联合国 A/CN.9/WG.IV/WP.120

大 会

Distr.: Limited
27 July 2012
Chinese
Original: English

联合国国际贸易法委员会
第四工作组（电子商务）
第四十六届会议
2012 年 10 月 29 日至 11 月 2 日，维也纳

身份管理综述

美国律师协会身份管理问题法律工作队提交的背景文件

秘书处的说明

在为第四工作组（电子商务）第四十六届会议做准备的框架内，美国律师协会身份管理问题法律工作队向秘书处提交了所附的文件。

附件中的文件按秘书处收到时的原样转载。

V.12-55145 (C) GX 030812 030812

请回收

一. 导言

1. 2011 年，经合组织的一份报告指出，“数字身份管理是互联网经济进一步发展的基础。”[1] 它是所有实质形式电子商务的一项根本要求。

2. 本文件综合介绍身份管理、身份管理在电子商务中的作用、身份管理提出的法律问题和身份管理面临的法律障碍。[2] 本文件以美国律师协会身份管理问题法律工作队正在开展的工作为基础，[3] 作为背景文件提交，以便就相关问题向工作组提供信息。[4]

3. 委员会 2011 年第四十四届会议商定，应当召集第四工作组（电子商务），在电子可转移记录领域开展工作。[5] 与此同时，委员会商定，将在未来一届会议上审议是否扩大工作组的任务范围以包括 A/CN.9/728 和 Add.1 号文件论及的其他专题，并将这些专题作为单独的主题处理（不讨论其与电子可转移记录可能具有的关系）。[6] 这些专题包括身份管理、单一窗口和移动支付。[7]

4. 如下文所述（第 6-7 段），身份管理是委员会第四十四届会议审议的每个专题（电子可转移记录、单一窗口和移动支付）的一项根本要求。因此，身份管理对于工作组目前就电子可转移记录开展的工作非常重要，对于今后可能就其他专题开展的工作也非常重要。

5. 身份管理在促进值得信任的电子商务方面的核心重要性得到广泛认可。无数政府间团体、国家、私营国际团体和商业实体积极探讨身份管理问题和机会，制定技术标准和商业流程，并试图实施可行的身份系统。例如：

---

[1] 经合组织（2011 年），“自然人的数字身份管理：促进互联网经济中的创新和信任—给政府决策者的指导意见，”《经合组织数字经济文件》，第 196 号，经合组织出版社，第 3 页；网址：www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en。

[2] 本文件侧重于预期用于商业环境的商业性身份管理系统，包括用于企业对企业、企业对政府和企业对消费者通信。

[3] 美国律师协会商法科网络空间法律委员会身份管理问题法律工作队；http://apps.americanbar.org/dch/committee.cfm?com=CL320041。本文件所表达的观点未经美国律师协会代表大会或理事会核准，因此不应解释为代表美国律师协会的政策。

[4] 2011 年 2 月 14 日至 16 日在纽约举行的贸易法委员会电子商务专题讨论会议事录中载有更多材料，网址：www.uncitral.org/uncitral/en/commission/colloquia/electronic-commerce-2010.html。

[5] 《大会正式记录，第六十六届会议，补编第 17 号》（A/66/17），第 250 段。

[6] 同上，第 251 段。

[7] 同上，第 241-249 段。

(a) 就身份管理问题和标准积极开展工作的政府间团体包括经济合作与发展组织（经合组织）、[8] 国际标准化组织（标准化组织）[9] 和国际电信联盟（国际电联）；[10]

(b) 经合组织进行的一项调查 [11] 查明 18 个经合组织成员国在积极推动身份管理国家战略（澳大利亚、奥地利、加拿大、智利、丹麦、德国、意大利、日本、卢森堡、荷兰、新西兰、葡萄牙、大韩民国、斯洛文尼亚、西班牙、瑞典、土耳其和美利坚合众国）。[12] 另一些国家如爱沙尼亚、印度和尼日利亚，也在积极推动此类战略。

(c) 欧洲联盟内部正在开展几个区域身份项目，其中包括 PrimeLife（欧盟委员会第七框架方案下的一个项目）、[13] 全球个人身份联网—支助行动、[14]STORK（旨在建立一个欧洲电子身份互操作平台）[15] 以及欧洲网络和信息安全局；[16]

(d) 在国际层面就身份标准和政策开展工作的私营组织包括结构化信息标准促进组织、[17] 开放身份交换组织、[18]Kantara 举措、[19]Open ID 基金会、[20]tScheme[21] 和互联网协会。[22]

(e) 几个商业性身份系统已在少数领域建立并在全球范围内运作。其中包括航天业和国防业的环球安全协作方案（TSCP）[23] 和 CertiPath、[24] 生物制药业的 SAFE 生物制约协会、[25] 金融部门的 IdenTrust、[26] 管理网上 EV-SSL 证书的

---

[8] www.oecd.org/document/38/0,3746,en_2649_34255_49319782_1_1_1_1,00.html。

[9] www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306。

[10] www.itu.int/ITU-T/studygroups/com17/fgidm。

[11] Bernat, L.（2011 年），“经合组织国家的数字身份管理国家战略和政策”，《经合组织数字经济文件》，第 177 号，经合组织出版社，doi: 10.1787/5kgdzvn5rfs2-en；网址：www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en。

[12] 同上，第 28-35 页列有与各国家文件的链接。

[13] www.primelife.eu。

[14] www.gini-sa.eu。

[15] https://www.eid-stork.eu。

[16] www.enisa.europa.eu。

[17] www.oasis-open.org/home/index.php。

[18] www.openidentityexchange.com。

[19] http://kantarainitiative.org，以前称作自由联盟，www.projectliberty.org。

[20] http://openid.net/foundation。

[21] www.tscheme.org。

[22] www.internetsociety.org。

[23] www.tscp.org.

[24] https://www.certipath.com.

[25] www.safe-biopharma.org.

[26] www.identrust.com.

CA/Browser 论坛[27]以及 FiXs——身份与交互认证系统联盟。[28]这些团体的工作主要专注于技术标准和商业流程问题而非法律问题。

二. 身份管理与电子商务有何关系？

6. 身份管理是多数电子商务交易和其他网上活动的一个根本问题。验证远程当事方的身份是一项根本关切，例如确定谁在寻求访问网上敏感信息数据库，谁在试图在网上从一账户转移资金，谁在电子合同上签了字，谁远程授权发运产品，或者谁发送了电子邮件。许多低风险网上交易的参与者愿意相信他们在与一个特定的人或实体打交道，但随着交易的敏感性或价值提升，确保关于远程当事方身份的准确信息的可获得性和可靠性以便在信任基础上作出决定的重要性也在提高。

7. 身份管理是电子签名、电子可转移记录专题以及今后可能就其他专题（单一窗口和移动支付）开展工作的一项基本要求。[29]

(a) 确立签名人的身份是建立有效的电子签名的要求之一。《贸易法委员会电子商务示范法》（1996 年）第 7 条和《联合国国际合同使用电子通信公约》（2005 年，《电子通信公约》）均要求，作为有效电子签名的一个条件，“用来识别”签名人“身份的方法”既适合生成或传送数据电文所要达到的目的，而且也同样可靠。《贸易法委员会电子签名示范法》第 2 条也要求有“可用来确定签名人身份”的数据，以此作为电子签名的组成部分。

(b) 身份验证也是电子可转移记录、单一窗口和移动支付的一项关键要求。目前关于电子可转移记录的法律要求既确定记录签名人的身份，也确定有权执行该记录的持有人的身份。[30] 单一窗口程序要求确定海关单证签名人的身份，以及提交单证的人或实体的身份和有权执行单证的人或实体的身份。[31] 而移动支付如其他支付系统一样，要求（为授权目的）确定意图转移资金的人的身份。[32]

三. 什么是身份管理？

8. 就其实质而言，身份管理意在答复网上交易的每个当事方提出的关于对方的两个简单问题。“你是谁？”以及“如何证明？”能够就这两个问题提供可靠和值得信任的答复正在迅速成为电子商务活动的一项关键要求，特别是随着这些交易的种类、重要性和敏感度增加。利用对这两个问题的答复，网上交易当

---

[27] www.cabforum.org.

[28] www.fixs.org.

[29] 《大会正式记录，第六十六届会议，补编第 17 号》（A/66/17），第 241-252 段。

[30] A/CN.9/WG.IV/WP.115，第 24-24 段和第 45-48 段。

[31] A/CN.9/728/Add.1，第 42 和 45 段。

[32] 见 A/CN.9/728，第 52 段。

事方就可以确定是否进行交易（例如是否与对方订立合同，是否允许对方访问敏感数据库，或者是否给予对方某种别的特权或访问权）。

9. 每一个参与数字交易的实体都可以建立自己的系统以查明和认证每个商业伙伴的身份（许多企业目前通过具体登记程序加上用户名和密码系统实现这一点），但事实越来越证明，这样做代价高且不合适，使得难以将系统扩及更广泛的群体。此外，需要跨组织协作的情况越来越多，人们对安全感到担心，以及存在用户密码管理问题，这些表明以前由公司签发或销售商签发的用户名和密码办法已不再适合。

10. 因此，由第三方身份提供者（或属性提供者）发挥关键作用的身份系统正在出现，成为一种优选办法。目标是使企业和政府机构能够依赖若干不相关的第三方提供者中任何一家提供的身份信息和认证过程，与远程当事方进行电子交易。这通常被称为“联合”身份系统。换言之，经一个实体验证的身份信息在不同系统上以商定和得到管理的方式提供给因不同目的而需要身份信息的多个当事方。这将例如使个人和企业能够利用其自己选择的身份证书与无数企业进行网上交易，正如个人可以使用驾驶证与不同实体进行各种不同的线下交易一样，如购买酒精、获得许可进入机场登机区或开设银行账户。

11. 开发联合身份系统要求将技术标准和系统、[33] 商业流程和程序以及法律规则综合在一起，这些要素共同建立一个值得信任的系统，用来：㈠验证身份并将该身份与个人、法人、设备或数字对象联系起来，㈡向需要该身份信息以便授权一项交易的当事方提供该身份信息，㈢在该信息的生命周期维护并保护该信息。使这种系统能够在商业环境中发挥作用的关键，是要求有一个适当并且一般以合同为基础的法律框架，来界定各当事方的权利和责任、分配风险并为执行提供基础。该法律框架往往称作“操作规则”或“信任框架”。

四. 身份管理基本问题

12. 虽然“身份管理”一词相对较新，但这一概念并不新。基本的流程在线下环境中长期被使用。护照、驾驶证和雇员身份卡都是身份系统的组成部分（即它们是一个实体向经验证的个人签发的证书，以便这些个人可以随后证明其身份）。确定个人身份并签发证书的流程可由同时接受证书的当事方（如公司签发的雇员身份卡）完成，也可由第三方（如驾驶证或护照）完成。联合系统中有一个第三方签发人，此类系统的一个关键因素是对这些身份证书的使用并非限于与签发这些证书的实体进行的交易。而是设计和部署此类系统时即预期在需要证明个人身份的某些属性（如姓名或年龄）时，证书将为第三方接受（例如，就驾驶证而言，为机场安全人员、银行或酒吧间售酒精饮料的人接受）。

13. 难题是在网上环境中落实类似的功能。也就是建立一个可在各种系统上由各种实体远程使用的安全、可靠和值得信任的数字身份证书系统（即开发一个

[33] 公钥基础设施是可用来建立身份系统的一种办法。不过，许多其他技术和办法也在开发和实施当中。

联合身份系统）。这使数据主体能够使用相同的身份证书自证身份，以便使用多个组织的资源或与多个组织进行交易。

14. 虽然有多种不同的身份管理办法，但身份管理实质上涉及两个基本过程：㈠收集并验证个人（或实体、设备或数据对象）[34] 某些身份属性并签发身份证书以反映这些属性的过程（“确定身份”），㈡随后证实出示该证书并声称就是以前被确定身份的人确实是该人的过程（“认证”）。其中每个基本过程涉及不同的分过程，视数据的性质和两个过程的背景而定。一旦某个个人的身份属性得到成功认证，打算依赖经认证的身份确定将赋予该人什么权利和特权（例如，是否与该人订立合同，或是否准许该人访问一个数据库、一个网上银行账户）的实体，将进入称作“授权”的第三套过程。

A. 确定身份

15. 确定身份的过程意在回答“你是谁”的问题。该过程由发挥身份提供者作用的某人执行，[35] 涉及将用来确定身份的属性（如姓名、会员号码、地址或出生日期）与某个人相关联，以便在足以服务于设想目的的程度上界定该个人。该过程有时称作“身份证明”或“注册”，往往是一次性事件。该过程一般涉及身份提供者收集有待确定身份的人（称作“主体”）的信息，并往往依赖政府签发的多种证件（例如出生证、社会保障卡、驾驶证和护照），以及私营部门实体签发的证书（例如雇员徽章、移动无线 SIM 卡和信用卡）。虽然此类身份证件和证书是为其他目的签发的，但往往也可再用来便利随后在新的情况下的确定身份过程。例如，某人在收到雇员身份徽章时提供驾驶证来证明身份即属于这种情况。

16. 在确定身份过程结束时，主体的相关身份属性一般在身份提供者签发、称作身份证书的电子文件中用数据表示。证书提供用来认证所声称的个人、实体或设备数字身份或属性的数据（或者与这些数据相联系或相关联）。[36] 证书可以采用各种媒介。在现实世界中，身份证书的例子包括王室印章、驾驶证、护照、图书借阅卡或雇员身份徽章。在网络世界中，身份证书可以简单如用户身份号，或者复杂如可保存在计算机、移动电话、智能卡、ATM 卡、闪存盘或类似设备上的加密数字证书。

B. 认证

17. 当一人出示证书（如在机场出示驾驶证，或者在一个公司网络上输入用户身份号），声称是证书所确定身份的人，并寻求行使赋予该个人的权利或特权（例如登机、访问公司网络或敏感数据库），“依赖方”利用认证过程确定该人

---

[34] 可以针对个人、法律实体、设备和数字对象收集和验证身份信息，并签发身份证书。本文件侧重于针对个人的身份系统。

[35] 有时，确定身份过程仅需要选定的属性，这时由称作属性提供者的实体发挥此种作用。

[36] 《经合组织电子认证指导意见》（2007 年），第 12 页，网址：http://www.oecd.org/dataoecd/32/45/38921342.pdf。

是否确实是其自称的某人。换言之，一旦某人宣称其是谁（声称是身份证书所确定身份的人），认证意在回答“好的，你如何证明呢？”的问题。这是特定交易中的事件，涉及将某个人与身份证书相关联，以证实试图进行交易的人确实是证书以前确定身份的人。

18. 认证一般要求有某个事物，一般称为认证依据，将该人与证书联系起来。如果证书是驾驶证或护照，则认证依据为照片，一般通过将驾驶证或护照上的照片与出示者进行比对来完成关联。使用电子证书时，认证依据一般是个人“知悉的”某事（例如密码或个人身份号）、个人“占有的”某物（例如私人密钥、物理设备如智能卡、USB 或其他类型的令牌），或个人“具有的”某个特征，如身体特征（例如照片、指纹或其他生物测定数据）。

C. 授权

19. 一旦一个人被成功认定，则依赖方可利用自身的授权过程确定赋予该人何种权利和特权（例如是否准许该人访问一个网站、数据库、进入酒吧或机场登机区）。该过程处理“你可做什么？”的问题。因此，身份认证并非到此为止。身份认证往往用来便利依赖方做出授权决定，如赋予权利或特权（如利用网上系统资源），或达成交易。例如，试图访问一个计算机网络的某人的身份一旦被认证，系统拥有者（即依赖方）即可利用授权过程确定赋予该人何种访问权利。同样，试图达成一项电子交易（例如电子合同）的某人的身份一旦被认证，依赖方即可利用授权过程确定是否与该主体继续进行交易或者以别的方式依赖该通信。

D. 联合身份

20. 就网上交易而言，传统上确定身份和签发证书由同时打算依赖证书的相同当事方完成。例如，企业将确定雇员的身份，向其签发用户名和密码，以便他能够访问公司的网络。在此情况下，公司既是身份提供者（因为它确定该人是其雇员并签发了身份证书），又是依赖方（因为它也接受并依赖这些身份证书以准许访问其网络）。

21. 在“联合”身份系统中，身份提供者和依赖方的职能不一定由同一当事方来履行。而是没有关系的多个依赖方可依赖若干独立身份提供者之一提供的身份证书。在这种模式下，单一的身份证书可为与原来签发证书没有直接关系的无数组织所依赖。

22. 人们所熟悉的联合身份管理过程的一个线下例子是目前签发和使用驾驶证的方式。驾驶证由一个政府机构签发，无数没有关系的依赖方可利用它们验证关于驾驶证主体的身份的属性。例如，安全人员用来验证试图进入机场登机区的人的身份，或酒吧间售酒精饮料的人用来验证购买饮料的人的年龄。

23. 联合身份系统的网上例子是自动取款机系统。在典型的自动取款交易中，在 A 银行拥有账户的个人可利用其银行签发的身份证书（自动取款卡）从 B 银行（他与之并无关系）运营的自动取款机上提取现金。为了完成该交易，尽管

不存在上述关系，B 银行通过自动取款机网络联系 A 银行，以确定该个人是否 A 银行的有效客户，让 A 银行认证该个人的身份（即该个人输入正确的密码），并从 A 银行获取该个人的某些身份信息（例如该个人账户上是否有足够资金来满足他所要求的取款，以及该个人账户上的余额，以便 B 银行可以在交易收据上打印出来）。

四. 身份系统的风险

24. 参加身份系统和依赖身份数据有若干潜在风险。这些风险包括：

(a) 确定身份方面的风险：所收集和确定的关于主体的身份信息的可靠性对于任何身份系统的使用都至为关键。确定身份方面的风险是所收集并与特定主体关联的身份属性数据不准确。此种风险往往取决于主体为证明身份提供的线下身份证书的质量。

(b) 认证方面的风险：如果依赖方没有能力进行认证（即将所声称的身份属性与正确的主体相关联），则确定身份就毫无价值。认证方面的风险既包括合法主体不能被正确认证的风险，也包括认证过程错误地表明冒名顶替者系合法主体的风险。

(c) 隐私风险：就个人而言，身份管理涉及身份提供者收集和验证关于一个主体的个人信息并与多个依赖方分享该信息。此外，基于身份的交易也可能为跟踪个人的行动提供便利，从而产生额外的个人信息。隐私风险侧重于有权获得个人信息的当事方之一未经授权或滥用主体的个人信息，以及这些当事方在处理和保护此类数据方面的守规义务。

(d) 数据安全风险：保护个人主体的个人信息，并维护创建安全身份证书、传达准确的身份信息、验证身份证书的现状并对主体进行认证所必需的各个过程的安全，对于任何身份系统都至关重要。安全风险包括未经授权的当事方可获得个人数据的风险，以及放弃对身份系统的总体运作或任何具体的身份交易至关重要的任何过程的风险。

(e) 赔偿责任风险：任何身份系统都不可避免会发生故障，这样会导致损害赔偿。身份系统的各参与方必须处理以下风险，即需要对因它们所导致的问题而给别人造成的损害以及对它们被认为负有法律责任的事情承担赔偿责任的风险。赔偿责任风险的一个关键方面是，对于身份系统参与方任何特定的作为或不作为应当承担的责任存在着法律上的不确定性，特别是对于跨越多个行业部门和法域运行的身份系统。

(f) 执行风险：执行风险是赔偿责任风险的补充。此种风险即一个参与方不能够执行㈠其让另一参与方遵守规则的权利，或者㈡其受到实际损害而另一参与方负有法律“赔偿责任”的情况下得到损害赔偿的权利。某件事出错和某个人寻求得到损害赔偿即属于此种风险。问题尚未显现，但一个或多个参与方不履约可能使整个身份系统处于危险之中，此类情况也属于这种风险。这一点在跨法域系统中尤为重要。在此情况下，执行风险既指是否能够发现问题，也指是否能够要求参与方纠正其履约行为或者从系统中退出。

(g) 守规风险：许多情况下，参加身份系统带来一个或多个参与者遵守法律的问题（即参与者的行为是否符合适用的当地法律）。另一些情况下，参加身份系统本身就是为了遵守对参与者提出的法律要求。例如，金融机构可能为了履行适当认正准许在网上访问银行账户和使用支付设施的个人的法律义务而参加身份系统并依赖身份证书。在此类情况下，守规风险侧重于此类参加是否履行其法律义务。

25. 与任何系统一样，上述风险取决于所使用的技术、实施的各种流程以及参与者自身履行义务或不履行义务的方式（以及外来者可能的影响）。建立可靠的身份系统要求采取措施处理这些风险，即旨在确保参与者可以信任所使用的技术（即系统将顺利运作）、所实施的流程（即这些流程将产生正确的结果）和其他参与者（即他们将适当履行自身的义务）。

五. 处理功能与风险：操作规则

26. 为使一个联合身份系统能够在网络环境中行之有效，并处理类似上文提到的风险，不仅要求实施适当的技术，而且要求所有参与者（例如主体、身份提供者和依赖方）遵守一套共同的技术标准、操作要求和法律规则。商业性身份系统一般通过制定各参与者以合同方式受到约束的适当“操作规则”（有时称作信任框架）来实现这一目标。

27. 身份系统操作规则包括两大类组成部分：㈠系统能够发挥作用和值得信任所必需的商业和技术操作规则和规范，和㈡基于合同的法律规则，除适用法律和条例之外，这些规则界定特定身份系统各当事方的权利和法律义务并在必要时为执行提供便利。

(a) 商业和技术操作规则界定身份系统适当运作的各项要求，界定各参与方的作用和运作责任，并就身份系统的流程和数据的准确性、完整性、私密性和安全性提供保证（即各当事方愿意参与；系统值得信任）；在许多情况下，此类规则是在现有标准基础上制定的。

(b) 基于合同的法律规则包括参与方双方或多方之间基于合同的协议，其中界定各参与方相对于具体身份系统的法定权利、责任和赔偿责任，澄清各参与方因参与身份系统而承担的法律风险（例如保证、对于损失的赔偿责任、其个人数据面临的风险），并在各当事方发生争议时提供纠正办法，包括争议解决办法、执行机制、终止权以及损害赔偿金、罚金和其他形式赔偿责任的计算标准。这些规则还规定产业和技术操作规则在法律上对于各参与方具有约束力并可强制执行。

28. 当然，商业和技术操作规则与基于合同的法律规则均须服从适用于各当事方的成文法和行政法所规定的其他现有职责和义务，并且往往是参考这些职责和义务而制定的。身份系统操作规则的两个组成部分（即商业和技术操作规则与法律规则）均须服从运作或使用身份系统所在的法域所适用的现行法规和条例。

29. 身份系统操作规则很像信用卡系统或电子支付系统所使用的操作规则，这些系统必须能够按照一套通用的规则容纳不同法域的无数参与者。例如，信用卡操作规则对签发人、处理机构、依赖方商家和个人持卡人作出规范，并提供适用于网上信用交易和随后的处理过程的各参与者的规范和规则。[37] 同样，电子资金转账系统操作规则对支付过程中所有银行以及在有限程度上对消费者或所涉其他付款人的责任作出规范，并在电子资金转账（例如 SWIFT 转账）用来便利网上交易支付时提供适用于各参与者的规范和规则。[38]

30. 尽管普遍承认需要包含适当法律规则的身份系统操作规则，但制定此类规则是一个在很大程度上未加探索的领域。有无数法律问题和法律障碍必须予以查明和处理。

六. 规范身份系统的法律

31. 在多数法域，有许多现行法律和条例对参加身份系统具有规范方面的重大影响（并可能造成障碍、提出守规要求和（或）带来赔偿责任风险）。此外，考虑到互联网具有全球性，不同法域的法律之间的差异导致监管情况互不一致，这本身给法律架构造成挑战。其中一些法律和条例专门侧重于与身份有关的活动。不过，多数是在与身份管理完全无关的背景下制定的（例如侵权法、合同法和保证法），但也可能产生重大影响，这种影响往往是在原来通过时未曾想到的。

32. 适用于身份系统（或身份系统的参与者）的其中一些法律类别包括下列几种：

(a) 规范身份信息准确性的法律：身份系统的活动侧重于身份提供者或属性提供者收集和验证关于主体的信息，并将其中一些信息发给依赖方。这往往发生在该信息的准确性和（或）可靠性非常重要的情况下。因此，关于不管是出于故意还是出于疏忽而提供虚假或不正确信息的法律，与评价身份系统参与者的权利、义务和赔偿责任是有关系的。其中重要的有规范出于疏忽的错误表述、出于疏忽的赞同以及诽谤行为的侵权法，以及保证法、身份盗窃法和规范不公平和欺骗性商业行为的法律。

(b) 规范身份信息隐私性的法律：就其性质而言，身份管理一般涉及（身份提供者或其代理人）收集并（向依赖方）提供关于一个主体的个人信息。[39]

---

[37] 信用卡操作规则包括对处理银行和商家有约束力的信用卡签发人规范和规则（例如，Visa 国际操作条例，网址：http://usa.visa.com/merchants/operations/op_regulations.html，和支付卡行业数据安全标准，网址：https://www.pcisecuritystandards.org/security_standards/index.php），以及处理银行与持卡人之间的合同。此类操作规则由每个相关法域规范信用卡处理业务的法律和条例加以补充。

[38] 电子资金转账操作规则包括对各处理银行和商家有约束力的电子资金转账交易规范和规则（例如设在美国的电子支付协会操作规则和准则，网址：http：//www.nacha.org），以及商家和个人付款人之间的合同。此类操作规则由规范电子资金转账的法律和条例如（在美国）《电子资金转账法》和《条例 E》加以补充。

[39] 主体非个人——例如主体是公司、装置、软件应用等等——的情况除外。

这样，数据保护法、隐私法和关于收集、使用、处理、转移和存储个人数据的其他法律和条例将对身份管理活动产生重大影响。虽然许多此类法律是在数字身份系统出现之前制订的，因此未能设想此类系统所涉及的特定流程或潜在伤害，不过它们仍可能对这类活动产生直接影响。

(c) 规范身份信息收集的法律：除了隐私和数据保护法之外，规范公共部门信息的再次使用的法律也对基于来自公共部门的大量数据创建信息产品和服务的企业有影响。这些法律可能对在身份服务方面大规模使用公共部门机构保存的数据造成法律障碍。[40]

(d) 规范身份信息和流程安全性的法律：许多法律规定公司对个人信息（不同法域以及在特定部门的具体法律中对此有不同定义）及其掌握的其他数据的安全性负有义务。除了规定有义务采取安全措施以保护数据的法律和条例外，许多法域还颁布了法律和条例，规定有义务将涉及个人信息的安全漏洞告知受影响的人。

(e) 侧重于确定身份的义务的法律：许多法律和条例要求将身份作为一个组成要素，特别是在电子环境中。例如，《电子通信公约》明确要求将身份作为具有法律约束力的电子签名的组成部分。特别是，法律要求通信或合同应由当事方签署的情况下，《电子通信公约》规定使用一种方法既能确定当事方的身份，又能表明当事方对电子通信所载信息的意图的，即满足了签名要求。[41]

(f) 侧重于认证的义务的法律：一些法律对认证的一项或多项内容作出规范。一些法律规定企业有义务对与之远程交易的人进行认证，另一些则对认证过程的一些方面作出规范。一个突出的例子是美国银行监管者对于网上银行活动的认证要求。特别是，向客户提供基于互联网的产品和服务的金融机构必须“采用有效的方法认证使用这些产品和服务的客户的身份。”[42] 另一些国家如新加坡也采纳类似要求。[43]

(g) 专门规范身份系统活动的法律：一些法域拥有明确规范身份管理活动的某些方面的法规。一个例子是《欧洲联盟电子签名指令》，[44] 其中要求成员国规范某些身份提供者（称为认证服务提供者）收集关于主体的个人数据的行为，并规范签发证书事宜。[45] 同样，《贸易法委员会电子签名示范法》（第 8-12 条）也就创建某些电子签名所需的身份证书的签发和使用制定了规则。

---

[40] 一般情况见全球个人联网项目，“关于部署全球个人联网服务的法律规定”（2011 年 10 月 5 日），第 5 节，网址：www.gini-sa.eu/images/stories/2011.11.06_GINI_D3.1_Legal%20Provisions%20for%20Deploying%20INDI%20Services_FINAL.pdf。

[41] 《电子通信公约》，第 9(3)条。

[42] 联邦金融机构审查委员会，“互联网银行环境中的认证，”2005 年 10 月 12 日，第 1 页；网址：www.ffiec.gov/pdf/authentication_guidance.pdf。

[43] 新加坡金融管理局，SRD TR 02/2005 号通知，2005 年 11 月 25 日。

[44] 1999 年 12 月 13 日关于电子签名的共同体纲要的第 1999/93/EC 号指令（“欧洲联盟电子签名指令”），第 6-8 条以及附件一和二，网址：http://europa.eu/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.

[45] 《欧洲联盟电子签名指令》，第 8 条。

H. 挑战和法律障碍

33. 上述各类以及其他现行法律和条例给私营部门身份系统的发展和运作造成一些基本问题。这些挑战包括：

(a) 未制定处理身份管理的法律：身份管理过程提出的许多新问题根本未在现行法律中得到处理。适用于此类情形的多数现行法律不是从数字身份系统的角度制定的，因而往往不能充分或适当处理或规范身份活动。例如，现行法律往往对在评价身份证明文件的真实性时身份证明人必须履行的谨慎注意义务或对身份提供者对数据主体负有的披露义务的范围未作规定。

(b) 法律的不确定性/模糊性：有些身份管理问题可能在现行法律和条例中得到处理，但这些法律的适用性经常不明确或模糊不清，给身份系统参与者留下很大程度的法律不确定性，这可能阻碍发展、创新和投资。这样，即使在现行法律适用于身份管理的情况下，该法律如何适用于身份系统中的特定问题或所提议办法可能不明确。侧重于特定技术的法律尤其如此。这可能限制进行身份交易的各当事方评价和管理他们这样做所承担的风险的能力。

(c) 隐私问题：就其性质而言，身份管理一般涉及身份提供者收集并向依赖方提供关于一个主体的某些个人信息。为参加身份系统，主体必须披露个人信息，从而使自身暴露于此类信息被未经授权而使用或不适当使用的风险。此外，随着主体与多个依赖方互动，所需要的通信或者身份提供者对其信息的验证使得该提供者能够追踪每个主体的活动，从而令人担心此类交易信息会被收集和利用。因此，隐私是任何身份系统的一个关键问题。这可能涉及处理诸如以下问题：㈠身份提供者可以收集哪些信息？；㈡可以向依赖方提供多少信息？；㈢主体可对信息披露进行哪些控制？；㈣各当事方必须如何安全地处理数据？；㈤对身份提供者和各依赖方使用信息有何限制？这些问题往往由现行法律处理，也可能由基于合同的操作规则加以补充。

(d) 赔偿责任问题：对任何身份系统的参与者而言一个首要的合法关切是确定谁将承担与任何风险有关的赔偿责任（见上文第 24 段）。有许多制定法、普通法和合同理论在查明、界定和澄清此类潜在赔偿责任的来源和范围方面已经非常完善。[46] 然而，此类法律风险往往界定不当且不确定。围绕赔偿责任的担心是妨碍私营部门采用互操作性身份解决办法的一个主要障碍。通过操作规则或各参与方之间其他形式的合同协议处理赔偿责任往往是最佳办法，尤其是因为这使得能够根据需要“定制”合同，以处理每种情况都不相同的适当的风险分配。

(e) 法域差异和冲突：对于有些关键问题，现行法律和条例对身份活动的适用在各个法域之间有很大差异。规范参与者赔偿责任的法律和规范个人信息隐私的数据保护法往往属于这种情况。此外，某些情况下，对身份系统活动的规范或许可可能给身份系统的跨境运作造成额外的障碍。因此，身份系统跨越

[46] 见《认证赔偿责任分析》（提交美国银行家协会的研究报告，其中讨论经营认证机构的身份提供者的潜在赔偿责任风险；网址：http://64.78.35.30/article/ca-liability-analysis.pdf。

法域运作时，除有制定适当的操作规则的挑战之外，还存在不同法域之间的现行法律和挑战有差异（往往差异很大）的问题。

(f) 法律互操作性的必要性：各法域之间的适用法律可能有所不同，这给身份系统带来挑战。在缺乏规范身份系统活动的统一法律的情况下，身份系统往往寻求通过制定操作规则使整个系统具有法律互操作性来处理这一问题。各法域之间法律和条例的差异将对制定此类操作规则以及使各网上系统的系统参与者的行为更加统一所需要的其他合同造成挑战。

(g) 对于通过合同来修订法律的能力的限制：一些现行法律和条例可通过合同来修订。例如，许多法规载有合同理论或商业法理论，这些法规只是制定在各当事方未作明确选择情况下适用的“缺省规则”，但允许交易当事方通过协议修订此类规则。在此情况下，身份系统的当事方可自由地修订缺省规则并利用基于合同的适当操作规则填补空白。然而，在另一些情况下，强制性法律规则不能仅凭当事方协议就予以无视，因为这些规则服务于保护消费者或者第三方等公共政策目的。

34. 因此，现行法律可能对采用可以跨境运作的高效、可互操作和值得信赖的身份系统造成障碍。制定基于合同的身份系统操作规则是处理这类法律挑战并减少参与者的不确定性的主要方法。这样做也有利于随着市场在努力解决身份管理问题而试验不同的系统和不同的办法。

35. 事先公平地分配参与流程所产生的赔偿责任风险并尽可能减少此类风险，对联合身份系统的所有参与者都有好处。如果不处理应当如何分配赔偿责任或者谁最适合承担风险的问题，现有的法律不确定性会成为实施值得信任的身份系统的主要障碍。随着身份管理过程用于比较重大的交易，各当事方的风险随之增长，实施适当的操作规则以事先处理这些风险并通过要求每个参与方履行特定义务而（尽可能）降低此类风险，对所有当事方都有很大好处。

36. 建立用于商业交易的跨境和可互操作私营部门身份系统是摆在面前的挑战。如同信用卡和电子支付系统一样，身份系统操作规则很有可能以合同为基础，特别是在意图跨越法域在互联网范围内部署此类系统的情况下。也许应当考虑制订旨在消除妨碍此类系统的障碍（而非规范此类系统）的立法。

* * *

定义

[注：这些定义是一般性的，仅为帮助理解前面的正文而提供]

属性：一个主体所固有或被赋予的带名称的特性或特征，如姓名、住址、年龄、性别、头衔、薪资、净值、驾驶证号、社会保障号等等（对人而言）、品牌和型号、序列号、位置、能力等等（对设备而言），等等。同义词：身份属性

属性提供者：作为主体身份的一个或多个属性的权威来源，并负责与收集和维护此类属性相关的流程的实体。属性提供者针对身份提供者和依赖方提出的属

性请求，提供得到信任、经过证实的关于属性的说法。属性提供者的例子包括政府所有权登记处、国家征信机构或商业性营销数据库。

认证：通过确认主体与证书的关联性来验证主体所声称的身份的过程。例如，推定输入与用户名关联的密码会证实该用户即是被授予用户名的人。同样，将出示护照的人与护照上的照片进行比对，会验证或确认他/她就是护照上所描述的人。

认证依据：用来验证主体与证书间的关系的某件事物，通常是一个物体、一项知识或占有者的某种特征，用来将该人与身份证书联系起来。例如，密码是用户身份的认证依据，照片是护照或驾驶证的认证依据。

授权：基于依赖方确定的标准赋予经认证的主体以权利和特权的过程；意在控制对信息或资源的获取，以便只有经专门许可使用这些资源者才被准许获取这些资源。

证书：作为主体所声称的身份的证据出示的数据。纸质证书的例子包括护照、出生证、驾驶证和雇员身份卡。数字证书的例子包括用户名、智能卡和数字证书。

联合身份系统：主体可使用若干身份提供者中任何一个签发的身份证书向不同系统上多个不相关的依赖方进行认证的身份系统。

确定身份：收集、验证并证实关于具体主体的足够身份信息以便在特定情况下界定和确认其身份的过程。（同义词：注册；身份证明）

身份：关于特定主体的以允许在特定情况下足以区分主体的一种或多种属性为表现形式的信息。允许在特定情况下将某人与他人相区分的该人的一组属性。

身份管理：收集、验证、汇总并向依赖方提供关于一个主体的身份信息的过程、职能和能力，以便依赖方可以核实该身份信息与特定主体相符。

身份提供者：负责确定个人、法律实体、设备和（或）数字对象的身份，签发相应的身份证书并维护和管理主体的此类身份信息的实体。（同义词：证书服务提供者；认证机构；属性提供者（提供有限的属性数据时））

身份系统：由一套操作规则规范的身份系统网上环境，其中由于权威的来源确定并认证了身份，个人、组织、部门和设备可以相互信任

操作规则：规范特定身份系统运作的商业流程、技术规范和由合同界定的法律规则。此类规则往往由私人制定（例如身份系统的运营者），并通过合同而对各参与方具有约束力和可执行性。（同义词：信任框架；系统规则；共同操作规则；操作条例）

依赖方：依赖身份证书或关于身份的断言就特定应用情况下可采取什么行动作出决定的个人或法律实体，此类行动包括处理交易或准许访问信息或系统等。（同义词：服务提供者）

主体：特定证书所确定身份并可由身份提供者认证和保证的个人、法律实体、设备或数字对象。（同义词：数据主体；用户）