



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（第一部分，第二章，A和B节）。

* 由于缺少人手，联合国国际贸易法委员会秘书处提交本文件的时间被推迟。



附件

目录

	段次	页次
第一部分 电子签名和认证方法（续）	1-46	3
二、电子认证和签名的法律待遇	1-46	3
A. 法律文本的技术模式	5-19	4
1. 最低限度模式	6-12	4
2. 技术模式	13-15	7
3. 两级或双轨模式	16-19	8
B. 电子签名和认证方法的证据价值	20-46	10
1. “认证”和电子记录的一般归属	21-29	10
2. 达到法定签名要求的能力	30-35	14
3. 努力为特殊形式的签名开发出等效的电子签名	36-46	18

第一部分

电子签名和认证方法

[……]

二、电子认证和签名的法律待遇

1. 对电子商务的发展而言，建立信任非常重要。为提高电子商务使用过程中的确定性和安全性，可能有必要制定一些特殊的规则。可以提供这类规则的各种法律文本包括：国际法律文书（条约和公约）；跨国示范法；国家立法（通常以各类示范法为基础）；自律性文书；¹ 或契约协定。²

2. 许多电子商务交易都是在封闭网络中完成的，也就是说，封闭网络是由参与者数量有限而且只对先前获得授权的个人或公司开放的一些团体组成。封闭网络支持单个实体或一个现存的封闭用户群的运作，如参与银行同业支付系统、证券和商品交换的金融机构，或航空公司和旅行社组成协会。在这些情况下，网络的参与者常常仅限于先前获准进入该团体的机构和公司。在这些网络中，大多数都已存在了数十年。它们使用高端技术，并掌握了运作该系统方面的高级专业知识。在过去十年里，电子商务快速成长，促进了其他网络模式的发展，如供应链或贸易平台。

3. 尽管与当时已经存在的大多数封闭网络一样，这些新团体最初的组建结构都是采用计算机之间直接相连的方式，但是，使用公开可获的手段如因特网作为共同连接工具的趋势正日渐明显。即使是在这些较新的模式下，封闭网络仍然保留着一些独有的特征。特别是，封闭网络是依照先前商定的且名称各不相同的各种契约标准、协定、程序和规则运作的，如“系统规则”、“业务规则”或“贸易伙伴协定”，它们的目的是为团体成员提供并确保必要的业务功能、可靠性和安全性。这些规则和协定往往会涉及下列事项：对电子通信的法律价值的承认、发送或接收数据电文的时间和地点、获准进入该网络的安全程序以及当事方要使用

¹ 例如，见题为“电子商务自律性文书（行为守则）”的欧洲经济委员会联合国贸易促进与电子商务中心建议 32（ECE/TRADE/277），载于 http://www.unece.org/cefact/recommendations/rec_index.htm，2007年3月28日查阅。

² 许多国家和国际一级举措的目的都是为了制定示范合同。例如，见题为“在商业上交换使用电子数据协定”（TRADE/WP.4/R.1133/Rev.1）的欧洲经济委员会促进国际贸易程序工作组建议 26；以及题为“电子商务协定”的联合国贸易促进与电子商务中心建议 31（ECE/TRADE/257），两份文件均载于 http://www.unece.org/cefact/recommendations/rec_index.htm，2007年3月28日查阅。

的认证或签名办法。³ 在适用法律规定的契约自由范围内，这些规则和协定常常具有自我实施的性质。

4. 然而，如果没有契约规则，或如果适用法律可能会限制其可执行性，则当事方所用电子认证和签名方法的法律价值将由适用的法律规则来确定，而这种法律规则可采用默认或强制规则的形式出现。本章讨论了在不同管辖区域内为建立电子签名和认证法律框架而采用的几种备选方案。

A. 法律文本的技术模式

5. 在国际和国家各级，电子认证方面的法律和法规采用了多种不同的形式。已确定的处理签名和认证技术的主要模式有三种：(a) 最低限度模式；(b) 技术模式和 (c) 两级或双轨模式。⁴

1. 最低限度模式

6. 一些管辖区域遵守技术中立政策，承认各种电子签名技术。⁵ 这种办法又称最低限度模式，因为它会给予各种形式的电子签名以最低的法律地位。在最低限度模式下，人们认为电子签名和亲笔签名具有同等效力，条件是所采用的技术意图是要履行某些特定的功能，并且达到了某些技术中立的可靠性要求。

7. 贸易法委员会《电子商务示范法》⁶为在电子签名和亲笔签名之间建立一般功能等效关系提供了一套最广泛采用的立法标准。《示范法》第7条第1款规定：

“(1) 法律要求在数据电文上签名的，在具有以下情形时视为符合了该项要求：

“(a) 使用一种方法鉴定了该人的身份，并且表明该人认可了数据电文内含的信息；和

“(b) 从所有各种情况来看，包括根据任何相关协议，所用方法是可靠的，对生成或传递□□电文的目的来说也是适当的。”

³ 关于对贸易伙伴协定常涉的问题的讨论，见 Amelia H. Boss, “电子数据交换协定：走向全球的私人合同”，《西北国际法律与商业杂志》，第13卷，第1(1992)号，第45页。

⁴ Susanna F. Fischer, “保护虚拟世界中的罗生克兰和盖登思邓？对近期全球电子签名立法的比较研究”，《科学和技术法学报》，第7卷，第2(2001)号，第234页及以后。

⁵ 如澳大利亚和新西兰。

⁶ 见注[……][联合国出版物，出售品编号：E.99.V.4]。

8. 这项规定考虑到了亲笔签名的两个主要功能：鉴定签字人的身份，表明签字人对所签署信息的意向。根据《电子商务示范法》，任何具备这两项功能的电子技术都应被视为符合签名方面的法律要求。因此，从技术角度讲，《示范法》是中立的；也就是说，它并不取决于或预先假定使用任何特定类型的技术，可被适用于各类信息的交流和存储。考虑到技术创新的速度，技术中立性具有重要的意义，它有助于确保立法能够持续适应今后的发展，而不会很快被废除。因此，《示范法》非常谨慎，并未在任何地方提及传输或存储信息的特定技术方法。

9. 许多国家的法律都纳入了这条一般原则。技术中立原则还使得立法能够适应今后的技术发展。另外，这种模式强调，当事方有选择适合其需要的技术的自由。这样，确定所用技术对其交流是否足够安全的责任就落在了当事方身上。如此一来，既可避免技术方面过于复杂，也避免了相关费用。⁷

10. 欧洲的立法主要受欧洲联盟所发布指令的影响，⁸ 除此以外，大多数制定了电子商务相关法律的国家都是以《电子商务示范法》为模版的。⁹ 此外，《示范法》

⁷ S. Mason, “实践中的电子签名”, 《高技术法学报》, 第四卷, 第 2 (2006) 号, 第 153 页。

⁸ 特别是, 欧洲议会和电子签名共同框架理事会的第 1999/93/EC 号指令 (见注[……]) [《欧洲共同体公报》, L 13]。继电子签名指令之后, 欧洲议会和理事会于 2000 年 6 月 8 日发布了一份更具普遍意义的指令, 即关于内部市场中各种信息社会服务特别是电子商务的某些法律问题的第 2000/31/EC 号指令 (电子商务指令) (《欧洲共同体公报》, L 178, 2000 年 7 月 17 日), 它涉及到提供信息技术服务的各个方面以及一些有关签订电子合同的事项。

⁹ 截至 2007 年 1 月, 至少有下列国家通过了贸易法委员会《电子商务示范法》的立法执行条款: 澳大利亚, 1999 年《电子交易法》; 中国, 《电子签名法》, 2004 年颁布; 哥伦比亚, *Ley de comercio electrónico*; 多米尼加共和国, *Ley sobre comercio electrónico, documentos y firmas digitales* (2002 年); 厄瓜多尔, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos* (2002 年); 法国, *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* (2000 年); 印度, 《信息技术法》, 2000 年; 爱尔兰, 《电子商务法》, 2000 年; 约旦, 《电子交易法》, 2001 年; 毛里求斯, 2000 年《电子交易法》; 墨西哥, *Decreto por el que se reforman y adicionan diversas disposiciones del código civil para el distrito federal en materia federal, del Código federal de procedimientos civiles, del Código de comercio y de la Ley federal de protección al consumidor* (2000 年); 新西兰, 2002 年《电子交易法》; 巴基斯坦, 《电子交易条例》, 2002 年; 巴拿马, *Ley de firma digital* (2001 年); 菲律宾, 《电子商务法》(2000 年); 大韩民国, 《电子商务框架法》(2001 年); 新加坡, 《电子交易法》(1998 年); 斯洛文尼亚, 《电子商务和电子签名法》(2000 年); 南非, 《电子通信和交易法》(2002 年); 斯里兰卡, 《电子交易法》(2006 年); 泰国, 《电子交易法》(2001 年); 委内瑞拉玻利瓦尔共和国, *Ley sobre mensajes de datos y firmas electrónicas* (2001 年); 以及越南, 《电子交易法》(2006 年)。采用《示范法》的还有: 英国王国属地根息行政区 (2000 年《根息电子交易法》)、泽西行政区 (2000 年《泽西电子通信法》) 和马恩岛 (2000 年《电子交易法》); 大不列颠及北爱尔兰联合王国海外属地百慕大 (1999 年《电子交易法》)、开曼群岛 (2000 年《电子交易法》) 与特克斯和凯科斯群岛 (2000 年《电子交易条例》); 以及中国香港特别行政区 (《电子交易条例》(2000 年))。除另有规定外, 下文提到的这些国家的法规条款指的就是上文所列法规中包含的条款。

也是加拿大¹⁰ 和美利坚合众国¹¹ 等联邦制国家对电子商务立法进行国内协调的依据。除个别情况外，¹² 颁布《示范法》的国家都保留了其技术中立模式，既不规定也不倾向于使用任何一种特定的技术。贸易法委员会《电子签名示范法》（2001 年通过）¹³ 和最近的《联合国国际合同使用电子通信公约》¹⁴（大会于 2005 年 11 月 23 日通过，自 2006 年 1 月 16 日起开放供签署）都采用了相同的模式，尽管前者包含了一些附加语言（见下文，第[……]-[……]段）。

11. 事实证明，当立法采用了最低限度模式时，电子签名是否具有同等效力的问题常常会交由法官、仲裁员或公共当局来确定，所采用的方式一般都是所谓的“适当可靠性测试”。根据这种测试，各类达到检验要求的电子签名都会被视作有效；因此，测试体现了技术中立原则。

12. 要在各种情况下判定一种特定认证方法是否提供了适当程度的可靠性，可能要考虑大量的法律、技术和商业因素，其中包括：（a）各方当事人所使用设备的精密程度；（b）他们所从事的贸易活动的性质；（c）双方进行商业交易的频率；（d）交易的性质和规模；（e）签名要求在特定的法规和管理环境下的作用；（f）

¹⁰ □示范法》在加拿大国内立法中的具体体现是加拿大统一法联合会于 1999 年通过的《统一电子商务法》（载于 <http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia>，附官方评注，2007 年 4 月 12 日查阅）。加拿大的多个省和行政区都已颁布了这一法案，其中包括艾伯塔省、不列颠哥伦比亚省、马尼托巴省、新不伦瑞克省、纽芬兰-拉布拉多省、新斯科舍省、安大略省、爱德华王子岛省、萨斯喀彻温省和育空地区。魁北克省颁布了特殊立法（《建立信息技术法律框架法》（2001 年）），尽管这部法律的范围更广、起草方式也有所不同，但是，它实现了《统一电子商务法》的多项目标，而且，基本符合贸易法委员会《电子商务示范法》。有关《统一电子商务法》颁布情况的最新信息载于 <http://www.chlc.ca/en/cls/index.cfm?sec=4&sub=4b>，2007 年 2 月 7 日查阅。

¹¹ 在美利坚合众国，国家统一州法委员会以贸易法委员会《电子商务示范法》为依据，编制了《统一电子交易法》。美国已于 1999 年通过该法案（法案案文和官方评注载于 <http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm>，2007 年 2 月 7 日查阅）。哥伦比亚特区和下列 46 个州都已颁布了《统一电子交易法》：亚拉巴马州、阿拉斯加州、亚利桑那州、阿肯色州、加利福尼亚州、科罗拉多州、康涅狄格州、特拉华、佛罗里达、夏威夷、爱达荷州、印第安纳州、衣阿华州、堪萨斯州、肯塔基州、路易斯安那州、缅因、马里兰、马萨诸塞州、密歇根州、明尼苏达州、密西西比、密苏里州、蒙大拿州、内布拉斯加州、内华达州、新罕布什尔州、新泽西州、新墨西哥州、北卡罗来纳州、北达科他州、俄亥俄州、俄克拉何马州、俄勒冈州、宾夕法尼亚州、罗德岛州、南卡罗来纳州、南达科他州、田纳西州、德克萨斯州、犹他州、佛蒙特州、弗吉尼亚州、西弗吉尼亚州、威斯康星州和怀俄明州。其他各州，包括已通过《电子商务安全法》（1998 年）颁布贸易法委员会《示范法》的伊利诺伊州，很可能在不久的将来通过执行性立法。有关《统一电子交易法》颁布情况的最新信息载于 http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp，2007 年 2 月 7 日查阅。

¹² 哥伦比亚、多米尼加共和国、厄瓜多尔、印度、毛里求斯、巴拿马和南非。

¹³ 见注[……][联合国出版物，出售品编号：E.02.V.8]。

¹⁴ 见注[……][大会第 60/21 号决议，附件]。

通信系统的能力；(g) 对中间人所规定的认证程序的遵守情况；(h) 任何中间人所提供认证程序的范围；(i) 对贸易惯例和做法的遵守情况；(j) 有无防范擅自发出电文的保险机制；(k) 数据电文所含信息的重要性和价值；(l) 替代鉴定方法的可利用情况和实施费用；以及 (m) 相关行业或领域在就鉴定方法达成一致时以及传输数据电文时，对这种方法的接受或不接受程度。

2. 技术模式

13. 对促进媒介中立性的关注提出了另外一个重要问题。不仅是在电子商务领域，在纸张环境中也存在不可能确保完全避免欺诈和传输错误的问题。在为电子商务制定规则时，立法人员往往都倾向于以现有技术提供的最高安全性为目标。¹⁵ 毋庸置疑，我们确实需要采取严格的安全措施，以避免未经授权便获取数据，确保通信的完整性并保护计算机和信息系统。然而，从私营企业法的角度看，以类似于纸张环境所经历法律安全程度的步伐，逐步制定安全性要求可能会更适当。在纸张环境中，商人在大多数情况下都可以从大量方法中自由选择，以实现通信的完整性和真实性（例如，在简单合同和公证行为的文件中可以看到不同标准的亲笔签名）。如果采用技术模式，条例将规定一种具体的技术，用以满足电子签名有效性的法律要求。例如，在这种情况下，以较高安全性为目标的法律会要求采用以公用钥匙基础结构为基础的方法。由于这种模式规定要采用一种特定的技术，它也会被称作“指示性”模式。

14. 技术模式的缺点包括：由于偏向于某几种特定类型的电子签名，它“可能会使得其他一些或许更高级的技术无法进入市场参与竞争”。¹⁶ 这种模式可能会产生一些负面影响，而不是促进电子商务的成长和电子认证技术的使用。技术立法承担着一定的风险，即它可能会在某项特定的技术成熟之前便确定出各项

¹⁵ 最早期的一个例子是《犹他州数字签名法》，该法于 1995 年获得通过，但自 2006 年 5 月 1 日起即被第 20 号州法案废止，该法案载于 <http://www.le.state.ut.us/~2006/htmldoc/sbillhtml/sb0020.htm>，2007 年 3 月 28 日查阅。许多国家都存在犹他州法案中出现的技术偏见。在这些国家，法律只承认在公用钥匙基础结构（PKI）框架内创建的数字签名是有效的电子认证方式。例如，下面几部法律均出现了上述情况：阿根廷法律，*Ley de firma digital*（2001 年）和第 2628/2002 号法令（*Reglamentación de la Ley de firma digital*）；爱沙尼亚，《数字签名法》（2000 年）；德国，《数字签名法》，作为 1997 年 6 月 13 日《信息与通信服务法》第 3 条颁布；印度，2000 年《信息技术法》；以色列，《电子签名法》（2001 年）；日本，《电子签名和认证服务法》（2001 年）；立陶宛，《电子签名法》（2000 年）；马来西亚，1997 年《数字签名法》；波兰，《电子签名法》（2001 年）和俄罗斯联邦，《电子数字签名法》（2002 年）。

¹⁶ Stewart Baker 和 Matthew Yeo 与国际电信联盟秘书处合作编写，《与认证和国际电联有关的背景和问题》，提交给电子签名和认证机构专家会议的简报文件：《电信问题》，日内瓦，1999 年 12 月 9 日和 10 日，第 2 号文件，载于 www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html，2007 年 4 月 12 日查阅。

要求。¹⁷ 这样一来，立法就可能会阻碍技术在后期的积极发展，或是因为后期的发展而迅速过时。还有一点，就是并非所有情况都要求有可与某些具体技术如数字签名所提供安全性相媲美的安全程度。此外，还可能会出现这样一种情况，即对当事人而言，通信的速度和便利程度或其他因素要比通过任何特定程序确保电子信息的完整性更重要。要求使用极度安全的认证方法会造成成本和精力的浪费，进而可能会阻碍电子商务的传播。

15. 技术立法特别倾向于使用公用钥匙基础结构框架内的数字签名。根据政府干预程度的不同，各国构建公用钥匙基础结构的方式也各不相同。在这方面，我们也可以确定三种主要模式：

(a) **自我调节** 在这种模式下，认证活动的范围是非常广泛的。虽然政府会在各部门和相关组织中建立一个或多个认证组织，但是，私营部门可以视情况而定，自由设立商业性或其他性质的认证机构。没有强制性的高级认证机构，认证服务商负责按照建立认证机构的目标，确保与国内和国际级的其他服务商之间的互用性。对认证服务商没有许可证或技术核准方面的要求（消费者保护条例可能除外）；¹⁸

(b) **有限的政府干预** 政府可能会决定建立一个自愿或强制性的高级认证机构。在这种情况下，认证服务商可能会发现有必要与高级认证机构建立互用关系，以使其认证□□（或其他认证符）在自身系统以外也被接受。在这种情况下，还必须尽快出版认证服务商技术和管理规范，以便政府部门和私营部门做出相应规划。各认证服务商可能会需要进行许可证和技术方面的核准；¹⁹

(c) **政府引导的进程** 政府可能会决定成立唯一一家中央认证机构。经政府核准之后，可能还会设立一些专门用途的认证服务商。²⁰另一种方法就是身份管理系统（见上文第[···]-[···]段），借此，政府可以间接引导数字签名进程。一些政府已经启动了各种方案来向其公民分发给有数字签名功能的机器可读身份证件（“电子身份证”）。

3. 两级或双轨模式

16. 在这种模式下，立法规定电子认证方法满足较低的要求阈值即可获得某种最

¹⁷ 不过，考虑到当前的公用钥匙基础结构已相当成熟和完善，这些关切问题中，有些已无须像从前那么关注。

¹⁸ 亚洲-太平洋经济合作组织，《亚太经合组织经济体无纸贸易评估报告》（北京，亚太经合组织秘书处，2005年），第63和64页，以美国为例说明了这种模式的应用情况。

¹⁹ 同上，以新加坡为例进行了说明。

²⁰ 同上，以中国和马来西亚为例进行了说明。

低法律地位，并赋予某些电子认证方法具有较高的法律效力（系指各种安全的、高级的或增强型的电子签名，或合格证书）。²¹在基础一级，采用两级体系的立法一般都会根据技术中立标准，授予电子签名与亲笔签名相同的功能地位。高级签名适用于某些可反驳的推定，这些签名必须遵守一些可能与某种特定技术有关的特殊要求。目前，这类立法通常会从公用钥匙基础结构技术方面对这类安全签名加以界定。

17. 认为在其立法中提出某些技术要求比较重要、但同时又希望为技术发展留出一定空间的管辖区域一般都会选择这种模式。它把从商业方面判断使用一种更安全方法带来的成本及其不便是否适合需要的权力留给了当事方，因此，在电子签名的灵活性和确定性之间实现了平衡。这些文本还为在认证机构模式下承认电子签名的标准提出了指导意见。一般而言，都可以类似于技术模式下所采取的方式（见上文第[···]-[···]段），把两级模式与任何类型的认证模式相结合（无论是自我调节、自愿鉴定还是政府引导模式）。这样一来，一些规则可能足够灵活，可以适应不同的电子签名认证模式，而另一些系统则只承认得到许可的认证服务商是可以发布“安全”或“合格”认证的人。

18. 让已通过的立法采用两级模式的第一批司法管辖区域包括新加坡²²和欧洲联盟。²³许多其他国家紧随其后。²⁴贸易法委员会《电子签名示范法》允许制定法律的国家通过法律法规建立两级体系，尽管它并没有积极宣传这一体系。²⁵

²¹ Aalberts 和 van der Hof, 《数字签名盲区……》（见注[……]，第 3.2.2 段）。

²² 新加坡《电子交易法》第 8 条承认一切形式的电子签名，不过，只有符合该法案第 17 条各项要求的安全电子签名（即那些“(a) 是使用者唯一的签名；(b) 能证实使用者的身份；(c) 通过某种使用者可以唯一控制的方式或方法创设；或者 (d) 和相关的电子记录以某种方式具有密切联系，一旦该记录被修改，则签名也随之失效”的电子签名）符合第 18 条所列推定（除其他外，该签名“属于对应的签名人”，而且“签名者附加这一安全数字签名是为了签署电子记录或对电子记录表示同意”）。对本法案而言，符合本法案第 20 条各项规定的、值得信任的认证所支持的数字签名会被自动视为“安全电子签名”。

²³ 和新加坡《电子交易法》一样，欧洲联盟电子签名指令（见注[……]）区分了“电子签名”（第 2 条第 1 款给出了定义，即“作为一种认证方式，一种电子数据附属于或在逻辑上与其他电子资料存在关联的认证方式”）和“高级电子签名”（第 2 条第 2 款给出了定义，即符合以下条件的电子签名：“(a) 只能和唯一的签名者联系在一起；(b) 使人能够识别签名者；(c) 以一种能使签名者独自控制的签名方式创造出来；(d) 和资料紧密关联，以致于任何外来的改动都能被发现”）。指令第 5 条第 2 款规定，欧洲联盟各成员国必须确保不会仅仅因为电子签名“是电子形式，或没有合格认证，或没有经验证的认证服务商签发的合格认证，或非由一个安全签署签字设备生成”“等理由而否认其在法律诉讼中作为证据的法律效力和可接受性。”然而，只有“基于合格认证和由安全签署签字设备生成”的高级电子签名才“(a) 正如亲笔签名符合那些与纸质数据有关的要求一样，符合与电子数据有关的签名方面的法律要求；(b) 可以在法律诉讼中被接受为证据。”（见指令第 5 条第 1 款）。

19. 关于第二级，建议各国不要因为与国际商业贸易有关的格式要求而要求使用第二级签名，而且，“安全”电子签名应局限于不会对国际贸易产生重大影响的法律领域（如信托、家庭法、不动产交易等）。²⁶ 此外，建议两级法律应该明确增强关于使用和承认电子签名的契约协定的效力，以确保以合同为基础的全球认证模式不会与国家法律要求相抵触。

B. 电子签名和认证方法的证据价值

20. 贸易法委员会《电子商务示范法》与贸易法委员会《电子签名示范法》的主要目标之一，就是为电子和纸张签名和认证方法之间建立功能等效关系确立一般标准，以预防不协调和可能出现的过度管制。虽然贸易法委员会《电子商务示范法》已得到广泛认可，而且有越来越多的国家以它为依据来制定其电子商务立法，但是，我们仍不能认为《示范法》的各项原则适用于所有情况。不同司法管辖区在电子签名和认证方面采取的态度通常都反映了管辖区书面要求的一般模式和电子记录的证据价值。

1. “认证”和电子记录的一般归属

21. 使用电子认证方法涉及到对当前讨论非常重要的两个方面。第一个方面涉及到电文是否出自其所谓创建者的一般问题。第二个方面涉及到当事方为满足具体的格式要求特别是法定签字要求而采用的鉴别方法是否适当。另外，暗示存在某种亲笔签名的一些法律概念也很重要，如一些法律体系中“文件”的概念。虽然这两个方面经常是结合在一起的，或者可能无法明确区分开来（只是程度不同而已），但对其进行单独分析还是有用的，法院采取的做法正是这样，它们往往会根据认证方法所附属的职能得出不同的结论。

22. 《电子商务示范法》第 13 条涉及数据电文的归属。该条文的渊源是贸易法委员会《国际信用划拨示范法》第 5 条，²⁷ 该条界定了支付命令发送人的义务。对于一封电子信函是否真由其中所示创建者发送，如果发生疑问，即应适用《电

²⁴ 如毛里求斯和巴基斯坦。各法规的详细信息，见上文注 [9]。

²⁵ 贸易法委员会《电子签名示范法》（见注 [……]）第 6 条第 3 款规定，具有以下情形的电子签名将被视为可靠的电子签名：（a）签字生成数据在其所使用的环境中与签字人发生关联，而与任何其他他人无关的；（b）签字生成数据在签字时处于签字人的控制之下，而不处在任何其他他人控制之下的；（c）凡在签字后对电子签名的一切修改均可被察觉的；以及（d）要求签字的法律目的是确保签字所涉信息的完整性，而在签字后对该信息的一切修改均可被察觉的。

²⁶ Baker 和 Yeo，“与认证……的背景和问题”（见注[16]）。

²⁷ 联合国出版物，出售品编号：E.99.V.11，载于 <http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf>。

子商务示范法》第 13 条。在书面信函中，问题往往发生在有人指称该信函创建者的签字有诈。在电子环境中，也会发生未经授权的人发出一项电文，但其使用密码、加密等手段或类似手段进行的核证都是正确无误的。第 13 条的目的不是为了查找数据电文的归属，也不是为了确定当事方的身份。更确切地说，它涉及到数据电文的归属，它设定了多种情况，在这些情况下，一方当事人可以假定数据电文确实是由其中所示的创建者发出的。

23. 《电子商务示范法》第 13 条第 1 款提及一项原则，即创建者如果事实上发送了一项数据电文，就得受该电文的约束。第 2 款涉及的情况是，电文不是由创建者发出，而是由有权代表创建者行事的另一人发出。第 3 款涉及收件人可以相信一项数据电文是创建者的数据电文的两种情况：第一种情况是收件人正确地使用了一种事先经创建者同意的认证程序；第二种情况是数据电文是由某一人的行为而产生的，该人由于与创建者的关系，得以动用创建者的认证程序。

24. 许多国家都采用了《电子商务示范法》第 13 条中的规则，包括该条第 3 款确定的关于归属的推定。²⁸ 一些国家明确提及将编码、口令或其他识别手段用作对归属做出推定的要素。²⁹ 第 13 条还存在着较为笼统的模式，其中，通过事先约定的程序进行适当验证而做出的推定被重新措辞为可用于归属目的的各种要素的表示。³⁰

25. 然而，其他一些国家仅采用了第 13 条中的一般性规则，即在下述情况下，数据电文为创建者的电文：数据电文由创建者本人发送或由代表创建者行事的人发送，或由创建者编程或代表创建者行事的人编程而自动运作的系统发送。³¹ 另外，《电子商务示范法》的一些执行国并未列入以第 13 条为依据的任何具体条文。

²⁸ 哥伦比亚（第 17 条）；厄瓜多尔（第 10 条）；约旦（第 15 条）；毛里求斯（第 12 条第 2 款）；菲律宾（第 18 条第 3 款）；大韩民国（第 7 条第 2 款）；新加坡（第 13 条第 3 款）；泰国（第 16 条）；委内瑞拉玻利瓦尔共和国（第 9 条）。同样的规则还载于下列各地的法律中：英国皇家属地泽西（第 8 条）和英国海外属地百慕大（第 16 条第 2 款）以及特克斯和凯科斯（第 14 条）。各项法规的详细信息，见上文注[9]。

²⁹ 墨西哥（见上文注[9]），第 90 条第 1 款。

³⁰ 例如，美国《统一电子交易法》（见注[10]）第 9 条（a）款规定：电子记录或电子签名“属于其行为人。行为可以通过任何方式予以表现，包括显示用以确定电子记录或电子签名归属的安全程序的效力。”第 9 条（b）款进一步规定，（a）款规定的电子记录或电子签名归属的效力，“可以根据其创设、执行、通过时的上下文和周围情形，包括当事人之间的协议确定，若有可能，未决之处由法律规定”。

³¹ 澳大利亚（第 15 条第 1 款）；基本相同的方式，印度（第 11 条）；巴基斯坦（第 13 条第 2 款）；斯洛文尼亚（第 5 条）；英国王国属地马恩岛（第 2 条）；和中国香港特别行政区（第 18 条）。各项法规的详细信息，见上文注[9]。

³² 这些国家的推定是，不需要订立任何具体规则，最好使用与确定书面文件归属相同的普通取证方法确定归属：“对任何签字表示相信的人都必须承担签字无效的风险，这条规则不会因为电子签名而有所改变。”³³

26. 但其他一些国家更喜欢把《电子商务示范法》中有关归属的条款与有关电子签名的条款分开，单独列明。采用这种方法的根据是，他们认为文件环境中的归属主要是为合理的信任提供依据，与狭义的用来确定个人身份的方法相比，它可能包含了更广泛的手段。一些法律，如美国《统一电子交易法》强调了这一原则，例如，它规定“电子记录或电子签名属于其行为人”，行为“可以通过任何方式予以表现，包括显示用以确定电子记录或电子签名归属的安全程序的效力。”³⁴ 这种关于归属的一般性规则并不妨碍将签名用作确定一项记录归属于某人的手段，不过，其基础是承认“签名并不是确定归属的唯一方法。”³⁵ 根据对美国法案的官方评注：

“4. 在电子环境中存在的某类信息似无法确定归属，但可确定某人与某记录之间的确切联系。数字编码、个人识别号码、公钥和私钥的各类组合都有助于确定电子记录所属当事方。当然，安全措施也是用于确定归属的另一种证据。

“由于在电子环境中，安全措施具有无法替代的重要性，因此，作为证明归属的一种手段专门提及安全措施是有益的。在某些程序中，技术和科技安全措施可能是让检验人相信某电子记录或签字属于某人的最佳方式。在某些情形下，为纠正黑客干预的说法，可能有必要使用安全措施以确定记录和有关的签字均为某人业务上的所为。提及安全措施的目的并不是说，关于确定归属的其他类型的证据的说服力就应该低一些。还应强调的是，某种措施的具

³² 例如，加拿大、法国、爱尔兰、新西兰和南非。

³³ 加拿大，《统一电子商务法》（附官方评注）（见注[10]），对第 10 条的评注。

³⁴ 美国，《统一电子交易法》（1999 年）（见注[11]），对第 9 条的官方评注第 9 条第 1 款提供了下列实例，其中，电子记录和电子签名都可被归属于某一人：“将本人姓名作为电子邮件订购单一部分输入的”；“雇员按照授权将雇主姓名作为电子邮件订购单一部分输入的”；或是“某人的计算机按照编程预定在特定参数范围内收到库存品信息后即订购物品，该计算机发出了订购单其中载有该人姓名或其他用于识别身份的信息作为订购单一部分的”。

³⁵ 同上。对第 9 条的官方评注第 3 款表示“使用传真传送提供了不以签字而以其他信息确定归属情况的一些例子。传真页页首处打印出的信息显示发送传真的机器，因而可以据此确定该传真属于某人。同样，传真页中可能包括显示发送者身份的印有抬头的信笺。有些情况表明，印有抬头的信笺实际上构成签字，因为它是发送者用以确定其传真真实性的一种标志。然而，在这种情况下，对意图作必要调查以后方可确定签字的归属。在其他情况中，由于未发现必要的意图，因此，通过传真传送的印有抬头的信笺无法作为签字。关键一点是，无论有否签字，电子记录中所载信息可能足以提供确定电子记录属于某当事方所需的事实。”

体效力并不影响该措施作为安全措施的地位，而只是会影响安全措施在确定归属时作为证据的分量。”³⁶

27. 还有一点非常重要，即应当铭记关于归属的推定本身无法取代有关签字法律规则的适用，根据此类法律规则，为确定某种行为的效力或证据，必须有签字。一旦确定记录或签字归属于某当事方，“记录或签字的效力可以根据上下文和周围情形，包括当事人之间的协议”以及“根据上下文而加以考虑的其他法定要求”加以确定。³⁷

28. 根据这种灵活理解归属问题的背景，美国的法院对于在民事诉讼程序中可否采信包括电子邮件在内的电子记录作为证据，采取了放宽限制的做法。³⁸ 美国的法院驳回了关于数据电文因未经核证并且属于口头证据而不得采信作为证据的说法。³⁹ 相反，法院认定，原告在法院查询阶段提供的电子邮件本身是自我核证的，因为“在查询阶段当事人从本人档案中出示文件足以证明其自我核证的结论是正确的。”⁴⁰ 法院常常会将所有现行证据一并加以考虑，并且不会将电子记录斥之为不够充分的表面证据。

29. 没有通过《电子商务示范法》的国家似乎并未颁布任何以类似方式处理归属问题的具体立法条文。在这些国家，归属通常取决于对电子签名的法律承认和对使用特殊类型的电子签名加以核证的记录所作的推定。对于篡改电子记录的风险的担忧已使得一些国家的法院驳回了在法院诉讼程序中以电子邮件作为证据的价值标准，理由是电子邮件并不能充分确保完整性。⁴¹ 对电子记录的证据价值和归属采取更严格的限制性做法的其他范例可见于最近涉及互联网拍卖的案件，在此类案件中，法院就确定数据电文的归属适用了严格的标准。这些案件通常涉及以未支付被指称在互联网拍卖中所购货物的货款为由而提出的对违反合同的诉

³⁶ 同上，对第9条的官方评注。

³⁷ 同上，对第9条的官方评注第6款。

³⁸ *Commonwealth Aluminum Corporation 诉 Stanley Metal Associates*，美国肯塔基西区地方法院，2001年8月9日，联邦补充案例，第2辑第186卷第770页；以及 *Central Illinois Light Company (CILCO) 诉 Consolidation Coal Company (Consol)*，美国伊利诺伊中区地方法院，2002年12月30日，联邦补充案例，第2辑第235卷第916页。

³⁹ *Sea-Land Service, Inc. 诉 Lozen International, LLC*，美国第九巡回上诉法院，2002年4月3日，联邦汇编，第3辑第285卷第808页。

⁴⁰ *Superhighway Consulting, Inc. 诉 Techwave, Inc.*，美国伊利诺伊北区地方法院，东区分院，1999年11月16日，U.S. Dist. LEXIS 17910。

⁴¹ 德国，波恩地方法院，案件号3 C 193/01，2001年10月25日，*Jur-PC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 332/2002，载于 <http://www.jurpc.de/rechtspr/20020332.htm>，2003年9月11日查阅。

讼。原告坚持认为被告就是买方，因为物品的最高出价是使用被告的命令加以核证的，并且是从被告的电子邮件地址发出的。法院裁定，根据这些要素，并不足以有把握地推断出被告事实上参与了拍卖并就物品提交了获胜的出价。法院使用了各种论据来证明该立场的合理性。例如，口令并不可靠，因为任何知道被告口令的人都可以在任何一台计算机上使用其电子邮件地址，并冒用被告的姓名参与拍卖，⁴² 某些法院估计，这种风险“很高”，依据是专家曾表示，特别是通过使用能够“偷取”某人口令的“特洛伊木马”，互联网通信网络的安全面临着种种威胁。⁴³ 使用特定媒介发出货物或服务要约的当事方应承担对方的识别手段（口令）被冒用的风险，因为从法律上无法推定经由某人的入网口令通过互联网发送的电文应该归属于某人。⁴⁴ 可以设想法律定义的“高级电子签名”附带这一推定，但简单“口令”的持有者不应承担该口令被未经准许的人滥用的风险。⁴⁵

2. 达到法定签名要求的能力

30. 在有些国家，法院往往会对签字要求做出广义的解释。如前文所述（见导言，第[···]-[···]段），就关于欺诈的法规的要求即某些交易必须有书面文件和签名方可有效而言，这种情况在一些英美法系国家非常典型。此外，美国的法院愿意接受在立法上承认电子签名，它们承认在授权法未明确规定的情形下可以使用电子签名，如签发司法令状等。⁴⁶ 对合同而言，更重要的是，法院还可以根据当事人之间的交易情况评估认证的充分性，而不是对所有情况适用一种严格的标准。因此，对于当事人经常利用电子邮件进行谈判的情形，法院认定，创建者在电子邮件中

⁴² 德国，爱尔福特地方法院，案件号 28 C 2354/01，2001 年 9 月 14 日，*JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 71/2002，载于 <http://www.jurpc.de/rechtspr/20020071.htm>，2003 年 8 月 25 日查阅；另见波恩地区法院，案件号 2 O 472/03，2003 年 12 月 19 日，*JurPC, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 74/2004，载于 <http://www.jurpc.de/rechtspr/20040074.htm>，2007 年 2 月 2 日查阅。

⁴³ 德国，康斯坦茨地区法院，案件号 2 O 141/01 A，2002 年 4 月 19 日，*JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 291/2002，载于 <http://www.jurpc.de/rechtspr/20020291.htm>，2003 年 8 月 25 日查阅。

⁴⁴ 德国，波恩地区法院，案件号 2 O 450/00，2001 年 8 月 7 日，*JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 136/2002，载于 <http://www.jurpc.de/rechtspr/20020136.htm>，2003 年 8 月 25 日查阅。

⁴⁵ 德国，科隆高等地方法院（上诉法院），案件号 19 U 16/02，2002 年 9 月 6 日，*JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 364/2002，载于 <http://www.jurpc.de/rechtspr/20020364.htm>，2003 年 8 月 25 日查阅。

⁴⁶ *Department of Agriculture 和 Consumer Services 诉 Haire*，佛罗里达第四巡回上诉法院，案件号 4D02-2584 和 4D02-3315，2003 年 1 月 15 日。

的署名符合法定的签字要求。⁴⁷ 一个人“有意选择在所有电子邮件的末尾打上其姓名”的行为会被视为有效的认证。⁴⁸ 美国法院愿意接受那些能够符合书写要求的电子邮件及署名，⁴⁹这是对“签名”这一概念的较宽泛的解释，认为它包括“一当事人为验证一份文件而书写或采用的任何符号”，因此，在某些情况下，“文件中的署名或印有抬头的信笺足以符合签名要求”。⁵⁰ 如果当事人不否认曾经以电子邮件的形式书写或接收过信件，那么，法定的签字要求就得到了满足，因为法院“早已承认具有约束力的签名可能是当事人认为适当的、具有约束力的任何符号或标记”，条件是作者“打算受到约束”。⁵¹

31. 大不列颠及北爱尔兰联合王国的法院采取了类似的办法，在通常情况下，他们认为签名的形式没有其所要实现的功能重要。所以，法院会从确定一项记录属于某人以及显示某人对记录的意见两方面，考虑媒介的适合度。因此，电子邮件就构成了“文件”，电邮上的署名可能就是“签名”。⁵² 一些法院已宣布，它们“确定如果当事人创建并发送了一份电子文件，那么，我们会认为他签署了该文件，这相当于从法律上讲视同他签署了同一份文件的硬拷贝”，而且，“文件是以电子方式生成还是以硬拷贝的形式出现并无任何差别。”⁵³法院曾经驳回了关于电子邮件构成欺诈法规意义上的已经签署的合同的的主张，主要是因为签字人没有打算受签字约束的意图。不过，似乎并没有先例表明法院会先验性地拒绝那些已经达到法定书面要求和签字要求的电子邮件和其中的署名。在某些案件中，我们会发现关于欺诈的法规要求并未得到满足，因为所讨论的电子邮件仅反映了进行中的谈判，而不是最后协定，理由包括谈判期间，一方当事人认为有约束力的合同是在

⁴⁷ *Cloud Corporation 诉 Hasbro, Inc.*, 美国第七巡回上诉法院, 2002 年 12 月 26 日, 联邦汇编, 第 3 辑第 314 卷第 296 页。

⁴⁸ *Jonathan P. Shattuck 诉 David K. Klotzbach*, 马萨诸塞最高法院, 2001 年 12 月 11 日, 2001 Mass. Super. LEXIS 642。

⁴⁹ *Central Illinois Light Company 诉 Consolidation Coal Company*, 美国伊利诺伊中区地方法院, 皮奥里亚分区, 2002 年 12 月 30 日, 联邦补充案例, 第 2 辑第 235 卷第 916 页。

⁵⁰ 同上, 第 919 页: “内部文件、发票和电子邮件都可被用来满足伊利诺伊[统一商法典]关于欺诈的法规的要求”。不过, 在具体的案件中, 法院发现指称的合同无法满足关于欺诈的法规的要求, 不是因为所指的电子邮件不能有效地记录合同条款, 而是因为没有明示电子邮件的作者和其中所提到的人是被告的雇员。

⁵¹ *Roger Edwards, LLC 诉 Fiddes & Son, Ltd.*, 美国缅因地方法院, 2003 年 2 月 14 日, 联邦补充案例, 第 2 辑第 245 卷第 251 页。

⁵² *Hall 诉 Cognos Limited* (赫尔劳资争议裁判庭, 案件号 1803325/97) (未报告)。

⁵³ *Mehta 诉 J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch), (联合国、英格兰和威尔士高等法院, 大法官分庭), [2006] 2 Lloyd's Rep 244 (联合国、英格兰和威尔士, 劳氏航运法律报告)。

签署“协议范本”之后而非之前生效的。⁵⁴ 在另外一些案件中，法院表示，它们倾向于承认“电子邮件末尾”或“电子邮件主体任何地方”的创建者“姓名或首字母缩写”是签名，不过它们认为，“作为发送和/或接收方的[因特网服务提供商]自动在所传送文件后面插入的电子邮件地址”并不是“打算用作签名”的。⁵⁵ 尽管与美国法院相比，英国法院对关于欺诈的法规的书面要求的解释似乎更为严格，但是，它们一般都会承认所使用的任何类型的电子签名或认证方法，即使不在任何具体法规授权范围之内，只要所述方法具有与亲笔签名一样的作用。⁵⁶

32. 大陆法系国家的法院普遍倾向于采用较为严格的办法，有人争论说是因为这些国家中的大多数而言，“文件”的概念通常都暗指使用某种形式的认证，因此，很难把文件与“签字”分离开来。例如，在通过明确承认电子签名的效力的立法之前，法国的法院都不愿意接受电子鉴定方法等同于亲笔签名。⁵⁷ 但有些决定采取了比较宽松的方式，它们承认以满足法定最后期限为目的而采用以电子方式提出行政诉讼，但至少要在事后以普通邮件加以确认。⁵⁸

33. 与其在确定合同订立中数据电文的归属方面采取具限制性的做法相比，德国法院似乎完全接受在法院诉讼程序中将鉴定方法等同于亲笔签名的做法。有越来越多的人使用法律顾问签字的扫描图像来证明从一台计算机终端通过调制解调器直接发往法院传真机的申诉书计算机传真件的真实性，德国已围绕这个问题展开了讨论。在以前的案件中，上诉法院⁵⁹和联邦法院（*Bundesgericht-*

⁵⁴ *Pretty Pictures Sarl 诉 Quixote Films Ltd.*, 2003年1月30日 ([2003] EWHC 311 (QB)), (联合王国、英格兰和威尔士高等法院, 王座分庭法律报告, [2003] All ER (D) 303 (一月)) (联合王国, 《全英法律报告》(摘要))。

⁵⁵ *Mehta 诉 J. Pereira Fernandes S.A.* (见注[55])。

⁵⁶ *Mehta 诉 J. Pereira Fernandes S.A.* (见注[55]), 第25号: “值得注意的是, 法律委员会对[欧洲联盟电子商务指令(2000/31/EC)]的意见是, 要求签字的法规无需做出重大变动, 因为可以通过一种功能性的方式测试那些要求是否得到了满足, 即询问准签署人的行为是否向合理的人表达了一种认证意图……因此, 正如我已经说过的, 如果发送电子邮件的一方当事人或当事人的代理人依照现有判例法的要求或许可在一封电子邮件中打出了其本人或者其委托人的名字, 那么, 在我看来, 就[关于欺诈的法规]而言, 那足以构成签名”。

⁵⁷ 最高法院裁定对使用电子签名的上诉书不予受理, 因为对创建签名者的身份存有怀疑, 而且该上诉书的电子签名发生在承认电子签名法律效力的法律于2000年3月13日生效之前 (Cour de cassation, Deuxième chambre civile, 30 avril 2003, *Sté Chalets Boisson c/ M. X.*, 载于 www.juriscom.net/jpt/visu.php?ID=239, 2003年9月12日查阅)。

⁵⁸ 法国, Conseil d'État, 28 décembre 2001, N° 235784, *Élections municipales d'Entre-Deux-Monts*, 载于 www.rajf.org/article.php3?id_article=467, 2003年9月12日查阅。

⁵⁹ 例如, 卡尔斯鲁厄高等地方法院 (上诉法院), 案件号 14 U 202/96, 1997年11月14日, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 09/1998, 载于 www.jurpc.de/rechtspr/19980009.htm, 2003年9月12日查阅。

shof)⁶⁰ 均认定, 亲笔签名的扫描图像并不符合现行的签字要求, 而且无法提供对某人的身份证明。可以设想把德国法律所定义的“高级电子签名”与某种鉴别手段相关联。不过, 一般而言, 确定书面信息与通过数据传输发送的无形通信在何种条件下彼此等同, 应该是立法机关的责任, 而不是法院。⁶¹ 鉴于联邦其他高等法院一致接受可使用数据电文附签字扫描图像的电子通信手段提交诉讼程序, 故这一不成文的规定最终被撤销。⁶²

34. 有趣的是, 我们注意到, 即使是哥伦比亚等一些已通过立法表示倾向于使用以公钥基础结构为基础的数字签名的大陆法系国家的法院,⁶³ 也采用了类似宽松的办法, 例如, 它们确认完全以电子通信方式开展的诉讼程序是可以接受的。这类诉讼期间往来的文件是有效的, 即使其中没有数字签名, 因为电子通信所采用的方法允许我们确定当事人的身份。⁶⁴

35. 关于电子签名的判例法仍是少之又少, 而且, 迄今为止的法院判决数量也不多, 并不能提供足以得出明确结论的充分依据。尽管如此, 从对现有判例的简单审查中, 仍可以看出一些趋势。针对电子签名和认证采取的立法办法似乎对法院在此问题的态度产生了影响。有人主张, 立法把重点放在电子“签名”上而没有附带一般性归属规则, 已使得人们过多地关注认证方法确定身份的功能。在一些国家, 这种做法已使得对任何不符合电子“签名”法定定义的认证方法都抱有某

⁶⁰ 德国, 联邦法院, 案件号 XI ZR 367/97, 1998 年 9 月 29 日, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 05/1999, 载于 <http://www.jurpc.de/rechtspr/19990005.htm>, 2003 年 9 月 12 日查阅。

⁶¹ 同上。

⁶² 在向德国联邦法院提起诉讼的一则案件中(见注[62]), 德国联邦最高法院合议庭在其判决中指出, 法院诉讼程序中的形式要求本身并不是目的。它们的目的是确保足以可靠地(“hinreichend zuverlässig”)确定书面内容, 及发送者的身份。合议庭注意到, 为适应电传或传真等此前发生的技术变革, 形式要求的实际应用也在不断变化之中。合议庭认为, 接受使用带有签字扫描图像的数据电文等电子通信手段提交某些诉讼程序与现行判例法的精神是一致的(Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmS-OGB 1/98, 2000 年 4 月 5 日, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 160/2000, 载于 <http://www.jurpc.de/rechtspr/20000160.htm>, 2003 年 9 月 12 日查阅)。

⁶³ 例如, 哥伦比亚已通过了贸易法委员会《电子商务示范法》, 包括其第 7 条中的一般性规定, 但它只是对数字签名做出了合法的真实性推定(*Ley de comercio electrónico*, 第 28 条)。

⁶⁴ 哥伦比亚, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper 诉 Jaime Tapias*, 21 julio 2003, Rad. 73-624-40-89-002-2003-053-00。法院裁定, 尽管电子邮件上没有数字签名, 但是以电子手段展开的诉讼程序是有效的, 因为 (a) 完全可以确定数据电文发送者的身份; (b) 数据电文的发送者同意并承认所发送数据电文的内容; (c) 数据电文被安全地存放在法庭里; 而且 (d) 随时都可以查阅电文(载于 http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf, 2007 年 2 月 2 日查阅)。

种程度的不信任。因此，有一点令人怀疑，即那些在司法和行政申诉中采用宽松办法的法院在处理合同有效性的问题时，能否对签名要求采取同样的宽松尺度。实际上，虽然在签有契约情况下，一方当事人要承担另一方当事人拒不承认协议的风险，但在民事诉讼程序中，一般只有使用电子签名或记录的当事人才对确认其认可记录及记录内容感兴趣。

3. 努力为特殊形式的签名开发出等效的电子签名

(a) 加注*

36. 有人说，1961年10月5日在海牙缔结的《废除要求认证外国公文书的公约》的精神和内容并不妨碍使用现代技术。⁶⁵ 第一次电子公证和电子加注问题国际论坛得出了上述结论，并指出可通过依赖这类技术进一步改善《公约》的适用和运作情况。⁶⁶ 根据作用相等原则阐释《公约》的话，它应该允许主管当局坚持进行电子登记并发布电子加注，以增强进一步的国际法律援助和政府服务。

37. 2006年4月，海牙国际私法会议和美国国家公证人协会启动了电子加注试验方案（e-APP）。根据该方案，海牙会议和国家公证人协会加上所有感兴趣的州，为下列活动开发、推广和协助实施软件模型：（a）电子加注的发布和使用；（b）电子加注登记系统的运作。⁶⁷

(b) 印章

38. 由于在当今社会，印章已不再具有重要意义，故一些管辖区域已经取消了关于印章的要求。经证明（有证人见证）的签字已被取代。⁶⁸ 其他一些管辖区域则制定立法，允许以高级电子签名来满足印章要求。例如，爱尔兰制定了具体条款，规定如果要求或允许把加盖印章的文件交给某人或公共机构，那么，在该个人或公共机构同意的情况下，可以用经适当验证的高级电子签名来替代

* 综合性参考文件的最后定本将进一步展开这部分内容。

⁶⁵ 海牙国际私法会议，“海牙加注、证据和服务公约实际应用问题特别委员会通过的结论和建议：2003年10月28日至11月4日”（海牙，2003年）。

⁶⁶ 2005年5月30日和31日在美国拉斯维加斯举行的第一次电子公证和电子加注问题国际论坛通过的结论，载于 http://www.hcch.net/upload/concl_forum.pdf，2007年2月7日查阅。

⁶⁷ 电子加注试验方案旨在利用现有已被广泛使用的技术。推荐技术的基础是嵌入可扩展标记语言（XML）的PDF文件。更多信息可登录 http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37，见“第二次电子公证和电子加注问题国际论坛”（2006年5月27日至29日在华盛顿哥伦比亚特区举行）项下。

⁶⁸ 例如，联合王国，1989年《物权法（杂项规定）法案》，该法案执行了关于“契约和第三方保存契据”的法律改革委员会报告（法律委员会，第143号，1987年）。

印章。⁶⁹ 加拿大规定，高级电子签名可以满足某些联邦法律关于个人印章的要求，它认为高级电子签名和个人印章是一样的。⁷⁰

39. 许多国家都已实施各种举措，打算在涉及契约的土地交易中使用电子文件和签名。澳大利亚的维多利亚州所采用的模式是准备通过因特网使用安全数字签名技术，并由验证机构签发数字卡片。在联合王国，其模式是准备通过因特网由律师代表其客户签署契约。在一些立法中，法律已承认有可能用“电子印章”来代替“手工印章”，不过，电子印章形式方面的技术细节还有待单独确定。⁷¹

40. 美国《统一不动产电子记录法》⁷²明确规定，有图章、印记或印章的有形或电子图像时，不必再附带电子签名。从本质上讲，我们所需要的只是印章上的信息，而非印章本身。该法案还规定，电子签名可以满足要求有个人或公司图章、印记或印章的一切法规、条例或标准。这些有形标记不适用于纯电子版的文件。尽管如此，该法案要求必须把在其他情况下会包含于图章、印记或印章中的信息附加到电子形式的文件或签名上，或是从逻辑上将二者联系起来。⁷³因此，根据该法案，一些州的法律所要求的公证图章或印记在进行电子公证时并不需要，一些州的法律要求用以核证公司官员行为的公司图章或印记也不需要了。

(c) 公证*

41. 美国有三部重要法规涉及到公证问题：《统一电子交易法》、《全球和国内商务电子签名法》（《电子签名法》）⁷⁴ 和《统一不动产电子记录法》。⁷⁵ 综合而言，

⁶⁹ 爱尔兰，《电子商务法》，第 16 条。不过，如果要求或允许把将要盖章的文件交给一个公共机构或代表公共机构行事的个人，那么，同意使用电子签名的公共机构仍可能会要求这种签名满足特定的信息技术和程序要求。

⁷⁰ 加拿大，《个人信息保护和电子文件法》（2000 年），第二部分，第 39 条。所提及的联邦法律包括《联邦不动产法》和《联邦不动产条例》。

⁷¹ 范例见关于由已获得授权或已经注册的专业人士确认文件的要求，例如《工程和地球科学专业法》（加拿大马尼托巴省），它将“电子印章”定义为由行业协会为任何成员发布的、将以电子方式用于确认计算机可读文件的一种身份形式（见 <http://apegm.mb.ca/keydocs/act/index.html>，2007 年 4 月 4 日查阅）。

⁷² 美国《统一不动产电子记录法》由国家统一州法委员会编制，载于 http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm，2007 年 2 月 7 日查阅。亚利桑那州、特拉华州、哥伦比亚特区、堪萨斯州、北卡罗来纳州、得克萨斯州、弗吉尼亚州和威斯康星州都已通过了这部法案（见 http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-urpera.asp，2007 年 2 月 7 日查阅）。

* 综合性参考文件的最后定本会进一步展开这部分内容。

⁷³ 类似于美国《统一电子交易法》所包含的标准。

⁷⁴ 已被编撰为《美国法典》第 15 标题，第 96 章，第 7001-7031 节。

⁷⁵ 见注[74]。

这三部法规规定，在文件需要公证、确认、核实、见证或宣誓时，该文件或签名上附有经授权实施上述行为者的电子签名或与该文件存在逻辑关联的签名以及其他适用法律所要求包含的所有其他信息的，则该文件的法律要求或与其有关的签名法律要求即得到了满足。

42. 在奥地利，cyberDOC 电子文件档案库是奥地利民法公证人协会和西门子公司共同成立的一个独立公司，专门为公证人提供包括具有认证功能的电子档案。⁷⁶ 根据法律规定，奥地利的公证人必须把 2000 年 1 月 1 日以后完成的所有公证契约都记录并存储在该档案库中。

(d) 宣誓

43. 有人认为，传统的见证程序，如宣誓，并不完全适用于以电子方式签署的文件，因为我们并不能确保屏幕上的图像实际上就是将要进行电子签名的文件。见证人和签署人所能看到的，只是人类能够看到的、能够所谓存入内存当中的计算机屏幕显示。见证人看签署人敲击键盘时，并不确切知道实际上正在发生什么事。因此，只有按照可信的评价标准，通过可信途径对计算机进行评估之后，才可能确保计算机屏幕所显示的内容与计算机内存所保存的内容一致，才能确保签署人在键盘上输入的内容与其意图一致。⁷⁷

44. 然而，安全电子签名可以通过确定声称签署契约的人的身份，履行类似的宣誓见证的功能。在没有人见证的情况下使用安全电子签名，可能能够核实签名的真实性，签名所属个人的身份，文件的完整性，甚至是签署的日期和时间。从这个意义上讲，安全电子签名甚至比普通的亲笔签名更有优势。另外，切实进行见证以证明安全数字签名几乎没有什么好处，除非签名的自愿性受到了质疑。⁷⁸

45. 现有立法还没有发展到完全以电子签名取代宣誓要求的地步，只是允许见证人使用电子签名。新西兰《电子交易法》规定，见证人的电子签名满足法律对需要被见证的签名或印章的要求。并未对制作电子签名时使用的技术作明确规定，

⁷⁶ 见 Österreichische Notariatskammer (奥地利民法公证人协会)，载于 <http://www.notar.at/de/portal/einrichtungen/cyberdocgmbhcok/>，2007 年 2 月 7 日查阅。

⁷⁷ 这个即文献中所说的“所见即所得”(WYSIWYS)问题。见 V. Liu 等人，“视觉加封和数字签署的文件”，计算机协会，《计算机协会国际会议录》，第 56 卷，《第二十七次澳大拉西亚计算机科学会议记录》，第 26 卷，(新西兰达尼丁，2004 年)，第 287 页(另见关于可信显示控制器的讨论)。

⁷⁸ 见新加坡信息通信发展局和总检察署的联合讨论，《信息通信发展局——总检察署电子交易法第二阶段联合审查：电子交易法第 4 条下的除外情况》，咨询文件 LRRD No. 2/2004 (新加坡，2004 年)，第 5 和第 8 部分，载于 www.agc.gov.sg，在“出版物”项下。

只要符合下列条件即可：“足以确定见证人的身份并足以显示签名或印章已被见证”；而且“考虑到要求见证人签名的目的和环境，该技术具有适当可靠性。”⁷⁹

46. 加拿大《个人信息保护和电子文件法》规定，如果每个签署人和见证人都以其安全的电子签名签署电子文件，则联邦法律对需要见证的电子文件签名的要求就得到了满足。⁸⁰ 某些联邦法律要求声明人宣布或证明其所提供的信息真实、准确或完整，如果声明人使用本人的安全电子签名签署声明，则其可以采用电子形式做出上述声明。⁸¹ 联邦法律要求在有人监誓的情况下做出声明的，如果声明人使用其安全的电子签名在声明上签字，而且声明的见证人和声明的监誓人也使用其本人的安全电子签名在声明上签字，则该声明也可以采用电子形式做出。⁸² 作为一种替代办法，为了进一步保证电子签名的有效性，有人建议由律师或公证人等接受委托的专业人员进行电子签名或由他们在场的情况下进行电子签名。⁸³

⁷⁹ 新西兰，《电子交易法》（见注[9]），第 23 条，载于 http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes，2007 年 4 月 4 日查阅。

⁸⁰ 加拿大，《个人信息保护和电子文件法》（见注[72]），第二部分第 46 条。

⁸¹ 同上，第 45 条。

⁸² 同上，第 44 条。

⁸³ 撰写转让契据的律师必须从公认验证机构那里获得电子签名和认证。买方和卖方可能需要以书面凭据授权律师签署文件。见“电子业权转让：在英格兰和威尔士实施电子业权转让的战略”（联合王国，土地注册处，2005 年），载于 http://www.landregistry.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc，2007 年 4 月 7 日查阅。该项目预计将于 2006 至 2009 年间分期实施。