增进对电子商务的信心：国际使用电子认证和签名方法的法律问题

联合国

联合国国际贸易法委员会

增进对电子商务的信心：国际使用电子认证和签名方法的法律问题

联合国
2009 年，维也纳

联合国出版物
出售品编号：C.09.V.4
ISBN 978-92-1-730178-0

前言

联合国国际贸易法委员会（贸易法委员会）第四工作组（电子商务）在2004年完成了其有关《国际合同使用电子通信公约》的工作以后，请秘书处继续跟踪与电子商务有关的各种问题，包括与电子签名的跨国界承认有关的问题，并发表其研究结果，以便就今后有否可能在这些领域开展工作向委员会提出建议（见A/CN.9/571，第12段）。

2005年，贸易法委员会注意到其他组织在与电子商务有关的各个领域内开展的工作，请秘书处编写一份更为详细的研究报告，其中应列入就综合参考文件的形式和性质提出的各种建议，综合参考文件讨论的是确定有利于电子商务的法律框架所需各个要件，因此贸易法委员会今后似宜考虑编写一份综合参考文件，以便向世界各国的立法机关和决策机关提供帮助。[1]

2006年，贸易法委员会审议了其秘书处依照该请求编写的一份说明(A/CN.9/604)。该说明将以下方面列作综合参考文件可能包括的内容：(*a*)对电子签名的认证和跨国界承认；(*b*)信息服务提供者的赔偿责任和行为准则；(*c*)电子发票和与电子商务供应链有关的法律问题；(*d*)通过电子通信进行的有形货物权利和其他权利的转让；(*e*)电子商务中的不公平竞争和欺骗性贸易做法；及(*f*)电子商务中的隐私和数据保护。该说明还列举了其他问题，也可采取摘要的形式将这些问题列入该文件：(*a*)知识产权保护；(*b*)未经请求的电子通信（垃圾邮件）；及(*c*)网络犯罪。在该届会议上，有与会者支持这样一种观点，即认为贸易法委员会拟定一份综合参考文件，论及秘书处列举的各项专题，将会给各国，尤其是给发展中国家立法机关和决策机关的工作提供极大的便利。另据认为，这份文件还将有助于贸易法委员会确定，今后究竟可以在哪些方面开展协调统一的工作。贸易法委员会请其秘书处编拟综合参考文件的样本部分，专门论及与对电子签名的认证和跨国界承认有关的问题，供委员会2007年第四十届会议审查。[2]

---

[1]《大会正式记录，第六十届会议，补编第*17*号》(A/60/17)，第214段。

[2]同上，《第六十一届会议，补编第*17*号》(A/61/17)，第216段。

秘书处根据上述请求编写的样章（A/CN.9/630 和 Add.1-5）已提交贸易法委员会第四十届会议审议。贸易法委员会赞扬秘书处编写该样章，并请秘书处将样章作为独立出版物发表。[3]

本出版物分析了在国际交易中使用电子签名与认证方法产生的主要法律问题。第一部分概要介绍了电子签名与认证所用方法以及各法域在法律上的对待做法。第二部分审议了在国际交易中对电子签名与认证方法的使用情况，列举了同这些方法的跨国界承认有关的主要法律问题。据指出，从国际角度来看，电子签名与认证方法的跨国界使用更有可能造成法律上的问题，因为这种使用需要第三方参与签名或认证过程。例如，由可信第三方认证服务提供者签发证书提供支持的电子签名与认证方法即为如此，尤其是根据公钥基础设施提供的数字签名更是如此。为此原因，本出版物第二部分特别重视国际上使用公钥基础设施下的数字签名问题。不应将重视该问题误解为赞同或认可这种或任何其他某种类型的认证方法或技术。

[3] 同上，《第六十二届会议，补编第 *17* 号》(A/62/17)，第 195 段。

目录

导言

1. 信息和计算机技术开发了以电子形式将信息与特定的人或实体联结在一起的各种手段，目的是确保这类信息的完整性，或者使人们得以表明，其有资格或得到授权，利用某种信息服务或访问储存的信息。这些功能有时通称电子“认证”或电子“签名”方法。但有时又对电子“认证”和电子“签名”加以区分。术语的使用不仅前后不一，而且在某种程度上令人误导。在纸质环境中，“认证”和“签名”这两个词及其相关行动在不同的法律体系中有着不尽相同的涵义，其实际功能与所谓电子“认证”和“签名”方法的用途和功能未必一致。此外，“认证”一词有时泛用于对信息的来源和完整性所作的任何保证，但某些法律体系可能会对这些要素加以区分。因此，为确定本文件的范围，有必要概要介绍在术语和法律理解上的区别。

2. 根据普通法对民事证据的规定，有证据表明文件或记录“为其提出者所主张的”，[1] 记录或文件即被视为“真实的”。“文件”这一概念的范围很广，通常包括“记录任何类型的信息的载体”[2]。这将包括墓碑和房屋的照片[3]、账簿[4]、图画和计划[5]等。确定文件作为证据的适切程度的方法是，将文件与人、地点或物联结在一起，一些普通法的法域将这一进程称之为“认证”[6]。签署一份文件是“认证”的一种常见——

---

[1] 美利坚合众国，《联邦证据规则》，第 901 条 (*a*) 项：“证据足以支持所涉事项为其提出者所主张的这一结论的，即可满足作为可采性先决条件的认证或身份鉴别要求。”

[2] 大不列颠及北爱尔兰联合王国，《1995 年民事证据法》，第 38 章第 13 条。

[3] *Lyell v. Kennedy* (No. 3) (1884) 27 Ch.D. 1（联合王国，大法官法庭）。

[4] *Hayes v. Brown* [1920] 1 K.B. 250（联合王国，《判例汇编》，王座法庭）。

[5] *J. H. Tucker & Co., Ltd. v. Board of Trade* [1955] 2 All ER 522（联合王国，《全英判例汇编》。

[6] *Farm Credit Bank of St. Paul v. William G. Huether*，1990 年 4 月 12 日 (454 N.W.2d 710, 713)（美国，北达科他最高法院，西北报道员）。

但不是唯一的——手段，并且视具体情况，可将“签署”和“认证”用作同义词。[7]

3. “签名”又是“一方当事人所使用的以构成其签名为目的的任何名称或符号”[8]。法规要求特定文件由特定人签名的目的是确认文件的真实性[9]。签名的范式为，签名人姓名由签名人亲手写在纸质文件上（“手写的”或“印刷体书写的”签名）[10]。但手写签名并不是唯一可以想象的签名类型。由于法院将签名视为“只是一种标志”，除非有关法规要求签名为手迹，否则，“有需要签署文件的当事人的印刷字体的姓名即可”，或签名“可以是刻有签名人普通签名复制品的图章在文件上盖上的印记”，但前提是，对于这些情况，举出证据证明，“图章上印有的姓名是由签名人附上的”，或此种签名“得到承认或被签名人认定得到他的授权，目的是确定特定文书的归属”。[11]

4. 在英国的《防止欺诈法》[12]和其他国家的类似法律[13]中可以找到普通法法域将法定签名要求作为某些行为具备有效性先决条件的典型规定。随着时间的推移，法院倾向于对《防止欺诈法》作宽泛的解释，因为法院承认，其严格的格式要求是在特定背景下提出的[14]，严格遵守

---

[7] 具体到《美国统一商法典》经修订的第 9 条，例如，“认证”被界定为“(A) 签名；或 (B) 执行或以其他方式采纳一种符号，或对记录全部或部分加密，或进行类似的处理，当下的意图是，对该人进行认证，以确定该人的身份，采纳或接受一记录。”

[8] *Alfred E. Weber v. Dante De Cecco*，1948 年 10 月 14 日 (1 N.J. Super. 353, 358)（美国，新泽西高等法院判例汇编）。

[9] *Lobb v. Stanley* (1844), 5 QB 574, 114 E.R. 1366（联合王国，《判例汇编》，王座法庭）。

[10] Lord Denning in *Goodman v. Eban* [1954] QBD 550 at 56：“在现代英语用法中，要求某人签署一份文件即意味着他必须亲手在文件上写上自己的姓名。”（联合王国，王座法庭）。

[11] *R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324（联合王国，维多利亚判例汇编）。

[12] 英国于 1677 年最早通过了《防止欺诈法》，旨在“防止许多欺诈做法，而伪证罪和唆使作伪证罪通常就是设法维持这些做法。”英国在 20 世纪期间废除了其中大多数条文。

[13] 例如，《美国统一商法典》第 2-201 款第 1 项对《防止欺诈法》作了如下表述：“除了本款另有规定外，不得以诉讼或抗辩的形式强制执行价格为 500 美元或高于 500 美元的货物销售合同，除非有某种书面形式足以指明，销售合同由双方当事人订立，并由寻求对其加以强制执行的当事人签署，或由得到其授权的代理人或经纪人签署。”

[14] “在通过《防止欺诈法》的时期，立法机关有些倾向于规定，应当根据固定的规则裁定案件，而不是交由陪审团逐案认真研究证据的效力。毫无疑问，这在一定程度上是由于，在那一时期，原告和被告并非是有作证能力的证人。”（J. Roxborough 在 *Leeman v. Stocks* [1951] 1 Ch 941 at 947-8（联合王国，《判例汇编》，大法官法庭）中的论述，援引于对 J. Cave 在 *Evans v. Hoare* [1892] 1 QB 593 at 597（联合王国，《判例汇编》，王座法庭）中的观点的赞同）。

其规则可能会毫无必要地剥夺合同的法律效力[15]。因此，在最近150年内，奉行普通法的法域对“签名”这一概念已从最初强调格式转为重视功能[16]。英国的法院不时考虑在这一问题上作出一些变动，其中包括使用交叉符号[17]、首字母[18]等简单的修改，使用假名[19]和表明身份的短语[20]，用印刷体书写姓名[21]、由第三方当事人签名[22]和使用图章[23]等。在所有这些情形中，法院都能通过与印刷体签名进行类比而解决签名是否有效的问题。因此可以说，在存在某种僵硬的一般格式要求的背景下，奉行普通法法域的法院通常对“认证”和“签名”的概念有着宽泛的理解，重点是了解当事人的意图，而不是其作为的形式。

5. 奉行大陆法的法域对“认证”和“签名”的做法与普通法所采取的做法不尽相同。奉行大陆法的多数法域对于私法事项遵行合同安排格式自由的规则，但在这条规则上或明[24]或暗地[25]存在许多例外

---

[15] 按照康希尔的宾厄姆勋爵的解释，“很快有情况显示，如果17世纪的解决办法消除了一种损害，则也能够引起另一种损害：一方当事人拟定被视为具有约束力的口头协议，并照此行事的，将会发现，等到强制执行时，其商业期望将会落空，而另一方当事人成功地将缺少书面备忘录或协议说明作为其依据。”（*Actionstrength Limited v. International Glass Engineering*，2003年4月3日，[2003] UKHL 17（联合王国，上议院））。

[16] Chris Reed，“什么是签名？”，《信息、法律和技术杂志》，第3卷，2000年，并参考其中的案例法，可查阅http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/（2008年6月5日查阅）。

[17] *Baker v. Dening* (1838) 8 A. & E. 94（联合王国，Adolphus和Ellis的《王座法庭判例汇编》）。

[18] *Hill v. Hill* [1947] Ch 231（联合王国，大法官法庭）。

[19] *Redding, in re* (1850) 14 Jur. 1052, 2 Rob.Ecc. 339（联合王国，法学家报告和Robertson的教会报告）。

[20] *Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689（联合王国，《全英判例汇编》。

[21] *Brydges v. Dicks* (1891) 7 T.L.R. 215（援引自Brennan v. Kinjella Pty Ltd.，新南威尔士最高法院，1993年6月24日，1993 NSW LEXIS 7543, 10）。*Newborne v. Sensolid*d (Great Britain), Ltd. [1954] 1 QB 45（联合王国，《判例汇编》，王座法庭）中也对打字书写作了考虑。

[22] *France v. Dutton*，1891年4月24日 [1891] 2 QB 208（联合王国，《判例汇编》，王座法庭）。

[23] *Goodman v. J. Eban Ltd.*, [1954] 1 QB 550，援引自 *Lazarus Estates, Ltd. v. Beasley*，上诉法院，1956年1月24日 ([1956] 1 QB 702); *London County Council v. Vitamins, Ltd.*, *London County Council v. Agricultural Food Products, Ltd.*，上诉法院，1955年3月31日 [1955] 2 QB 218（联合王国，《判例汇编》，王座法庭）。

[24] 在《瑞士债务法》第11条第1款中得到承认。同样，《德国民法典》第215条规定，协议只有在未遵守法律指定的或双方当事人商定的格式时，方可归于无效。除了这类专门情形外，普遍的理解是，私法合同不必遵守专门的格式要求。法律明确指定特定格式的，将对该要求做严格的解释。

[25] 例如，在法国，从民法有关合同订立的基本规则中，可以作出格式自由的推定。根据《法国民法典》第1108条，允诺人的同意、其法定资格、某种对象、合法诉因等为合同有效的必要条件；根据第1134条，一旦满足这些条件，合同即为“双方当事人之间的法律”。《西班牙民法典》第1258和1278条也有这一规则。意大利也遵守了同样的规则，但不够明确（见《意大利民法典》，第1326和1350条）。

情况，究竟有多少例外须视有关法域而定。这就意味着，作为一条通则，“书面”或“已签名”并非合同有效并且可加以执行的必然条件。但遵行大陆法的有些法域通常要求，除商事事项外[26]，必须以书面的形式证明合同的内容。与奉行普通法的法域不同，奉行大陆法的国家对证据规则的解释通常十分严格。一般来说，民事证据规则把证明民事和商事合同内容的证据分成几等。排位最高的是由公共机关签发的文件，其次是得到认证的私人文件。根据将证据分成几等的这种做法，“文件”和“签名”的概念尽管表面上有所不同，但实际上几乎无法区分[27]。不过还有一些奉行大陆法的法域认为，“文件”的概念与“签名”的有无有着正面的联系[28]。这并不意味着，未签署的文件必然被剥夺了作为证据的任何价值，不过对这种文件不得想当然地作出任何推定，并且通常应将其视为“证据的开始”[29]。奉行大陆法的多数法域对“认证”这一概念的理解十分狭窄，认为指的是文件的真实性得到主管公共机关或公证机关的核实和认证。在民事程序中，通常改用文件“原始性”的提法。

6. 根据普通法的做法，在奉行大陆法的国家，签名的范式为手写签名。关于签名本身，有些法域尽管对证据采取了基本上重视格式的做法，但仍然倾向于承认各种等同签名，其中包括对签名的机械性复制[30]。还有一些法域虽然在商事交易上承认机械性签名[31]，不过在计算机技术问世以前，仍然要求以手写签名作为其他类型的合同的

---

[26]《法国民法典》第 1341 条规定，合同超过一定价值的，必须以书面形式作为合同的证据。但《商法典》第 109 条采纳各类证据，而没有划分特定的等级。法国最高法院 1892 年据此承认商事事项证据自由一般原则（Cass. civ. 1892 年 5 月 17 日，DP 1892.1.604；援引自 Luc Grynbaum, *Preuve, Répertoire de droit commercial Dalloz*，2002 年 6 月，第 6 和 11 节）。

[27]因此，例如根据德国法律，签名不是“文件”概念的一项基本要素 (Urkunde)（Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozess-ordnung*（慕尼黑，Beck，1992 年），第 415 条，第 6 号）。但《德国民事诉讼法》第 415、416 和 419 条确定的文件证据等级将签名与文件明确联在一起。事实上，有关私人证件 (*Privaturkunden*) 证据价值的第 416 条规定，私人文件凡由著作者签名或属于公证签名的，即构成文件所含信息的“充分证据”。由于对未附签名的文件未作任何规定，这类文件看来属于有缺陷的文件（即错乱的、受损的文件），其证据价值由法院“自由确定”（《德国民事诉讼法》，第 419 条）。

[28] 因此，在法国，签名是私人文件的一项“基本要素”(*actes sous seing privé*)（见 *Recueil Dalloz, Preuve*，第 638 号）。

[29] 法国的情况即为如此，例如见 *Recueil Dalloz, Preuve*，第 657-658 号。

[30] 有人在评论《德国民事诉讼法》时指出，要求手写签名即意味着排除一切形式的机械签名，而这种结果与惯常做法和技术进步是背道而驰的（见 Gerhard Lüke and Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung*（慕尼黑，Beck，1992 年），第 416 条，第 5 号）。

[31] 例如，法国（见 *Recueil Dalloz, Preuve*，第 662 号）。

证据[32]。因此可以说，在商业合同订立格式自由的一般背景下，奉行大陆法的国家倾向于对评估私人文件证据价值实施严格的标准，对无法根据签名立即辨认其真实性的文件持排斥态度。

7. 上述讨论显示，不仅对签名和认证的概念无法有统一的理解，而且其在各个法律体系中的职能也各不相同。尽管有这些区别，但仍然能够找到一些基本的共同要素。“认证”和“真实性”这两个概念在法律上通常被理解为是指文件或记录的真实性，即，文件系按照其所记录的格式，原封不动地对所载信息提供支持的“原件”。而在纸质环境中，签名又主要行使三个职能：通过签名得以确定签名人的身份（确定身份的职能）；签名提供了该人亲自参与签名行为的确定性（证据职能）；及签名确定了签名人与文件内容的联系（归属职能）。据说，签名还可行使其他各种职能，这类职能具体取决于所签署的文件的性质。举例说，签名可证实一方当事人受已签名合同内容约束的意图；一人赞同文本著作来源的意图（从而表明认识到签名行为可能会产生各种法律后果）；一人赞同他人撰写的文件内容的意图；以及一人在某一地点的事实与时间。[33, 34]

8. 但是应当指出的是，即便根据签名的有无通常就可对其真实性作出推定，但单凭签名仍然无法“认证”文件。根据具体情况的不同，这两个要素甚至有可能是分开的。签名可保留其“真实性”，即便对附签的文件随后又作了改动。同样，即使文件中所含的签名是伪造的，文件仍有可能是“真实的”。此外，对交易进行干预的职权和所涉人士的实际身份尽管是确保文件或签名真实性的重要成分，但既无法仅凭签名而充分展示，也不足以确保文件或签名的真实性。

9. 从这一意见可以引出目前所讨论的问题的另一方面。无论具体的法律传统如何，除为数极少的例外情况外，签名均无法独立存在。其法律效力将取决于签名与签名归属人之间的联系。在实务中，可采取各种步骤，核实签名人的身份。各方当事人同一时间在同一地点的，仅凭其面孔即可认出对方；通过电话商谈的，则必须能够分辨对方的

---

[32] 例如在法国，不得使用印章或指纹以十字形记号或其他符号代替签名（见 *Recueil Dalloz, Preuve*，第 665 号）。

[33]《贸易法委员会电子签名示范法及其颁布指南 *2001* 年》（联合国出版物，出售品编号：E.02.V.8），第二部分，第 29 段（可查阅 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html，2008 年 6 月 6 日查阅）。

[34] 该分析已经构成先前《贸易法委员会电子商务示范法及其颁布指南（*1996* 年）以及 *1998* 年通过的附加第 *5* 条之二》第 *7* 条有关功能等同标准的基础（联合国出版物，出售品编号：E.99.V.4，可查阅 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html（2008 年 6 月 6 日查阅）。

声音。这类事情中有很多是自然发生的，并不依赖于具体的法律规则。但各方当事人使用信函往来方式商谈的，或按照合同约定的连锁关系发送已签名文件的，则可能就没有多少手段能够确定某一文件上的签名确实是同签名人姓名看来有关的人，也无法确定是否只有得到适当授权的人才是应当使某人受到约束的签名制作人。

10. 尽管手写签名是熟悉的“认证”形式，很适合在已知当事人之间传递交易文件，但对于许多商业和行政文件，签名不很安全。文件依赖方通常既不了解获得签名授权的人的姓名，也没有可资对照的签名样本。[35] 外国在国际贸易交易中所依赖的许多文件尤其如此。即便有可资对照的授权签名样本，但只有专家才能够辨别精确逼真的伪造签名。有大量文件需要处理的，除最为重要的交易外，甚至有时都不需要对签名进行对照。信任是国际商事关系的基本基石之一。

11. 多数法律体系均设有目的在于提高手写签名可靠度的特别程序或要求。为了确保某些文件的法律效力，有些程序可能为强制性程序。这些程序也可以为任择性程序，当事人在希望防止就某些文件的真实性发生可能的争执时可援用这些程序。下文列入了这方面的典型范例，这通常要求签名人亲自到场办正理公证：

(*a*) 公证。 在某些情况下，由于同特别仪式相关的强化信任，签名行为在形式上具有特殊的意义。公证等即为如此，公证系公证机关为确定法律文件上签名的真实性而作出的认证，这通常要求签名人亲自到场办理公证；

(*b*) 见证。 见证系目睹某人签署法律文件，然后签上本人姓名以作为证明的行为。见证的目的是保全签名的证据。通过见证，证人申明并确认，由其目睹在文件上签名的人事实上已经签名。见证并不延及于证明文件的准确性或真实性。可以要求证人就签名的情形作证；[36]

---

[35] 法律在某些方面承认，手写签名具有内在的不安全性，对法律行为的效力坚持严格的格式要求不切实际，法律并且承认，在某些情形下，即便伪造签名都无法剥夺文件的法律效力。因此，例如，1930 年 6 月 7 日，在日内瓦订立了载有统一汇票和本票法的公约，该公约所附《统一汇票和本票法》第 7 条规定，“汇票附有以下签名的，在汇票上签名的其他人所承担的义务仍然有效，这些签名为：无法受汇票约束的人的签名、或伪造签名、或虚拟之人的签名、或出于任何其他理由而无法使汇票签名人或在汇票上签名的人所代表的人受约束的签名”（国联，《条约汇编》，第 143 卷，第 3313 号）。

[36] Adrian McCullagh, Peter Little and William Caelli, “Electronic signatures: understand the past to develop the future”，《新南威尔士大学学报》，第 21 卷，第 2 号 (1998)；见有关作证概念的第三章 D 节。

(*c*) 盖章确认。 使用盖章补充或替代签名的做法很普通，特别是在世界的某些地区[37]。举例说，作了签名或盖章即提供了证明签名人身份的证据；签名人同意受协议的约束，并且是自愿受约束的；而且文件已然定稿，完备齐全；或在签名以后内容未有改动[38]。这种做法还可提醒签名人保持警惕，并表示有意以具有法律约束力的方式行事。

12. 除了这些特殊情形外，几百年来在国内和国际商事交易中一直使用了手写签名，但没有任何特别设计的立法或作业框架。已签名文件的收件人或持有人根据签名人所享有的信任程度逐案评价签名的可信度。事实上，即便确有“书面形式”的话，绝大多数国际书面合同也并不一定附带任何特殊的形式程序或认证程序。

13. 涉及公共机关的，对已签名文件的跨国界使用就更为复杂了，因为外国的接收机关通常要求有证明签名人身份和权威的某种证据。满足这些要求的传统做法为所谓的“合法化认证”程序，即把签名载于国内文件中，由外交机构认证，供在国外使用。相反，意图使用文件国家的领事或外交代表也可对原籍国外国公共机关的签名进行认证。领事和外交机关通常只对签发国某些高级权威人士的签名进行认证，因此，文件最初由低级官员签发的，或需要由签发国公证机关事先对签名进行公证的，则可能需要分若干层级对签名进行确认。合法化认证在多数情况下系繁锁、费时并费钱的程序。因此，1961 年 10 月 5 日在海牙经过谈判形成了《废除要求认证外国公文的公约》[39]，目的是使用标准简化形式（“加注”）取代现行要求，这种简化形式用于对《公约》缔约国的某些公文进行认证[40]。只有公文来源国指定的主管机关方可签发加注。加注所认证的是签名的真实性、文件签名人的行为能力、并在适当时认证文件上的印章或图章的身份，但这种认证不涉及有关文件本身的内容。

---

[37] 中国和日本等东亚一些国家使用了印章。

[38] Mark Sneddon, “Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book”，《新南威尔士大学学报》，第 21 卷，第 2 号 (1998)；见第二部分第二章“书面和签名要求的政策目标”。

[39] 联合国，《条约汇编》，第 527 卷，第 7625 号。

[40] 这些文件包括来自一国法院或法庭相关权威人士或官员的文件（包括由行政、宪政或宗教事务法院或法庭、公共检察官、书记官或送达传票官签发的文件）；行政文件；公证行为；放在个人以私人身份签署的文件内的官方证书。

14. 正如上文所述，在许多法律体系中，放在文件内载列或以书面形式体现并不总是商事合同具有效力的必要条件。即便有书面形式的，合同对当事人具有约束力并不一定需要有签名。当然，法律要求合同为书面形式的或有签名的，未满足这些要求将会使合同归于无效。比合同效力格式要求更为重要的或许是在证据方面的格式要求。难以提出口头协议的证据是以书面文件反映或通过信函往来记录商事合同的主要原因之一，即便口头协议如能提出证据即为有效。当事人使用附有签名的书面形式记录其义务的，也就无法否认其义务的内容。文件证据严格规则的目的通常在于使符合这些规则的文件具有高度的可依赖性，普遍认为，后者提高了文件的法律确定性。但与此同时，证据要求越全面，当事人就越是有机会援用形式上的瑕疵，以合同在商业上处于不利地位等为由，否认其不再有意履行的义务具有效力或能够得到执行。因此，必须平衡兼顾在促进安全交换电子通信方面的利益和有使恶意商人得以轻而易举地放弃其自由承担的法律义务的风险。为求得这种平衡，拟定国际公认并且可以在各国执行的规则和标准，是决策机关在电子商务领域面临的一项主要任务。本文件的目的是，帮助立法机关和决策机关确定国际使用电子认证和签名方法所涉及的主要法律问题，考虑有可能解决这些问题的方法。

第一部分

电子签名和认证方法

目录

一． 定义与电子签名和认证方法

A. 关于术语的一般性评论

15. “电子认证”和“电子签名”这两个用语被用来指市场上现有的或仍在拟定的各种方法，这些方法的目的是在电子环境下重复被确定为手写签名或其他传统认证方法的特点的某些或全部职能。

16. 历年来开发了一些不同的电子签名方法。每一种方法的目的都是为了满足不同的需要，提供不同层次的安全，所含的技术要求也不同。电子认证和签名方法可分为三类：以用户或接收者知情为依据的（例如，密码、个人识别号码），以用户外形特征为依据的（例如，生物鉴别技术）和以用户对物体的占有为依据的（例如，磁卡上储存的代码或其他信息）。[41] 第四类可包括各种类型的认证和签名方法，这些类型的方法虽然无法归入以上各类，但仍可用来指明电子通信的发件人（例如手写签名的复制本，或电文末尾处的打字签名）。目前使用的技术包括公钥基础设施内的数字签名、生物鉴别做法、个人识别号码、由用户界定或分配的密码、经过扫描的手写签名、以数字笔为手段的签名、可点击的“同意”或“接受”方框[42]。以兼用不同技术为依据的混合解决办法正日渐通行，例如兼用密码和传输层安全 / 安全套接层，这种技术混合使用了公钥加密办法和对称钥匙加密办法。下文对目前使用的主要技术的特征作了介绍（见第 25-66 段）。

17. 正如通常的情况那样，技术的开发远远早于该领域法律的问世。由此在法律与技术之间形成的差距，不仅造成专家拥有的知识程度有别，而且还导致用语的使用前后不一。已开始使用各国法律下相沿成习并具有特殊含义的表述方法来介绍电子做法，而电子做法与法律上使用的相应概念在功能和特点上并不一定相同。如上文所述（见第 7-10 段），“认证”、“真实性”、“签名”和“身份”等概念尽

[41] 见 1998 年 1 月 19 日至 30 日在维也纳举行的电子商务工作组第三十二届会议的工作报告（A/CN.9/446，第 91 段及其后各段）。

[42]《贸易法委员会电子签名示范法……》，第二部分，第 33 段。

管在某些背景下密切相关，但不尽相同，也无法互换。信息技术业的做法基本围绕对网络安全的关切展开，但这些做法所适用的类型并不一定与法律著述相同。

18. 在某些情况下，“电子认证”的表述方法被用来指称视使用的背景而可能涉及各种要素的技术，其中包括查明个人的身份、确认一人的职权（通常代表另一个人或实体行事）或特权（例如，作为一机构的成员或订购一项服务）或确保信息的完整性。在某些情况下，仅以查明身份为重点，[43] 但有时也延伸至确认职权 [44]，或兼用其中任何或所有要素。[45]

19. 《贸易法委员会电子商务示范法》[46] 和《贸易法委员会电子签名示范法》[47] 均未使用“电子认证”这一用语，其原因是，在各个法律体系中，“认证”的含义不同，有可能混同于特别的程序或格式要求。《电子商务示范法》转而使用了“原始格式”的概念，规定了“真实的”电子信息功能等同的标准。根据《示范法》第 8 条，如法律要求信息须以其原始形式展现或留存，倘若情况如下，则一项数据电文即满足了该项要求：

(*a*) 有办法“可靠地保证自信息首次以其最终形式生成，作为一项数据电文或充当其他用途之时起，该信息保持了完整性；”和

---

[43] 例如，美国商务部技术管理司将电子认证界定为“对以电子方式提供给信息系统的用户身份的信任确定过程”（美国商务部，*Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-63, version 1.0.2（马里兰州盖瑟斯堡，2006 年 4 月），可查阅 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf（2008 年 6 月 5 日查阅））。

[44] 例如，澳大利亚政府拟定了电子认证框架，将电子认证界定为“确定在线交易或电话交易时对陈述的真实性或有效性所持信任度的过程。电子认证通过在一定程度上保证有关当事人的交易为合法交易，协助建立对在线交易的信任。这些陈述可包括：身份细节；专业资格；或下放进行交易的权力”（澳大利亚财政和行政管理部，*Australian Government e-Authentication Framework: An Overview*（澳大利亚联邦，2005 年），可查阅 http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication（2008 年 6 月 5 日查阅））。

[45] 例如，加拿大政府编拟的电子认证原则将认证界定为“证明电子通信参与方的属性或通信完整性的过程。”属性又被界定为“有关参与方或其他被认证实体身份特权或权利的信息”（加拿大工业部，*Principles for Electronic Authentication: a Canadian Framework*（渥太华，2004 年 5 月），可查阅 http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html（2008 年 6 月 5 日查阅））。

[46]《贸易法委员会电子商务示范法……》。

[47]《贸易法委员会电子签名示范法……》。

(*b*) 如要求将信息展现，该信息“能够被显示给观看信息的人。”

20. 根据多数法律体系对作为一种“认证”手段的签名（或替代使用的印章）和有关文件或记录质量“真实性”所作的区分，这两份示范法使用“签名”的概念对“原始性”的概念作了补充。《贸易法委员会电子签名示范法》第 2 条 (*a*) 项将电子签名界定为：以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于“鉴别与数据电文相关的签名人”和“表明签名人认可数据电文所含信息”。

21. 贸易法委员会的各种文本故意对“电子签名”定义的范围作了宽泛的规定，是为了涵盖所有现存或未来的“电子签名”方法。只要所使用的方法“根据各种情况，包括根据任何有关协议，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”，[48] 则应被视为满足了有关签名的法律要求。贸易法委员会有关电子商务的文本和大量其他法律文本均以技术中立原则为依据，其目的是顾及各种形式的电子签名。因此，贸易法委员会有关电子签名的定义将涵盖所有各种“电子签名”做法，其中包括与公钥基础设施办法（普通形式的“数字签名”（见第 25-53 段））有关的加密签名保证做法等高级别安全技术和未加密代码或密码等较低级别的安全技术。在电子邮件电文末尾处简单地打上作者的姓名是最为普通的电子“签名”方式，凡有理由使用这种低层次安全方法的，均可用其行使正确查明电文作者身份的职能。

22. 除此之外，贸易法委员会示范法并不述及与管制访问或确认身份有关的问题。这也符合以下事实，即在纸质环境中，签名或许是表示身份的标志，但一定能确定身份的归属。但《贸易法委员会电子商务示范法》述及数据电文收件人有权推定数据电文实际上来自其预期发端人。事实上，《示范法》第 13 条规定，就发端人和收件人之间而言，数据电文在下列情况下发送时，应视为发端人之数据电文：由“有权代表发端人就该数据电文行事”的人发送，或由“发端人设计程序或他人代为设计程序的一个自动运作的信息系统”发送。就发端人与收件人之间而言，收件人有权将一项数据电文视为发端人的数据电文，并按此推断行事，条件是：(*a*) 为了确定该数据电文是否为发端人的数据电文，“收件人正确地使用了一种事先经发端人同意的核对程序”，或 (*b*) 收件人收到的数据电文是由某一人的行为而产生的，该人由于与发端人或与发端人之任何代理人的关系，得以动用本应由发端人用来鉴定数据电文确属源

[48]《贸易法委员会电子商务示范法……》，第 7 条第 1 款 (*b*) 项。

自其本人的某一方法。从整体来看，这些规则允许一方当事人对他人的身份作出推定，而不论数据电文是否是电子“签名的”，也不论用于确定数据电文属于发端人的方法是否可有效地用于“签名”目的。这符合纸质环境下的现行做法。核对他人的声音、外形特征或身份证件（例如私人护照）即可足以断定某人为意图与相关人通信的人，但在多数法律体系下，这种核对没有资格作为这类人的“签名”。

23. 在纸质环境与电子环境下，这些用语的技术和法律用法并不相同，尽管该事实造成了困惑，但以前提及的各种技术（见上文第 16 段和下文第 24-66 段更为详细的讨论）可根据具体情况而用于不同的目的，提供不同的功能。例如，密码或代码可用于“签署”一份电子文件，但也可用于访问网络、数据库或另一种电子服务，就如同可将钥匙用于开启保险箱或开门。但在第一个例子中，密码是证明身份的证据，而在第二个例子中，密码是显示权力的一种证书或象征，尽管后者通常与特定的人有关，但仍然能够转给他人。在数字签名的情况下，现行术语的不合适甚至更为明显。数字签名被普遍视为“签署”电子文件的一种特殊技术。但是至少有疑问的是，从法律的角度来看，将不对称加密方法用于认证目的是否应当称作数字“签名”，因为其职能超出了手写签名的典型职能。数字签名提供了“核实数据电文真实性”和“保证内容完整性”的手段。此外，数字签名技术不只是确定个人签名的来源或签名所需的完整性，而且也可用于对服务器、网站、计算机软件或数字传输或储存的任何其他数据进行认证，从而使数字签名的用法远比手写签名电子替代办法更广。[49]

B. 电子签名和认证的主要方法

24. 为进行本讨论，将讨论四个主要的签名和认证方法：数字签名；生物鉴别方法；密码和混合方法；以及扫描或打字签名。

---

[49] Babette Aalberts and Simone van der Hof, Digital Signature Blindness: *Analysis of Legislative Approaches toward Electronic Authentication*（1999 年 11 月），第 8 页，可查阅 http://rechten.uvt.nl/simone/Digsigbl.pdf（2008 年 6 月 5 日查阅））。

1. 依靠公用钥匙加密的数字签名

25. “数字签名”系指使用非对称加密技术，也称为公钥加密体系，以确保电文的真实性，并保证这些电文内容完整性的技术应用程序的名称。数字签名有许多不同形态，诸如失败一终止数字签名、盲签名和不可抵赖数字签名。

(a) 技术概念和术语

(i) 加密

26. 数字签名采用加密技术予以创建和核查，而加密技术是应用数学的一个分支，涉及将电文转换为表面上不可懂的形态和还原为原有形态。数字签名使用所谓的公用钥匙加密技术，常常依靠算法函数产生两套不同但数学上相关的“钥匙”（即利用一系列数学公式产生的大数乘以素数）。[50] 其中一套钥匙用于产生数字签名或将数据转变为表面上不可懂的形态，另一套钥匙用来核查数字签名或将电文还原为原有形态。[51] 利用这两套钥匙的计算机设备和软件合起来称为“密码系统”，如果它们依靠的是使用非对称算法，则可以更具体地称为“非对称密码系统”。

(ii) 公用钥匙和私人钥匙

27. 用于数字签名的互补钥匙称作“私人钥匙”，它仅供签名人用以创建数字签名，因此应当保密；“公用钥匙”，一般更广为人知，而且由依靠方用于核查数字签名。这种私人钥匙可能保留在智能卡上，或可以通过个人识别号码检索，或者通过生物测定学鉴别装置，例如通过拇指纹识别装置进行检索。如果许多人需要核实签名人的数字签名，

---

[50] 但是，应该指出的是，上面所讨论的“公用钥匙加密法”这一概念不一定意味着对基于素数的计算法的使用。目前还在使用其他数学技术或正在开发其他的技术，诸如依靠椭圆曲线的加密系统，通常称它们用大大缩短的钥匙长度提供高度安全。

[51] 使用加密技术是数字签名的主要特征之一，但不应将用数字签名认证含有数字形式信息的电文与泛泛利用加密技术进行保密相混淆。保密性加密技术是一种电子通信编码方法，只让电文的发件人和收件人能够阅读。在一些国家，由于公共政策可能会涉及国防考虑，使用加密技术进行保密受到了法律的限制。但是，因认证之目的而使用加密技术，创建一个数字签名，并不一定意味着使用加密技术来使通信过程中的任何信息成为机密，因为加了密的数字签名可能仅仅是附加于一则未加密的电文之后而已。

公用钥匙就必须提供或分发给他们中每个人，具体做法是，例如，在签名上附上证件，或采取其他方式确保依赖方以及只有不得不核查签名的人才能获得有关证件。这两套成对钥匙具有数学联系，但如果是安全地设计和实施了非对称密码系统，那么通过对公用钥匙的了解求出私人钥匙几乎是不可能的。使用公用钥匙和私人钥匙进行加密的最常用算法是以大素数的一个重要特点为基础的：一旦二者相乘得出一个新数，要断定是哪两个素数产生了这个新的更大数字，就特别困难，特别耗时。[52] 这样，许多人可能知道某个签名人的公用钥匙而且用它来核实签名人的签名，但却不能发现该签名人的私人钥匙并用它来伪造数字签名。

(iii) *散列函数*

28. 除了生成密钥对之外，在创建和核实数字签名时还利用另一个基本程序，一般称为“散列函数”。散列函数是一种数学过程，它以建立电文的数字表示或压缩形式（常被称为“电文摘要”或电文的“指纹”）的算法为基础，表现为标准长度的“散列值”或“散列结果”，通常比电文短得多，但仍具有它明显的独特性。在使用同一散列函数时，电文的任何变动必然产生不同的散列结果。如果使用安全的散列函数——有时叫做“单向散列函数”，知道电文的散列值也几乎无法求出原有电文。散列函数的另一个特征是几乎不可能找到另一个提供同样摘要的二元物体（即不同于最初求出摘要的物体）。因此，散列函数能使创建数字签名的软件以较少和可预测的数据量运作，同时仍为原有电文内容提供可靠的证据相关性，从而有效地保证电文经数字签名后未被修改。

[52] 某些现有的标准提及“计算无法实行”这一概念，来描述预期的进程的不可扭转性，即，希望不可能从该用户的公用钥匙中推出用户的秘密私人钥匙。“‘计算无法实行’是一个相对概念，基础是受保护数据的价值、保护数据所需要的计算管理费用、数据需要保护的时间长度，以及袭击数据所需要的费用和时间，这些因素是目前根据未来的技术进步进行评估的。”（美国律师协会，《*数字签名指导方针：认证机构和安全电子商务法律基础结构*》（芝加哥，美国律师协会，1996 年 8 月 1 日），第 9 页，注 23，可查阅 http://www.abanet.org/scitech/ec/isc/dsgfree.html（2008 年 6 月 4 日查阅）。

(iv) 生成数字签名

29. 为了签署一份文件或任何其他的信息项目，签名人首先精确划定拟签名的内容范围。然后，签名人软件中的散列函数为拟签名的信息计算其独有的（就所有实用技术而言）的散列结果。签名人的软件接着使用签名人的私人钥匙将散列结果转变为数字签名。所产生的数字签名因此为所签名的信息和用以创建数字签名的私人钥匙所独有。典型的情况是，数字签名（用签名者的私人钥匙为电文的散列结果加密）附在电文之后并随电文一起存储或发送。不过，只要保持与电文的可靠联系，也可作为单独的数据单元发送或存储。由于数字签名为电文所独有，如果与原电文永久脱离联系，就毫无用处了。

(v) 数字签名的核查

30. 数字签名的核查是通过参照原有电文和某一给定公用钥匙对数字签名进行检查的过程，从而判定是否利用了与被参照的公用钥匙相对应的私人钥匙为该原有电文创建了数字签名。在核查数字签名时，还通过用于创建数字签名的同一散列函数计算原有电文新的散列结果。然后，核查人利用公用钥匙和新的散列结果，核对数字签名是不是利用相应的私人钥匙创建的，并核查新计算出来的散列结果是否与在签名过程中转变为数字签名的原散列结果相配对。

31. 在下列情况下，核查软件从加密的角度确认数字签名得到了“核查”：(*a*) 用签名人的私人钥匙对电文进行数字签名，用签名人的公用钥匙核查签名时，即认为属于此种情况，因为签名人的公用钥匙将只核查采用签名人的私人钥匙创建的数字签名；(*b*) 电文未经改动，当核查人计算的散列结果与在核查过程中从数字签名析取的散列结果相一致时，即认为属于此种情况。

(vi) 数字签名技术的其他用途

32. 数字签名技术比只以手写签名签署文件的方式“签署”电子通信有更为广泛的用途。确实，以数字方式签名的证书通常用于“鉴定”服务器或网站，以便向其用户确保服务器或网站跟原先设想的一样，或者的确附属于声称经营该服务器或网站的公司。数字签名技术还可以用来“鉴定”计算机软件，比如为了确保从网站上下载的一个

软件的真实性，或为了确保某一特定的服务器使用的技术是被广泛认可的技术，因为它提供了一定程度的连接安全，或者为了“鉴定”任何其他以数字形式传播或储存的数据。

(b) 公用钥匙基础设施和认证服务提供者

33. 为了核查数字签名，核查人必须取得签名人的公用钥匙，而且保证它与签名人的私人钥匙相对应。不过，公用和私人钥匙对与任何人都没有内在的联系；它们只是一对数字而已。需要有一种外加的机制才能将特定的个人或实体与密钥对可靠地联系起来。这一点十分重要，因为签名人和以数字方式签名的通信接收人之间可能没有以前就有的信任关系。为此，有关各方必须对发给的公用钥匙和私人钥匙有一定程度的信任。

34. 下述各方之间可能存在着所需的信任程度：它们彼此信任，它们彼此已打过一段时间的交道，它们在封闭系统上互相联系，它们在非对外的集团内部经营业务，或者它们能够采取合同的方式，例如贸易合伙人协议，来管理它们的交易。在只涉及两方的交易中，每方只需（采用较为可靠的渠道，如派信使送或用电话联系）将各自将使用的密钥对中的公用钥匙通知对方即可。然而，在下述这样的各方之间就可能不存在同样的信任程度：它们彼此不常打交道，在开放的系统上联系（例如因特网上的万维网），不属于一个非对外的集团，或者未订有贸易合伙人协议或没有管理它们之间关系的其他法律。此外，还应当考虑到，如若争端必须通过法院或仲裁的形式解决，可能很难证明公用钥匙的法定所有人是否真的将钥匙发给了接收人。

35. 未来的签名人可以发表一则公开声明，说明对于可用某个给定的公用钥匙加以核查的签名，应作为出自该签名人之手的签名对待。发布方国家的法律适用于此种声明的形式和法律效力。比如，可以通过在官方公告或公共机关确认为“真实”的文件中发表声明来推定某个电子签名属于某个特定的签名人。然而，其他各方可能不愿意接受这种声明，当事先没有合同能够有把握地证明这种公开声明的法律效力时尤其如此。如果交易最终证明对字面签名人不利，那么当事方若信赖此种在开放系统上所作的未经证明的公开声明，便将冒巨大的风险，疏忽大意地信任骗子，或不得不反驳对数字签名的凭空否认（常在数字方式签名的“不可抵赖性”环境下提到的一个问题）。

36. 解决这其中某些问题的一个办法是利用一个或多个第三方将认定的签名人或签名人的名字与某个具体的公用钥匙联系起来。在大多数技术标准和指导原则中，该第三方一般称做“认证机构”、“认证服务提供者”或“认证服务供应商”（在《贸易法委员会电子签名示范法》中选用了“验证服务商”一语）。在若干国家中，这类认证机构现正按等级编组成常常所称的公用钥匙基础设施。公用钥匙基础设施中的认证机构可以按照等级编组成立，因为一些认证机构只能证明其他的一些直接向用户提供服务的认证机构。在这样的编制下，一些认证机构是其他认证机构的下属。在其他可能的编制下，所有的认证机构可能在平等的基础上进行运作。在任何大型的公用钥匙基础设施中，可能同时会有下级认证机构和上级认证机构。其他解决办法包括，例如，依赖方颁发的认证。

(i) 公用钥匙基础设施

37. 建立公用钥匙基础设施是一种方法，用以使人们信任下列几点：(*a*) 用户的公用钥匙未被篡改，而且事实上与该用户的私人钥匙相对应；(*b*) 使用的加密技术是可靠的。为令人产生这种信任，公用钥匙基础设施可以提供多种服务，其中包括：(*a*) 管理用于数字签名的加密钥匙；(*b*) 验证一套公用钥匙对应于一套私人钥匙；(*c*) 为最终用户提供钥匙；(*d*) 公布公用钥匙或证书方面的废止信息；(*e*) 管理个人令牌（例如智能卡），它们能够以独特的个人识别信息识别用户或者能够生成和存储个人的私人钥匙；(*f*) 核实最终用户的标识并向它们提供服务；(*g*) 提供时间标记服务；以及 (*h*) 在获准使用加密钥匙时，管理用于保密性加密的加密钥匙。

38. 公用钥匙基础设施常以多层次的权力结构为基础。例如，某些国家为建立可能的公用钥匙基础设施而考虑的模式涉及下列层次：(*a*) 一个独一无二的“总根机构”，它将验证凡获准发布配对加密钥匙或签发与使用这些配对钥匙有关的证明的所有各方采用的技术和做法，并对下属的认证机构进行登记；[53] (*b*) 多个认证机构，置于总根机构之下，负责验证用户的公用钥匙实际上与该用户的私人钥匙相对应（即未经篡改）；(*c*) 多个地方登记机构，置于认证机构之下，接受用户对配对加密钥匙或与使用这些配对钥匙有关的证明而提出的申请，要求提出鉴定的证据并检查潜在用户的身份。在某些国家，设想可由公证人充当或支持地方登记机构。

[53] 关于政府是否应具有技术能力来保留或重新创造私人加密钥匙的问题可以在总根机构一级进行解决。

39. 具有等级体系的结构内组建起来的公用钥匙基础设施是可扩缩的，因为它们只要通过总根机构与新社区的总根机构建立一种信任关系将整个新的公用钥匙基础设施“社区”包含在内。[54] 新社区的总根机构可以直接被纳入公用钥匙基础设施的接收方“总根机构”之下，从而成为该公用钥匙基础设施内的下属认证服务提供者。新社区总根机构也可以成为现有公用钥匙基础设施内某一个下属认证服务提供者的下属认证服务提供者。具有等级体系的公用钥匙基础设施的另一个吸引人的特征是它使制定验证途径变得容易，因为它们只沿着一个方向，从用户的验证回到信任点。此外，具有等级体系的公用钥匙基础设施内的验证道路相对比较短，某一等级体系的用户则明白，在该等级体系内的认证服务提供者立场基础上可对一项验证作何应用。但是，具有等级体系的公用钥匙基础设施也有不利之处，主要是依赖于一个单一的信任点的缘故。如果总根机构失密，则整个公用钥匙基础设施也随着失密。此外，一些国家发觉很难选择一个单一的实体作为总根机构，以及很难向所有其他的认证服务提供者施加这种等级体系。[55]

40. 所谓的“网状”公用钥匙基础设施是具有等级体系的公用钥匙基础设施的一个备选。在这一模式下，认证服务提供者之间以同伴的关系相互联系。这一模式下的所有认证服务提供者都可以成为信任点。一般情况下，用户会信任发布证书的认证服务提供者。认证服务提供者之间彼此发布证书，这些证书描述相互的信任关系。此种系统缺乏等级体系，意味着认证服务提供者不能施加管理由其他认证服务提供者发布的证书的条件。如果一家认证服务提供者欲限制向其他认证服务提供者提供的信任，它必须在向其同伴所发布的证书中明确说明这些限制。[56] 但是，协调条件和相互承认可能是一个相当复杂的目标。

41. 第三个替代结构是所谓的“桥梁”认证服务提供者。这一结构可能在使各种已有公用钥匙基础设施社区相互信任彼此的证书方面特别有用。与网状公用钥匙基础设施中的认证服务提供者不同的是，“桥梁”认证服务提供者并不直接向用户发布证书。公用钥匙基础设施的用户也不会将“桥梁”认证服务提供者当作信任点，如总根认证服务提供者那样。相反，桥梁认证服务提供者与不同的用户社区建立起了同伴的信任关系，从而使用户能够在其各自的公用钥匙基础设施内保持其自然的信任点。如果一个用户社区执行了一个具有等级体系的公

---

[54] William T. Polk 和 Nelson E. Hastings，《桥梁认证机构：连接企业间公用钥匙基础设施》，国家标准和技术研究所（2000 年 9 月），可查阅 http://csrc.nist.gov/pki/documents/B2B-article.pdf（2008 年 6 月 5 日查阅）。

[55] Polk 和 Hastings（《桥梁认证机构……》）指出，在美国，很难在政府中单独划出一个机构来承担联邦公用钥匙基础设施的全部授权。

[56] *Polk 和 Hastings*，《桥梁认证机构……》。

用钥匙基础设施形式的信任域，则桥梁认证服务提供者将与该公用钥匙基础设施的总根机构建立关系。但是，如果用户社区通过创建一个网状公用钥匙基础设施而执行了一个信任域，则桥梁认证服务提供者将仅需与其中的一位公用钥匙基础设施认证服务提供者建立关系，因为此时这一提供者已经成为该公用钥匙基础设施内为了与另一公用钥匙基础设施建立“信任桥梁”的主要认证服务提供者。通过两个或两个以上与桥梁认证服务提供者有互相关系的公用钥匙基础设施将其结合起来的信任桥梁，使来自不同用户社区的用户能够通过具有特别信任水平的桥梁认证服务提供者开展互动。[57]

(ii) 认证服务提供者

42. 为使配对钥匙与未来的签名人联系起来，认证服务提供者（或认证机构）签发一份证书，这是一份电子记录，将公用钥匙和证书用户的名字合列在一起，作为证书的“内容”，而且可能确认证书中标明的未来签名人持有对应的私人钥匙。证书的主要作用是将公用钥匙与特定的签名人联系在一起。证书的“接收人”如果希望依赖证书中标明的签名人所创建的数字签名，可利用证书中所列的公用钥匙验查数字签名是否是采用对应的私人钥匙创建的。如果这种验查获得成功，则一定程度上从技术上保证数字签名是由该签名人所创建的，而且散列函数中所载电文（即对应的数据电文）经数字签名后未被改动过。

43. 为了保证证书的内容和来源的真实性，认证服务提供者给证书加上数字签名。签发证书的认证服务提供者在证书上的数字签名可以采用由另一个认证服务提供者签发的另一份证书中列出的该认证服务提供者的公用钥匙来核查（这另一个认证服务提供者可以是上级机构，但也不一定非得这样），而且该另一证书可以依次再由另一份证书中列出的公用钥匙验证，如此不断进行下去，直至依赖于数字签名的个人对其真实性确信无疑为止。把数字签名记录在认证服务提供者签发的证书（有时被称为“总”证书）上，也是核查数字签名的可能采取的方法。[58]

44. 在每一种情况下，签发证书的认证服务提供者可以在另一用来核查认证服务提供者数字签名的证书操作期内，在其自己的证书上进行数字签名。根据一些国家的法律，对认证服务提供者的数字签名建立信心的一种方法是在官方公告中公布认证服务提供者的公用钥匙或有关总证书的某些数据（诸如“数字指纹”）。

---

[57] 桥梁认证服务提供者是最终被选为美国政府设立公用钥匙基础设施系统的结构（Polk 和 Hastings，《桥梁认证机构……》）。这也是日本政府建设公用钥匙基础设施系统所遵循的模式。

[58]《贸易法委员会电子签名示范法……》，第二部分，第 54 段。

45. 与电文相应的数字签名，不管是签名人为了认证电文而创建的，还是认证服务提供者为了认证其证书而创建的，一般都应当打上可靠的时间标记，以使查验人能够确定数字签名是否是在证书中指出的操作期内创建的，以及该证书在有关时期内是否有效（比如，未在吊销列表中提及），因为这是能否查验数字签名的一个条件。

46. 为使公用钥匙及其与具体签名人的对应关系随时可接受核查，证书可公布在储存库中或由其他手段提供。一般情况下，储存库是证书和其他信息的联机数据库，可供检索和用以核查数字签名。

47. 证书一旦签发，可能证明并不可靠，例如签名人向认证服务提供者误报其身份就属此类情况。在其他情况下，一份证书在签发时可能具有可靠性，但之后就可能变得不可靠了。例如，由于签名人失去对其私人钥匙的控制，这种私人钥匙就属失密，如属此种情况，证书可能丧失其可信性或变得不可靠，认证服务提供者（按签名人的请求或甚至不经签名人的同意，视情况而定）可能中止（暂时中断操作期）或吊销（使永久无效）证书。在中止或吊销证书以后，认证服务提供者一般必须立即公布关于吊销或中止的通知，或通知那些查询有关事项的人或那些已为人所知收到按不可靠证书核查的数字签名的人。同样地，适当时也应当对认证服务提供者的证书进行可能被废止的审查，就如为了查验时间标记当局在时间标记口令牌上所作签名而签发的证书以及向时间标记当局签发了证书的认证服务提供者的证书。

48. 认证机构可由私营部门的服务商运作或由政府机构运作。若干国家设想，为了公共政策的原因，唯有政府实体才应获准充当认证机构。但是，在大多数国家，或者是认证服务完全由私营部门运作，或者是政府运作的认证服务提供者与私营部门的服务商同时存在。此外，还有封闭的验证系统，几个小组在此系统内配置自己的认证服务提供者。在一些国家，国有的认证服务提供者只签发公共行政部门所使用的数字签名证书。不管认证机构是由公共实体还是私营部门的服务商运作，也不管认证机构是否需要许可证进行运作，在公用钥匙基础设施中一般都有一个以上的认证服务提供者。一个特别令人关切的问题是各种认证机构之间的关系（见上文第 38-41 段）。

49. 认证服务提供者或总根机构可能有责任保证其政策要求持续不断地得到满足。认证机构的选择可能基于各种因素，其中包括使用的公用钥匙的强度和用户的身份，但任何认证服务提供者的可信度也可能取决于它对发证标准的执行情况和它对来自申请证书用户的数据进行的评估是否可靠。特别重要的是对任何认证服务提供者

实行的责任制度，即认证服务应持续不断地执行总根机构或上级认证服务提供者的政策和安全要求，或任何其他适用的要求。同样重要的是，认证服务提供者有按照其关于政策和实践的说明行事的义务，如《贸易法委员会电子签名示范法》第 9 条第 1 (*a*) 款所设想的那样。

(c) 公用钥匙基础设施实施过程中的切实问题

50. 尽管拥有对数字签名技术及其运作方式的丰富知识，但是，公用钥匙基础设施和数字签名计划在实际实施的过程中面临着一些问题，使数字签名的运用水平低于原先的期望。

51. 数字签名可以作为查验在证书有效期间创建的签名的办法。但是，一旦证书到期或被废止，相对应的公用钥匙就失去其有效性，即使配对密钥未失密也是如此。因此，公用钥匙基础设施计划将需要一套数字签名管理体系来确保一段时期内提供签名。造成主要困难的风险是，包括电子签名在内的“原始”电子记录（即构成记录信息的计算机文档的二进制数字，即“比特”）在一段时间之后可能变得不可阅读或不可靠，这主要是由软件、设备或两者的陈旧过时造成的。此外，数字签名可能变得不安全，原因在于加密分析的科学进展、签名查验软件可能在长时间内不可获得或文件失去其完整性。[59] 这通常会使电子签名的长时期保留成为问题。尽管数字签名在一段时期内被认为是档案记录所必须的，但是实际经验表明，数字签名并非不会受长期风险的影响。既然在创建签名之后对记录的每一次修改都将导致签名查验的失败，那么，意在为将来保留一份清晰记录的操作重组（诸如数据的移徙或转换）可能会影响签名的持久性。[60] 实际上，数字签名更多地被认为是为信息传播提供安全，

---

[59] Jean-François Blanchette，《定义电子认证：一场跨学科的旅行》，可查阅 http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf（2008 年 6 月 5 日查阅）（文章发表在 2004 年可靠性系统与网络国际会议 (DSN 2004) 的补充卷中，意大利佛罗伦萨，2004 年 6 月 28 日至 7 月 1 日），第 228-232 页。

[60] “最后，我们在电子环境下所能保存的只有比特。但是，早已很清楚的是，不可能永久性地保存一套比特。随着时间的流逝，这一套的比特变得难以辨认（对计算机和人而言都是如此），原因是应用程序的技术过时和（或）硬件技术过时（比如阅读器）。基于公用钥匙基础设施的数字签名的持久性问题由于十分复杂，至目前为止对其研究甚少。……虽然过去用的认证工具，比如手写签名、印章、图章、手印等等，也需要重定格式（比如缩微胶卷），因为输纸装置陈旧，但在重定格式后仍绝不完全失去用处。至少总有一个副本可以与其他最初的认证工具相比较”（Jos Dumortier 和 Sofie Van den Eynde，《电子签名和受托档案服务》第 5 页（可查阅 http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where，2008 年 6 月 5 日查阅）。

而不是为了长时间地保存信息。[61] 针对这一问题的举措还未找到一个长久的解决办法。[62]

52. 数字签名和公用钥匙基础设施计划可能造成实际问题的另一领域涉及数据安全和隐私保护。认证服务提供者必须安全保存用于在向其客户签发的证书上签名的钥匙，因为外人可能会企图未经核准利用钥匙（见下文第 223-226 段第二部分）。此外，认证服务提供者必须从证书申请者那里获得一系列的个人数据和商业信息。认证服务提供者必须储存这一信息，以备日后之用。认证服务提供者必须采取必要

[61] 1999 年，来自各个国家的案卷保管人发起了关于电子系统永久真实记录的国际研究 (InterPARES) 项目，目的在于“长期保存创建的和（或）以数字形式保存的真实记录所必须的理论和方法知识”（见 http://www.interpares.org，2008 年 6 月 5 日查阅）。作为项目第一阶段（InterPARES 1，2001 签署）一部分的真实性问题工作队的报告草稿（可查阅 http://www.interpares.org/documents/atf_draft_final_report.pdf，2008 年 6 月 5 日查阅）表明，“数字签名和公用钥匙基础设施 (PKI) 是作为认证在空间传播的电子记录的手段而开发和实施的技术例子。尽管记录保存者和信息技术人员信任认证技术以确保记录的真实性，但是，这些技术却从来都不是，现在也不是可以长期确保电子记录真实性的一种手段”（着重部分由作者标明），InterPARES 1 项目最终报告可查阅 http://www.interpares.org/book/index.htm（2008 年 6 月 5 日查阅）。项目 (InterPARES 2) 继续实施，旨在制定并明确界定可以确保创建并保存准确而可靠的记录并在 1999 年至 2001 年期间制定的艺术、科学和政府活动背景下长期保存真实记录的概念、原则、标准和方法。

[62] 例如，信息和通信技术标准委员会于 1999 年创立了欧洲电子签名标准化倡议 (EESSI)，该委员会是一个关于信息和通信技术方面标准化和有关活动的合作组织，它的成立是为了协调标准化活动，以支持对欧洲联盟关于电子签名指令的执行（见《欧洲共同体公报》，L 13/12，2000 年 1 月 19 日）。EESSI 联合会（寻求将欧洲关于电子签名的指令的各项要求转化为欧洲标准的标准化方面努力）力求满足确保长期保存经加密过签署的文件的需求，办法是采用其自己的关于电子签名格式（电子签名格式 ES 201 733, ETSI, 2000）的标准。该格式对签名测定时机有所区分：最初的测定和后来的测定。后期测定的格式包括所有在测定过程中可以最终使用的信息，诸如废止信息、时间戳、签名政策等等。这种信息是在最初的测定阶段收集的。这些电子签名格式的设计者担心的是由于加密强度的减弱而对签名测定所造成的安全威胁。为了防止加密强度的减弱，EESSI 签名会定期用与最新的加密分析方法相应的签署算法和钥匙规模重新加印时间戳。关于软件寿命的问题已经在 EESSI 2000 年的一份报告中得以解决，这份报告介绍了“受托档案服务”这一将由有待指明的主管机构提供的新型商业服务，其目的在于保证长期保存经加密签署的文件。报告列举了一些技术要求，比如档案服务应通过计算机硬件和软件提供“后向兼容性”等，办法是通过维护设备或仿真（见 Blanchette，《定义电子真实性》）。比利时鲁汶大学法律和信息技术跨学科中心关于 EESSI 有关受托档案服务的建议的后续研究，题目为《欧洲电子签名标准化倡议：受托档案服务》（第 3 阶段，最后报告，2000 年 8 月 28 日），可查阅 http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=（2008 年 6 月 5 日查阅）。EESSI 于 2004 年 10 月关闭。执行 EESSI 建议的系统目前似不再运作当中（见 Dumortier 和 Van den Eynde，《电子签名和受托档案服务》……）。

的措施，以确保根据适用的数据保护法律查阅此种信息。[63] 但是，未经核准查阅信息仍然是一种实际存在的威胁。

2. 生物测定技术

53. 生物测定是一种通过个人固有的物理或行为特征查明一个个人的测定办法。可以在生物测定技术中作识别用的特征包括脱氧核糖核酸、指纹、虹膜、视网膜、手部和面部几何特征、面部温度记录图、耳朵形状、声音、体味、血管形态、笔迹、步态和打字模式。

54. 生物测定设备的使用通常包括捕捉一个个人生物特征的生物测定样本。这一样本为数字形式。然后，从这一样本中抽取生物测定数据，以创建一个参考模板。最后，将个人的生物测定数据与储存在参考模板上的生物测定数据进行比较，即可确认生物测定样本所关联的人的身份，并可证实据认为是由该人发端的通信的真实性。[64]

55. 由于生物测定模式通常不能被废止，生物测定数据的储存就存在一些风险。当生物测定系统失密后，合法用户不能追诉，而只能废止身份查验数据，并转向另一套未失密的身份查验数据。因此，需要防止滥用生物测定数据库的特别规则。

56. 生物测定技术的准确性不是绝对的，因为生物特征本身就易于变化，并且任何测量都可能有偏差。就这一点来说，生物测定技术不是独一无二的识别技术，而是半独特的识别技术。为了调解这些偏差，可以通过为参考模板和抽取的样本相匹配设置门槛来控制生物测定技术的准确性。但是，低门槛可能会导致虚假的接受，而高的门槛则会导致虚假的拒绝。尽管如此，由生物测定技术提供的认证的准确性在绝大多数的商业应用中是足够的。

---

[63] 见经济合作与发展组织（经合组织）关于保护隐私和个人数据跨国界流动的指导方针（巴黎，1980 年），可查阅 http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_ 1_1_1_1,00.html（2008 年 6 月 5 日查阅）；《欧洲委员会在自动处理个人数据方面保护个人公约》（欧洲委员会，《欧洲条约集》，第 108 号），可查阅 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm（2008 年 6 月查阅）；管理计算机化的个人数据资料指导方针（大会第 45/95 号决议）；以及欧洲议会和欧洲委员会 1995 年 10 月 24 日关于在处理个人数据方面保护个人和关于个人数据自由流动的第 95/46/EC 号指令（《欧洲共同体公报》，L 281，1995 年 11 月 23 日可查阅 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett（2008 年 6 月查阅））。

[64] 国际生物测定学会和国际计算机安全协会，《*1999* 年生物测定术语词汇》（秘书处可提供副本）。

57. 此外，在生物测定数据的储存和披露中会出现数据保护和人权方面的问题。数据保护法律[65]尽管不一定明确提到生物测定，但其目的在于保护有关自然人的个人数据，而对原始个人数据和模板数据的加工是生物测定技术的核心。[66]此外，可能需要采取措施保护消费者免受因私下使用生物测定数据和身份窃取所造成的风险。其他法律域，包括劳动和卫生法，也可能会发挥作用。[67]

58. 技术解决办法可能有助于解决某些问题。比如，将生物测定数据储存在智能卡或口令牌上可以防备未经核准查阅数据，而如果数据储存在一个中央计算机系统中，可能发生未经核准查阅。此外，已经开发了最佳做法，以减少在不同领域中的风险，诸如范围与能力；数据保护；个人数据的用户控制；以及披露、审核、问责和监督。[68]

59. 一般认为生物测定设备提供了高水平的安全性。虽然这些设备能与一系列的用途相兼容，但是，它们目前主要用在政府应用程序上，特别是执法应用程序上，诸如入关查验和进出控制。

60. 商业应用程序也已开发出来，常常在需要提供个人所具有的要素（生物测定技术）和个人所知要素（一般为密码或个人识别号码）的两要素认证进程中利用生物测定技术。此外，还开发了储存和比较个人手写签名特征的应用程序。基于数字的签名笔书写板记录了签名过程的运笔压力和持续时间。然后，把这些数据作为算法储存起来，用来与将来的签名比较。但是，鉴于生物测定的内在特征，也应该注意关于其在例行商业交易使用中逐渐地、不受控制地增加的风险。

61. 如果用生物测定签名替代手写签名，可能会出现证据的问题。如前所述，生物测定证据的可靠性在使用的技术和已选定的虚假接受率当中有所不同。此外，还有可能篡改或歪曲以数字形式储存的生物测定数据的可能性。

---

[65] 见注 63。

[66] Paul de Hert,《生物测定技术：法律问题及意义》欧盟委员会未来技术研究所背景文件（欧洲共同体，联合研究中心总局，2005 年）第 13 页，可查阅 http://cybersecurity.jrc.es.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf（2008 年 6 月 5 日查阅）。

[67] 比如，在加拿大，讨论生物测定技术的使用，涉及《个人资料保护和电子文件法》（2000，c. 5）在工作场所的适用（见 Turner v. TELUS Communications Inc., 2005 FC 1601，2005 年 11 月 29 日（加拿大联邦法院））。

[68] 比如，最佳做法见《国际生物测定技术组生物隐私倡议》中的“注重隐私的生物测定技术最佳做法”，可查阅 http://www.bioprivacy.org（2008 年 6 月 5 日查阅）。

62. 《贸易法委员会电子签名示范法》和《贸易法委员会电子商务示范法》,以及最近的《联合国国际合同使用电子通信公约》[69]规定的一般可靠性测试，可以适用于生物测定签名。为确保统一性，制定关于生物测定方法使用和管理的国际指导方针可能也是有用的。[70]鉴于当前生物测定技术的发展状况，以及可能危及生物测定技术持续发展的风险，必须对此种标准是否不成熟进行认真审议。

3. 密码和混合方法

63. 密码和代码被用于控制获取信息或服务,以及“签署”电子信件。在实践当中，后者的使用较前者要少，因为在未经加密的电文传输中会有失密的风险。但是，密码和代码是各种交易，包括多数网上银行交易、自动取款机现金提取和消费者信用卡交易中，为控制访问和查验身份而使用的最广泛的“认证”方法。

64. 应当承认，可以用复合技术来“认证”一宗电子交易。可以利用若干项技术或通过对一项技术的若干次使用来完成一项交易。比如，供认证的签名动态可以与加密技术相结合，以确保电文的完整性。如其不然，可以在因特网上发送密码，用加密技术（比如浏览器中的SSL）保护密码，同时使用生物测定技术生成一个数字签名（非对称加密技术），在收到该数字签名后会生成一张 Kerberos 票（对称加密技术）。在制定处理这些技术的法律和政策框架过程中，必须考虑复合技术的作用。电子认证法律和政策框架必须足够灵活，以包含混合技术办法，如同那些侧重于可以阻止使用复合技术的专门技术一样。[71]技术中立规定将促进对此种混合技术办法的接受。

---

[69] 国际合同使用电子通信公约草案获得贸易法委员会第三十八届会议（维也纳，2005 年 7 月 4 日至 15 日）核准，该公约在大会 2005 年 11 月 23 日第 60/21 号决议中获得通过。

[70] 这些可以与载于《贸易法委员会电子签名示范法颁布指南》中所述的可靠性标准相比较（《贸易法委员会电子签名示范法……》，第二部分，第 75 段）。

[71] 见信息政策研究基金会应欧盟委员会的请求编写的《签名指令协商汇编》，1998 年 10 月 28 日，汇编了在欧洲联盟关于电子签名指令草案协商过程中所作的答复。可查阅 www.fipr.org/publications/sigdirecon.html（2008 年 6 月 5 日查阅）。

4. 扫描签名和打字姓名

65. 欲在私法领域对电子商务进行立法的主要原因，是对新技术可能如何影响其他媒体法律规则的适用的关切。这一对技术的关注，有意无意地导致了对尖端技术的侧重，因为尖端技术为电子认证和签名方法提供更高水平的安全。在这样的背景之下，经常忽略的是，全世界的商务通信，如果不是绝大多数，也是许多，都没有利用任何特别的认证或签名技术。

66. 在日常实践中，全世界的公司通常都满足于用电子邮件交换电文，除了在邮件下方打上姓名、职衔和地址外，未使用任何形式认证或签名。有时候会使用手写签名的传真或扫描图像，赋予更正式的外观，但这只不过是手写原件数字化形式的一个副本而已。但是，在不加密电子邮件电文上的姓名和扫描的签名都不能提供高水平的安全性，也不能明确证明电子通信件发端人的身份。但是，为了通信的方便、快捷和有成本效益，企业实体自由地选择使用这些形式的“认证”。立法者和决策者在审议管理电子认证和签名时，必须铭记这些普遍商业做法。对电子认证和签名的严格要求，特别是采用一种特殊的方法或技术，可能会在不经意间使人对每日没有使用任何认证或签名的大量交易的有效性和可执行性产生怀疑。反过来，这可能导致恶意行事的当事人质疑其自己的电子通信的真实性，以避免它们自由承担的义务所带来的后果。期望施加一些高水平的认证和签名要求最终会使有关各方每天都使用，是不切实际的。最近使用数字签名这样的尖端方法的经验已经表明，对费用和复杂情况的担忧通常会限制对认证和签名技术的实际运用。

C. 电子身份管理

67. 在电子世界，自然人或法人都能够获得一些提供商的服务。一个人每次在服务提供商那里登记以获得其服务时，一个电子“身份”便会被创建。此外，一个身份可以与每个申请或平台的若干账户链接。身份及其账户的增加可能会妨碍用户和服务提供商对它们的管理。这些困难可以通过一人一电子身份的方式加以避免。

68. 在服务提供商处进行登记和电子身份的创建需要在个人与提供商之间建立互相信任的关系。创建单一电子身份要求将这些双边关系整合起来并纳入一个更为广泛的框架当中，以便对其进行联合管理，这称为身份管理。对提供商来说，身份管理的益处可能包括提高安全性、使照章办事更简便，使商务更灵活；对用户而言，益处可能包括便于获取信息。

69. 身份管理可以联系以下两种办法来描述：

(*a*) *传统用户使用办法。* 这一办法遵循登录模式，一般基于对智能卡等工具所载或另由消费者持有并由消费者用于登记一项服务的信息的使用。身份管理的用户使用办法侧重于在一个或多个应用程序或系统中对用户认证、使用权利、使用限制、账户情况、密码和其他属性的管理。它的目的在于促进并控制对应用程序和资源的使用，同时保护个人和商业信息不被未经核准的用户所使用；

(*b*) *服务办法。* 这一办法是一种较为创新的模式，基于一种向用户及其各种装置提供个性化服务的系统。这一办法下，身份管理的范围变得更为广泛，包括公司为提供在线服务而使用的所有资源，诸如网络设备、服务器、门户、内容、应用程序和产品，以及用户的证件、地址簿、偏好以及应享权利。在实践中，身份管理的范围可以包括例如有关父母亲控制的设置和参与忠诚方案。

70. 正在努力扩大在企业和政府一级的身份管理。但是，应该指出的是，两种情况下的政策选择可能会大不相同。例如，政府的办法可能更倾向于更好地为满足公民的需求服务，因此，可能倾向于与自然人进行接触。而商业应用程序则必须考虑在企业交易中对自动化机器使用的日益增加，从而可以采纳能够满足这些机器的特定需求的特征。

71. 有关身份管理系统的困难，包括与误用独特识别器有关的风险造成的隐私关切。此外，适用法律条例的差异，特别是有关授权代表他人行事的可能性方面的差异，可能会导致出现问题。有人建议建立一个所谓的信任圈，要求圈内人都信赖其他成员所提供资料的正确性和准确性，以此为基础开展自愿商业合作，在自愿合作的基础上寻求解决办法。但是，这一办法可能还不足以管理所有相关问题，也可能仍然需要通过一个法律

框架。现在还制定了指导方针，为遵守信任圈基础结构提供法律框架。[72]

72. 关于技术的互操作性，国际电信联盟已经成立了一个关于身份管理的重点小组，以促进并推进制定一个发现自主传播的身份、身份联合会以及执行情况的通用身份管理框架和手段。[73]

73. 目前还在电子政务的框架内提供身份管理的解决办法。比如，在欧洲联盟“i2010：一个促进增长和就业的欧洲信息社会”倡议[74]背景之下，启动了一项关于电子政务中身份管理的研究，以便在欧洲联盟成员国现有专门知识和倡议的基础上，促进欧洲联盟电子政务身份管理方面找到一种协调统一办法。[75]

74. 作为电子政务举措的一部分，发放电子签名装置日益普遍。电子签名装置的形式通常是智能卡。目前已经在全国范围发放智能卡，例如，在比利时，最早是 2003 年在若干省份推行智能卡，[76]经过成功的试行阶段后，最终推广到全国。[77]比利时的系统主要包括发行带有芯片的实体身份证，芯片上载有公民进行电子签名所需的数据。[78]

---

[72] “图书馆联盟项目”（见 www.projectliberty.org）是一个由全球 150 多家公司以及非营利性组织和政府组织组成的联盟。该联盟致力于为支持所有目前以及新出现的网络设备的联合网络身份制定公开的标准。联合身份为企业、政府、雇员和消费者提供更为方便和安全的方式，以便在今天这个数字经济中管理身份资料，也是促进使用电子商务和个性化数据服务以及网络服务的一个关键组成部分。所有的商业和非商业组织均可加入。

[73] 见 http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html（2008 年 3 月 20 日查阅）。

[74] 欧洲共同体委员会发给欧洲理事会、欧洲议会、欧洲经济和社会委员会以及区域委员会的信函：“i2010 – 欧洲信息社会促进增长和就业”，COM (2005) 229 终稿（布鲁塞尔，2005 年 6 月 1 日），可查阅 http://eur-lex.europa.eu（2008 年 3 月 20 日查阅）。

[75] 见《关于电子政务中身份管理的方式研究：身份管理问题报告》（欧盟委员会，信息社会和媒体总局，2006 年 9 月 18 日），第 9-12 页，可查阅 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi（2008 年 6 月 6 日查阅）。

[76] 电子身份卡是比利时 2003 年依据 2003 年 3 月 25 日对 1983 年 8 月 8 日《国家个人登记处组织法》和 1991 年 7 月 19 日关于人口登记和身份证并修订 1983 年 8 月 8 日《国家个人登记处组织法》的法律加以修订的法律推行的（Moniteur belge, Ed. 4，2003 年 3 月 28 日，第 15921 页）。

[77] 见 2004 年 9 月 1 日《皇家法令》,其中载有关于着手推行电子身份证的决定（Moniteur belge, Ed. 2，2004 年 9 月 15 日，第 56527 页）。一般信息见 http://eid.belgium.be（2008 年 6 月 6 日查阅）。

[78] 一般信息见 http://eid.belgium.be（2008 年 6 月 6 日查阅）。

75. 奥地利已经开发出一种身份管理系统，该系统记录每个奥地利公民的身份识别特征，但不将这些特征纳入公民的正式身份文件。奥地利选择了技术中性的标准，因此消费者已经开发并采用了一系列的技术解决办法。奥地利的系统以“个人身份链接”为基础，这是经公共签发机关批准的一个系统，将一人的唯一身份识别特征（例如登记号码）放在属于该人的一种或多种证书上。这样，当一人在某一程序进行期间与公共主管机关接洽时，个人身份链接可用于自动唯一识别该人的身份。[79] 这一“唯一身份识别特征”可储存在个人选择的任何智能卡上（例如自动提款卡、社会安全卡、学生身份证、劳工联盟成员卡或专业人员协会成员卡、个人计算机或便携式计算机）。签名装置还可通过移动电话传输，其形式为移动电话服务供应商作为公民唯一身份识别特征的保管人而特别编制的一次性密码。

76. 可利用这一系统签发具体部门的身份标识，这些标识是严格单独保存的，但都与中央身份储存库相连系。这种结构避免了数据分享问题，并保护数据隐私权。这种卡称为“公民卡”，其用意是成为用于办理电子行政程序（如通过互联网提交申请）的正式身份文件。公民卡所建立的安全基础设施可供包括商业客户在内的所有人使用。各公司可以公民卡所提供的基础设施为基础，为其客户开发安全的网上服务。

77. 由于开展了上述这类举措，众多公民缴纳很低的费用便可获得具有安全电子签名等功能的装置。虽然这类举措的主要目的可能不是商业上的目的，但这类装置同样可用于商业领域。这两种应用范围的共同点已经越来越多地得到承认。[80]

---

[79] 奥地利安全信息技术中心 (A-Sit)，《个人身份链接的 *XML* 语言定义》，可查阅 http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell/（2008 年 6 月 6 日查阅）。

[80] 例如，见《*2006* 年韩国互联网白皮书》（首尔，韩国国家互联网开发机构，2006 年），第 81 页，其中提及了《大韩民国电子签名法》在电子政务和电子商务应用软件方面的双向适用（可查阅 http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1，2008 年 6 月 6 日查阅）。

二． 电子认证和签名的法律待遇

78. 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；[81] 或契约协定。[82]

79. 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的协会。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，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。

80. 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。封闭网络通常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”，它们的目的都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

---

[81] 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便利化与电子商务中心建议 32 (ECE/TRADE/277)，可查阅 http://www.unece.org/cefact/recommendations/rec_index.htm（2008 年 6 月 5 日查阅）。

[82] 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“在商业上使用关于交换电子数据的交换协定”(TRADE/WP.4/R.1133/Rev.1) 的欧洲经济委员会国际贸易程序便利化工作组建议 26；以及题为“电子商务协定”的联合国贸易便利化与电子商务中心建议 31 (ECE/TRADE/257)，两份文件均可查阅 http://www.unece.org/cefact/recommendations/rec_index.htm（2008 年 6 月 5 日查阅））。

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的认证或签名办法。[83] 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。

81. 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。本章讨论了在不同法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

82. 在国际和国家两级，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。[84]

1. 最低限度模式

83. 一些法域遵守技术中立政策，承认各种电子签名技术。[85] 这种办法称为最低限度模式，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手写签名具有同等效力，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。

84. 《贸易法委员会电子商务示范法》为在电子签名和手写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：

---

[83] 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。

[84] 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 年）号，第 234 页及其后各页。

[85] 例如澳大利亚和新西兰。

“(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，对生成或传递数据电文的目的来说也是适当的。”

85. 这项规定考虑到了手写签名的两个主要功能：鉴定签名人的身份，表明签名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，技术中立性具有非常重要的意义，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。

86. 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，责任就落在了当事方确定其通信是否足够安全的能力。如此一来，既可避免技术方面过于复杂，也避免了相关费用。[86]

87. 欧洲的立法主要受欧洲联盟所发布指令的影响，[87] 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

---

[86] S.Mason，“实践中的电子签名”，《高技术法学报》，第六卷，第2 (2006) 号，第153页。

[87] 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（《欧洲共同体公报》L 13，2000年1月19日）。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（《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。

模版的。[88] 此外，《示范法》也是加拿大[89]和美利坚合众国[90]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，[91] 颁布

[88] 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，《电子商务、电子签名和数据电文法》（*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，《数字签名法》（*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，《数据电文和电子签名法》（*2001* 年）；以及越南，《电子交易法》（2006 年）。采用《示范法》的还有：英国皇家属地根息行政区（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》）；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。

[89]《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》（可查阅 http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia，附官方评注，2008 年 6 月 6 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可查阅 http://www.ulcc.ca（2008 年 6 月 5 日查阅）。

[90] 在美国，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 年通过了该法案（法案案文和官方评注可查阅 http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm，2008 年 6 月 6 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、阿拉斯加、亚利桑那、阿肯色、加利福尼亚、科罗拉多、康涅狄格、特拉华、佛罗里达、夏威夷、爱达荷、印第安纳、衣阿华、堪萨斯、肯塔基、路易斯安那、缅因、马里兰、马萨诸塞、密歇根、明尼苏达、密西西比、密苏里、蒙大拿、内布拉斯加、内华达、新罕布什尔、新泽西、新墨西哥、北卡罗来纳、北达科他、俄亥俄、俄克拉何马、俄勒冈、宾夕法尼亚、罗得岛、南卡罗来纳、南达科他、田纳西、德克萨斯、犹他州、佛蒙特、弗吉尼亚、西弗吉尼亚、威斯康星和怀俄明。其他各州，包括已通过《电子商务安全法》（1998 年）颁布了贸易法委员会《示范法》的伊利诺伊州，很可能会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可查阅 http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp（2008 年 6 月 6 日查阅）。

[91] 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。

《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）和最近的《联合国国际合同使用电子通信公约》（大会在其 2005 年 11 月 23 日第 60/21 号决议中通过，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措词（见下文第 95 段）。

88. 当立法采用了最低限度模式时，电子签名是否证明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，各类达到要求的电子签名都会被视为有效；因此，测试体现了技术中立原则。

89. 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*) 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

90. 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，在纸质文件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。[92] 毋庸置疑，

[92] 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，该法案可查阅 http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm（2008 年 6 月 6 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设施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，《数字签名法》（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）。

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定安全程度的步伐，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手写签名）。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定要求。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设施为基础的应用。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。

91. 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”。[93] 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要求。[94] 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，就是并非所有的应用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。

92. 技术立法通常倾向于使用公用钥匙基础设施框架内的数字签名。根据政府干预程度的不同，各国构建公用钥匙基础设施的方式也各不相同。在这方面，也可以确定三种主要模式：

(*a*) 自我调节。 在这种模式下，认证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

---

[93] Stewart Baker 和 Matthew Yeo 与国际电信联盟（国际电联）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：电信问题专家会议（日内瓦，1999 年 12 月 9 日和 10 日）的简报文件，第 2 号文件，可查阅 www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html（2008 年 6 月 6 日查阅）。

[94] 不过，考虑到当前的公用钥匙基础设施技术已相当成熟和完善，这些关切问题中，有些已无须像从前那么关注。

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）；[95]

(*b*) *有限的政府介入。* 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，以使其认证令牌（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；[96]

(*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。[97] 另一种方法就是身份管理系统（见上文第 67-77 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配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

93. 在这种模式下，立法规定电子认证方法满足较低的起码要求即可获得某种最低法律地位，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）。[98] 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，授予电子签名与手写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设施技术方面对这类安全签名加以界定。

---

[95] 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。

[96] 见亚洲 – 太平洋经济合作组织的《……评估报告》，以新加坡为例进行了说明。

[97] 见亚洲 – 太平洋经济合作组织的《……评估报告》，以中国和马来西亚为例进行了说明。

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

94. 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法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其需要这一点留给了当事方，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 90-92 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安全的或合格的证书的可能签发者。

95. 让已通过的立法采用两级模式的第一批法域包括新加坡[99]和欧洲联盟。[100]许多其他国家紧随其后。[101]《贸易法委员会电子签名示范法》允许颁布国通过法规建立两级体系，尽管它并没有积极宣传这一体系。[102]

---

[99] 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；以及 (*d*) 和相关的电子记录以某种方式具有联系，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、值得信任的证书所支持的数字签名会被自动视为“安全电子签名”。

[100] 和新加坡《电子交易法》一样，欧洲联盟电子签名指令（《欧洲共同体公报》，L 13/12，2000 年 1 月 19 日）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，附属于或在逻辑上与其他电子数据存在关联的电子形式数据”）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*) 独特地与签名者联系在一起；(*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*) 和数据紧密关联，以致于任何随后的改动都能被发现”）。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，或没有合格证书，或没有经验证的认证服务商签发的合格证书，或并非由一个安全签名生成设备生成”“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“基于合格证书和由安全签名生成设备生成”的高级电子签名才“(*a*) 正如手写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）。

[101] 例如毛里求斯和巴基斯坦。各法规的详细信息见上文注 88。

[102]《贸易法委员会电子签名示范法》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*) 签名生成数据在其所使用的环境中与签名人发生关联，而与任何其他人无关的；(*b*) 签名生成数据在签名时处于签名人的控制之下，而不处在任何其他人控制之下的；(*c*) 凡在签名后对电子签名的一切修改均可被察觉的；以及 (*d*) 要求签名的法律目的是确保签名所涉信息的完整性，而在签名后对该信息的一切修改均可被觉察的。

96. 关于第二级，建议各国不要因为与国际商业交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）。[103] 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

97. 《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，仍不能认为《示范法》的各项原则适用于所有情况。不同法域在电子签名和认证方面采取的态度通常都反映了法域对书面要求采取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

98. 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名要求而采用的鉴别方法是否适当。另外，暗示存在某种手写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。

[103] Baker 和 Yeo，“与认证……有关的背景和问题”。

99. 《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》[104] 第 5 条，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《电子商务示范法》第 13 条。在纸质信函中，问题往往发生在有人指称所称信函创建者的签名有诈。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。

100. 《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。

101. 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。[105] 一些国家明确提及将密码、口令或其他识别手段用作对归属做出推定的要素。[106] 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。[107]

---

[104] 联合国出版物，出售品编号：E.99.V.11，可查阅 http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf（2008 年 6 月 6 日查阅）。

[105] 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）。同样的规则还可查阅下列各地的法律中：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 88。

[106] 墨西哥（见上文注 88），第 90 条第 1 款。

[107] 例如，美国《统一电子交易法》（见注 90）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”。

102. 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。[108] 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。[109] 这些国家的推定是，不需要订立任何具体规则，最好使用与确定纸质文件归属相同的普通取证方法确定归属："对任何签名表示相信的人都必须承担签名无效的风险，这条规则不会因为是电子签名而有所改变。"[110]

103. 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。"[111] 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。"[112] 因此，美国法案的评注指出：

---

[108] 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）。中国香港特别行政区（第 18 条）和英国皇家属地马恩岛（第 2 条）。各项法规的详细信息见上文注 88。

[109] 例如，加拿大、法国、爱尔兰、新西兰和南非。

[110] 加拿大，《统一电子商务法》（附官方评注）（见注 89），对第 10 条的评注。

[111] 美国，《统一电子交易法》（1999 年）（见注 90），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"。

[112] 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名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笺头。有些情况表明，笺头实际上构成签名，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名的归属。在其他情况中，由于未发现必要的意图，因此，传真件笺头无法作为签名。关键一点是，无论有否签名，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人所需的事实。"

“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人。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名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名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。”[113]

104. 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名法律规则的适用，根据此类法律规则，为确定某种行为的效力或证据，必须有签名。一旦确定记录或签名归属于某当事人，“记录或签名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。[114]

105. 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电文在内的电子记录作为证据，似乎采取了放宽限制的做法。[115] 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。[116] 相反，法院认定，原告在法院查询阶段提供的电子邮件电文本身是自我核证的，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

[113] 对第 9 条的官方评注。

[114] 对第 9 条的官方评注第 6 款。

[115] *Commonwealth Aluminum Corporation v. 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) v. 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。

[116] *Sea-Land Service, Inc. v. 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。

结论是正确的。”[117] 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排斥为不可采用的表面证据。

106. 没有采用《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，归属的确定通常是一种对电子签名的法律承认功能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电文作为证据的价值标准，理由是电子邮件电文并不能充分确保完整性。[118] 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口令加以核证的，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，[119] 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。[120] 使用特定媒介发出货物或服务要约的当事人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

---

[117] *Superhighway Consulting, Inc. v. 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。

[118] 德国，波恩地方法院，案件号 3 C 193/01，2001 年 10 月 25 日，*JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*，JurPC Web-Dok. No. 332/2002，可查阅 http://www.jurpc.de/rechtspr/20020332.htm（2008 年 6 月 6 日查阅）。

[119] 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，可查阅 http://www.jurpc.de/rechtspr/20020071.htm（2008 年 6 月 6 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，可查阅 http://www.jurpc.de/rechtspr/20040074.htm（2008 年 6 月 6 日查阅）。

[120] 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，可查阅 http://www.jurpc.de/rechtspr/20020291.htm（2008 年 6 月 6 日查阅）。

归属于某人。[121] 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。[122]

2. 达到法定签名要求的能力

107. 在有些国家，法院往往会对签名要求做出广义的解释。如前文所述（见导言，第 2-4 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，这种情况在一些普通法法域非常典型。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。[123] 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，创建者在电子邮件电文中的署名符合法定的签名要求。[124] 一个人有意选择在所有电子邮件电文的末尾打上其姓名的行为会被视为有效的认证。[125] 美国法院愿意接受那些能够符合书写要求的电子邮件电文及署名，[126] 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书面文件而书写或采用的任何符号”，因此，在某些情况下，“文件中的署名或笺头足以符合签名要求”。[127] 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，法定的签名要求就得到了

---

[121] 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，可查阅 http://www.jurpc.de/rechtspr/20020136.htm（2008 年 6 月 6 日查阅）。

[122] 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，可查阅 http://www.jurpc.de/rechtspr/20020364.htm（2008 年 6 月 6 日查阅）。

[123] *Department of Agriculture and Consumer Services v. Haire*，佛罗里达第四地区上诉法院，案件号 4D02-2584 和 4D02-3315，2003 年 1 月 15 日。

[124] *Cloud Corporation v. 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。

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

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

[127] 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电文不能有效地记录合同条款，而是因为没有明示电子邮件电文的作者和其中所提到的人是被告的雇员。

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”。[128]

108. 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，它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向两方面，考虑媒介的适合度。因此，电子邮件电文就构成了“文件”，电邮电文上的署名可能就是“签名”。[129] 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，就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。”[130] 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主张，主要是因为签名人没有打算受签名约束的意图。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名要求的电子邮件和其中的署名。在某些案件中，据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签署“协议范本”之后而非之前生效的。[131] 在另外一些案件中，法院表示，它们可能倾向于承认“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某人的电子邮件地址”并不是“打算用作签名”的。[132] 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手写签名一样的作用。[133]

---

[128] *Roger Edwards, LLC v. Fiddes & Son, Ltd.*，美国缅因区地方法院，2003 年 2 月 14 日，联邦补充案例，第 2 辑第 245 卷第 251 页。

[129] *Hall v. Cognos Limited*（赫尔劳资争议裁判庭，案件号 1803325/97）（未报告）。

[130] *Mehta v. J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch)，（联合王国、英格兰和威尔士高等法院，大法官法庭），[2006] 2 Lloyd’s Rep 244（联合王国、英格兰和威尔士，Lloyd’s List Law Reports）。

[131] *Pretty Pictures Sarl v. 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，王座法庭判例汇编，[2003] All ER (D) 303（一月））（联合王国，《全英判例汇编》（摘要））。

[132] *Mehta v. J. Pereira Fernandes S.A.* ……。

[133] *Mehta v. J. Pereira Fernandes S.A.* ……，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，要求签名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”。

109. 大陆法系法域的法院普遍倾向于采用较为严格的办法，有人争论说是因为对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“签名”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手写签名。[134] 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。[135]

110. 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手写签名的做法。有越来越多的人使用法律顾问签名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[136] 和联邦法院[137] 均认定，手写签名的扫描图像并不符合现行的签名要求，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。[138] 鉴于联邦其他高等法院一致接受可使用数据电文附签名扫描图像的电子通信手段提交诉讼程序，上述谅解最终被撤销。[139]

---

[134] 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（法国最高法院第二民事法庭，2003 年 4 月 30 日，*Sté Chalets Boisson c/ M. X.*，可查阅 http://www.juriscom.net/jpt/visu.php?ID=239（2008 年 6 月 6 日查阅））。

[135] 法国，Conseil d’État，2001 年 12 月 28 日，No. 235784, *Élections municipales d’Entre-Deux-Monts*（秘书处现有原件）。

[136] 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，可查阅 http://www.jurpc.de/rechtspr/19980009.htm（2008 年 6 月 6 日查阅）。

[137] 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，可查阅 http://www.jurpc.de/rechtspr/19990005.htm（2008 年 6 月 6 日查阅）。

[138] 同上。

[139] 德国联邦最高法院合议庭在就德国联邦法院向其提交的一则案件所作的判决中指出，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，接受使用带有签名扫描图像的数据电文的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，可查阅 http://www.jurpc.de/rechtspr/20000160.htm（2008 年 6 月 6 日查阅））。

111. 有趣的是，据注意到，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设施为基础的数字签名的大陆法系法域的法院，[140] 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确定当事人的身份。[141]

112. 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，一方当事人可能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. 为开发特殊签名形式的等效电子签名而开展的工作

(a) 国际应用：电子加注

113. 2003 年 10 月 28 日至 11 月 4 日，在海牙举行了特别委员会会议，审查《废除要求认证外国公文的公约》(《海牙加注公约》)、《民商事司法和司法外文件国外送达公约》(《海牙送达公约》)[142] 和《关于

---

[140] 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）。

[141] 哥伦比亚，Juzgado Segundo Promiscuo Municipal Rovira Tolima，*Juan Carlos Samper v. Jaime Tapias*，2003 年 7 月 21 日，Rad. 73-624-40-89-002-2003-053-00。法院裁定，尽管电子邮件电文上没有数字签名，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（可查阅 http://www.camara-e.net/_upload/80403--0-7- diaz082003.pdf，2008 年 6 月 6 日查阅）。

[142] 联合国，《条约汇编》，第 658 卷，第 9432 号。

民事或商事外国取证的公约》(《海牙取证公约》)[143] 的实际运作情况。出席《海牙加注公约》、《海牙送达公约》和《海牙取证公约》实际运作问题特别委员会会议的有来自 57 个国家的 116 名代表，这些国家有会员国、所审查的公约中的一部或多部公约的缔约国，也有观察员国。特别委员会强调说，这三部公约的运作环境取决于重要的技术发展。尽管在通过这三部公约时无法预见到这一发展情况，但特别委员会着重指出，现代技术是现今社会不可分割的一部分，使用现代技术是理所当然的。[144] 在这方面，特别委员会指出，这三部公约的精神和字句都不妨碍使用现代技术，而且这三部公约的适用和运作可依靠这些技术得到进一步改善。[145] 特别委员会建议，这三部公约的缔约国和海牙国际私法会议常设局应当努力开发用于生成电子加注的技术，“并特别考虑到贸易法委员会关于电子商务和电子签名的示范法，这两项示范法都以非歧视和功能等同原则为基础。”[146] 2006 年 4 月，海牙国际私法会议常设局和美国国家公证人协会启动了电子加注试点方案。按照这一方案，海牙会议和国家公证人协会正在同感兴趣的国家一道，为下述活动开发、推广和协助实施软件模型：(*a*) 电子加注的发布和使用；(*b*) 电子加注登记的运作。[147] 该方案设想了两个截然不同但在根本上没有区别的电子加注形式。这两种办法都保护基本文件和电子加注证书不受未经授权的修改，只是每种办法向收受人提供的界面不同。

114. 按照第一种办法，主管机关可在已有的基本公共文件的最后一页附上具有特定格式的加注证书（电子加注试点方案设想文件以便携文件格式 (PDF) 进行交换）。收受人打开文件后会看到文件最后一页是电子加注证书。如果选择这种格式，基本公共文件和电子加注证书便构成一个连续文件，或者，换句话说，构成一个独立的电子文件，可以选择打印这一独立文件中的一页或几页，因此可以单独打印电子加注证书。[148]

---

[143] 同上，第 847 卷，第 12140 号。

[144] 海牙国际私法会议“海牙加注、取证和递送公约实际运作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”，第 4 段（可查阅 http://hcch.e-vision.nl/upload/wop/lse_ concl_e.pdf，2008 年 6 月 6 日查阅）。

[145] 海牙国际私法会议“……特别委员会通过的结论和建议”。

[146] 海牙国际私法会议“……特别委员会通过的结论和建议”，第 24 段。

[147] Christophe Bernasconi 和 Rich Hansberger，“电子加注试点项目：签发电子加注的拟议模式的一些潜在技术问题备忘录”，可查阅 http://www.hcch.net/upload/wop/genaff_pd18e2007.pdf（2008 年 5 月 26 日查阅）。

[148] “电子加注试点方案……”，第 18 段。

115. 按照第二种办法，基本公共文件单独作电子加注证书的附件。收受人收到的仍然是一个 PDF 文件，但打开文件时，用户首先看到的是电子加注证书，然后可以打开所附的基本公共文件，作为单独的 PDF 文件查看。据指出，这种办法为加注文件的收受人提供了一个更为直观的界面（例如，美国国务院已经采用这种办法处理电子专利登记，并以此作为电子加注的示范）。之所以将基本公共文件作为电子加注证书的附件，是为了在收受人第一次打开文件时显示其正在处理的是电子加注。然后收受人可以打开基本公共文件，查看其中的内容。[149]

116. 在上述任何一种模式中，电子加注的运作都包括《海牙加注公约》所述的签发由适当主管机关以数字形式签署的电子证书。每个主管机关除此之外都将保留电子形式的登记，用以核实为证明电子加注而签发的证书。[150]

117. 在已经废除认证要求或加注要求的国家，可能会开发系统，用于在核实初始公证人的电子签名或使用的认证方法的基础上，对经过外国公证的记录予以法律认可。初始公证人的电子签名必须是文件用户（通常是另一公证人）能够简便而迅速地核实的。可通过互联网核实，也就是访问初始公证人的认证服务提供者的网站。至少在欧洲，这一提供者通常是公证人所属的国家机构。一个相关的问题关系到核实初始公证人按照管辖其业务的法律制度是否有权对记录进行认证。为了给这一过程提供便利并免于向负责发放公证人执照的外国监督机构（如果有的话）查询，有人建议，在公证人机构的主持下设立的认证服务提供者应仅向目前有权履行公证人职能的公证人签发证书，这样如果公证人的权力被中止或撤销，便自动停止认证该公证人的签名。[151]

---

[149] “电子加注试点方案……”，第 19 段。

[150] 关于电子加注运作问题的更多信息见电子加注试点方案网站 http://www.e-app.info/（2008 年 6 月 6 日查阅）。

[151] Ugo Bechini and Bernard Reynis, “La signature électronique transfrontalière des notaires: une réalit européenne”, *La semaine juridique (édition notariale et immobilière)*），第 39 号（2004 年 9 月 24 日），第 1447 页。

(b) 国内适用：印章、公证和见证

118. 由于在当今社会，印章已不再具有重要意义，故一些法域已经取消了印章要求。经证明（有证人见证）的签名已被取代。[152] 其他一些法域则制定立法，允许以安全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安全电子签名来替代印章。[153] 加拿大规定，安全电子签名若是作为个人印章签署的，即满足某些联邦法律关于个人印章的要求。[154]

119. 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要通过互联网使用安全数字签名技术，并由认证机构签发数字卡片。联合王国的模式是要通过互联网由律师代表其客户签署契约。一些立法正式承认有可能用“电子印章”来代替手盖印章，不过，电子印章形式方面的技术细节还有待单独确定。[155]

120. 美国《统一不动产电子记录法》[156] 明确规定，电子签名不必附带图章、印记或印章的有形或电子图像。从本质上讲，所需要的是印章上的信息，而不是印章本身。该法案还规定，电子签名可以满足要求加盖个人或公司图章、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文件。不过，该法案仍

---

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

[153] 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要求和程序要求。

[154] 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》。

[155] 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，例如关于马尼托巴省专业工程师和地球科学家协会的《工程和地球科学专业法》（加拿大马尼托巴省），其中将“电子印章”定义为由该协会向任何成员签发的、用于以电子方式确认计算机可读文件的一种身份证明形式（见 http://apegm.mb.ca/keydocs/act/index.html，2008 年 6 月 6 日查阅）。

[156] 美国《统一不动产电子记录法》由全国统一州法专员会议编制，可查阅 http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm（2008 年 6 月 6 日查阅）。亚利桑那州、阿肯色州、康涅狄格州、特拉华州、哥伦比亚特区、弗罗里达州、爱达荷州、伊利诺伊州、堪萨斯州、明尼苏达州、内华达州、新墨西哥州、北卡罗来纳州、南卡罗来纳州、田纳西州、得克萨斯州、弗吉尼亚州、华盛顿州和威斯康星州都已通过了这部法案（见 http://www.nccusl.org，2008 年 3 月 20 日查阅）。

然要求必须把在不使用电子签名的情况下包含于图章、印记或印章中的信息以电子方式附在文件或签名上，或者将二者合理地联系起来。[157] 因此，根据该法案进行的电子公证并不要求加盖一些州的法律所要求的公证图章或印记，也无需加盖一些州的法律对于非电子公证所要求的用以证明公司高级职员行为的公司图章或印记。

121. 在大陆法系法域中，印章不常用于私人文件，但这类法域大多广泛利用公证确定人的身份并确保文件的真实性。在一些大陆法系法域，信息和通信技术已经成为公证人的标准工作工具。在许多国家，公证人机构已经设立了认证服务提供者，以签发证书，支持成员公证人（有时还有公众）使用电子签名（通常为数字签名）。

122. 在意大利，公证人理事会于 2002 年 9 月 12 日得到政府信息技术局的授权，为意大利公证人提供认证服务，可在网上验证公证人的数字签名。[158] 此外，意大利公证人正在逐渐改为完全使用电子技术向公共登记处传送记录。例如，向商业登记处传送备忘录和公司章程及其修正的工作已经完全不用纸面文件了。在电子传送涉及不动产的交易记录方面，也取得了很大进展，不过仍然在用纸面文件，据说是因为在法院系统推行电子通信技术的工作有些拖延。1997 年公证人理事会和国家基金会特别设立了一个公司，目的是为意大利公证人提供信息和通信技术服务，上述服务就是在这家公司的支助下提供的。[159] 西班牙使用的系统与之相似，公证人总理事会设立了自己的认证机关，公证人已经建立了以电子方式向贸易登记处提交记录的系统。[160]

123. 在法国，例如《民法》第 1317 条的修订版允许在国务委员会所规定的条件下以电子手段记录“公证书”。法国公证人最高委员会已经为法国公证人使用的数字签名建立了认证系统。[161] 法国政府的若干机构设立了一家公司提供认证服务，法国公证人使用的系统经过了这家公司的认证。法国公证人还没有像意大利和西班牙公证人那么广泛地使用电子方式传输记录，不过 2006 年 5 月开发了

---

[157] 即类似于美国《统一电子交易法》所规定的标准。

[158] 见 http://ca.notariato.it（2008 年 6 月 6 日查阅）。

[159] 见 www.notariato.it，在“Servizi Notartel”栏下（2008 年 6 月 6 日查阅）。

[160] 见 http://www.notariado.org/n_tecno（2008 年 6 月 6 日查阅）。

[161] “La signature électronique notariale certifiée”, *La revue fiscale notariale*，第 10 号（2007 年 10 月），Alerte 53。

Télé@actes 应用程序，公证人应该能够藉此以纯电子方式与抵押登记处相互传送所有权契约。另外还正在将不动产契约的复印件电子化。

124. 在德国，根据 1993 年《加快登记程序联邦法案》，[162] 可以通过电子方式履行房地产登记、商业登记和其他法定登记要求。国家以下各级司法行政机关已经在不同程度上，通过各种技术办法对这一规定加以利用。[163] 实行电子登记制度后，德国公证人得以通过电子通信直接与登记处交流信息。为了确保经公证的电子记录与经公证的纸面记录具有同等程度的可靠性，德国公证人按照《德国电子签名法》的要求设立了认证服务提供者。2000 年 12 月 15 日，德国电信管理部门向认证服务提供者发放了许可。与其他国家的情况一样，德国公证人建立的认证系统以公钥基础设施为基础，使用数字签名技术。联邦公证人公会的认证服务提供者签发的认证不仅认证公证人用以签署文件的公用钥匙，还认证签署人作为宣誓公证人的权力。按照德国制度，数字签名用于在建立和复制记录时证明记录的真实性。联邦公证人公会发布的指导方针提醒公证人必须确保安全传送电子文件，例如只使用有安全套层保护的连接。[164] 为了方便登记处处理电子记录，或方便客户使用电子记录，要求德国公证人编写标准格式的文件（可扩展标记语言 XML）。[165] 德国关于签发真实电子记录的规则要求公证人作双重证明。所有电子记录以及其附件和载有公证人数字签名的文件，都有链接相连，一同存入一个 ZIP 文件，整个 ZIP 文件再以公证人的数字签名证明。

125. 在奥地利，经公证的记录的电子等同文件也得到越来越多的应用。奥地利电子公证系统的基本特点与德国系统的基本特点大体相似。不过，奥地利系统的一个独特之处是，建立了一个中央电子登记处（“cyberDOC”），用于保存电子文件。奥地利民法公证人公会和西门子公司共同成立了一个独立公司，专门向公证人提供具有

---

[162] 德国，Bundesgesetztblatt，第一部分，1993 年 12 月 20 日，第 2182 页。

[163] 见 http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html 关于德国联邦公证人公会实行电子登记的情况（2008 年 6 月 6 日查阅）。

[164] 见“*Empfehlungen zur sicheren Nutzung des Internet*”, Rundschreiben 13/2004 der Bundes-notarkammer vom 12.03.2004（可查阅 http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Internetnutzung.html，2008 年 6 月 6 日查阅）。

[165] 见“*Hinweise und Anwendungsempfehlungen für den elektronischen Handels-, Genossenschafts- und Partnerschaftsregisterverkehr*” Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006（可查阅 http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html，2008 年 6 月 6 日查阅）。

证明功能的电子档案。[166] 法律规定奥地利公证人必须把 2000 年 1 月 1 日以后完成的所有公证契约记录并存储在该档案库中。

126. 一般来说，可以利用电子认证和签名办法，在电子环境中重复公证人对签名进行认证的职能，但其他职能就需要有更为广泛的解决办法。经公证的记录通常必须酌情提及记录的创建日期、登记日期和签署或复制日期。据认为，简单地使用自动技术便可取代公证人认证的日期。[167]

127. 不过，更重要的是以何种程序维持经公证的记录的电子记录。法律通常规定公证人必须将其接收或编写的文件记录备案。在电子环境中复制这种总记录有若干难题。还有一个更为重要的问题，即公证人备案时所用的不同软件和设备可能在技术上互不兼容。由于信息和通信技术的迅速发展，越来越多地需要将数据从一种格式或媒介转换到另一种格式或媒介。但并不一定能保证数据转换到新的格式和媒介后仍然可读。因此有必要设计控制程序，以便能够核实记录内容在转换前后是否完整无损。如前所述，以公钥基础设施为基础的加密技术不一定能确保数字签名本身随着时间的推移保持可读性（见上文第 51 段）。这就需要对转换过程进行严格管理，可能还需要确认最初的认证。据认为，为了确保一致性和互操作性，最好委托可信赖的第三人而非个别公证人来履行这一职能。[168]

128. 例如，法国立法者最终选择了上述模式。最近对经公证的记录所遵守的规则进行了改革，大体规定了经公证的纸面记录和电子记录之间功能等同应符合哪些条件。[169] 在主要涉及信息安全的规定中，新规则规定建立经公证的电子记录的中央档案，确保：电子记录的保存方式能够保持其完整无损；电子记录只能由编制电子记录的公证人查阅；电子记录根据技术需要转换成新格式后内容不变；电子记录能够记录公证人后来提供的信息而不改变最初的内容。

---

[166] 见 Österreichische Notariatskammer (Austrian Chamber of Civil Law Notaries)，可查阅 http://www.notar.at, under “Cyberdoc”（2008 年 6 月 6 日查阅）。

[167] Didier Froger, “Les contraintes du formalisme et de l’archivage de l’acte notarié établi sur support dématérialisé”, La semaine juridique (édition notariale et immobilière)，第 11 号（2004 年 3 月 12 日），第 1130 页。

[168] Didier Froger, “Les contraintes du Formalisme ……”。

[169] 法国。“Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires”, Journal Officiel（2005 年 8 月 11 日）第 96 页。

129. 尽管近年来取得了进展，但仍有人怀疑，对经公证的纸面记录的电子等效记录予以认可的新规则怎样才能与真实文件的基本要素相一致，特别是需要当事人亲自到场办理公证的问题。[170] 假定建立真实的法律记录必须有当事人在场，难题就在于对现有形式进行可能的改变以适应未来技术。[171] 在这方面，据称密码学不能取代代表公共主管机关的有形标志和代表当事人同意的有形标志。[172] 因此，一些规则要求当事人和证人能够实际在屏幕上看见自己的签名；同样，所有记录均应显示公证人的印章。[173]

130. 美国有三部与电子公证有关的主要法规:《统一电子交易法》、[174]《国际和国内商务电子签名法》(《电子签名法》)[175] 和《统一不动产电子记录法》[176]。按照这三部法规的规定，在需要对文件或与文件有关的签名进行公证、确认、核实、见证或宣誓时，该文件或签名若附有经授权实施上述行为者的电子签名和其他适用法律所要求包含的所有其他信息，或与之具有合理关联，则对该文件或与其有关的签名的法律要求即得到了满足。此后，一些州开发了电子公证系统。例如，宾夕法尼亚州务部同一个由县记录员组成的特别小组一道开发了电子公证登记和电子公证印章程序，可利用这一程序对公证进行实时认证，并在网上安全发送经验证的电子公证印章。这一电子公证系统的目的是简化政府官员和企业之间的业务往来，并更有力地保护公众不受造假和诈骗行为的损害，同时保留公证的基本组成要素。该系统使用了商业服务提供者提供的数字认证服务。[177]

131. 有兴趣参加这一电子公证举措的公证人必须向州委员会、选举和立法局提出申请，成为获准电子公证人。公证人必须缴纳费用取得数字证书，证书的形式是电子公证印章，发放证书的认证机关是

---

[170] Pierre-Yves Gautier 和 Xavier Linant de Bellefonds, “De l’écrit électronique et des signatures qui s’y attachent”, *La semaine juridique (édition générale)*， 第 24 号（2000 年 6 月 14 日），I 236, 第 8-10 节。

[171] Pierre Catala, “Le formalisme et les nouvelles technologies”, *Répertoire du notariat Defrénois*，第 20 号（2000 年），第 897-910 页。

[172] Luc Grynbaum, “Un acte authentique électronique pour les notaires”, Communication Commerce électronique，第 10 号（2005 年 10 月），com. 156。

[173] 第 71-941 号法令，经第 2005-973 号法令修正（见注 169），第 17 条第 3 款。

[174] 见注 90。

[175] 已被编撰为《美国法典》第 15 编，第 96 章，第 7001-7031 条。

[176] 见注 156。

[177] Anthony Garritano, “National e-notary standards in progress”, *Mortgage Servicing News*（纽约）第 10 卷，第 2 号（2006 年 3 月 1 日），第 11 页。

得到联邦认证并经过宾夕法尼亚州行政办公室和州务卿核准的，由参加电子公证举措的契约记录员选择。在取得数字证书前，获准电子公证人必须亲自与任何一名参加电子公证举措的契约记录员会面，并向其出示州务部的核准函和符合要求的身份证明。获准电子公证人必须确保，对于每项电子公证，正在公证、认可或核实的电子签名或电子记录都附有以下信息，或与这些信息有合理的关联：电子公证人的全名以及“公证人”字样、电子公证人办公室所在的城市名和县名，以及电子公证人职务期满的日期。电子公证人必须确保办理电子公证的人每办理一次电子公证都亲自到场。宾夕法尼亚州务部表示，公证的基本组成要素仍然适用，包括文件签署人亲自面见公证人。不过已经没有纸面文件和公证印章的橡皮图章，文件的存在形式是计算机可读的电子数据，公证人以数字方式在文件后附上自己的身份信息。[178]

132. 与大陆法系法域相同的是，在英美法系法域，也对能否以电子手段重复传统公证和证明办法的功能进行了讨论。既然公证基本上仅限于确认文件的完整性和签署人的身份，使用电子通信作为纸面文件的等效手段似乎没有无法克服的困难。但是，如果核实文件或记录是否真实的方法是公证人确认核实文件或记录的行为发生时某人在场，情况就没有那么明确了。[179]

133. 有人认为，传统的见证程序，如见证，其使用可能涉及也可能独立于公证人对公共契约的起草，并不完全适用于以电子方式签署文件，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、能够所谓存入信息系统当中的屏幕显示。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

---

[178] 见 http://www.dos.state.pa.us/dos/site/default.asp，在“Notaries”, “Electronic Notarization” 栏下（2008 年 6 月 5 日查阅）)。

[179] “利用现今的技术，位于不同城市甚至不同国家的当事人可以举行‘电话会议’，因此将来‘亲自到场’的法定定义的范围很可能会扩大，位于洛杉矶的公证人可见证从伦敦通过电视播放的签名过程。这类远程电子公证的前提条件似乎是公证人与未到场的签署人的音频交流以及实时取得签署人的视频影像。在这些电子公证行为中，公证人在一地，而认证人或宣誓人在另一地，没有音频交流起码是可以想象的，电子邮件的广泛应用即可证明这一点，但视频互动似乎是必不可少的。否则公证人如何判断远方的签署人没有受到无理胁迫，如何记录视频影像以证明发送人不是利用盗窃的私人钥匙行事的冒名顶替者？ 1984 年，内布拉斯加最高法院（*Christensen v. Arant*）认为，隔着一道门的音频联系不足以成为传统法律意义上的亲自到场，因此仅仅通过非视频媒介进行的电子联系也不足以成为未来法律意义上的亲自到场”（Charles N. Faerber，“在场：亲自面见公证人的重要性”），The John Marshall Law Review，第 31 卷（1998 年春），第 749-776 页）。

按照可信的评价标准，通过可信途径对信息系统进行确认之后，才可能确保屏幕所显示的内容与信息系统的内容一致，才能确保签署人在键盘上输入的内容与其意图一致。[180]

134. 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手写签名更有优势。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。[181]

135. 现有立法还没有发展到完全以电子签名取代见证要求的地步，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，但必须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。[182]

136. 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。[183] 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。[184] 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名，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名，则该声明

---

[180] 这个即文献中所说的“所见即所签”(WYSIWYS) 问题（另见关于可信显示控制器的讨论）。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议事录丛刊》，第 56 卷；及《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。

[181] 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，可查阅 www.agc.gov.sg，在“出版物”项下（2008 年 6 月 6 日查阅）。

[182] 新西兰，《电子交易法》（见注 88），第 23 条。

[183] 加拿大，《个人信息保护和电子文件法》（2000 年），第二部分第 46 条。

[184] 加拿大，《个人信息保护……》，第 45 条。

也可以采用电子形式做出。[185] 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。[186]

[185] 加拿大，《个人信息保护……》，第 44 条。

[186] 撰写转让契据的律师必须从公认认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），可查阅 http://www.cofrestrfatir.gov.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc（2008 年 6 月 5 日查阅）。该项目预计将于 2006 至 2009 年间分期实施。

第二部分

电子签名和认证方法的跨国界使用

目录

一． 对外国电子认证和签名方法的法律承认

137. 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

138. 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降低使用电子通信预计带来的速度和效率上的提高。

139. 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

140. 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）和《联合国国际合同使用电子通信公约》（第 9 条第 3 款）。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。

141. 可以认为，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。

142. 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相关。其中的原因很简单：若法律不赋予某些类型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。

143. 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。

144. 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。

145. 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。[187] 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）信息安全与隐私权工作组（以下称“经合组织信息安全与隐私权工作组”）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。[188] 经合组织信息安全与隐私权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，但问题是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隐私权工作组指出，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隐私权工作组认为，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。*[189] 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隐私权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隐私权工作组在这方面采取的任何举措提供有益参考；

---

[187] Baker 和 Yeo，“与认证……有关的背景和问题”。

[188] 经济合作与发展组织信息安全与隐私权工作组，*The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL)，可查阅 http://www.oecd.org/dataoecd/1/10/35809749.pdf（2008 年 6 月 6 日查阅）。

[189] 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志。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”，可查阅 http://www.cdt.org/privacy/authentication/030513interim.shtml（2008 年 6 月 5 日查阅）。

(*d*) 目前使用的各种认证方法。 经合组织信息安全与隐私权工作组发现，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隐私权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隐私权工作组认为，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。

146. 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。

2. 正在形成的共识

147. 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 2-6 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 83-112 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。[190]

148. 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”[191]，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

[190] Baker 和 Yeo，“与认证……有关的背景和问题”。

[191] Baker 和 Yeo，“与认证……有关的背景和问题”。

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。[192] 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。

149. 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隐私权工作组的发现[193] 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隐私权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。* 虽然几乎所有问卷答复者都指出，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；

(*c*) *公钥基础设施的普遍使用。* 经合组织信息安全与隐私权工作组发现，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。

---

[192] Baker 和 Yeo，“与认证……有关的背景和问题”。

[193] 经济合作与发展组织，*The Use of Authentication across Borders in OECD Countries*……。

150. 另外，经合组织信息安全与隐私权工作组还发现，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（即《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[194]）为基础的。

151. 这种新出现的一致性的基本要点已经在经合组织理事会 2007 年 6 月 12 日通过的关于电子认证的建议中得到重申，该建议除其他外请各国：

(*a*) 合作制定技术中性办法，以便在国内和跨国界环境下对个人和实体进行有效的电子认证；

(*b*) 扶持体现健康商务做法的电子认证产品和服务的开发、提供和使用，包括满足参与者需要的技术性和非技术性保障，特别是在其信息和身份的安全和隐私权方面；

(*c*) 在私营部门和公共部门鼓励各种认证方案在商务和法律上彼此兼容，在技术上具有互操作性，以促进跨部门和跨法域的网上互动和交易，并确保认证产品和服务在国家和国际层面上均可使用；[195]

(*d*) 采取步骤使包括非成员国经济体在内的所有参与者更多地了解电子认证在国家和国际层面上应用的益处。

152. 这些建议大部分符合贸易法委员会在电子商务领域采取的总体办法（例如提供便利而非规范、技术中性、尊重合同自由、非歧视）。不过，还需要解决一些法律问题，才能促进电子认证和签名办法在国际或跨国界环境下的应用。

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

[195]（2007 年 6 月，巴黎），可查阅 http://www.oecd.org/dataoecd/32/45/38921342.pdf（2008 年 6 月 6 日查阅）。

B. 对外国电子认证和签名方法予以承认的标准

153. 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[196]或区域一级的政府间组织[197]及公共部门和私营部门混合组织。[198]

154. 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。[199]但是，这项重要工作在很大程度上主要与技

---

[196] 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。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））， 可查阅 http://www.oasis-open.org/committees/pki/pkiactionplan.pdf（2008 年 6 月 6 日查阅）。

[197] 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）（可查阅 http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf（秘书处现有原件））。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。

[198] 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）。

[199] 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（即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（“白单”），还包括被取消或废除的服务（“黑单”）。（见 http://portal.etsi.org/stfs/STF_HomePages/STF290/draft_ ts_102231v010201p&RGW.doc，2008 年 6 月 6 日查阅）。

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

155. 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。另一个可能性是，要使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。这些做法可结合在一起。[200]

156. 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。[201] 欧洲联盟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。[202] 通过将与欧洲联盟标准实质性等同的要求

---

[200] 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）。

[201] 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”。

[202] 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”。

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。[203]

157. 欧洲联盟电子签名指令第 7 条得到了变通实施。[204] 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，即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

158. 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。

159. 《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》。[205] 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

[203] 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。

[204] Jos Dumortier 等，“The legal and market aspects of electronic signatures”……，第 92-94 页。

[205]《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）。

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。[206]

160. 《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型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。

161. 《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。[207]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。[208]

[206]《贸易法委员会电子签名示范法……》，第二部分，第 83 段。

[207] 同上，第 157 段。

[208] 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）。

二． 确定法律等同性的办法和标准

162. 如上所述，经合组织信息安全与隐私权工作组进行的调查发现，如果符合当地的要求或其等同要求，多数立法框架至少原则上对外国电子签名和认证不加歧视，也就是说，这些立法框架并不否认与外国提供的服务相关的签名具有法律效力，但先决条件是，制作这些签名的条件与国内法所认可的条件相同。[209] 不过经合组织信息安全与隐私权工作组还注意到，承认外国认证服务的机制通常不很发达，因此认定今后似有必要在该领域开展工作。鉴于在该领域的任何工作与互操作性这一更为笼统的题目密切相关，经合组织信息安全与隐私权工作组建议将这些专题合并。该工作组建议似可拟定一套最佳做法或准则。最近，经合组织注意到，已开发出承认外国认证服务的机制，但在跨法域应用方面的经验有限。此外，各法域需要有一些对其伙伴的信任框架进行评估的手段。虽然经合组织表示希望其自己的准则和它们提供的框架在这方面会有所帮助，但该组织指出，需要就这一问题开展更全面的工作。[210] 以下各节论述了有关国际互操作性的法律安排和机制以及赔偿责任制度具有等同性的决定因素。这些章节主要侧重于国际上使用由受托第三方认证服务提供者签发的证书提供支持的电子签名和认证方法所引起的问题，特别是利用公钥基础设施提供数字签名问题，其原因是，跨国界使用电子签名和认证方法因需要第三方参与签名或认证过程，所以更有可能造成法律上的难题。

A. 交叉承认的类型和机制

163. 国内在技术上的要求给外国认证服务提供者造成的额外负担，有可能成为影响国际贸易的一个障碍[211]。举例说，在各国主管机关承

---

[209] 经合组织，*The Use of Authentication across Borders in OECD Countries*……。

[210] *OECD Recommendation on Electronic Authentication* ……，第 27 页。

[211] 见 Alliance for Global Business, “A discussion paper on trade-related aspects of electronic commerce in response to the WTO’s e-commerce work programme”，1999 年 4 月，第 29 页（可查阅 http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf，2008 年 6 月 6 日查阅）。

认外国电子签名和证书所使用的手段方面，相关的法律可能会构成对外国企业的歧视。迄今为止，凡对该问题加以审议的立法机关，均在其法律中列入与外国认证服务提供者所应遵守的标准有关的某种要求，因此，该问题与各国标准互有冲突这一更广的问题是密不可分的。与此同时，法律还可能在地域或程序方面实施其他限制，防止对电子签名予以跨国界承认。

164. 由于国际公钥基础设施的缺失，在承认由外国认证主管机关签发的证书上可能会出现一些问题。对外国证书的承认通常使用了称作“交叉认证”的方法，而其必要条件是，大体等同的认证主管机关（或对其他认证主管机关签发的证书愿意承担某些风险的认证主管机关）承认彼此提供的服务，以便各自的用户能够更为有效地相互通信，并且对所签发的证书的可信度更有信心。涉及多个安全政策的，则在交叉认证或证书信任链方面可能会出现法律上的问题，例如确定因谁处理不当而造成损失以及用户应依赖谁的陈述问题。

1. 交叉承认

165. 交叉承认系互操作性安排，公钥基础设施领域的依赖方可以使用另一公钥基础设施领域的权威信息来认证另一公钥基础设施领域中的对象[212]。为此通常需经过在另一公钥基础设施的领域正式发放许可证或进行资格认可，或者对公钥基础设施领域具有代表性的认证服务提供者进行正式的审计[213]。决定是否信任外国公钥基础设施领域的应当是应用或服务的依赖方或所有人，而不是依赖方直接委托的认证服务提供者。

166. 交叉承认通常是在公钥基础设施层面，而不是在个别认证服务提供者的层面进行。因此，一公钥基础设施承认另一公钥基础设施的，即为自动承认根据该公钥基础设施计划而通过资格鉴定的任何认证服务提供者。承认有赖于对其他公钥基础设施资格鉴定过程展开评价，而不是逐一评价已通过其他公钥基础设施资格鉴定的个别认证服务提供者。公钥基础设施发放多种证书的，则交叉承认过程涉及确定其在这些领域的使用均获认可的一类证书，并以该类证书作为评价的基础。

---

[212] 交叉承认的概念是 2000 年由当时的亚太经济合作电信和信息问题工作组下属电子认证问题专门工作组拟定的（见《电子认证：与其选择和使用有关的问题》，亚太经合组织出版物 202-TC-01.2（2002 年，亚太经合组织），可查阅 http://www.apec.org/apec/publications/all_publications/telecommunications.html（2008 年 6 月 6 日查阅））。

[213] 该定义所依据的是亚太经合组织电信和信息问题工作组下属电子认证问题专门工作组的工作。

167. 交叉承认仅涉及应用一级的技术互操作性问题，即应用必须能够处理外国证书，登陆外国公钥基础设施领域目录系统以查验外国证书的地位。应当指出的是，在实务中，认证服务提供者所发放的证书可靠程度各不相同，确定可靠程度的依据是客户打算使用证书的目的。证书和电子签名的可靠程度有别，所产生的法律效力也就各不相同，无论是在本国，还是在国外。例如，在某些国家，甚至有时被称为“可靠程度低”或“价值低”的证书也可能在某些情况下（例如当事方以合同约定使用这类文书）产生法律效力（见下文第 202-210 段）。因此，能够确定等同性的系在功能上具有可比性的证书。

168. 如上所述，在交叉承认方面，决定是否信任外国证书的是依赖方，而不是其认证服务提供者。交叉承认并不一定要在两个公钥基础设施域之间订立合同或协议。对发证政策[214]和发证做法说明[215]的详细阐述也是没有必要的，因为依赖方决定可否接受外国证书的依据，是证书是否由值得信任的外国认证服务提供者签发。由正式的许可证发放机构发放了许可证的，或通过了资格鉴定机构的资格鉴定的，或者经过受托独立第三方的审计的，才被认为是值得信任的认证服务提供者。依赖方根据外国公钥基础设施域的发证政策或发证做法说明中规定的政策，单方面作出知情决定。

2. 公钥基础设施之间的交叉认证

169. 交叉认证指的是通常以合同的形式承认另一认证服务提供者的公钥达到约定信任程度的做法。交叉认证基本上会导致将两个公钥基础设施域（全部或部分）合并为一个较大的域。对于一认证服务提供者的用户来说，另一认证服务提供者的用户只是外延扩大的公钥基础设施范围内的签名人。

170. 交叉认证涉及技术互操作性问题以及对认证政策和认证做法说明的协调统一。之所以需要以协调统一认证政策和认证做法说明为形式求得政策上的协调统一，是为了确保在其证书管理业务（即证书的签发、中止或撤销）及其遵守类似的运营和安全要求方面，公钥基础设施域均具有兼容性。与此有关的还有赔偿责任所涉数额。这一步骤十分复杂，因为这些文件通常数量庞大并涉及多个问题。

---

[214] 发证政策系列举一套规则，指明证书对有着共同安全要求的特定社区和（或）一类应用所具有的可适用性。

[215] 发证做法说明系认证服务提供者在签发证书时所使用的做法说明。

171. 最适合交叉认证的是相对封闭的商业模式，例如，两个公钥基础设施域共享电子邮件或金融应用等一系列应用和服务。如果系统在技术上兼容和可操作，协调一致的政策和相同的法律结构会大大便利交叉认证。

172. 单方面的交叉认证（即公钥基础设施域的一方信任另一方，但另一方则不然）并不常见。信任方公钥基础设施域必须单方面确保其政策与被信任方公钥基础设施域保持兼容。这种认证的使用似乎限于所涉交易所需的信任为单方面信任的应用和服务，例如，商家必须在客户提交保密信息之前向客户证明其身份的应用。

B. 行为准则和赔偿责任制度的等同性

173. 不论国际上使用电子签名和认证方法所依据的是交叉承认还是交叉认证方法，如果要就承认全部公钥基础设施或一个或多个外国认证服务提供者或者就确定在不同公钥基础设施下所签发的各类证书的等同程度作出决定，都必须首先对国内和外国的认证做法和证书是否具有等同性作出评估[216]。从法律角度来看，这就要求对三大要件之间的等同性作出评估：法律价值的等同性、法定义务的等同性以及赔偿责任的等同性。

174. 法律价值的等同性系指赋予外国证书和签名与国内等同证书和签名相同的法律效力。由此产生的国内法律效力将基本上根据国内法赋予电子签名和认证方法的价值加以确定，对此已经作过论述（见上文第 107-112 段）。承认法定义务和赔偿责任制度具有等同性，必然得出这样的结论：对在公钥基础设施制度下运作的当事方规定的义务实际上与国内制度下的既有义务相同，其就违反这些义务所承担的赔偿责任也基本相同。

175. 电子签名下的赔偿责任可能会产生许多问题，所使用的技术和认证基础设施不同，所造成的问题也就不同。由认证服务提供者等专门的第三方提供认证特别有可能造成一些复杂的问题。这类情况涉及的当事方基本上有三方，即认证服务提供者，签名人和作为第三方的依赖方。任何一方的作为或不作为给其他任何一方造成损害，或违背其明示或默示义务，都有可能承担赔偿责任，或丧失对另一当事方主张赔偿责任的

---

[216] 例如，美国联邦公钥基础设施政策局下设证书政策问题工作组拟定了判断政策各要素之间等同性的方法（以 2527 号意见征求书所界定的框架为依据）。在筹划不同的公钥基础设施或按照这些准则筹划一公钥基础设施时均可使用该方法（见 http://www.cio.gov/fpkipa，2008 年 6 月 6 日查阅）。

权利。在使用数字签名所涉及的赔偿责任问题上，已经采取了不同的立法方针：

(*a*) 对行为准则或赔偿责任不作任何具体规定。一种选择是，法律在该问题上保持沉默。在美国，2000 年《国际和国内商务电子签名法》[217] 未对认证服务所涉任何一方当事人的赔偿责任作出规定。一般而言，大多数对电子签名采取最少干预做法的其他多数法域（如澳大利亚）采用了这种做法；[218]

(*b*) 只针对认证服务提供者的行为准则和赔偿责任规则。另一种做法是，法律仅对认证服务提供者的赔偿责任作出规定。欧洲联盟有关电子签名共同体纲要的第1999/93/EC号指令[219]即采取了这种做法，其中的说明部分 22 称，正如该指令第 6 条所概述，“向公众提供认证服务的认证服务提供者必须遵守有关赔偿责任的国家规则”。值得指出的是，第 6 条仅适用于“合格的签名”，这种签名当下仅指以公钥基础设施为基础的数字签名；[220]

(*c*) 针对签名人和认证服务提供者的行为准则和赔偿责任规则。某些法域对签名人和认证服务提供者的赔偿责任作了法律规定，但未确立依赖方的谨慎标准。中国 2005 年《电子签名法》所作规定即为如此。新加坡 1998 年《电子交易法》所作规定也是如此；

(*d*) 对各方当事人的行为准则和赔偿责任规则。最后一种做法是，法律可对行为准则作出规定，并确定所涉各方当事人的赔偿责任依据。《贸易法委员会电子签名示范法》采取了这种做法，该示范法指明了与签名人（第 8 条）、认证服务提供者（第 9 条）和依赖方（第 11 条）的行为相关的义务。可以说，《示范法》申明了评估这些当事人的行为所依据的标准。但是，《示范法》规定由国内法来确定无力履行各种义务所产生的后果以及可能影响到参与实施电子签名系统的各方当事人的赔偿责任依据。

---

[217]《美国法典》，第 15 编，第 96 章，第 7031 条。

[218] 例如，据认为，得到澳大利亚法律承认的私法机制，例如合同约定的除外情形、弃权和免责声明以及普通法对其实施所施加的限制，均较之于制定法条款更适合规范赔偿责任（见 Mark Sneddon，《法定赔偿责任和电子交易：关于国家电子认证理事会的概括研究》（国家信息经济办公室，堪培拉，2000 年），第 43-47 页，可查阅 http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf（2008 年 6 月 6 日查阅））。

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

[220] 欧洲联盟通过的法律采取了这种做法，例如，《德国电子签名法》(SignatureGesetz-SigG) 和相关的法令 (SigV)、2001 年《奥地利联邦电子签名法》(SigG) 和大不列颠及北爱尔兰联合王国 2002 年《电子签名条例》第 4 条。

176. 在国内赔偿责任制度方面的区别可能会构成电子签名跨国界承认的一个障碍。构成这种障碍的原因主要有两个，首先，认证服务提供者可能不愿意承认外国证书或由外国认证服务提供者颁发的钥匙，因为后者的赔偿责任或谨慎标准可能低于本国的认证服务提供者。其次，电子签名和认证方法的用户也可能担心，降低对外国认证服务提供者的赔偿责任限额或谨慎标准，可能会限制其在出现伪造或冒名依赖等情况下可以利用的救济。出于同样的原因，如果法律对使用电子签名和认证方法或对认证服务提供者的活动作出规定，那么对于外国证书或认证服务提供者的承认，法律通常要求必须就其是否与国内证书和认证服务提供者所提供的可靠性实质上等同作出某种评估。各方当事人必须遵守的谨慎标准和赔偿责任程度构成了衡量等同性的主要法律基准。此外，认证服务提供者能否对其赔偿责任作出限制或加以否认，也将会影响到赋予其证书的等同程度。

1. 公用钥匙基础设施框架下的赔偿责任依据

177. 影响公钥基础设施框架下赔偿责任分配的方式基本上有两种：合同条文或法律（先例、制定法或两者兼备）。认证服务提供者和签名人之间的关系通常由合同约定，因此，赔偿责任通常根据其中任何一方当事人对合同义务的违背来加以确定。签名人和第三方当事人之间的关系将取决于其在任何具体情况下的交易性质。其是否以合同为依据并不确定。最后，认证服务提供者和作为第三方的依赖方之间的关系在多数情况下并不以合同为依据。[221] 在大多数法律制度下，赔偿责任的依据（不论是合同还是侵权法）将会对赔偿责任制度产生广泛的严重后果，尤其是在以下方面：(*a*) 一方承担赔偿责任所必须达到的过失程度（换言之，一方当事人必须对另一方遵行何种“谨慎标准”）；(*b*) 哪些当事人可以主张损害赔偿以及其能够追回多少损害赔偿；(*c*) 过失方是否并且在多大程度上能够对其赔偿责任加以限制或否认。

178. 从上文得出的结论是，赔偿责任标准不仅因国而异，就是在一国内部也会根据应承担赔偿责任的一方与受害方之间关系的性质而有所不同。此外，无论赔偿责任制度是由合同约定的，还是根据普通法

[221] Steffen Hindelang 详细讨论了英国法之下认证服务提供者与第三方建立合同约定关系的可能性，最后得出的结论是否定的 “No remedy for disappointed trust：the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared”，*Journal of Information, Law and Technology*，No. 1，2002，可查阅 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang（2008 年 6 月 6 日查阅）。但在有些法域，可能会有一种合同约定的关系。

或制定法形成的，各种法律规则和理论总会对赔偿责任的这个或那个方面产生影响，有时甚至会缩小两种制度之间的区别。本研究报告无意对这些笼统的问题展开详尽周全的分析，而是侧重于在公钥基础设施的环境下提出的具体问题，并对国内法如何处理这些问题简要加以论述。

(a) 谨慎标准

179. 尽管法律制度不同，所使用的排位系统和理论也就有所区别，但为本研究报告之目的，可以假设公钥基础设施框架所涉各方当事人的赔偿责任基本上以三个有可能成立的标准为依据：一般疏忽或过失；推定疏忽（或举证责任倒置的过失）；和严格赔偿责任。[222]

(i) 一般疏忽

180. 根据这一笼统的标准，法律规定一人必须就其作为造成的不利后果向他人提供赔偿，但先决条件是，其与他人的关系为法律所规定的产生谨慎注意义务的关系。此外，通常所要求的谨慎标准系“合理谨慎注意”，可将其明确界定为具备一般谨慎、知识和预见的人在同样或类似情形下的注意程度。奉行普通法的法域通常将这种标准称之为“理性人”的标准，而某些奉行大陆法的法域通常将这种标准称作“好家长”(*bonus pater familias*) 标准。具体从企业的角度来看，合理谨慎系指具备一般谨慎和能力的人在类似情况下从事相同行业或工作的谨慎程度。如果赔偿责任通常以一般疏忽为依据，则受害方有义务证明损害是由另一方违背其义务的过失所造成的。

181. 合理谨慎（或一般疏忽）系《贸易法委员会电子签名示范法》所设想的一般谨慎标准。这一标准适用于认证服务提供者签发与撤销证书和披露信息的事宜。[223] 在评价认证服务提供者是否遵守其一

---

[222] 有关这方面对赔偿责任制度的论述，见 Balboni，“认证服务提供者的赔偿责任……”，第 232 页及其后各页。

[223]《示范法》第 9 条第 1 款称：“如认证服务提供者提供服务，支持可用作具有法律效力的签名而使用的电子签名，认证服务提供者应当做到如下：[……] (*b*) 采取合理的谨慎措施，确保其作出的关于证书整个周期的或需要列入证书内的所有重大表述均精确无误和完整无缺；(*c*) 提供合理可及的手段，使依赖方得以从证书中证实下列内容：[……]；(*d*) 提供合理可及的手段，使依赖方得以在适当情况下从证书或其他方面证实下列内容：[……]。”

般谨慎标准时，可能会援用若干要素。[224] 相同的标准也适用于签名人防止他人擅自使用和保管签名制作装置。[225]《示范法》将同样的一般合理谨慎标准延伸适用于依赖方，要求其采取合理步骤核实电子签名的可靠性以及证书的效力、中止或撤销，并遵守对证书的任何限制。[226]

182. 通常系《贸易法委员会电子商务示范法》颁布国的一些国家在认证服务提供者的行为问题上采用了一般“合理谨慎”标准[227]。某些国家看来对认证服务提供者“最有可能衡之以普通合理谨慎标准”，尽管认证服务提供者实质上属于具有专门技能的当事人，外行对其的信任超出对普通市场参与方的信任，因此“可能最终赋予其专业地位或以其他方式要求其负有更高的谨慎义务，这种义务就其专业技能而言为合理义务。”[228] 实际上，如上所述（见第 189 段），多数国家的情形似乎即为如此。

183. 关于签名人，采纳《贸易法委员会电子签名示范法》的某些法域规定了一般合理谨慎标准。[229] 各国的法律或多或少均广泛列举了各种积极的义务，同时既未说明谨慎标准，也未指明不履行这些义务

---

[224]《电子签名示范法……》《颁布指南》第 146 段称，“在评估认证服务提供者的责任时，除其他外，还应考虑到下列因素：(*a*) 获得证书所需的费用；(*b*) 所验证的信息的性质；(*c*) 是否存在对证书可能用途的任何限制及其限制范围；(*d*) 是否存在限制认证服务商责任范围或程度的任何声明；(*e*) 依赖方的任何促成行为。在编写示范法时，普遍一致认为，在确定可在颁布国获得补偿的损失时，应侧重于认证服务提供者设立地国或依照有关法律冲突规则而应适用的任何其他国家的法律中有关责任限度的规则。”

[225]《示范法》第 8 条称：“如签名制作数据可用于制作具有法律效力的签名，各签名人应当做到如下：(*a*) 采取合理的谨慎措施，避免他人擅自使用其签名制作数据；(*b*) 在发生下列情况时，毫无任何不应有的迟延，[……] 使用认证服务提供者提供的手段或作出合理努力，向按签名人合理预计可能依赖电子签名或提供支持电子签名服务的任何人员发出通知：(i) 签名人知悉签名制作数据已经失密；或 (ii) 签名人知悉签名制作数据很有可能已经失密的情况”。此外，签名人必须“采取合理的谨慎措施，确保签名人作出的关于证书整个周期的或需要列入证书内的所有重大表述均精确无误和完整无缺”。

[226] 第 11 条，(*a*)、(*b*) (i) 和 (*b*) (ii) 项。

[227] 例如，开曼群岛，2000 年《电子交易法》，第 28 条；泰国，《电子交易法》（2001 年），第 28 条。

[228]“认证机关：赔偿责任问题”，Thomas J. Smedinghoff 为美国银行家协会编拟，1998 年 2 月，第 1.1 节（可查阅 http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf），（2008 年 6 月 6 日查阅）。

[229] 例如，泰国，《电子交易法》（2001 年），第 27 条。

所产生的后果。[230] 但在某些国家，法律在列举义务的同时还就签名人因违背义务而承担的赔偿责任明确作了一般的陈述[231]，此种违背义务在某种情形下甚至构成犯罪[232]。或许可以说不存在单一的谨慎标准，而是有一种相互交错的制度，在签名人的义务问题上，将一般合理谨慎标准作为缺省规则，但是对于某些具体义务则将该标准提升为担保标准，这些具体义务通常与所作陈述的准确性和真实性有关。[233]

184. 依赖方的情形很特别，其原因是，签名人或认证服务提供者都不会因依赖方的作为或不作为而受到损害。在多数情形下，依赖方注意不够的，就必须承担其作为所产生的后果，但不会对认证服务提供者承担任何赔偿责任。因此，在论及依赖方的作用时，国内法有关电子签名的规定很少超出笼统列举依赖方的基本义务，也就不足为奇了。采纳《贸易法委员会电子签名示范法》的法域通常即为如此，该《示范法》提出了针对依赖方行为的合理谨慎标准[234]。但在某些情形下，对这一要求未加明确阐述。[235] 应当指出的是，无论是依赖方的明示义务还是默示义务，对认证服务提供者来说都无关紧要。

---

[230] 例如，阿根廷，《数字签名法》（*2001* 年），第 25 条；开曼群岛，2000 年《电子交易法》，第 31 条；智利，《电子单证、电子签名和电子签名认证服务法》（*2002* 年），第 24 条；厄瓜多尔，*Ley de comercio electrónico, firmas electrónicas y mensajes de datos*，第 17 条；印度，2000 年《信息技术法》，第 40-42 条；毛里求斯，2000 年《电子交易法》，第 33-36 条；秘鲁，*Ley de firmas y certificados digitales*，第 17 条；土耳其，《关于执行电子签名法相关程序和原则的条例》（2005 年），第 15 条；突尼斯，《贸易和电子商务相关法》，第 21 条；委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 19 条。

[231] 中国，《电子签名法》（2004 年颁布），第 27 条；哥伦比亚，《关于电子商务的第 *527* 号法律》，第 40 条；墨西哥，《商务法典：电子签名法令》（*2003* 年），第 99 条；多米尼加共和国，《电子商务、电子单证和电子签名法》（*2002* 年），第 53 和 55 条；巴拿马，《数字签名法》（*2001* 年），第 37 和 39 条；俄罗斯联邦，《联邦电子化数字签名法》（*2002* 年），第 12 条；委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 19 条；越南，《电子交易法》，第 25 条。

[232] 巴基斯坦，2002 年《电子交易法》，第 34 条。

[233] 例如新加坡，《电子交易法》第 88 章）。该法第 37 条第 2 款规定，签名人接受证书，即向所有合理依赖证书中所载信息的人证实：(*a*) 签署人依法持有与证书中所列公钥相应的私钥；(*b*) 签署人向认证机构所作的所有表述和就证书中所列信息而提供的材料均为真实的；(*c*) 签署人所了解的证书中的所有信息均为真实的。而第 39 条第 1 款仅规定，有义务采取合理的谨慎措施，保留对同这类证书中所列公钥相应的私钥的控制权，防止将其披露给未获授权制作签署人数字签名的人。委内瑞拉玻利瓦尔共和国似乎也作了这样的规定，其《数据电文和电子签名法》第 19 条将避免他人擅自使用签名制作装置的义务明确定性为“合理谨慎”义务，而对其他义务则作了明确无误的表述。

[234] 开曼群岛，2000 年《电子交易法》，第 21 条；墨西哥，*Código de Comercio: Decreto sobre firma electrónica (2003)*，第 107 条；泰国，《电子交易法》2001 年），第 30 条。

[235] 土耳其，《关于执行电子签名法相关程序和原则的条例》（2005 年），第 16 条；越南，《电子交易法》，第 26 条。

事实上，依赖方违反其谨慎义务，反倒可以使认证服务提供者得以对依赖方所主张的赔偿责任提出抗辩，譬如说，认证服务提供者能够证明，依赖方如果采取合理措施，查明证书的有效性或证书可能具备的用途，本来可以避免或减轻其所遭受的损害。

(ii) 推定疏忽

185. 第二种可能性是以过失为依据、举证责任倒置的制度。在这种制度下，凡造成损害的原因可以归因于一方当事人的作为，即推定该当事人犯有过失。这种制度存在的基本理由是，通常可推定，在某些情况下，只有一方当事人未履行其义务或遵守预期的行为标准，才有可能在事件的正常演进过程中发生损害。

186. 在大陆法中，对违约责任[236]及其他各种侵权责任均可作出犯有过失的推定。这方面的范例包括对受雇人、代理人、婴儿或动物的行为所承担的替代责任、某种商业或工业活动（环境损害、对相邻财产的损害、交通事故）过程中产生的责任。为举证责任倒置辩护的各种理论和接受举证责任倒置的具体情形因国而异。

187. 在实务中，这类制度所导致的结果类似于普通法期望专业人员遵守的强化谨慎标准。专业人员必须具备作为其所从事的专业的一名成员所需要掌握的最基本的专业知识和技能，并且有义务按照该专业中有理性的成员在特定情况下行事的方式行事。[237]这并不一定意味着举证责任倒置，但期望专业人员有更高的谨慎标准，在实践中就意味着专业人员将被视为有能力避免对以下人员造成伤害，即雇用其服务的人员或如果其根据这些标准行事即可以其他方式将福利交由其负责的人员。但是，在某些情况下，

[236] 例如，《德国民法典》第 280 条第 1 款宣称，债务人对违反合同义务造成的损害承担赔偿责任，除非债务人对违约不负有责任。《瑞士债法》第 97 条第 1 款以更为明确的措辞阐明了这项原则：债权人未争取到履约的，债务人对由此造成的损害承担赔偿责任，除非其能证明未履约并非由于其本人的过失所致。《意大利民法典》第 1218 条载有类似的规则。根据法国法律，合同涉及对某种结果作出承诺的，总是推定过失的存在，但合同的目的系规定履约标准而不是具体成果的，则必须确定过失的存在（见 Gérard Légier，“Responsabilité contractuelle”，*Répertoire de droit civil Dalloz*，第 58-68 号，1989 年 8 月）。

[237] W. Page Keeton 及其他人，*Prosser and Keeton on the Law of Torts*，第五版（Saint Paul，Minnesota，West Publishing，1984），第 32 条，第 187 页。

所谓按照事情本身说明的法律规则，允许法院若无相反证据即可推定，只有一人未能合理谨慎注意，才有可能在“事物的正常演进过程中”发生损害。[238]

188. 该规则若适用于认证服务提供者的活动，即意味着，只要依赖方或签名人因使用电子签名或证书而遭受损害，而且该损害可以归因于认证服务提供者未按照其合同约定或制定法规定的义务行事，即可推定认证服务提供者有疏忽之过。

189. 推定疏忽似乎是在国内法中使用的主要标准。例如，根据欧洲联盟有关电子签名的指令，除非认证服务提供者证明其未疏忽行事，否则对合理依赖合格证书的任何实体，认证服务提供者均将承担损害赔偿责任。[239] 换言之，认证服务提供者所负的赔偿责任以疏忽为依据，举证责任倒置：认证服务提供者必须证明其作为并非疏忽行事，这是因为，认证服务提供者掌握专门技能并有机会获取相关信息（签名人和作为依赖方的第三人可能均未掌握这类技能和信息），因此最有条件提供这种证据。

190. 不属于欧洲联盟的一些国家的国内法所作规定也是如此，这些国家的法律广泛列举了认证服务提供者必须遵守的各项义务，根据这些义务，认证服务提供者通常必须对未遵守其法定义务而造成的任何损失承担赔偿责任。[240] 这些法律是否实际上都要求举证责任倒置，这一点并不十分清楚，但其中有些法律相当明确地规定举证

---

[238] “必须有过失存在的合理证据。如果已证明，所涉事物归被告或其受雇人管理，并且在正常的情况下，如果管理者采取适当的谨慎措施，事故就不会发生，则在被告未作出解释的情况下，即为有合理证据表明，事故因缺乏谨慎所致。”（C. J. Erle in Scott v. *The London and St. Katherine's Docks Co.*, Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)）。

[239]《欧洲共同体公报》，L 13/12，2001 年 1 月 19 日。该指令第 6 条规定了最低赔偿责任标准。颁布国既可建立严格的赔偿责任制度，也可将赔偿责任延伸适用于不合格证书，以此加强认证服务提供者的赔偿责任。但迄今为止尚未实现，而且也不可能实现，其原因是，这将使一国的认证服务提供者处在相对于其他欧洲联盟认证服务提供者较为不利的地位（Balboni，“认证服务提供者的赔偿责任……”，第 222 页）。

[240] 阿根廷，《数字签名法》（*2001* 年），第 38 条；智利，《电子单证、电子签名和电子签名认证服务法》（*2002* 年），第 14 条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第 31 条；巴拿马，《数字签名法》（*2001* 年），第 51 条；突尼斯，《贸易和电子商务相关法》，第 22 条。

责任倒置，要么是泛泛地规定[241]，要么就是针对具体义务作出此种规定。[242]

191. 之所以赞成推定过失的制度，是因为担心以一般疏忽为依据的赔偿责任对依赖方不公平，后者可能既缺乏技术知识，又未掌握相关信息，因此无法履行证明认证服务提供者疏忽行事的责任。

(iii) *严格赔偿责任*

192. 严格赔偿责任即“客观赔偿责任”是各种法律制度用来在未发现过失或违反谨慎义务的情况下确定一人（通常是潜在危险或危害产品或设备的制造商或运营商）赔偿责任的规则。一人只要将有缺陷的产品推向市场或一件设备发生故障，即可推定其负有赔偿责任。由于完全是从损失或损害已经发生这一事实推定赔偿责任，因此无须为确定一项作为（如疏忽、违反保证或蓄意行事）而确定其所必需的个别法律要素。

193. 在大多数法律制度下，严格赔偿责任都是一种例外规则，除法律明文规定外，通常不得作此推定。对于电子签名和认证方法，严格赔偿责任可能会给认证服务提供者施加过重的负担，而这又可能在这一行业的早期发展阶段妨碍其商业上的活力。目前，无论是对认证服务提供者还是对电子签名程序所涉其他任何当事方，似乎没有任何国家规定了严格赔偿责任。的确，在列出认证服务提供者所应承担的各种积极义务的国家，对认证服务提供者的谨慎标准通常定得很高，在某些情况下接近于严格赔偿责任制度，但是，如果认证服务提供者能够证明其已按规定谨慎行事，仍可免除其赔偿责任。[243]

---

[241] 中国，《电子签名法》（2004 年颁布），第 28 条：“电子签名人或者电子签名依赖方因依据电子认证服务提供者提供的电子签名认证服务从事民事活动遭受损失，电子认证服务提供者不能证明自己无过错的，承担赔偿责任”；另见土耳其，《2004 年电子签名法》，第 13 条：“电子认证服务提供者应当对第三方违反本法的条文或根据本法公布的法令而造成的损害承担赔偿责任。电子认证服务提供者证明未犯有过失的，不应承担赔偿责任”。

[242] “在以下情况下，得到授权的认证服务提供者对通过鉴定的证书所提供的信息中出现的错误不承担赔偿责任：(*a*) 由通过鉴定的证书中所指定的人或其代表提供的信息；(*b*) 认证服务提供者能够证明其已采取所有相当符合实际的措施，对该信息加以核实。”（巴巴多斯，308B 章，《电子交易法》（1998 年），第 20 条）；另见百慕大，1999 年《电子交易法》，第 23 条第 2 (*b*) 款。

[243] 例如，在智利、厄瓜多尔和巴拿马。

(b) 有权索赔当事方和可获赔偿范围

194. 在确定认证服务提供者和签名人责任范围上的一个重要问题是，对于任何一方当事人违背其合同约定的义务或法定义务而造成的损害，究竟哪一种人可能有权提出赔偿的主张。另一个相关事项是，提供赔偿的义务范围和应予以赔偿的损害种类。

195. 合同约定的赔偿责任通常随违背合同约定的义务而来。具体到公钥基础设施，签名人和认证服务提供者之间通常会有一个合同。可适用的合同法规定，一方违背其对另一方所承担的合同约定义务究竟会产生何种后果将根据合同的条文确定。关于电子签名和证书，赔偿责任超出明确界定的合同关系的情形通常是，一人因合理依赖认证服务提供者或签名人中任何一方提供的信息遭到损害，而这种信息已证明是虚假的或不准确的。作为依赖方的第三方通常不会与认证服务提供者订立合同，或许除依赖认证外根本就不会与认证服务提供者有任何接触。这就会造成某些法域所无法完全回答的棘手问题。

196. 在大多数大陆法系制度下均可作这样的推定，即对于依赖方因依赖不准确的或虚假的信息而遭受的损失，即便述及电子签名的专门法律未有这方面的具体规定，认证服务提供者仍将承担赔偿责任。在一些法域，这种赔偿责任可能来自大多数大陆法系的法律所颁布的普通侵权赔偿责任条文[244]，但有少数例外情况[245]。在有些法域，认证服务提供者与公证人的活动之间的关系可能存在类似之处，通常认为后者对疏于履行其义务所造成的损害承担赔偿责任。

197. 但普通法法域的情况可能并不十分清楚。在实施受合同管辖的行为时发生侵权的，普通法法域历来要求侵权行为人和受害方之间存在某种合同上的利害关系。由于作为依赖方的第三方未与认证服务提供者订立合同，并且除依赖虚假认证外，或许同认证服务提供者根本就没有任何接触，因此，在某些普通法法域（除了法律明确

---

[244]《法国民法典》第 1382 条规定，凡是人的作为对他人造成损害的，过失方均有义务提供赔偿。其他各国的类似条文即受这一普通赔偿责任规则启发而来，例如《意大利民法典》第 2043 条和《葡萄牙民法典》第 483 条。

[245]《德国民法典》载有三条一般性规定（第 823 I、823 II 和 826 条）和若干条具体规则，后者述及有些定义很窄的复杂情形。主要条文是第 823 I 条，该条与《法国民法典》的区别是，其明确提及对他人“生命、身体、健康、自由、财产或其他权利”的伤害。

规定外），依赖方可能难以确立针对认证服务提供者的诉讼理由[246]。没有合同利害关系的，普通法所规定的侵权诉讼理由则要求证明侵权行为人违反了他对受害方应尽的谨慎义务。认证服务提供者是否对于所有可能的依赖方都有这种义务，并不完全清楚。一般来说，普通法并不愿意规定，某人因出于疏忽作不实陈述而“对类别不定的人承担数额不定、时间不定的赔偿责任”，[247] 除非疏忽之词“是在明知或注意到将会因此而有所行动的情况下向某人直接说出，说话的人与该人存在着由于合同或其他性质的公职而产生的某种义务关系，要求其在必须行事时谨慎行事”。[248]

198. 在此情形下，关键问题是确定认证服务提供者（或在该事项上签名人）对哪些人负有谨慎义务。为了确定在这种情形下哪些范围内的人可以对认证服务提供者提出有效的主张，基本上有三个标准可以使用：[249]

(*a*) *预见性标准。* 这是最为宽松的赔偿责任标准。根据该标准，对于任何可以合理地预见到将依赖虚假陈述的人，签名人或认证服务提供者都将承担赔偿责任；

(*b*) *以意图和知情为依据的标准。* 这是一种范围较窄的标准，将赔偿责任限定于下面这类人所遭受的损失：将从预期提供的信息中获益或获得指导的人或知悉接收人打算提供该信息的人；

(*c*) *利害关系人标准。* 这是范围最有限的标准，创设了一种纯粹对客户应尽的义务或纯粹对信息提供人与其有具体接触的人应尽的义务。

199. 《贸易法委员会电子签名示范法》无意对可能属于“依赖方”的各类人的范围作出限定，其中可能包括“无论是否与签名人或认证服务

---

[246] 例如，针对英国普通法，一位著作者得出的结论是，“若无法律规定，[认证服务提供者] 对 [第三方] 承担的赔偿责任很不确定，然而，[第三方] 预计会因其过失而遭受损失。此外，很难理解 [第三方] 如何能够进行自我保护。如果没有赔偿责任的话，至少有可能存在疏漏，[认证服务提供者] 的过失尤其造成了明显的疏漏。不成文法或许可以弥补这一疏漏，但弥补的程序既不确定，也不可靠”（Paul Todd，电子商务法（Abingdon，Oxon，Cavendish Publishing Limited，2005），第 149-150 页）。针对澳大利亚的法律得出了类似的结论，见 Sneddon，*Legal liability and e-transactions*……，第 15 页。

[247] 在 *Ultramares Corporation v. George A. Touche et al* 案件中法官 Cardozo 说的话，纽约上诉法院，1931 年 1 月 6 日，174 N.E. 441，第 445 页。

[248] 在 *Ultramares Corporation v. George A. Touche et al* 案件中法官 Cardozo 说的话……，第 447 页。

[249] Smedinghoff，“认证机关：赔偿责任问题”……，第 4.3.1 条。

提供者有合同关系的任何人”。[250] 同样，根据《欧洲联盟电子签名指令》，认证服务提供者对“合理依赖”合格证书的“任何实体或法人或自然人”承担损害赔偿责任。欧洲联盟的这一指令显然是围绕公钥基础设施计划制定的，因其只适用于数字签名（合格证书）的情形。实体的概念通常被解释为是指作为依赖方的第三方，从这个意义上说，除两个欧洲联盟成员国外，该指示在其他所有成员国均得到实施。[251]

200. 同《贸易法委员会电子签名示范法》一样，欧洲联盟电子签名指令并未缩小可能有资格成为依赖方的各类人的范围。因此有人建议，即便根据普通法，“在提供认证服务方面，不言而喻的是，对于在特定交易中可能依赖其证书来决定是否接受特定电子签名的任何人，认证服务提供者都应负有谨慎义务，其原因是，签发证书的根本目的就是为了对这种依赖加以鼓励。”[252]

201. 另一个有关问题涉及可从签名人或认证服务提供者那里得到补救的损失的性质。例如，在某些普通法法域，是无法在侵权诉讼中得到对产品瑕疵造成纯经济损失的索赔的。但有人将故意欺诈案件，或甚至有些法域将过失不当陈述视为有关经济损失的规则的例外。[253] 在这方面，耐人寻味的是，联合王国 2002 年《电子签名条例》并未照用欧洲联盟电子签名指令有关赔偿责任的条文，而是适用了有关赔偿责任的标准规则，此处则与损害的邻近关系的检验标准有关。[254] 可获得的损害赔偿额通常可交由普通合同法或侵权法处理。有些法律明确要求认证服务提供者购买赔偿责任保险，或以其他方式向所有潜在签名人公开其或有赔偿责任的财务担保及其他信息。[255]

(c) 以合同方式限制或排除赔偿责任的能力

202. 预计认证服务提供者通常将尽可能寻求限制其对签名人和依赖方的合同赔偿责任和侵权赔偿责任。就签名人而言，责任限制条款通常将载于认证做法说明等合同文件的要素之中。这类说明可对每

---

[250]《贸易法委员会电子签名示范法……》，第 150 段。

[251] 丹麦和匈牙利为例外情况（Balboni，“认证服务提供者的赔偿责任……”），第 220 页。

[252] Lorna Brazell，《电子签名：法律和条例》(London, Sweet and Maxwell, 2004)，第 187 页。

[253] Smedinghoff，“认证机关：赔偿责任问题”……，第 4.5 条。

[254] Dumortier 及其他人，“The legal and market aspects of electronic signatures”……，第 215 页。

[255] 土耳其，2004 年《电子签名法》，第 13 条；阿根廷，《数字签名法》（*2001* 年），第 21 (*a*) (1) 条；另见墨西哥，《商务法典：电子签名法令》（*2003* 年），第 104 (III) 条。

起事故、每批事故或每段时期的赔偿责任的上限作出规定，并将某些类别的损害排除在外。另一种方法是，在证书中列入证书所适用的交易最高价款，或将证书的使用完全限定于某些目的。[256]

203. 尽管大多数法律制度普遍承认合同当事方有权通过合同条文限制或排除赔偿责任，但这种权利通常受到各种限制和条件的约束。例如，在大多数大陆法法域，完全排除一人对其本人过失承担赔偿责任是无法接受的[257]，或者必须对这种排除作出明确的限制。[258]此外，如果合同条款非自由谈判而成，而是由其中一方当事人规定或事先确定（“附合合同”），则某些类型的责任限制条款可能会被认为有“滥用性”并因此而归于无效。

204. 在普通法法域，可从各种理论中得出类似的结果。例如在美国，法院通常不得强制执行被认定为“显失公平”的合同条款。虽然这一概念通常依赖于对个案特定情形的认定，但一般是指这样的合同条款，“一方面，任何有理智的或未受幻觉支配的人不会订立，另一方面，任何公平、诚实之人不会接受”，[259] 这类条款的特点是，“一方当事人缺乏有意义的选择，同时合同条款又对另一方当事人过分有利”。[260] 与“附合合同”这一大陆法概念类似的是，使用该理论是为了防止享有强势议价地位的当事方采取“强卖强销的商业做法”的情况出现。[261] 以这种方式订立的合同条款并非都是无效的。但是，尽管法院通常对在条款上没有议价能力的情形强制执行格式合同或附合合同，甚至对消费合同也不例外，但如果格式合同加入一条款会导致意外的不公平，法院有时也会拒绝执行这类条款。[262]

---

[256] 见 Smedinghoff，“认证机关：赔偿责任问题”，第 5.2.5.4 条；及 Hindelang，“对失信不予救济……”，第 4.1.1 条。

[257] 在法国，原则上可以把违反合同造成的赔偿责任排除在外。但在实践中，法院只要认定有关条款将使当事方免于承担对违反“基本”合同义务的后果，经常裁定此种条款无效（见 Légier，“Responsabilité contractuelle”……，第 262 和 263 号）。

[258] 大多数大陆法国家的法律禁止免除对严重过失或违反公共政策规则规定的义务所造成的赔偿责任。有些国家在这方面有明确的规定，例如《瑞士债法》第 100 II 条和意大利《民法典》第 1229 条。葡萄牙等其他国家未有类似的制定法规则，但所取得的结果与意大利基本相同（见 António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985)，第 217 页）。

[259] *First Financial Ins. Co. v. Purolator Security, Inc.*，388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979)，援引 Hume v. U.S., 132 U.S. 406, 410 (1975)，后者又引自 Smedinghoff 的“认证机关：赔偿责任问题”……，第 5.2.5.4 条。

[260] *First Financial Ins. Co. v. Purolator Security, Inc.* ……，援引 *Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 315, 320 (D.C. 1965)，引自 Smedinghoff 的“认证机关：赔偿责任问题”……，第 5.2.5.4 条。

[261] *First Financial Ins. Co. v. Purolator Security, Inc.*, 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979)，引自 Smedinghoff 的“认证机关：赔偿责任问题”……，第 5.2.5.4 条。

[262] Raymond T. Nimmer, *Information Law*，第 11.12[4][a] 条，11-37，引自 Smedinghoff 的“认证机关：赔偿责任问题”……，第 5.2.5.4 条。

205. 最后，在大陆法和普通法的制度中，在有些情况下，如果赔偿责任限制将实际剥夺签名人享有的为适用法律所承认的权利或救济，保护消费者规则可以大大削弱认证服务提供者限制其对签名人承担赔偿责任的能力。

206. 在大多数情况下，对于认证服务提供者限制其对依赖方承担赔偿责任的可能性，甚至会做出更严格的规定。在封闭式商业模式下，依赖方必须同意合同条款[263]，除了这些模式外，依赖方往往不会由于合同而对认证服务提供者，甚至不会对签名人负有任何义务。因此，万一依赖方对认证服务提供者或签名人提出侵权诉讼，这些当事方可能不具备有效限制其赔偿责任的任何手段，因为大多数法律制度要求将赔偿责任限制的适当通知发给依赖方。在发生损害以前不了解依赖方的身份，可能会妨碍认证服务提供者（可以说更有可能妨碍签名人）建立一个有效限制其赔偿责任的制度。这种问题是开放制度遇到的典型问题，在开放制度下，陌生人在事先没有任何接触的情况下互动，使签名人可能遭受毁灭性后果。[264] 许多人士，特别是认证业的代表认为，由于认证服务提供者难以对其赔偿责任风险作出评价，这种情况是影响推广电子签名和认证方法的一大障碍。

207. 由于期望在这方面对法律作出澄清，许多国家明确承认认证服务提供者有权对其赔偿责任加以限制。例如，根据《欧洲联盟电子签名指令》，欧洲联盟成员国有义务确保认证服务提供者在合格证书中指明“对使用证书作出的各种限制”，只要这些限制“能够为第三方所承认”。[265] 这些限制通常可分为两类：对于可以使用特定证书或特定级别证书的交易类型，可以实施限制；对于与可以使用的证书或证书级别有关的交易价值也可以作出限制。其中任一假设都明确排除认证服务提供者对“超出规定的限制使用合格证书而造成的损害”承担赔偿责任。[266] 此外，《欧洲联盟电子签名指令》授权欧洲联盟成员国确保认证服务提供者“可在合格证书中指明对能够使用证书的交易价值的限制，但先决条件是，这类限制能够为第三方所

[263] 例如，按照美国政府总务管理局所管理的电子认证联合会的设想（见电子认证联合会，临时法律文件系列，第 4.0.7 版，可查阅 http://www.cio.gov/eauthentication/documents/LegalSuite.pdf（2008 年 6 月 6 日查阅）。

[264] Sneddon，“法定赔偿责任和电子交易……”，第 18 页。

[265]《欧洲联盟电子签名指令》，第 6 条第 3 款。

[266]《欧洲联盟电子签名指令》……。

承认。”[267] 在这类情形下，认证服务提供者不应对超出该最高限额所造成的损害承担赔偿责任。[268]

208. 《欧洲联盟电子签名指令》未对认证服务提供者可能承担的赔偿责任设定上限。但该指令的确允许认证服务提供者对可使用证书的每项交易的最高值作出限制，从而排除认证服务提供者对超出该价值上限承担赔偿责任。[269] 作为一则商业惯例，认证服务提供者通常还根据合同约定对其赔偿责任规定了总的上限。

209. 其他一些国内法也支持这些合同约定的做法，承认认证服务提供者对任何受到潜在影响的当事方所承担的赔偿责任是有限制的。这些法律通常允许按照认证服务提供者的认证做法说明中的规定实施限制，在某些情况下，如果证书用于签发证书以外的用途，[270] 则明确排除认证服务提供者承担赔偿责任。此外，有些法律承认认证服务提供者有权签发不同级别的证书并确定所建议的不同可靠度，[271] 这通常根据所支付的费用而规定了不同级别的限额（和担保额）。但除了对证书的使用或证书的价值加以限制外，有些法律明文禁止对赔偿责任实施任何限制。[272]

210. 采取最少干涉做法的国家又会将立法干预视为总体上是不可取的，而主张将该事项交由各方当事人以合同方式加以规范。[273]

---

[267]《欧洲联盟电子签名指令》……，第 6 条第 4 款。

[268]《欧洲联盟电子签名指令》……。

[269] Dumortier 及其他人，“The legal and market aspects of electronic signatures”，第 55 页；另见 Hindelang，“对失信不予救济……”，第 4.1.1 条；Balboni，“认证服务提供者的赔偿责任……”，第 230 页）。进而称，“根据第 6 (4) 条，只能对交易 [……] 的价值加以限制，而这与限制该交易可能产生的损害赔偿潜在数额无关”。

[270] 阿根廷，《数字签名法》(*2001* 年)，第 39 条；巴巴多斯，第 308B 章，《电子交易法》(1998 年)，第 20 条第 3 和 4 款；百慕大，1999 年《电子交易法》，第 23 条第 3 和 4 款；智利，《电子单证、电子签名和电子签名认证服务法》(*2002* 年)，第 14 条；越南，《电子交易法》，第 29 条第 7 和 8 款（但后者未明确排除赔偿责任）。

[271] 新加坡，1998 年《电子交易法》(第 88 章)，第 44 和 45 条；毛里求斯，2000 年《电子交易法》，第 38 和 39 条。

[272] 土耳其，2004 年《电子签名法》，第 13 条。

[273] 有关澳大利亚，见 Sneddon，《法定赔偿责任和电子交易》……，第 44-47 页；有关美国，见 Smedinghoff，“认证机关：赔偿责任问题”……，第 5.2.51 条。

2. 公用钥匙基础设施框架中赔偿责任的特别实例

211. 关于电子签名和认证方法的使用方面的赔偿责任的讨论主要着重于认证服务提供者赔偿责任的基础和特征。据普遍承认，认证服务提供者的基本义务是，使用可靠的系统、程序和人力资源，并按其所作出的关于其政策和做法的表述行事。[274] 此外，认证服务提供者还应当采取合理的谨慎措施，确保其作出的关于证书的所有实质性表述均准确无误和完整无缺。上述所有活动都可能会使认证服务提供者面临不同程度的赔偿责任，视可适用的法律而定。以下段落指出了认证服务提供者面临较大的赔偿责任风险的情况，并概述了各国内法律处理这类赔偿责任的方法。

(a) 不签发或迟延签发证书

212. 认证服务提供者通常在签名申请人提出申请时签发证书。如果申请符合认证服务提供者的标准，认证服务提供者便可签发证书。申请人符合标准却仍被拒绝或延误的情况是有可能发生的，有的是因为认证服务提供者确实出了差错，有的是因为认证服务提供者故意不开放或因意外无法开放申请设施，还有的是因为认证服务提供者出于不可告人的动机，希望延迟或拒绝向申请人签发证书。在上述情况下，被拒绝或延误的申请人可以向认证服务提供者提出索赔。[275]

213. 在有一个竞争性认证服务市场的情况下，一个认证服务提供者因意外或故意拒绝签发证书，可能不会对申请人造成实际的损害。但是，在缺乏有意义的竞争的情况下，如果被拒绝的申请人没有证书就无法开展某种特定的业务，那么认证服务提供者拒绝或迟延签发证书就可能造成严重的损害。即使有与之竞争的其他认证服务提供者，但假设申请人为某一特定交易申请证书，由于延误或被拒绝而无法为想要进行的交易及时取得证书，从而不得不放弃有重大价值的交易，则可以想象特定的交易因这种情况而遭受的损失。[276]

---

[274]《贸易法委员会电子签名示范法……》，第 9 条第 1 款 (*a*) 项和 (*b*) 项。

[275] Smedinghof，“认证机关：赔偿责任问题”……，第 3.2.1 节。

[276] Smedinghof，“认证机关：赔偿责任问题”……，第 3.2.1 节。

214. 上述情形在国际环境中不太可能发生，因为大多数签名人更有可能找位于本国的认证服务提供者提供服务。

(b) 签发证书时出现疏忽

215. 证书的主要功能是将签名人的身份同公用钥匙联系起来。因此，认证服务提供者的主要任务是，按照其表述的做法，证实申请人即为署名的签名人，且掌握着与证书中所列的公用钥匙相对应的私人钥匙。认证服务提供者若未这样做就可能面临对签名人或依赖证书的第三方承担赔偿责任。

216. 例如，如果错误地向盗用身份的冒名顶替者签发证书，就可能对签名人造成损害。认证服务提供者自己的雇员或合同人可能会串通起来，利用认证服务提供者预防冒名顶替者的不当申请的签名钥匙签发错误的证书。这些人还可能因疏忽而错发证书，原因是在审查冒名顶替者的申请时未正确履行认证服务提供者所表述的核实程序，或者使用认证服务提供者的签名钥匙制作了未经核准的证书。最后，犯罪分子可能会使用貌似真实的伪造身份文件冒充签名人，认证服务提供者尽管谨慎而一丝不苟地遵守了其公开阐明的政策，仍然不免上当，向冒名顶替者签发证书。[277]

217. 错误地向冒名顶替者签发证书有可能造成严重的后果。在网上与冒名顶替者进行交易的依赖方可能会依赖错误签发的证书上不正确的数据，而运送货物、划拨资金、发放信贷或进行其他交易，以为与之做交易的是被冒名顶替的一方。等骗局被识破时，依赖方可能已经遭受重大损失。在这种情况下，受到损害的有两方：一方是因错误签发的证书而受骗的依赖方，另一方是在错误签发的证书中身份被假冒的人。这两方都会向认证服务提供者提出索赔。还有一种情形可能是因疏忽而向一个虚构的人签发证书，在这种情况下，遭受损害的只有依赖方。[278]

218.《贸易法委员会电子签名示范法》第 9 条除其他外规定，认证服务提供者应当采取合理的谨慎措施，确保其作出的关于证书整个有效期的或被列入证书内容的所有实质性表述均准确无误和完整

[277] Smedinghof，“认证机关：赔偿责任问题”……，第 3.2.1 节。

[278] Smedinghof，“认证机关：赔偿责任问题”……，第 3.2.1 节。

无缺。执行《示范法》的若干国家的国内法已经原封不动地列入了这项一般性义务，[279] 但某些国家似乎将合理的谨慎这一标准提高到了保证的标准。[280]

219. 《欧洲联盟电子签名指令》所建立的制度要求欧洲联盟各成员国“最低限度地”确保，认证服务提供者应在向公众签发合格的证书或为该证书向公众提供保证时，在以下几个方面对合理地依赖该证书的任何实体、法人或自然人承担损害赔偿责任：(*a*) 合格证书在签发时所载的所有信息的准确性以及该证书实际载有合格证书按规定应载有的所有详细信息；(*b*) 保证在证书签发时，合格证书上指明的签名人持有与证书中所提供或指明的签名核实数据相应的签名制作数据；(*c*) 保证在认证服务提供者生成签名制作数据和签名核实数据的情况下，这两种数据可互补使用；但认证服务提供者证明自己没有疏忽行事除外。[281]

220. 其他国内法一般不约而同地规定认证服务提供者有义务核实签发证书所依据的信息的准确性。在一些国家中，一般认定认证服务提供者自经正式认可的证书签发之日起，应在该证书所含全部信息的准确性方面，对合理依赖证书的任何人负有赔偿责任，[282] 或为其准确性作出“保证”，[283] 不过在其中一些国家认证服务提供者可以通过在证书中列入一条适当的声明来限定这一保证。[284] 但一些法律明确规定，认证服务提供者只要根据验证惯例声明进行了核实，对签名人提供的不准确信息便不承担赔偿责任，条件是认证服务提供者能够证明其采取了一切合理措施对信息进行了核实。[285]

---

[279] 例如，泰国《电子交易法》（2001 年）第 28 条第 2 款；以及开曼群岛（英属海外领土）2000 年《电子交易法》，第 28 (*b*) 条。

[280] 例如，中国《电子签名法》第 22 条：“电子认证服务提供者应当保证电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项”，标出了强调部分。

[281]《欧洲联盟电子签名指令》……，第 6 条第 1 款。

[282] 巴巴多斯，《电子交易法》（1998 年），第 308B 章第 20 条第 1 (*a*) 款；百慕大，1999 年《电子交易法》，第 23 条；中国香港特别行政区，《电子交易条例》，第 39 条；印度，2000 年《信息技术法》，第 36 (*e*) 条；毛里求斯，2000 年《电子交易法》，第 27 条第 2 (*d*) 款；新加坡，《电子交易法》，第 29 条第 (2)(*a*) 和 (*c*) 项和第 30 条第 (1) 项。

[283] 突尼斯，《贸易和电子商务相关法》，第 18 条；越南，《电子交易法》，第 31 (*d*) 条。

[284] 例如巴巴多斯、百慕大、中国香港特别行政区、毛里求斯和新加坡。

[285] 阿根廷，《数字签名法》（*2001* 年），第 39 (*c*) 条。

221. 还有一些国家不是通过法定保证，而是通过规定认证服务提供者一般有义务在签发证书之前核实签名人所提供的信息，[286] 或有义务建立核实此类信息的系统，[287] 来达到与上文相同的结果。在一些情况下，若发现所签发的证书所依据的信息是不准确或虚假的，有义务立即撤销证书。[288] 但在少数情况下，法律对证书的签发不作规定，仅要求认证服务提供者遵守其验证惯例声明 [289] 或按照与签名人的约定来签发证书。[290] 这并不表示法律没有考虑到认证服务提供者的任何赔偿责任。相反，一些法律明确设想了认证服务提供者的赔偿责任，其中要求认证服务提供者购买第三方赔偿责任保险，该保险应足以涵盖在合同内外对签名人和第三方所造成的损害。[291]

222. 认证服务提供者核实所提供信息的准确性的义务是以签名人的下述义务为补充的："采取合理的谨慎措施，确保签名人作出的关于证书整个有效期的或需要列入证书内的所有实质性表述均准确无误和完整无缺。"[292] 因此可以认定，签名人若在申请证书时向认证服务提供者提供了虚假或不准确的信息，须对认证服务提供者或依赖方承担赔偿责任。这有时表述为一种向认证服务提供者提供准确信息的一般性义务，[293] 或采取合理的谨慎措施确保信息准确的一般性义务；[294] 有时明确说明签名人未遵守这一特定要求须对因此而造成的损害承担赔偿责任。[295]

---

[286] 阿根廷，《数字签名法》（*2001* 年），第 21 (*o*) 条；智利，《电子单证、电子签名和电子签名认证服务法》，第 12 (*e*) 条；墨西哥，《商务法典：电子签名法令》（*2003* 年），第 104 (I) 条；和委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 35 条。

[287] 厄瓜多尔，《电子商务、电子签名和数据电文法》，第 30 (*d*) 条。

[288] 阿根廷，《数字签名法》（*2001* 年），第 19 (*e*)(2) 条。

[289] 秘鲁，《关于电子签名和电子证书法的条例》，第 29 (*a*) 条。

[290] 哥伦比亚，《关于电子商务的第 *527* 号法律》，第 32 (*a*) 条；多米尼加共和国，《电子商务、电子单证和电子签名法》（*2002* 年），第 40 (*a*) 条；巴拿马，《数字签名法》（*2001* 年），第 49 条第 7 款。

[291] 委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 32 条。

[292] 《贸易法委员会电子签名示范法……》，第 8 条，第 1 款 (*c*) 项。

[293] 阿根廷，《数字签名法》（*2001* 年），第 25 条；智利，《电子单证、电子签名和电子签名认证服务法》（*2002* 年），第 24 条；墨西哥，《商务法典：电子签名法令》（*2003* 年），第 99 (III) 条。

[294] 开曼群岛，2000 年《电子交易法》，第 31 (*c*) 条。

[295] 哥伦比亚，《关于电子商务的第 *527* 号法律》，第 40 条；多米尼加共和国，《电子商务、电子单证和电子签名法》（*2002* 年），第 55 条；墨西哥，《商务法典：电子签名法令》（*2003* 年），第 99 (III) 条；巴拿马，《数字签名法》（*2001* 年），第 39 条。

(c) 擅自使用签名或破坏验证惯例声明

223. 擅自使用签名制作办法和证书有两个方面，一方面，签名制作装置可能没有得到适当的保管或因其他原因而失密，如被签名人的代理人盗用。另一方面，认证服务提供者的签名实际层级系统可能失密，例如，认证服务提供者自己的签名钥匙或根钥匙丢失，或被透露给未经授权的人或被未经授权的人使用，或因其他原因而失密。

224. 签名层级系统失密的方式可能多种多样。认证服务提供者、其雇员或合同人可能意外破坏钥匙或失去对钥匙的掌控，持有私人钥匙的数据中心可能意外受到破坏，或者认证服务提供者的钥匙可能被某人为了非法目的（如黑客）而故意毁坏或泄密。签名层级系统失密的后果可能会十分严重。例如，如果私人签名钥匙或根钥匙落入罪犯手中，他会伪造证书并使用这些证书假冒真正的或虚构的签名人，给依赖方造成损失。此外，认证服务提供者一旦发现有损坏，必须撤销所签发的所有证书，这可能导致签名人因失去使用权而集体大规模提出索赔。

225. 这一事项在《贸易法委员会电子签名示范法》中没有详细述及。可以说，《示范法》所规定的认证服务提供者“使用可信赖的系统、程序和人力资源提供其服务”[296]的义务可以解释为规定认证服务提供者有义务采取一切必要措施预防其自身的钥匙（进而预防其整个签名层级系统）失密。一些国内法明确规定了这种义务，通常将其与认证服务提供者使用可信赖的系统的义务结合在一起。[297]有时规定了采取措施避免伪造证书这一具体义务。[298]认证服务提供者有义务避免制作或接触签名人的签名制作数据，还可能因其雇员故意这样做而承担赔偿责任。[299]认证服务提供者往往有义务在其签名制作数据失密的情况下要求撤销自身的证书。[300]

---

[296] 第 9 条第 1 款 (*f*) 项。

[297] 阿根廷，《数字签名法》（*2001* 年），第 21 (*c*) 和 (*d*) 条；哥伦比亚，《关于电子商务的第 *527* 号法律》，第 32 (*b*) 条；毛里求斯，《2000 年电子交易法》，第 24 条；巴拿马，《数字签名法》（*2001* 年），第 49 条第 5 款；泰国，《电子交易法》（2001 年），第 28 条第 6 款；突尼斯，《贸易和电子商务相关法》，第 13 条。

[298] 委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 35 条。

[299] 阿根廷，《数字签名法》（*2001* 年），第 21 (*b*) 条。

[300] 阿根廷，《数字签名法》（2001 年），第 21 (*p*) 条。

226. 还要求签名人采取一切适当的谨慎措施。例如，《贸易法委员会电子签名示范法》要求签名人“采取合理的谨慎措施，避免他人擅自使用其签名制作数据”。[301] 多数国内法规定了类似的义务，但有一些不同之处。在某些情况下，法律严格规定签名人有义务确保单独控制签名制作办法并预防其被擅自使用，[302] 或使签名人完全负责保护签名制作装置的安全。[303] 但这项义务往往被界定为保持充分控制签名制作装置或采取充分措施保持控制签名制作装置的义务，[304] 或努力避免擅自使用，[305] 或采取合理的谨慎措施避免其签名装置被擅自使用。[306]

(d) 未中止或撤销证书

227. 认证服务提供者还可能因未中止或撤销已经失效的证书而承担赔偿责任。为使数字签名基础设施正常发挥职能并得到信任，关键是有一个到位的机制，实时判断某一证书是否有效，或该证书是否已被中止或撤销。例如，每当私人钥匙失密时，冒名顶替者可能已经获得了私人钥匙的拷贝，因此，撤销证书是签名人避免冒名顶替者进行欺诈交易的首要机制。

228. 因此，认证服务提供者在接到签名人请求后撤销或中止签名人证书的速度是至关重要的。从签名人请求撤销证书到实际撤销证书并发布撤销通知这段时间内，冒名顶替者就有可能进行欺诈交易。因此，如果认证服务提供者无故延迟，不把已撤销的证书及时放到

---

[301] 第 8 条第 1 款 (*a*) 项。

[302] 阿根廷，《数字签名法》(*2001* 年)，第 25 (*a*) 条；哥伦比亚，《关于电子商务的第 *527* 号法律》，第 39 条第 3 款；多米尼加共和国，《电子商务、电子单证和电子签名法》(*2002* 年)，第 53 (*d*) 条；巴拿马，《数字签名法》(*2001* 年))，第 37 条第 4 款；俄罗斯联邦，《联邦电子数字签名法》(2002 年)，第 12 条第 1 款；以及土耳其，《关于执行电子签名法的程序和原则条例》(2005 年)，第 15 (*e*) 条。

[303] 突尼斯，《贸易和电子商务相关法》，第 21 条。

[304] 智利，《电子单证、电子签名和电子签名认证服务法》(*2002* 年)，第 24 条；越南《电子交易法》，第 25 条第 2 (*a*) 款。

[305] 委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 19 条。

[306] 开曼群岛，2000 年《电子交易法》，第 39 (*a*) 条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第 17 (*b*) 条；印度，2000 年《信息技术法》，第 42 条第 1 款；毛里求斯，《2000 年电子交易法》，第 35 条第 1 (*a*) 和 (*b*) 项；墨西哥，《商务法典：电子签名法令》(*2003* 年)) 项；墨西哥，《商务法典：电子签名法令》(2003 年)，第 99 (II) 条；新加坡，《电子交易法》(第 88 章)，第 39 条；泰国，《电子交易法》(2001 年)，第 27 条第 1 款。

撤销清单上，或没有这样做，签名人和受骗的依赖方可能会因依赖了所谓的有效证书而遭受重大损失。此外，作为其认证服务的一部分，认证服务提供者可主动维持网上储存库和证书撤销清单供依赖方查阅。维持这一数据库有两个基本风险：一个风险是，数据储存库或证书撤销清单可能不准确，因而会提供错误信息，而信息接受人可能会因依赖错误信息而遭受损失；还有一个风险是，数据储存库或证书撤销清单可能无法查阅（如由于系统故障），从而妨碍签名人和依赖方完成交易。

229. 如前文所述，《贸易法委员会电子签名示范法》假定认证服务提供者可签发各种等级的、可靠程度和安全程度不一的证书。因此，《示范法》不要求认证服务提供者始终保持撤销系统可供查阅，因为对某些类型的“低价值证书”来说，这在商业上可能是不合理的。《示范法》仅要求认证服务提供者提供“合理可及的手段”，使依赖方得以从证书中主要证实以下两点：是否存在签名人发出通知的途径，通知签名制作数据已经失密；以及是否开设及时的撤销服务，[307] 如果开设了及时的撤销服务，认证服务提供者有义务确保其可供使用。[308]

230. 《欧洲联盟电子签名指令》所确立的制度要求欧洲联盟各成员国“最低限度”确保向公众签发了合格证书的认证服务提供者，若未对撤销证书的情况进行登记，便应当对合理地依赖证书的任何实体、法人或自然人因此而遭受的损失承担赔偿责任，除非该认证服务提供者证明其并未疏忽行事。[309] 一些国内法规定认证服务提供者有义务采取措施防止伪造证书的行为[310]，或在发现签发的证书所依据的是不准确或虚假的信息时立即撤销证书。[311]

231. 签名人和其他有授权的人也可能有类似的义务。例如，《贸易法委员会电子签名示范法》要求签名人在知悉签名制作数据已经失密或知悉签名制作数据很有可能已经失密的情况时，毫无任何不应有的迟延，使用认证服务提供者所提供的手段或作出其他合理的努力，向按签名人合理预计可能依赖电子签名或提供支持电子签名服务的任何人员发出通知。[312]

---

[307] 第 9 条，第 1 (*d*)(v) 和 (vi) 项。

[308] 第 9 条，第 1 (*e*) 项。

[309]《欧洲联盟电子签名指令》……，第 6 条第 2 款；另见该指令附件二 (*b*) 段。

[310] 巴拿马，《数字签名法》（*2001* 年），第 49 条第 6 款。

[311] 阿根廷，《数字签名法》（*2001* 年），第 19 (*e*)(2) 条。

[312] 第 8 条第 1 (*b*)(i) 和 (i) 项。

232. 国内法律常常认定签名人有义务在签名制作数据可能已经失密的任何情况下请求撤销证书，[313] 但在某些情况下，法律仅要求签名人有义务将该项事实告知认证服务提供者。[314] 一些国家的法律已经采用了《贸易法委员会电子签名示范法》的表达方式，规定签名人有义务进一步通知按签名装置持有人合理预计可能依赖电子签名或提供支持电子签名服务的任何人员。[315] 一些法律制度可能暗示了违反该义务的后果，但某些国家的法律明确说明签名人若未通报对私人钥匙失去控制一事或未请求撤销证书，应承担赔偿责任。[316]

结论

233. 电子认证和签名方法的广泛应用可能是在国际交易中减少贸易文件和降低相关费用的重要一步。虽然在很大程度上来说，该领域的发展速度主要取决于技术解决办法的质量和安全性，但法律可以为便利电子认证和签名方法的使用作出重要的贡献。

234. 许多国家已经朝这个方向采取了国内措施，通过了承认电子通信法律价值的立法，并为其与纸质通信的等同性制定了标准。规范电子认证和签名方法的条款常常是这类法律的一个重要组成部分。《贸易法委员会电子商务示范法》成为该领域立法的唯一最具影响力的标准，其广泛执行已经对促进国际上高度的统一协调有所助益。随着对《联合国国际合同使用电子通信公约》的广泛批准，将有一套特别的国际交易规则，带来更大的协调统一。

---

[313] 阿根廷，《数字签名法》（*2001* 年），第 25 (*c*) 条；哥伦比亚，《关于电子商务的第 *527* 号法律》，第 39 条第 4 款；多米尼加共和国，《电子商务、电子单证和电子签名法》（*2002* 年），第 49 条和第 53 (*e*) 条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第 17 (*f*) 条；毛里求斯，《2000 年电子交易法》，第 36 条；巴拿马，《数字签名法》（*2001* 年）第 37 条第 5 款；新加坡，《电子交易法》（第 88 章），第 40 条；俄罗斯联邦，《联邦电子数字签名法》（2002 年），第 12 条第 1 款。

[314] 印度，2000 年《信息技术法》，第 42 条第 2 款；和土耳其，《关于执行电子签名法的程序和原则的条例》（2005 年），第 15 条 (*f*) 和 (*i*) 项。

[315] 开曼群岛，2000 年《电子交易法》，第 31 (*b*) 条；中国，《电子签名法》，第 15 条；泰国，《电子交易法》（2001 年），第 27 条第 2 款；越南，《电子交易法》，第 25 条第 2 (*b*) 款。

[316] 中国，《电子签名法》，第 27 条；多米尼加共和国，《电子商务、电子单证和电子签名法》（*2002* 年），第 55 条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第 17 (*e*) 条；巴拿马，《数字签名法》（*2001* 年），第 39 条；俄罗斯联邦，《联邦电子数字签名法》（2002 年），第 12 条第 2 款；委内瑞拉玻利瓦尔共和国，《数据电文和电子签名法》，第 40 条。

235. 国际上对电子认证和签名方法的使用也可能因上述贸易法委员会标准的通过而受益。特别是，《联合国国际合同使用电子通信公约》中所载的电子签名和纸面签名功能等同的灵活标准可以提供一个国际共同框架，使电子认证和签名方法得以满足国外形式的签名要求。但是，某些问题可能会继续存在，特别是在电子认证和签名方法的国际使用方面，它要求在认证或签名过程中有值得信赖的第三方参与。

236. 这一特定领域中出现的各种问题在很大程度上是因为技术标准不一致或者设备或软件不兼容，因而缺乏国际互操作性。统一标准并改善技术兼容性的努力可能会为目前存在的难题找到一种解决办法。但是，还有一些与电子认证和签名方法有关的法律难题，特别是在一些国内法律方面。这些国内法律规定或主张电子签名使用某种特定技术，通常是数字签名技术。

237. 规定了数字签名法律价值的法律通常也赋予外国证书所支持的签名同样的法律价值，但以这些外国证书被认为等同于国内证书为限。在本次研究中所做的审查表明，对法律等同性的适当评估要求不仅对某一特定签名技术所附带的技术和安全标准进行比较，还要对管辖各有关当事人的赔偿责任的规则进行比较。《贸易法委员会电子签名示范法》提供了一套基本的通用规则，管辖认证和签名程序所涉及的各方当事人的某些可能对其各自的赔偿责任有影响的义务。另外还有区域性的文书，如《欧洲联盟电子签名指令》，为在该区域运营的认证服务提供者的赔偿责任提供了类似的立法框架。但是，这些文本都没有涵盖因国际上使用某些电子认证和签名方法而出现的所有赔偿责任问题。

238. 立法者和决策者必须理解各种国内赔偿责任制度之间的区别和共同要素，以便为承认外国证书所支持的签名拟定适当的办法和程序。各个国家的国内法律因为具有共同的法律传统或属于一个区域性统一框架等原因，可能已经对本出版物中讨论的各种问题做出了大体上等同的回答。这些国家可能认为拟定共同的赔偿责任标准或甚至统一其国内规则是有益的，这样可有利于跨国界使用电子认证和签名方法。

United Nations publication
ISBN: 978-92-1-730178-0
Sales No. C.09.V.4

FOR UNITED NATIONS USE ONLY

Printed in Austria
V.08-55697—March 2009—210