联合国 A/CN.9/WG.IV/WP.145

大 会

Distr.: Limited
20 February 2017
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第五十五届会议
2017 年 4 月 24 日至 28 日，纽约

与身份管理和信任服务有关的法律问题

美利坚合众国的建议

秘书处的说明

美利坚合众国向秘书处提交了一份文件，供工作组第五十五届会议审议。该文件按秘书处收到时的原样转载于本说明的附件。

V.17-01088 (C) 070317 070317

附件

一. 导言

第四工作组（电子商务）在第 54 届会议上开始讨论身份管理和信任服务这一议题。工作组暂定的初步结论如下：

> 118. 经过讨论，工作组一致认为，今后在身份管理和信认服务方面的工作应当限于为商业目的而使用身份管理系统，这一工作不应考虑身份管理服务供应商的私营或公营性质。
>
> 119. 工作组还一致认为，可以优先进行身份管理方面的工作。还一致认为，侧重点应当是多方身份系统以及自然人和法人，但不排除酌情对两方身份系统以及实体对象和数字对象进行审议。
>
> 120. 此外，会议一致认为，工作组应当为继续开展工作而进一步明确项目目标，具体指明项目范围，确定所适用的一般原则，并拟订必要的定义。

（A/CN.9/897，第 118-120 段）。

为帮助使工作组第五十五届会议的讨论有所侧重，美利坚合众国代表团编写了本文件，以期提供一个问题提纲供工作组审议。毫无疑问，工作组需要审议许多其他问题，但下面的初步清单可望用作指导初始讨论的起点，并帮助使工作组的工作有所侧重。我们希望通过讨论这些问题以及工作组可能查明的其他问题，可以向秘书处提供指导，以便其编写一份关于身份管理的工作文件。

我们理解专家们在闭会期间曾就相关术语进行非正式讨论。虽然我们认为最终必须认真考虑本项目拟使用术语的定义的措词，但在此初始阶段，我们建议工作组考虑使用初步定义，仅将其作为基础以便为讨论提供便利。不过，我们认识到，最终可能需要就更为详尽的法律和技术定义达成一致意见。

二. 项目的目的和目标

作为起点，工作组不妨考虑项目的总体目的和目标。鉴于已初步决定重点考虑为商业目的使用身份管理系统，工作组不妨考虑下列目的和目标有哪些可能适合本项目：

- 促进建立一个私营部门身份生态系统；
- 查明和消除商业身份交易面临的法律障碍；
- 消除对于现有法律是否适用于商业身份交易的模糊性；
- 鼓励商业上使用和依赖第三方数字身份证书；
- 促进网上商业身份交易所需要的信任；
- 通过为决定在商业交易中是否信任数字身份信息提供依据为私人当事人提供帮助；
- 查明和消除电子认证面临的跨境障碍；

- 便利跨境承认数字身份信息；以及
- 增进对电子商务的信心。

三. 拟议的第四工作组工作成果的性质

开始审议工作组在商业身份管理领域想要拿出的工作成果的类别也许有所助益。

四. 指导原则

不论工作组拟拿出的工作成果最终采取什么形式，工作组都不妨审议并酌情通过一些一般原则，以指导其身份管理方面的工作。如同拟订《电子商务示范法》和《联合国国际合同使用电子通信公约》一样，可用这些一般原则指导工作组的审议工作。此外，指导原则可能有利于帮助澄清工作范围。工作组似宜考虑的可能的指导原则包括下述原则：

A. 身份识别法定义务的来源

作为起点，工作且似宜考虑，除因其他法律而适用的识别商业交易当事人身份的义务之外，任何身份管理法规是否应载列此种义务。如果身份管理法规未载列识别当事人身份的任何义务，则识别商业交易当事人身份的法定要求将留待其他现有法律处理，如管辖公证的法律、“了解客户”要求、反洗钱法或管辖个人数据访问权限的法律。工作组在拟订《电子商务示范法》和《联合国国际合同使用电子通信公约》时对电子签名即采取这种办法。

B. 当事人意思自治

由于身份管理系统通常须遵循系统参与方商定的基于合同的系统规则，因此可能有必要考虑，管辖身份管理交易的任何法律是否以及在多大程度上应当承认并遵从此类系统规则。

因此，工作组似宜考虑当事人意思自治原则是否应适用于商业身份系统，以允许身份系统当事人通过协议变更任何法律规则或某些法律规则的条款。

C. 技术中性

可能会开发和实施许多不同类型的身份系统以用于商业交易。此类系统可能使用多种多样的技术。这些技术可能包括简单的用户名和密码、基于 PKI x.509 标准或其他标准如 SAML 或 OpenID Connect 的较复杂系统。此外，目前还在使用新技术开发一些系统，如 Blockchain。

因此，工作组似宜考虑，与身份管理有关的任何工作成果是否应当明确规定，任何身份管理规则均不应要求使用任何特定技术。

工作组似宜进一步考虑，贸易法委员会如何最佳地处理有多个商业身份系统存在和在用的情况。

当然，专门管辖身份管理的法规以外的法规可能要求当事人使用满足某些要求的身份管理。任何当事人自己可能坚持与其做生意的人们和实体使用特定的身份系统。例如，一个商业实体可能作出限制，只有使用该实体自己已加入的一个或多个特定身份系统的用户才能访问其服务。

D. 系统模式中性

除了所用技术之间的差异之外，目前正在组织结构和业务结构方面对商业身份系统进行大量试验。我们大概可望在将来看到各种身份系统模式之间非常大的差异，即使这些系统采用相同的基本技术。这些包括中间人或枢纽之类的安排 、单一身份供应商模式、单一依赖方模式、组织机构模式和许多其他不同办法。

因此，工作组似宜考虑是否应作为一项原则采用系统模式中性概念——即承认拿出的任何工作成果不应假定或要求身份系统使用任何特定的业务、组织或结构模式，并且能够容易地适应将来身份系统办法、结构和业务模式方面的任何变化。

E. 不歧视

工作组还似宜考虑不歧视原则在为商业目的使用身份系统方面是否适用。根据这项原则，例如，不应仅仅以身份识别采用电子形式为由而否定电子身份识别的法律效力（例如，满足身份识别的法定要求）或在法律程序中作为证据的可采信性。

F. 身份管理法和隐私法之间的关系

涉及身份证书的签发或使用的商业身份交易经常涉及一些个人数据。在此情况下，这种个人数据的隐私性可能很重要。

隐私法通常处理按照相关公共政策对个人数据的保护。因此，工作组似宜考虑这些法律和身份管理系统之间的关系。

G. 身份管理法和数据安全法之间的关系

数据安全对于身份交易的适当运作和可信性至关重要，不仅从保护此类交易所涉个人数据的机密性的角度是如此，对于确保构成交易本身的证书通信的适当运作和可信性来说也是如此。

数据保护法通常按照相关公共政策处理个人数据的安全性。同样，其他数据安全法对于保护身份交易通信的其他方面也发挥同样的作用。因此，工作组似宜考虑这些法律和身份管理系统之间的关系。

H. 基于合同的系统规则和其他法律之间的关系

由于身份管理系统一般须遵循此类系统的参与方商定的基于合同的系统规则（即信任框架），工作组似宜讨论这些规则和非直接与身份相关的适用法之间的关系。

五. 实质性议题

A. 法律承认

工作组不妨审议商业交易中认证的身份信息的法律承认这一议题。在这方面，工作组不妨处理什么是法律承认，法律承认寻求实现什么目的，以及获得法律承认的要求；谁提供法律承认；提供法律承认的目的；法律承认和要求某种形式的身份识别的法律之间的关系，如管辖公证、“了解客户”、反洗钱、个人数据访问权限的法律；以及，如果适用的话，法律承认如何适用于法律实体、设备或数字对象的身份。

B. 跨境相互承认

相互承认的概念非常重要，便利在商业上使用身份证书以及依赖这些证据，不管是在不同身份系统之间还是不同的管辖疆界之间。

对于相互承认议题，工作组似宜考虑许多问题。较为明显的一些问题包括处理：(a)是否应当要求承认证书，(b)如果要求承认证书，应当要求谁承认证书，(c)如果要求承认证书，应当承认哪一方当事人的证书，(d)此种承认的目的何在，(e)“相互承认”的确切含义是什么，(f)应当具备什么特点（例如保证级别）才能得到相互承认，(g)对于何时适用相互承认是否应有限制，以及(h)相互承认是否应当适用于法律实体、设备或数字对象的身份？

C. 确定身份信息归属一个主体

确定身份信息归属一个主体（以便纳入身份证书）常常是身份管理系统的一个关键因素。确定归属方面一个根本问题是何时以及在什么情况下确定证书上的身份数据归属一个特定主体。

工作组似宜从两个角度考虑这些问题。首先，身份供应商是否应当确保其列入身份证书的关于一个主体的信息确实是对证书中所称主体的描述？第二，使用身份证书时，依赖方如何确保证书中的信息与出示证书的主体有关？

D. 依赖/确定行为、数据电文或签名归属一个主体

对身份系统的所有参与方而言，一个关键问题是何时以及在什么情况下，一方当事人依赖一份身份证书是适当且合理的。一方当事人是否合理依赖影响到各种问题，包括何时依赖了错误的身份证书。

例如，《电子商务示范法》第 13 条即结合电子签名处理了这一问题。

E. 赔偿责任/风险分配

赔偿责任和风险分担问题常被称作影响实施商业身份系统的主要障碍。问题包括：(a)身份供应商和身份系统其他参与方担心现行法律下分配给他们的赔偿责任

风险不适当，或者太过繁重，以致他们无法开展工作，以及(b)身份系统参与方担心法律太模糊、含湖不清或不确定，使他们无法正确评估自身的参与风险。

工作组不妨考虑是否应当处理赔偿责任问题，如果是，处理身份系统中哪些角色的赔偿责任，以及如何处理。处理身份管理系统中赔偿责任的法律包括欧洲联盟电子身份识别和服务条例和《弗吉尼亚电子身份管理法》等等。

F. 透明度

身份供应商签发和验证身份证书所用的流程、程序和技术对于使用这些证书的任何身份交易的可信性产生重大影响。因此，身份系统其他参与方了解这些流程、程序和技术如何实施可能非常重要，以便他们能够自己对所进行的身份交易的可靠性和可信性进行评估。为此，工作组似宜考虑身份系统内某些参与方是否应有适当的透明度。如发生违背或损害任何流程、程序、技术、数据库或身份系统一方当事人保管的身份证书的情形，工作组似宜考虑是否应当披露关于此类损害的信息。

在某些情况下，透明度要求也被用来代替规定必须使用某些流程、程序或技术的条例。基于透明度的办法使各方当事人自己能够基于较为完备的信息作出有关可信性的决定。

G. 可信性/保证级别

许多身份系统界定了所谓的“保证级别”，以帮助参与方处理对于身份证书和身份交易可信性的关切。目前有几种保证级别办法，这些办法往往涉及保证的不同分级。例如，欧盟在其电子身份识别和服务条例中界定了三个保证级别（称作“低等”、“高等”和“实质性”），美国和其他地方则使用四个保证级别。

工作组似宜考虑如何最佳地促进身份系统参与方的信任。虽然通常使用保证级别的概念，但工作组还似宜考虑是否可使用其他机制帮助促进信任，如强制性透明度、第三方认证或其他办法。