联合国 A/CN.9/630/Add.3

大 会

Distr.: General
16 April 2007
Chinese
Original: English

联合国国际贸易法委员会
第四十届会议
2007 年 6 月 25 日至 7 月 12 日，维也纳

今后可能在电子商务方面开展的工作

关于建立有利于电子商务的法律框架所需各项要素的综合性参考文件：关于电子认证和签名方法国际使用的样本章节

秘书处的说明

增编

本说明附件载有一份综合性参考文件中述及电子认证和签名方法国际使用相关法律问题的部分样本章节（第二部分，第一章，A 和 B 节）。

V.07-82258 (C) GZ 150507 150507

附件

目录

第二部分

电子签名和认证方法的跨国界使用

一. 对外国电子认证和签名方法的法律承认

1. 法律不相符和技术不兼容是造成电子签名和认证方法跨国界使用困难的两个主要原因，在打算用这些方法代替一种具有法律效力的签名的情况下尤其如此。技术不兼容影响认证系统的互操作性。而法律不相符的原因可能在于，不同法域会对电子签名和认证方法的使用和效力规定不同的要求。

A. 国内法的国际影响

2. 虽然有些国家的法律允许使用等同于纸面认证方法的电子认证方法，但有关这些电子认证方法效力的标准可能并不一致。例如，若法律只承认数字签名，则其他形式的电子签名将不会被接受。承认电子认证和签名方法的标准可能还有其他不一致之处，这些不一致处原则上也许并不妨碍其跨国界使用，但不同法域规定了不同要求，遵守这些要求所导致的成本和不便可能会影响使用电子通信预计带来的速度和效率上的提高。

3. 以下各节论述对技术采取的不同法律处理办法对于扩大跨国界承认的影响，并还概述在采取哪些措施可以促进电子签名和认证方法的国际使用这一问题上形成的国际共识。

1. 各国做法不一致所造成的国际障碍

4. 技术中立的办法往往能够解决法律不相符问题，特别是含有“可靠性测试”的办法。采取这种办法的国际法律文书包括《贸易法委员会电子商务示范法》第 7 条第 1(b)款[1]和《联合国国际合同使用电子通信公约》第 9 条第 3 款。[2] 按照这种办法，电子签名或认证方法既能鉴别签名人又能表明签名人对电子通信所载信息的意图的，即为满足了签名要求，前提是须符合几项标准。在所有情况下，包括数据电文的发件人和收件人之间订立任何协议的情况下，必须证明签名或认证方法不仅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。或者，签名或认证方法本身必须证明或与其他证据一道证明其实现了这些目的。

5. 无疑，这种最低限度办法能够促进电子认证和签名的跨国界使用，因为按照这种办法，任何电子签名或认证方法只要符合上述一般条件，就可用于有效

---

[1] 见注[…][联合国出版物，出售品编号：E.99.V.4]。

[2] 见注[…][大会第 60/21 号决议，附件]。

签署或认证一项合同或通信。但采取这种办法往往只能事后确认是否满足了这些条件，而且法院是否承认所用的任何特定方法也并无保证。

6. 在要求使用或偏向于使用某一特定技术的制度下，电子认证和签名的跨国界使用已成为一个现实问题。这一问题的复杂程度与政府对电子签名和认证的管理水平以及法律赋予任何具体方法或技术的法律确定性直接正相关。其中的原因很简单：若法律不赋予某些类别的电子签名或认证以任何特定的法律意义或推定，而仅仅规定其一般等同于手写签名或纸面认证，则依赖电子签名的风险与现行法律下依赖手写签名所面临的风险是相同的。但是，若法律赋予某种特定的电子签名（通常是被认为“安全”或“高级”的签名）以更多的法律推定，所增加的风险就从一方转移到另一方。偏重某种技术的立法的一个基本假设是，某一特定技术只要符合某些标准和程序，则其即具有足够的可靠程度，从而可以实现这种假定的法律风险总体转移。这种办法的不利方面是，一旦预先判断使用某一特定技术（除其他条件外）具有假定的可靠性，则所有其他技术，甚至是在稍有不同的条件下使用的同一技术，就具有假定不可靠性，至少是具有假定不可靠性的嫌疑。

7. 因此，相互不一致的偏重某种技术的各国立法可能会抑制而不是促进电子签名在国际商务中的使用。其表现有两种虽不相同但却密切相关的方式。

8. 首先，如果电子签名和对电子签名进行认证的认证服务提供者需要遵守不同法域互不一致的法律和技术要求，则在电子签名无法同时满足各种法域要求的情况下，这可能会抑制或妨碍电子签名在许多跨国界交易中的使用。

9. 其次，偏重于某一特定技术的立法，特别是偏重于数字签名的立法（在两级方法中也是如此）往往导致各行其是，规定不一致的技术标准和许可要求，从而使得很难跨国界使用电子签名。一个允许各国规定自己标准的制度可能会妨碍当事各方签订相互承认和认证的协议。[3]实际上，仍然存在的一个尤其与数字签名有关的重要问题是跨国界承认的问题。经济合作与发展组织（经合组织）信息安全与保密问题工作组（以下称“经合组织信息安全与保密问题工作组”）指出，虽然大多数法域采取的办法似乎是非歧视性的，但当地要求的差异依然会产生互操作性问题。[4]经合组织安全与保密问题工作组发现的下列弱点可能与本研究报告有关：

(a) **互操作性**。据发现，互操作性方面的挑战和局限性非常普遍。在技术方面，虽然有着多种标准，但却缺乏有关某些技术的共同“核心”标准。在法律/政策方面，主要负责人员在理解其各自的受托范围包括责任和赔偿分配方面

---

[3] Stewart Baker 和 Matthew Yeo 与国际电信联盟秘书处共同撰写的“Background and issues concerning authentication and the ITU”，向 1999 年 12 月 9 日和 10 日在日内瓦举行的“电子签名和认证机构：电信问题”专家组会议提交的简介文件，第 2 号文件。

[4] 经济合作与发展组织信息安全与保密问题工作组，*The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL), http://www.oecd.org/dataoecd/1/10/35809749.pdf，2007 年 2 月 2 日查取。

存在困难，这是妨碍取得进展的一个因素。经合组织信息安全与保密问题工作组指出，这是一个“似乎需要密切审查的领域，以便在可能情况下开发通用工具，从而协助各个法域实现某一特定的应用程序或系统所需达到的互操作性水平”；

(b) **对外国认证服务的承认**。经合组织信息安全与保密问题工作组认为，各项努力一直侧重于确立国内服务。因此，承认外国认证服务的机制“通常发展不足”。因此，该工作组认为这“似乎是一个需要进一步开展工作的领域。由于该领域的工作将与互操作性这个更具一般性的问题高度相关，因此可将这两个专题加以结合”；

(c) **对证书的认可**。[5]在有些情况下，对其他实体签发的证书的认可成为互操作性的一个障碍。因此，经合组织信息安全与保密问题工作组建议考虑是否可能拟订一套关于为认证目的签发证书的最佳做法或准则。有些法域可能已就这一问题开展工作，这些工作可为经合组织信息安全与保密问题工作组在这方面采取的任何举措提供有益参考；

(d) **目前使用的各种认证方法**。经合组织信息安全与保密问题工作组发现，几乎所有经合组织成员国都在使用数种认证方法。这些方法包括密码、标识、数字签名和生物鉴别技术。根据具体的应用程序及其要求，这些方法可以单独使用，也可综合使用。虽然许多人认为这一点具有积极意义，但经合组织信息安全与保密问题工作组调查搜集的信息表明，由于可选择性太多，应用程序提供者和用户可能晕头转向，难以确定哪种方法适合其需要。经合组织信息安全与保密问题工作组认为，这说明应当开发一种参照工具，对各种认证方法及其特性在多大程度上满足了应用程序提供者或用户所确定的需要进行评估。

10. 随着《联合国国际合同使用电子通信公约》的广泛适用以及该公约对电子签名和认证采取的技术中立方法的应用，对于在国际交易中使用电子签名和认证方法的信心可能会有所增强。但若认为这会使得完全没有必要采取一种统一解决方法来处理不一致的法律和技术标准，将是不现实的。许多国家可能仍然规定在特定类型的交易中使用特定的认证方法。另外，有些国家可能认为需要提供更加具体的指导，以评估签名和认证方法特别是外国签名和认证方法的可靠性及其与国内使用或至少知晓的方法的等同情况。

---

[5] 证书是证明个人或某一特定装置已经通过认证过程的一种标识。用户证书对于鉴别目的而言非常重要。持有人证书对于有些类型的授权来说可能已经足够，例如有效的驾驶执照、个人社会保险号或其他识别号码，或智能卡。民主和技术中心，“Privacy principles for authentication systems”，http://tprc.org/papers/2003/183/CDTauthenticationTPRC.pdf，2007 年 4 月 12 日查取；另见民主和技术中心认证保密原则工作组，“ Interim report on privacy principles for authentication systems”，http://www.cdt.org/privacy/authentication/030513interim.pdf，2007 年 4 月 12 日查取。

2. 正在形成的共识

11. 国际上出现的政策分歧可能是各种因素发挥不同作用的结果。如上文所述（见上文第[…]-[…]段），有些国家往往对签名和文件规定比较严格和具体的形式要求，另有一些国家则侧重于签名方的意图，允许采用各种方法来证明签名的有效性。这些一般性的区别往往在涉及电子认证和签名方法的具体立法中表现出来（见上文第[…]-[…]段）。造成不一致的另一种原因是政府对电子认证和签名方法技术方面的干预程度不同。有些国家往往在制定新技术标准方面发挥直接作用，也许它们认为这会为本地产业带来竞争优势。[6]

12. 政策分歧可能还反映出对于认证方法如何发展所作的不同假定。有一种设想称为“普遍认证模式”[7]，这种设想假定认证技术的主要目的是对以前相互不存在任何关系并且对技术的共同使用不受合同协议约束的个人的身份和特征进行核实。因此，认证或签名技术应向无数人并为了无数目的而证实一个人的身份或其他特征。这种模式强调的是涉及受托第三方情况下技术标准和对认证服务提供者提出的运作要求的重要性。另一种设想称为“限定范围的认证模式”，该设想认为，认证和签名技术的主要用途是核实按照合同协议共同使用某种技术的个人的身份和特征。[8]因此，认证技术应当只为了一些专门限定的目的，并在所限定的需要遵守共同的技术使用条款和条件的潜在依赖方的群体范围内证实证书持有人的身份或其他特征。这种模式的重点是对合同协议的法律承认。

13. 虽然具有这些差异，而且有些差异还依然存在，但经合组织信息安全与保密问题工作组的发现[9]表明，目前似乎正就电子商务特别是电子签名应当适用的基本原则形成国际共识。以下发现与本研究报告尤其相关：

(a) **对“外国”签名和服务采取的非歧视性方法**。各种法律框架并不否定在其他国家提供的服务所产生的签名的法律效力，但条件是这些签名的制作条件应与在本国被赋予法律效力的签名的制作条件相同。因此，这种方法似乎是非歧视性的，只要满足当地要求或类似要求即可。这与经合组织信息安全与保密问题工作组以前开展的认证调查中的发现相一致；

(b) **技术中立性**。虽然几乎所有被调查者都指出，本国关于认证服务和电子签名的立法和管理框架都是技术中立性的，但其中大多数人指出，若涉及电子政务应用程序，或者要求电子签名具有最大的法律确定性，则规定应使用公用钥匙基础设施（公钥基础设施）。因此，虽然立法框架可能是技术中立性的，但政策决定似乎要求具体说明使用哪种技术；

---

[6] 见注[…][Background and issues concerning authentication and the ITU]。

[7] 同上。

[8] 同上。

[9] 见注[…] [*The Use of Authentication across Borders in OECD Countries*]。

(c) **公钥基础设施的普遍使用**。经合组织信息安全与保密问题工作组发现，如果要求电子签名能够有力地证明身份并具有高度的法律确定性，则公钥基础设施似乎是优先选择的认证方法。公钥基础设施为特定的“利益群体”所使用，这些群体中的所有用户以前似乎都有某种形式的商业关系。靠公钥基础设施启动的智能卡的使用以及将数字证书功能纳入应用软件的工作都降低了用户使用这种方法的复杂性。但普遍认为，并非所有的应用程序都需要公钥基础设施，并认为认证方法的选择应当以是否适合有关目的为基础。

14. 另外，经合组织信息安全与保密问题工作组还发现，所有被调查国的规范框架都有某种形式的立法或管理框架，这些框架在国家一级规定了电子签名的法律效力。该工作组发现，虽然不同法域的立法细节可能有所不同，但显然采取了一致的方法，因为大多数国内法都是以现行的国际或跨国框架（如《贸易法委员会电子签名示范法》、欧洲议会第 1999/93/EC 号指令和欧洲理事会关于电子签名的共同体框架[10]）为基础的。

B. 对外国电子认证和签名方法予以承认的标准

15. 如上文所述，跨国界使用电子签名和认证的一个主要障碍是缺乏互操作性，这是由于标准相互冲突或各不相同或者对这些标准的实施不一致所致。基于各项标准并具有互操作性的公钥基础设施是进行电子商务应用安全交易的基础，为促进这种公钥基础设施而设立了各种论坛，其中包括全球[11]或区域一级的

---

[10] 《欧洲共同体公报》，L 13/12，2000 年 1 月 19 日。

[11] 例如，结构性信息标准推广组织是一个非营利国际组织，于 1993 年成立，其目的是促进电子商务标准的拟订、统一和采用。该组织设立了一个由公钥基础设施用户、提供者和专家组成的公钥基础设施技术委员会，以解决与数字证书技术应用有关的问题。结构性信息标准推广组织公钥基础设施技术委员会制定了一项行动计划，该计划除其他外设想如下：拟订具体的概要或准则，说明如何在特定的应用程序中使用各项标准，以实现公钥基础设施的互操作性；根据需要制定新的标准；以及开展互操作性测试和检验活动（结构性信息标准推广组织公钥基础设施技术委员会，“PKI action plan”（2004 年 2 月）），http://www.oasis-open.org/committees/pki/pkiactionplan.pdf；2007 年 4 月 12 日查取。

政府间组织[12]及公共部门和私营部门混合组织[13]。

16. 有些此类技术工作的目的在于为提供满足某些法律要求所需的信息制定技术标准。[14]但是，这项重要工作在很大程度上主要与技术问题而不是法律问题有关，并且超出了本研究报告的范围。因此以下各节的讨论侧重于在形式上和实质上对跨国界承认电子签名的法律要求。

1. 来源地、互惠和当地认可

17. 来源地是对外国文件或行为进行法律承认的一个基本因素。法律承认通常是在互惠基础上进行的，以便使某另一国的签名和证明能够在本国生效，如同本国的签名和证书在该另一国被赋予法律效力一样。另一个相关因素是，要使

---

[12] 在亚太区域，亚洲－太平洋经济合作论坛（亚太经合论坛）编写了“签发可在跨法域电子商务中使用的证书办法准则”（电子安全工作组，亚太经合论坛电信和信息工作组，2004 年 12 月），http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf，2007 年 4 月 12 日查取。这些准则旨在协助制定具有潜在互操作性的办法，并对现行办法的互操作性进行审查。这些准则只涵盖跨国电子商务中使用的各类证书，而不打算涉及其他证书，也不打算将这些办法仅限于签发准则所涵盖的证书。

[13] 信息和通信技术标准委员会于 1999 年在欧洲联盟内设立了欧洲电子签名标准化倡议组织，以协调支持实施欧洲联盟关于电子签名的第 1999/93/EC 号指令的标准化活动。信息和通信技术标准委员会本身就是欧洲标准化委员会的一个倡议，由国家标准组织和两个非营利组织即欧洲电工技术标准化委员会和欧洲电信标准研究所设立。欧洲电子签名标准化倡议组织为促进互操作性制定了各种标准，但这些标准的执行率一直很低，据称是因其过于复杂（Paolo Balboni，“Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication”，《信息和通信技术法》，第 13 卷第 3 期，2004 年），第 211-242 页和第 214 页。

[14] 例如，欧洲电信标准研究所制定了一项关于实施非等级结构的标准（TS 102 231），该标准除其他外也可用于处理对公钥基础设施域名以及由此对证书效力的相互承认。从根本上说，欧洲电信标准化研究所的 TS 102 231 号技术标准规定了提供认证服务提供者（称为“委托服务提供者”）状况信息的标准。该标准采用一种经签名的清单作为提供这种信息的基础，即“委托服务状况清单”。欧洲电信标准研究所规定的这种委托服务状况清单考虑到有关以下情况的证据要求：即在提供服务时，或者在依赖于该项服务的交易发生时，委托服务提供者是否是在任何公认办法批准的情况下进行运作的。为了满足这项要求，委托服务状况清单必须包含一些信息，可根据这些信息确定认证服务提供者的服务在交易之时是否为办法实施人员所知晓以及如果知晓的话服务的情况如何（例如这项服务是否被批准、中止、取消或废除）。因此，欧洲电信标准研究所 TS 102 231 号技术标准所设想的委托服务状况清单不仅应包括服务现状，还应包括其历史状况。因此，该清单不仅包括有效服务（“白名单”），还包括被取消或废除的服务（“黑名单”）。（见 http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ts_102231v010201p&RGW.doc，2007 年 3 月 4 日查取）。

外国签名和证书在本国生效，必须由本国的认证服务提供者、认证机构或管理机构对其进行某种核实或确认。其中有些法律承认综合考虑了所有这些因素。[15]

18. 国内法明确否定对外国签名或证书予以法律承认的情况并不常见，这可能表明国内法具有非歧视性的特点。但在实践中，许多承认制度往往会产生歧视性影响，即便是无意的歧视。例如，欧洲联盟关于电子签名的指令总体上禁止歧视符合条件的外国证书（即采用公钥基础设施的数字签名）。但这主要对在欧洲联盟成员国领土内设立的认证服务提供者签发的证书有利。在非欧洲联盟国家设立的认证服务提供者要获得欧洲联盟对其证书的承认，可以有三个选择：一是满足欧洲联盟电子签名指令的要求并根据一成员国制定的办法获得资格认可；二是与在欧洲联盟成员国内设立的认证服务提供者建立相互认证关系；三是在国际协定规定的总体承认框架内运作。[16]欧洲指令规范国际方面的方式表明，确保为欧洲联盟的认证服务提供者进入外国市场提供条件是该指令的目标之一。[17]通过将与欧洲联盟标准实质性等同的要求和“根据一成员国制定的办法获得资格认可”这一额外要求相结合，欧洲联盟电子签名指令提出了一项有效要求，即外国认证服务提供者既要遵守其原在国的制度，也要遵守欧洲联盟的制度。与对在欧洲联盟成员国内获得资格认可的认证服务提供者提出的要求相比，这是一项更高的标准。[18]

19. 欧洲联盟电子签名指令第 7 条得到了变通实施。[19]例如，爱尔兰和马耳他承认外国数字签名（合格的证书，按欧洲联盟的术语）只要满足其他法律要求，则与本国签名具有同等效力。在另一些情况下，是否予以承认取决于本国核实情况（奥地利，卢森堡）或本国主管机构的决定（捷克共和国、爱沙尼亚、波兰）。这种坚持进行某种本国核实的倾向往往是由于对外国证书的可靠程度具

---

[15] 例如在阿根廷，在阿根廷和外国认证机构原在国之间订有互惠协议或“得到在阿根廷获得许可并经执行机构认证的认证机构确认”的情况下，外国证书和电子签名才会得到承认（见 *Ley de firma digital*（2001 年），第 16 条）。

[16] 实际上，按照该指令第 7 条，欧洲联盟成员国只须确保第三国认证服务提供者签发的证书被认为与在欧共体内设立的认证服务提供者签发的证书具有同等的法律效力，但条件是：(a)该认证服务提供者 “满足了本指令所规定的各项要求并已根据一成员国制定的自愿资格认可办法获得了资格认可”；或(b)在欧共体内设立并满足了本指令所规定的各项要求的认证服务提供者能够为该证书“提供保证”；或(c)该证书或认证服务提供者“根据欧共体与第三国或国际组织间的双边或多边协定得到了承认”。

[17] 从该指令第 7 条第 3 款的措辞可以明显看出对于确保欧洲认证服务提供者进入外国市场的担心，该款规定，“欧盟委员会如果获悉欧共体企业在进入第三国市场方面遇到的任何困难，可在必要时向欧洲理事会提出建议，以便使这些在第三国的欧共体企业能够获得适当授权，进行争取对等权利的谈判”。

[18] Jos Dumortier 等，“The legal and market aspects of electronic signatures”，Study for the European Commission Directorate General Information Society (Katholieke Universiteit Leuven, 2003)，第 58 页。

[19] 同上，第 92-94 页。

有某种合理的担心所致，在实践中会造成一种因地理来源地而歧视外国证书的制度。

2. 实质性等同

20. 根据长期以来的传统，贸易法委员会在提出有关承认外国证书和电子签名的各种因素时，对地理方面的考虑未予认可。实际上，《贸易法委员会电子签名示范法》第 12 条第 1 款明确规定，在确定某一证书或某一电子签名是否具有法律效力和具有多大的法律效力时，“不应考虑签发证书或制作或使用电子签名的地理位置或签发人或签名人营业地的地理位置”。

21. 《贸易法委员会电子签名示范法》第 12 条第 1 款是为了反映一项基本原则，即来源地本身无论如何不应成为确定外国证书或电子签名是否能够具有法律效力或具有多大法律效力的一个因素。确定某一证书或某一电子签名是否能够具有法律效力或具有多大法律效力，应当取决于其技术上的可靠性，而不是签发该证书或该电子签名的地点。有些国内制度中也有类似于《电子签名示范法》第 12 条的非歧视性条文，例如 2000 年《美国全球和国内商务电子签名法》。[20]这些条文规定，来源地本身不应成为确定外国证书或电子签名在颁布国是否具有法律效力和具有多大法律效力的一个因素。这些条文认为证书或电子签名的法律效力应当取决于其技术上的可靠性。[21]

22. 《示范法》没有考虑地理因素，而是确立了有关证书和签名可靠程度的实质性等同标准。因此，外国证书如具有与在颁布国签发的证书“基本等同的可靠性”，则应具有“同样的法律效力”。同样，在一国境外制作或使用的电子签名“如具有基本等同的可靠性”，则“应具有”与在该国境内制作或使用的电子签名“同样的法律效力”。本国和外国证书和签名的可靠程度是否等同，应根据公认的国际标准和任何其他相关因素来确定，包括当事各方之间关于使用某些类别的电子签名或证书的协议，除非根据适用法该协议无效或不具有效力。

23. 《示范法》不要求也不提倡互惠安排。实际上，《示范法》“并未具体指明颁布国可能采取哪种法律手段（例如一项单方面声明或一项条约）事先承认符合外国法律的证书和签名的可靠性”。[22]在编拟《示范法》过程中提到的能够实现这一结果的可能方法包括自动承认符合另一国法律的签名——如果外国法律要求的可靠程度至少等同于对相应的本国签名所要求的可靠程度的话。颁布国据以事先承认外国证书和签名可靠性的其他法律手段可包括单方面声明或条约。[23]

---

[20] 见注[…][《美国法典》，第 15 编，第 96 章，第 7031 条（关于在国际交易中使用电子签名的原则）]。

[21] 见《贸易法委员会电子签名示范法及其颁布指南》，第二部分，第 83 段。

[22] 同上，第 157 段。

[23] 见电子商务工作组第三十七届会议工作报告（A/CN.9/483），第 39 和 42 段。