务活动的法律制度应通过与各交易平台协议确立。

在上述内容的基础上，提议对网上解决程序规则作如下修改：

应将第 4A 条第 4(h)款重拟如下：

联合国电子商务中心“关于确保有法律意义信托跨界电子互动的建议”所载明的原告和（或）原告代表的签名或其他身份识别和认证手段。

应将第 4B 条第 2(g)款重拟如下：

联合国电子商务中心“关于确保有法律意义信托跨界电子互动的建议”所载明的被告和（或）被告代表的签名或其他身份识别和认证手段。

---

[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/。

关于联合国专门机构和相关国际组织
拟订跨界信任空间建立和运作系列
建议的构想和设计思路的增编

有法律意义跨界电子互动的共用信任基础设施

白皮书

建设的目的

互联网已成为各国个人和实体获取电子服务的惯用工具。此类服务的好处是显而易见的，但是存在一些组织和法律问题，妨碍这些服务在用户需要服务有某种信任级别的活动领域得到广泛使用。**主要问题之一是确保电子文件的有效性和一般电子互动的法律意义**。由于参与者的互动涉及不同国家的法域，这一问题迫切需要处理，不管是在国内一级即在特定法域内，还是在跨界一级。不同国际论坛包括联合国（联合国电子商务中心、贸易法委员会）以及区域层面——独联体、欧盟和亚太经合组织——曾多次审议该问题，但尚未找到令人满意的解决办法。

为促成可信的跨境电子互动，通信领域区域联合体[4]的专家着手基于共用信任基础设施（下称“信任设施”）创建跨界信任空间（下称“信任空间”）。其**主要目标是向信任设施用户提供不同资质的信任服务(基本、中等、高等)，供其在电子互动过程中使用。**这使得有可能由用户斟酌决定赋予电子互动以法律意义，而不论其地点和法域如何。

信任空间系统是一个基础性的易扩缩平台，提供对电子信任服务的统一访问。在此考虑了现有电子系统，使其纳入信任空间的升级要求可望降到最低程度。

在就信任空间系统开展工作的过程中，提出了信任设施体系结构，描述了其不同组成部分的互联及其与用户的互动，正在同时就三个方面进行设计：法律、组织和技术方面。通过分析实际实现过程所涉可变因素和信任设施使用说明，得以创建详尽说明该系统所必需的文件清单。

我们认为，推广该新产品的下一步可能是讨论有志于促进、简化跨界电子服务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。

还应当编制规范、组织和技术方面的系列文件，确保相应“信任域”框架内的互操作性[5]（见第 4 § 3 章）。

而且，还计划进而开展组建跨界信任空间这项具体工作，首先是创建国际协调机构并建立相应“信任域”范围内的信任设施体系结构，此后将着手实际实施有法律意义的跨界电子互动系统。

---

[4] 通信领域区域联合体。www.rcc.org.ru。

[5] 使用相同信任设施的信息和法律空间。

确保国际信任：信任设施体系结构

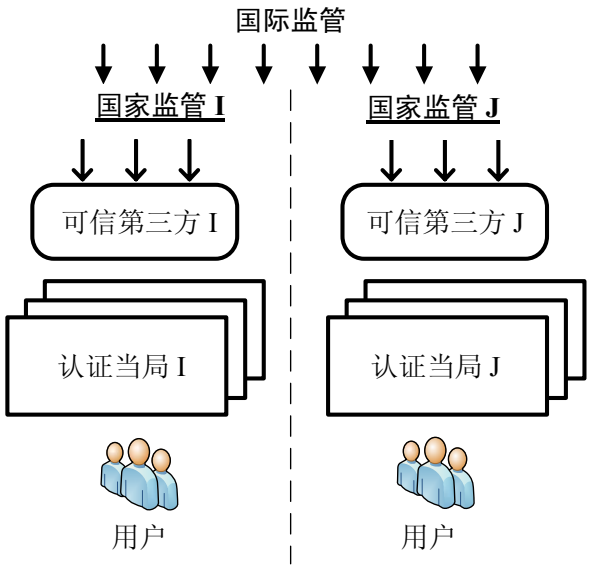
信任空间开发工作正在三个方面开展：法律层面、组织层面和技术层面。采用复合描述使系统作为一个整体及其各单个要素能够正确运作。

选择的信任设施体系结构能够容易地扩缩。它能够由于新参与方的加入而在考虑的任何层面容易地扩展，如新的法域、新的超国家参与方、新的信任服务运营商以及注册系统。

法律层面

信任空间可在单域或多域基础上创建。在法律和组织监管方面，多域基础是最复杂的变化因素。多域体系涉及适用可信第三方（下称“可信第三方”）手段。图一给出法律监管的总示意图。

图 1
跨界信任空间的法律监管



有法律意义跨界信任互动的法律监管可分为两个部分：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；
- 国际标准和条例；
- 跨界信息互动参与方就特定问题达成的协定；
- 示范文书。

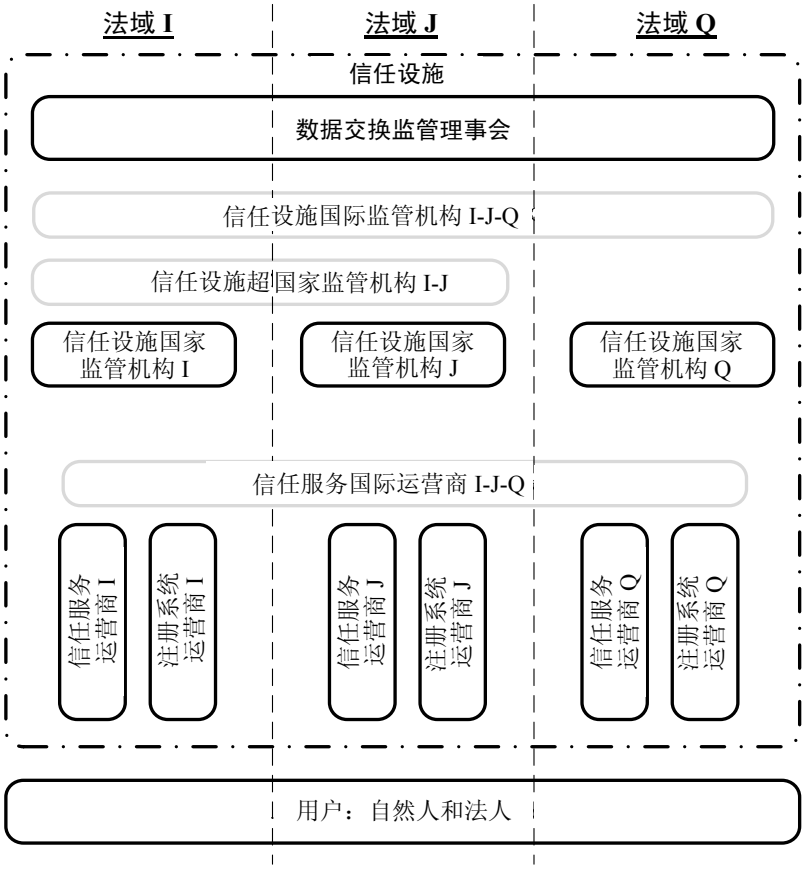
国家法律监管建立在每个特定法域既有的一套规范性文件的基础之上。

组织层面

对不同国家法域提供的信任服务的具有法律意义的相互承认通过信托电子数据交换监管机构协调理事会（下称“数据交换监管理事会”）的设立和运作得到实现。该机构的活动由数据交换监管理事会章程来规范，该章程须由得到授权的所有成员——即主要由信任设施国家监管机构所代表的电子数据交换监管机构——予以承认和签署。

组织方面的监管可见下图（见图 2）：

图 2
跨界信任空间的组织监管（灰框表示可选内容）



数据交换监管理事会发布了与其章程有关的若干文件：

- 对数据交换监管理事会成员的要求，与其交换信函是成为数据交换监管理事会正式成员的前提条件；
- 关于为获准加入数据交换监管理事会而进行“影子”监管和定期互审以保留数据交换监管理事会自愿会员资格的准则；

- 信任设施服务运营商和注册系统运营商须满足的合规标准，以及这些标准的适用方法；
- 对信任服务运营商和注册系统运营商是否满足这些标准的估计/核查方法。

在信任空间，每个法域由信任设施国家监管机构代表（见图 2，信任设施国家监管机构 I、J、Q），这些监管机构监管其法域内信任服务运营商和注册系统运营商的活动。

对于高度一体化的国家集团（例如，欧亚经济共同体或欧盟）而言，存在着组建信任设施超国家监管机构的可能性（见图 2，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。

通过数据交换监管理事会接纳新成员程序（新的法域和超国家参与方），以及对信任设施服务运营商和注册系统运营商（新的服务和注册系统运营商）是否满足数据交换监管理事会发布的标准进行核查的办法，信任设施的自然可扩缩性得到启用。

如果数据交换监管理事会成员（见下文）达到有条件的“中等”信任级别，它们可以着手创建信任设施国际监管机构和信任服务国际运营商（见图 2，信任服务国际监管机构 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和各信任设施国家监管机构的互动（根据数据交换监管理事会章程）和各信任设施国家监管机构之间的互动。

要想成为信任服务运营商或注册系统运营商，相应服务的供应商应接受相同法域信任设施国家监管机构的认证。信任服务国际运营商应接受信任设施国际监管机构的认证。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，均由数据交换监管理事会发布的合规标准和相应的监管机构可能发布的国家补充标准来规范。

在信任空间，电子服务的用户既可以是个人，也可以是法律实体。用户斟酌决定或通过协议选择必要信任级别的服务资质。

服务由相应供应商——信任服务运营商——提供。有些情况下，服务也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经由共用信任基础设施而融合在一起。

信任服务作为信任空间要素的实现可能涉及不同的变化因素，视信息互动参与方之间的信任级别而定。例如，若数据交换监管理事会成员之间是有条件的“高等”或“中等”互信级别，则使用按照商定标准实施的集中化国际服务效率较高。就有条件的“低等”信任级别而言，则根据分散原则建立信任服务——每个国家使用本国的服务。

技术层面

信任服务的实现可能有多种技术选择。对信任设施各要素的主要要求是互操作性。这一层面的监管通过适用数据交换监管理事会文件规定的不同标准和说明来实施。

信任服务在技术上是否可行可通过在跨界电子互动过程中核实电子签名来证明。为比较起见，给出实现信任设施所涉及的两个变化因素：分散性办法——信息互动参与方之间为有条件的“低等”信任级别（见图 3），以及集中化办法，它们之间为“中等”信任级别（见图 4）。

图 3

“低等”信任级别信任空间框架内的电子签名核实（分散性办法）

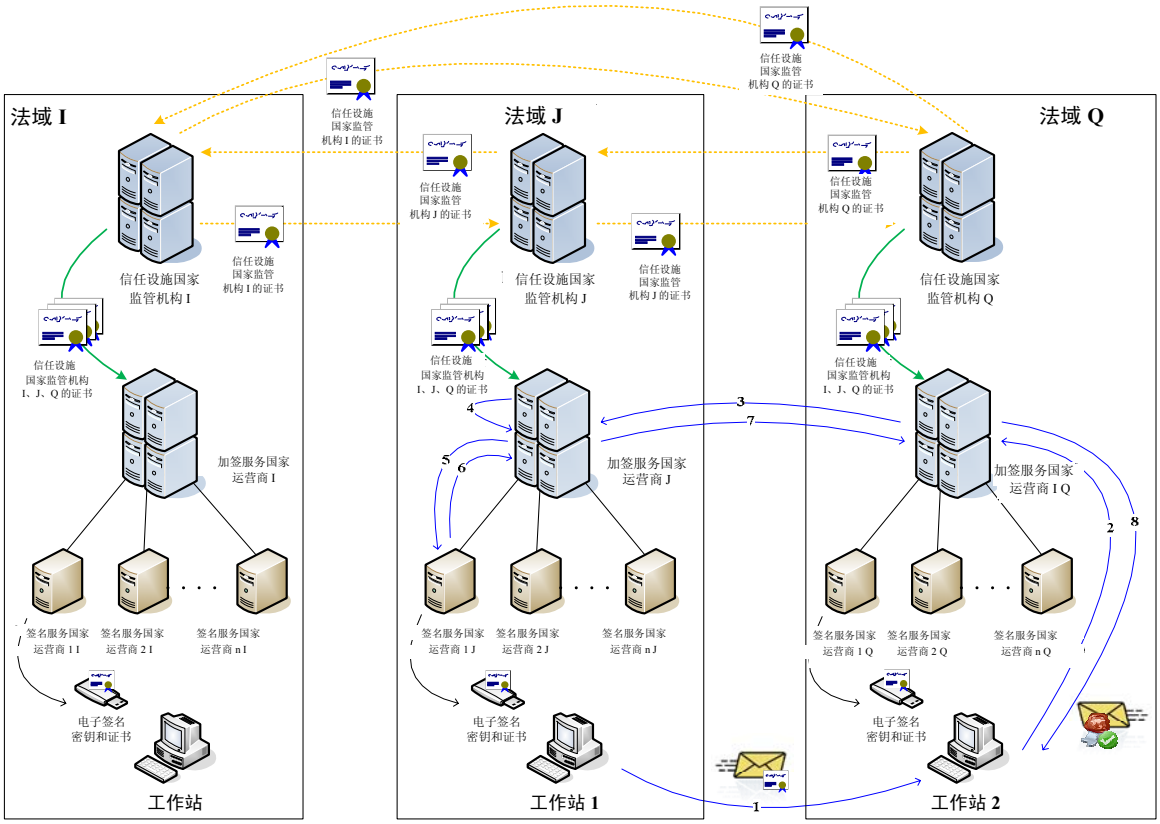


图 4

“中等”信任级别信任空间框架内的电子签名核实（集中化办法）

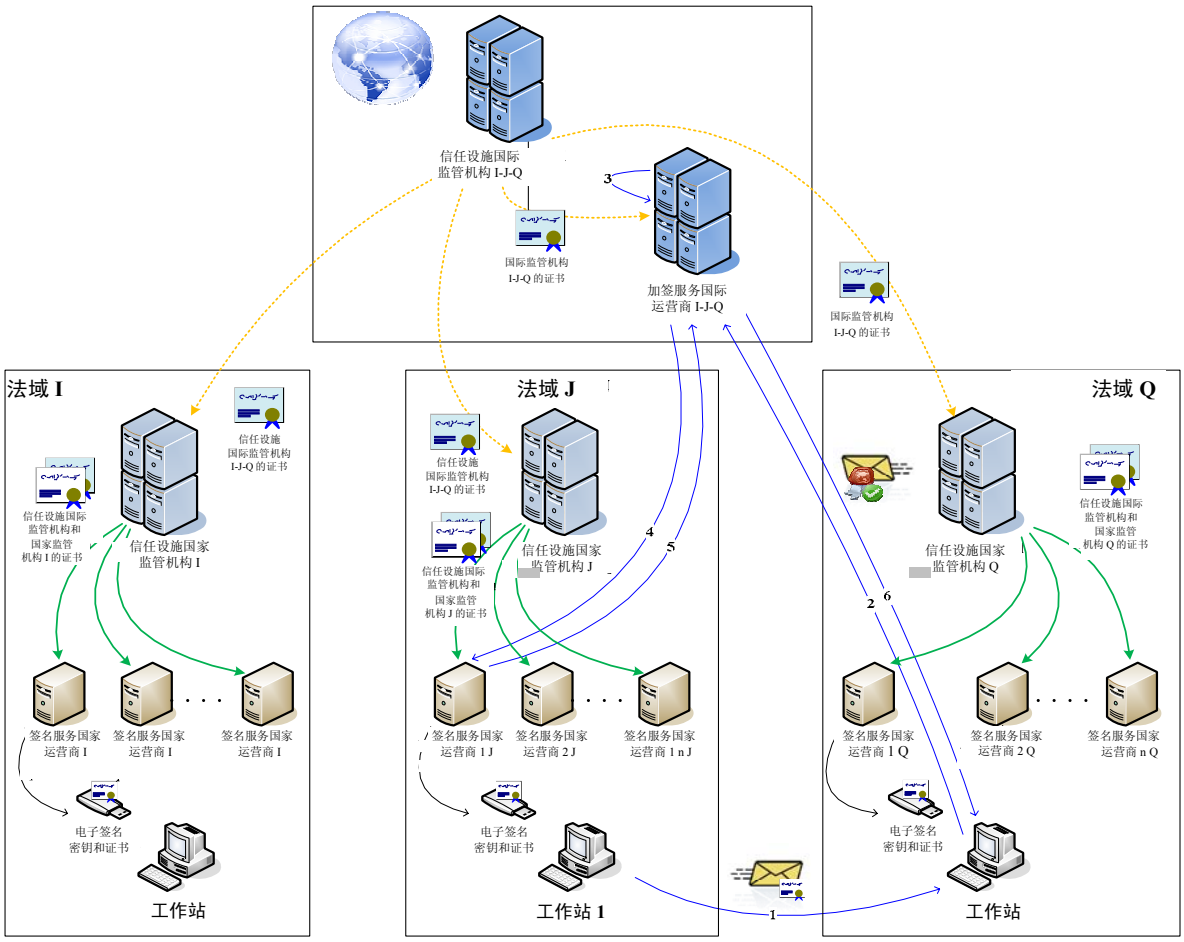


表 1 列示信任设施分散性办法和集中化办法的具体特点。表 2 描述实现信任设施所涉两个变化因素的电子签名程序。

表 1
用于“低等”和“中等”信任级别信息互动的信任设施特点

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（AS）运营商提供。 2. 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，相互交换证书（）。 4. 国家监管机构向属于其法域的信任服务国家运营商提供其证书和其他法域国家监管机构的证书（）。	1. 加签服务由 AS 国际运营商提供。 2. 不涉及国际组织：信任服务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实施国际监管机构实现互动。同样，信任服务国家运营商通过相应的国际运营商实现互动。 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. 国家监管机构向属于其法域的信任服务本国运营商提供其证书和国际监管机构的证书（）。

表 2
“低等”和“中等”信任级别选项的电子签名核实程序

低等信任级别（图 3）	中等信任级别（图 4）
1. 个人/实体 1 在法域 **J** 发送有电子签名的文件，同时选择信任设施提供的所用信任服务的必要资质等级(基本、中等或高等)。 2. 向属于法域 **Q** 的加签服务（AS）国家运营商转发要求核实附有 **J** 法域电子签名的文件的请求。 3. 向属于 **J** 法域的 AS 国家运营商转发要求核实文件的请求。 4. 对 **J** 法域的电子签名进行数学认证。 5/6. 向 **J** 法域签名服务（SS）国家运营商发送关于证书状况的请求/答复。 7. **Q** 法域的 AS 国家运营商收到关于 **J** 法域电子签名正确性的收条。 8. **Q** 法域 AS 国家运营商对收条作证明，并将其转发给个人/实体 2。	1. 个人/实体 1 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所用信任服务的必要资质等级(基本、中等或高等)。 2. 要求核实附有 **J** 法域电子签名的文件的请求转发给 AS 国际运营商 **I-J-Q**。 3. 对 **J** 法域的电子签名进行数学核实。 4/5. 向 **J** 法域签名服务国家运营商发送关于证书状况的请求/答复。 6. AS 国际运营商 **I-J-Q** 对收条作证明，并将其转发给个人/实体 2。

网上争议解决中原告和被告的身份识别

上述模式是，组建和运作作为一个矩阵的跨界信任空间，该矩阵由相互联系的区域群组和全球群组组成，其中包括在该信任空间框架内提供的功能服务，在该模式中，网上争议解决（下称“网上解决”）中原告和被告的身份识别问题可以如下方式解决：

- 一方组织专门支持跨界电子商务交易网上解决程序的功能性信任空间群组；
- 所有联合国会员国可参与该群组的布局；
- 该群组的运作通过一家专业运营商或一组相关运营商的业务活动得到维持；
- 专业运营商业务活动的内容可以是基于电子贸易平台框架采用的一组身份识别方法提供成套身份识别信任服务；
- 管辖专业运营商业务活动的法律制度应通过与各交易平台协议确立。

进一步的步骤

1. 促进这项开发工作的下一阶段可能是讨论有志于促进、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主要是政治和经济方面的。[6]已经部分参与这一工作领域的政治论坛既有超国家组织（例如独联体、亚太经合组织、欧盟、上海合作组织），也有一些国家之间的双边关系。有志于实现这一目标的经济论坛可能是，例如相应的联合国机构，如联合国电子商务中心/欧洲经委会、贸易法委员会（第三工作组和第四工作组）以及欧洲经委会、欧洲经济区、欧亚经济共同体等等。

2. 此外，还计划进而开展组建跨界信任空间这项具体工作，先是创建国际协调机构（信托电子数据交换监管机构协调理事会，见图 2）。该理事会应通过其章程和管辖其活动的其他规范文件（见第 3.2 章），确定共用信任基础设施（信任设施）的具体体系结构、拟提供的一套信任设施信任服务及其可能的资质等级（可能取决于提供这些服务的运营商的法域）。

世界不同区域现有的自然属性（历史、文化、政治、经济、技术等方面）可能导致不同的论坛按照每一论坛内的信任级别和上述自然属性创建“自身的”协调机构（数据交换监管理事会）和信任设施体系结构。

因此，我们设想，在本项目的最初阶段，不会有供整个地球使用的单个“信任

[6] 其他人道主义论坛也可能对这种产品感兴趣，例如，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信任空间，而不是支持新产品。

域”（例如联合国几个机构之间），而是会有若干个“信任域”。[7]

3. 在选定（相应“信任域”的）信任设施体系结构之后，将有可能进而拟订在数据交换监管理事会框架内商定的另一套组织、规范和技术文件。这套文件的系统性特点由第 2 步的结果确定。这样，将确保相应“信任域”框架内的互操作性。

制定和统一各种标准的国际组织可为支持这些项目作出重大贡献。

4. 数据交换监管理事会成员（在相应“信任域”内）采用这套文件将使得能够推进至实施有法律意义跨界电子互动系统的最后阶段。

[7] 使用相同信任设施的信息和法律空间。