联合国 A/CN.9/WG.IV/WP.155

大 会

Distr.: Limited
13 September 2018
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十七届会议
2018 年 11 月 19 日至 23 日，维也纳

身份管理和信任服务跨境法律承认文书草案——德国提案

秘书处的说明

德国向秘书处提交了一份文件，供工作组第五十七届会议审议。现将该文件按秘书处收到的原样转载于本说明的附件。

V.18-06083 (C) 021118 021118

附件

身份管理和信任服务跨境法律承认文书草案

重申深信发展信息和通信技术是可持续经济增长和普遍提高生活质量的先决条件；

注意到电子通信提高了国家管理和商业活动的效率，加强了对外经济关系，为以前遥远的当事人和市场提供了新的机会，从而在国家和国际经济发展中发挥了根本作用；

鉴于[文书草案][1]缔约国的国家和市政机构、个人和组织之间互动中电子文件流动的技术和法律监管不确定性构成了电子互动发展的障碍；

深信在电子互动所有参与方之间建立信任是其发展的一项必要条件；

假设统一规则应基于尊重当事人选择适当媒介、技术、身份识别和信任服务的自由，同时考虑到技术中性和功能等同原则，唯需当事人选择的手段与现行法律之目的相关；

认识到集中和分散信任系统所提供的机会和可行性，以及利用这些系统加速推动进步和数字经济，包括可信地实施电子商务和运输、电子争端解决、创建电子政务和电子公共服务、开发在线培训课程、电子保健、各种电子注册、电子金融服务；

兹商定如下：

第一节　适用范围

第 1 条　适用范围

1.　本[文书草案]界定跨境信任环境的基本特征，跨境信任环境是为在公共当局、个人和公司机构之间以电子形式跨境交换信息而建立信任所必需之监管、组织和技术方面条件的总合。

2.　在确定本[文书草案]的适用范围时，既不考虑跨境电子互动参与方的国家归属，也不考虑其民事和法律地位，而且也不考虑其所交换电子文件和电子信息的性质。

3.　跨境信任环境包括以下几个部分：

(1)　集中化——涵盖在电子文件交换中建立信任的监管、组织和技术方面的条件，其中包括对缔约国控制信任服务运营商的活动、这些运营商在跨境电子互动中使用的软件和硬件、信任服务、信任服务运营商合规评估程序以及软件和硬件设定约束性要求；

(2)　自我监管——涵盖在电子信息交换中通过分布式数据库和创建表明跨境电子互动自我监管性质的数据单位建立信任的监管、组织和技术方面条件。

4.　参与方利用跨境信任环境来确保电子互动各方之间的必要信任水平。根据本[文书草案]第 1 条第 3 款，选择跨境信任环境的特定部分或其各部分的组合，取决于需要跨境信任环境提供信任的具体数字服务的性质。

[1] [文书草案]的字样是实际案文的占位符，其形式应由贸易法委员会决定。

第二节　总则

第 2 条　定义

1.　在本[文书草案]中：

(1)　“跨境信任环境参与方”指公共当局、协调理事会、信任服务运营商、分布式数据库运营商以及个人和组织；

(2)　“电子信息”指使用信息和电信网络生成、发送、接收或存储的任何信息；

(3)　“电子文件”指使之法律意义得到承认而拥有必要和充分要件的电子信息，其真确性和真实性由信任服务运营商根据本[文书草案]予以确认；

(4)　“交易记录”指经分布式数据库运营商认证并由这些运营商包含在有意义（有效）数据块中的电子信息；

(5)　“有意义（有效）数据块”指根据分布式数据库运营商建立的规则生成的一组交易记录；不得对其增改；

(6)　“信任服务”指确认电子文件和/或其细节真确性和真实性的服务，包括但不限于与创建和使用电子签名、电子印章、电子时戳、电子交付和网站认证相关的服务；

(7)　“跨境电子互动”指跨境信任环境参与方之间通过信息系统交换电子信息和/或电子文件；

(8)　“协调理事会”指根据本[文书草案]设立的机构，该机构为信任服务运营商的活动、信任服务运营商用于实施跨境电子互动的软件和硬件以及信任服务运营商和硬件和软件符合要求的合规评估程序规定对成员具有约束力的一般要求；它还履行[文书草案]规定的其他职能；

(9)　“所在地”指跨境信任环境当事人指定为居住地的地点，未指定的，则指个人居住地或法律实体的注册地；

(10)　“信任服务运营商”指符合协调理事会规定的要求、持有通过协调理事会规定的程序获得的合规确认书、并在跨境信任环境的集中部分范围内提供信任服务的个人或法律实体；

(11)　“分布式数据库运营商（数据挖掘人）”指使用必要软件和硬件，通过记录交易并检查交易真实性、在分布式数据库中形成数据块并检查数据块完整性，参与跨境信任环境自我监管部分的个人或法律实体（包括匿名行事者）；

(12)　“用户”指作为电子信息和/或电子文件的发送人或接收人的公共当局、个人或组织，包括通过跨境信任环境自我监管部分提供的服务发送或接收的电子信息和/或电子文件；

(13)　“信息系统”指为在跨境电子互动中创建、发送、接收、存储或以其他方式处理电子信息——包括电子文件——的而设计和使用的信息技术和设备的总和；

(14) “电子签名/印章”指电子数据，其在物理上附加于其他电子数据上或在逻辑上与其他电子数据相关联，由签名人用来签名，并记录签名人与其他电子数据之间的某种关系，以便第三方以后能够验证这种关系的存在；

(15) “签名人”指用电子签名/印章签署电子文件的个人（电子签名）或法律实体（电子印章）；

(16) “电子签名/印章的合格证书”指将数据与自然人（签名）或法人（印章）联系起来以验证电子签名/印章并至少确认其身份的电子确认；合格证书由根据本[文书草案]第 8 条第 6 款通过了合规程序并且符合协调理事会的要求的信任服务运营商签发；

(17) “电子时戳”指将其他电子数据绑定到特定时间并记录该时间点电子数据存在的电子数据，允许电子互动参与方或第三方以后确定这一事实；

(18) “电子注册交付服务”指允许第三方之间进行电子数据传输并提供有关传输数据处理的证明的服务，包括数据发送和接收证明；此种服务保护所传输数据免于丢失、盗窃、损坏或未经授权更改；

(19) “合格网站认证证书”指一种电子确认，其允许通过网站认证将网站与信任服务运营商向其签发了该确认的自然人或法人实体相关联，信任服务运营商根据本[文书草案]第 8 条第 6 款通过了合规程序，并且符合协调理事会的要求；

(20) “身份”指关于特定主体（此处：用户）的信息，以一个或多个属性的形式允许在特定情况下充分区分该主体；

(21) “身份识别手段”指包含特定主体（此处：用户）身份的物质和/或非物质单元；

(22) “身份管理”指一组功能和能力（如行政管理和维护、发现、通信交换、关联和绑定、政策执行、认证和宣称），用于㈠保证身份信息（如标识符、证书、属性）；㈡保证实体身份；㈢支持商业和安全应用；

(23) “初级（基本）身份识别”指不论任何特定情况，收集、验证并核证特定主体（此处：用户）的充足身份属性以确定并确认其身份的过程。

初级身份识别通常由颁发当时相关基本身份证明（如出生证明、国民身份证、护照等）的机构进行。

(24) “二级（交易性）身份识别”指在特定环境下收集、验证并核证特定主体（此处：用户）的充足身份属性以确定并确认其身份的过程。

二级身份识别由信任服务运营商进行，或是(a)注册时申请人的身份识别，以便成为信任服务运营商所提供信任服务的用户，或是(b)用户的身份识别，以使用特定信任服务。

(a) 为在注册时对申请人进行身份识别，信任服务运营商通常使用基本身份证明或者申请人先前其他身份识别的现已存在的结果。在对申请人成功进行身份识别后，信任服务运营商建立/签发自备用户二级身份记录（二级身份证明）；

(b) 为使用特定信任服务而对用户进行身份识别，信任服务运营商要求已根据本定义(a)项拥有其用户身份的用户使用其二级身份证书（以知道、占有（包括生物识别）的方式）来证明其身份。

(25) “身份识别系统”指由一套系统规则加以规范的身份识别交易（网上）环境，在这种环境中，自然人或法人由于权威来源确定并认证其身份而能够彼此信任。身份识别系统涉及以下方面：(a)一套规则、方法、程序和常例、技术、标准、政策和流程，(b)适用于一组参与实体，(c)对收集、验证、存储、交换、认证以及依赖关于自然人或法人身份属性信息加以规范，(d)目的是便利身份识别交易。

(26) “身份识别交易”指涉及两个或多个参与方参与身份信息的确定、验证、签发、宣称、吊销、发送或依赖的任何交易。

(27) “身份识别提供商”指(a)负责对自然人或法人进行身份识别、签发相应身份识别手段并维护和管理此类身份信息的实体。

(28) “已备案身份识别系统”指下述身份识别系统：(a)符合协调理事会的要求，且(b)按照本[文书草案]第 5 条第 2 款的规定已由运营该身份识别系统的身份识别提供商报备协调理事会；

(29) “已备案身份识别系统的保证级别”指由运营该识别系统的身份识别提供商根据本[文书草案]第 5 条第 2 款所规定的对协调理事会的要求确定的已备案身份识别系统的属性（特征）；

(30) （协调理事会）“成员”指下述法律实体：㈠在相关国内法律中拥有执行对身份管理和信任服务的法律承认的法律权力和权限，且㈡正式承认本[文书草案]的所有条款。

第 3 条 解释

1. 在解释本[文书草案]时，应考虑到本[文书草案]的国际性，并考虑到促进本[文书草案]统一适用以及在跨境电子互动中遵守诚信和本[文书草案]第 5 条所载明的其他原则的必要性。

2. 涉及本[文书草案]所管辖事项的问题，未在本[文书草案]中明确解决的，应当按照本[文书草案]所依据的一般原则加以解决，在无此种原则的，应当按照国际私法规则指定的适用法律加以解决。

第 4 条 原则

跨境信任环境范围内的跨境电子互动基于以下原则，这些原则适用于跨境信任环境的两个部分：

(1) 技术中性

(2) 在所提供的身份管理和信任服务方面的功能等同；

(3) 在跨境电子互动中保护受限信息，即受国际法和缔约国国内立法保护的信息，包括商业秘密和个人数据；

(4) 任何信息、文件和信息的使用，包括分布式数据库中数据块的使用，完全是为了不违反国际法和缔约国国内立法之目的；

(5) 经济中立促成实现身份管理和所提供的信任服务方面的成本效益和不失真；

(6) 相称性，即行动的内容和形式必须与所追求的目标一致；

(7) 当事人意思自治：参与方选择适合其具体业务要求的媒介、技术、身份识别和信任服务的自由；

(8) 不歧视。

第三节 协调理事会

第 5 条 协调理事会的职能

1. 协调理事会在跨境信任环境的集中部分是履行理事机构职能的机构，在跨境信任环境的自我监管部分是履行便利人职能的机构。

2. 在跨境信任环境的集中部分范围内，协调理事会应至少核准下列一套要求、程序、政策和条件，参与方明显遵守这些要求、程序、政策和条件，即可支持对身份识别结果和身份识别手段以及信任服务使用结果的相互承认:

A. 身份管理

(1) 对用于进行可备案的初级身份识别的身份识别系统的特性和特征的要求。

这些要求应注意的是，身份识别系统是在缔约国国内环境下建立和运营的，必须尊重相关的国内立法，包括关于身份识别系统认证的国内规定。

这些要求应注意为确定已备案身份识别系统的不同保证级别提供机会；

(2) 已备案身份识别系统的身份识别提供商对任何损失的赔偿责任范围；

(3) 对所获得的身份识别结果和已备案身份识别系统的身份识别提供商所签发的身份识别手段给予相互承认的程序；

(4) 法律效力的确定——就本[文书草案]而言——以已备案身份识别系统的使用加以证实，包括相互承认所获得的身份识别结果和已备案身份识别系统的身份识别提供商所签发的身份识别手段；这方面应注意已备案身份识别系统的不同保证级别；

(5) 已备案身份识别系统的基本使用条件；

(6) 对用于信任服务运营商进行用户二级身份识别的身份识别系统的特性和特征的要求；

(7) 争议解决规则。

B. 信任服务

(1) 信任服务运营商操作程序要求，包括民事责任保险和信任服务运营商审计；

(2) 跨境电子互动所使用软件和硬件的要求；

(3) 信任服务运营商的合规评估程序，包括进行用户二级身份识别所使用的身份识别系统以及硬件和软件（审计）的合规评估；

(4) 信任服务运营商对任何损失的赔偿责任范围；

(5) 争议解决规则；

(6) 对从事信任服务运营商合规确认的机构和（或）个人的要求，包括进行用户二级身份识别所使用的身份识别系统以及硬件和软件（审计）的合规评估；

(7) 本[文书草案]第 15、16、17、18、19 和 20 条界定的使用信任服务的基本条件。

C. 本[文书草案]中规定的其他文件

3. 成员同意根据本[文书草案]执行或实施行公共实体和地方自治政府、用户、运营商以及在其管辖范围内的信任服务机构根据本条第 2 款制定的协调理事会的法律文件。

4. 在跨境信任环境自我监管部分，协调理事会：

(1) 核准关于确认分布式数据库运营商加入相应数据库的建议程序；

(2) 核准向协调理事会报备分布式数据库信息事件——即电子信息、交易记录、分布式数据库中数据块的使用方式违反国际法和成员的国内立法——的程序；

(3) 安排分布式数据库运营商向协调理事会报备自愿承担后者执行本[文书草案]要求的承诺的程序，以确保任何信息、文件和电文——包括分布式数据库中的数据块——的使用仅用于不违反国际法和成员的国内立法之目的；并向协调委员会通报分布式数据库信息事件。

5. 协调理事会通过的关于跨境信任环境自我监管部分的决定和文件属于咨询性质。

第 6 条 协调委员会的设立和程序

1. 协调委员会由其成员组成，任期四年。每一成员可指定一名经授权的代表。

2. 协调理事会可设立其认为于行使职务所必需之辅助机构。

3. 协调理事会每一成员应有一票表决权。

4. 协调理事会关于其工作管理的决定应以不低于理事会三分之二成员的赞成票作出。

5. 协调理事会关于通过第 5 条第 2 款所述法律文件的决定需获得一致同意。

6. 协调理事会应制定其程序规则，包括理事会主席的选举程序、在跨境信任环境成员的负责代表之间保持互信的程序，以及与核准本[文书草案]第 5 条规定的文件有关的决策程序。

第四节 跨境信任环境的参与方

第 7 条 缔约国的公共当局和地方自治政府

1. 公共当局参与跨境电子互动，以根据本[文书草案]确立的规则以及协调理事会根据本[文书草案]通过的法律文件履行缔约国国内法赋予它们的公共职能。

2. 公共当局有权自行决定参与跨境信任环境的自我监管部分。

3. 公共当局有权在协调理事会确定的情况下，对比本[文书草案]和协调理事会根据本[文书草案]通过的法律文件所确定的要求，设定进行电子互动的补充要求。

第 8 条 信任服务运营商

1. 信任服务运营商是跨境信任环境集中部分的参与方。

2. 信任服务运营商能够在某一成员的边界内和/或在所有缔约国全境提供信任服务。

3. 信任服务运营商有义务遵守协调理事会规定的要求，但取决于信任服务运营商提供服务的地区（缔约国全境或其中一部分），并应以协调理事会规定的方式确认其遵守这些要求。

4. 信任服务运营商必须在互联网上公布其获取或改变信任服务运营商地位的任何信息。信任服务运营商有义务将信任服务业务和信任服务运营商地位的任何变化通知负责成员的主管当局。信任服务运营商有义务向成员的主管当局和协调理事会提供关于跨境电子互动事件的任何信息。协调理事会确定提供跨境电子互动事件相关信息的程序和条款。

5. 信任服务运营商有义务根据协调理事会的要求提供民事赔偿责任保险或拥有足够的财政保障。

6. 信任服务运营商必须经过对信任服务运营商及其所提供的信任服务的合规评估程序（独立审计），包括以协调理事会规定的方式评估用于进行用户二级身份识别的身份识别系统以及硬件和软件是否符合协调理事会的要求。

第 9 条 合规独立审计。保险

1. 只有通过了合规独立审计的信任服务运营商才有权提供信任服务。

2. 根据协调理事会制定的程序被授权的机构或机关可以进行合规审计。

3. 信任服务运营商按照协调委员会规定的要求提供民事赔偿责任保险。

第 10 条　分布式数据库运营商

1. 分布式数据库运营商是跨境信任环境自我监管部分的参与方。

2. 分布式数据库运营商根据自我监管原则安排相互之间以及与用户之间的跨境电子互动，并确保在以下方面遵守本[文书草案]：任何信息、文件和电文——包括分布式数据库中的数据块——的使用，仅用于不违反国际法和缔约国国内立法之目的，以及向协调理事会报告分布式数据库内的信息事件。

3. 分布式数据库运营商自愿向协调理事会报备自愿遵守以下方面要求的通知，使之被承认为符合[文书草案]这些要求的分布式数据库运营商：任何信息、文件和电文——包括分布式数据库中的数据块——的使用，仅用于不违反国际法和成员的国内立法之目的，以及向协调理事会报告分布式数据库范围内的信息事件。此类通知的报备程序以及跨境信任环境成员分布式数据库运营商名单的维护程序由协调理事会制定。

如果协调理事会掌握名单上分布式数据库运营商违反国际法和缔约国国内立法的信息，协调理事会有权拒绝分布式数据库运营商的通知。

4. 分布式数据库运营商与协调理事会之间的互动，以及分布式数据库运营商与用户之间的互动，可在未对运营和使用分布式数据库的法律实体和个人进行身份识别的情况下进行。

5. 当协调理事会收到关于某一分布式数据库运营商违反本条第 2 款中规定的本[文书草案]的要求的信息时，该分布式数据库运营商可能被排除在加入跨境信任环境的分布式数据库提供商的公开名单之外。

第 11 条　用户

1. 用户是跨境信任环境两个部分的参与方。

2. 用户分别按照协调理事会和信任服务运营商制定的规则或者分布式数据库运营商制定的规则交换电子信息和电子文件，视跨境信任环境所在部分而定。

第五节　跨境信任环境的基础设施

第 12 条　信任服务运营商的硬件和软件

1. 信任服务运营商提供服务，仅使用成功通过第 8 条第 6 款和第 9 条第 1 款规定的合规评估程序的软件和硬件。

2. 对信任服务运营商软件和硬件的功能要求，以及对确认软件和硬件符合与技术中性原则一致的既定功能要求的程序的要求，由协调理事会根据第 8 条第 6 款和第 9 条第 1 款和第 2 款制定。

第 13 条　分布式数据库运营商的硬件和软件

分布式数据库运营商独立确定验证交易、创建和存储记录真实性和完整性以及验证数据块完整性所需的软件和硬件要求。

第 14 条　用户的软件和硬件

用户须自行制定关于跨境电子互动中使用的软件和硬件符合信任服务运营商要求的规定。

第六节　跨境信任环境集中部分范围内的信任服务

第 15 条　电子签名

1. 不得仅以电子签名为电子形式或不符合合格电子签名的要求为由，否定电子签名的法律效力和作为法律程序证据的可采性。

2. 高级电子签名应满足以下要求：

(a) 应与签名人有独一关联；

(b) 应能够识别签名人的身份；

(c) 应使用签字人使用的在其唯一控制下的电子签名创建数据创建电子签名；

(d) 应链接到以此签署的数据，其链接方式应能检测到数据的任何后续变化。

3. 合格电子签名是基于合格电子签名证书并使用根据第 8 条第 6 款验证的软件和硬件创建的高级电子签名。合格电子签名应具有与手写签名同等的法律效力。

高级电子签名不是合格电子签名的，在根据当事人关于使用此种签名的协议或根据缔约国的监管法律文件所确定的情况下，应具有与手写签名同等的法律效力。

4. 合格电子签名基于某一成员管辖下签发的合格证书的，应被所有其他成员承认为合格电子签名。

第 16 条　电子印章

1. 不得仅以电子印章为电子形式或不符合合格电子印章的要求为由，否定电子印章的法律效力和作为法律程序证据的可采性。

2. 高级电子印章应满足以下要求：

(a) 应与印章创建人有独一关联；

(b) 应能够识别印章创建人；

(c) 应使用印章创建人使用的在其唯一控制下的电子印章创建数据创建电子印章；

(d) 应链接到与其有关联的数据，其链接方式应能检测到数据的任何后续变化。

3. 合格电子印章是基于合格电子印章证书并使用根据第 8 条第 6 款验证的软件和硬件创建的高级电子印章。合格电子印章应享有数据完整性推定以及与合格电子印章相关联的该数据来源正确性推定。

高级电子印章不是合格电子印章的，在根据当事人关于使用此种印章的协议或根据缔约国的监管法律文件所确定的情况下，应享有数据完整性推定以及与合格电子印章相关联的该数据来源正确性推定。

4. 合格电子印章基于某一成员管辖下签发的合格证书的，应被所有其他成员承认为合格电子印章。

第 17 条 电子时戳

1. 不得仅以电子印章为电子形式或不符合合格电子印章的要求为由，否定电子印章的法律效力和作为法律程序证据的可采性。

2. 合格电子时戳产生对于此种合格电子时戳所证明的指定日期和时间的准确性以及数据完整性的推定。

3. 合格电子时戳应满足以下要求：

(a) 应将日期和时间与数据绑定，其方式应合理排除无法检测数据发生变化的可能性；

(b) 应基于与协调世界时连接的准确时间来源；

(c) 应使用高级电子签名签署，或加盖通过了第 8 条第 6 款规定的合规程序的信任服务运营商的高级电子印章。

4. 在一成员管辖下签发的合格电子时戳，应为其他所有成员承认为合格电子时戳。

第 18 条 电子登记交付服务

1. 使用电子登记交付服务发送和接收的数据，不得仅以其为电子形式或不符合合格电子登记交付服务的要求为由，否定其法律效力和作为法律程序证据的可采性。

2. 使用合格电子登记交付服务发送和接收的数据，产生对于数据完整性、此种数据由经识别的发送人发送、此种数据由经识别的接收人接收、以及合格电子登记交付服务所指明的发送和接收日期和时间准确性的推定。

3. 合格电子登记交付服务应满足以下要求：

(a) 由按照本[文书草案]第 8 条第 6 款通过了合规程序的一个或多个信任服务运营商提供；

(b) 以高度信任确保对发送人的身份识别；

(c) 确保在交付数据之前对收件人的身份识别；

(d) 数据发送和接收以合格信任服务运营商的高级电子签名或高级电子印章加以保证，其方式应排除无法检测数据发生变化的可能性；

(e) 向数据发送人和收件人清楚表明发送或接收数据所需数据的任何变化；

(f) 合格电子时戳注明数据发送、接收和任何变化的日期和时间。

4. 在一成员管辖下获得的使用合格电子登记交付服务的结果，应为其他所有成员承认是使用合格电子登记交付服务的结果。

第 19 条 网站认证

1. 合格网站认证证书应包含：

(a) 至少以适合自动处理的形式表明证书已作为网站认证的合格证书签发；

(b) 一组明确无误代表签发合格证书的信任服务运营商的数据；

(c) 系自然人的：至少包括获颁发证书人的姓名或假名；系法人的：至少包括获颁发证书法人的姓名，适用的，还包括官方登记册上注明的注册号；

(d) 获颁发证书自然人或法人的地址内容，至少包括城市和国家，适用的，还包括官方记录中载明的地址内容；

(e) 获颁发证书自然人或法人经营的域名；

(f) 证书有效期具体起讫时间；

(g) 证书识别码，该识别码必须是信任服务运营商独有的；

(h) 根据本[文书草案]第 8 条第 6 款通过合规程序的发证信任服务运营商的高级电子签名或高级电子印章；

(i) 可用以查询合格证书有效性状态的证书有效性状态服务的位置。

2. 基于在一成员管辖下颁发的合格网站认证证书的网站认证信任服务的使用结果，应被承认是其他所有成员使用基于合格网站认证证书的网站认证信任服务的结果。

第 20 条 其他信任服务

1. 协调理事会还可在其监管范围内包括本[文书草案]第 15-19 条未指明的其他信任服务。

2. 对其他信任服务的监管应当类似于对[文书草案]第 15-19 条中提及的信任服务的监管。

3. 为了促进这些服务的普遍跨境使用，应该有可能在所有缔约国的法律程序中作为证据使用信任服务。除本[文书草案]另有规定外，应由国内法界定信任服务的法律效力。

第 21 条　承认第三国及国际组织的信任服务

1.　如果协调理事会与第三国或国际组织获授权机构根据本条第 2 款达成协议，根据第三国或国际组织的立法获授权的运营商提供的信任服务，可被承认在法律上等同于根据本[文书草案]第 8 条第 6 款通过了合规程序的运营商提供的信任服务。

2.　本条第 1 款提及的协议除其他外应规定:

(1)　对第三国或国际组织的信任服务运营商的要求不低于对根据本[文书草案]提供信任服务的信任服务运营商的要求；

(2)　作为协议当事方的第三国或国际组织在其境内（在其管辖范围内）承认，根据本[文书草案]第 8 条第 6 款通过了合规程序的信任服务运营商所提供的服务，与根据签署协议的第三国或国际组织的立法获授权的信任服务运营商所提供的服务在法律上等同。

第七节　保护跨境电子互动参与方的权利和利益

第 22 条　司法保护

1.　电子文件和电子信息，包括[文书草案]第 15-20 条所述信任服务的使用结果，被成员的所有法院和仲裁法院接受为证据。

2.　电子文件所认证的法律上的权利具有与纸质文件所认证的权利同等的可执行性。

第 23 条　争端解决

1.　协调理事会通过在跨境信任环境的集中部分范围内行政解决跨境电子互动所引起的争端的规则。

2.　跨境电子互动参与方有权就跨境电子互动争端解决程序达成双边和多边协议。