联合国 A/CN.9/630/Add.1

大会

Distr.: General
25 April 2007

Chinese
Original: English

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

今后可能在电子商务领域开展的工作

关于建立健全的电子商务法律框架所需要素的综合参考文件：国际使用电子认证和签字方法的章节样本

秘书处的说明*

增编

本说明附件包含了关于国际使用电子认证和签字方法法律问题的综合参考文件章节样本的一部分（第一部分，第一章第 B 和 C 节）。

* 联合国国际贸易法委员会秘书处对本文件的提交因人员不足而延迟。

V.07-82779 (C) 260607 270607

附件

目录

第一部分

电子签字和认证方法

[…]

一、电子认证和电子签字的定义和方法

[…]

B. 电子签字和认证的主要方法

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

1. 依靠公用钥匙加密的数字签字

2. “数字签字”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。数字签字有许多不同形态，诸如失败一终止数字签名、盲签名和不可抵赖数字签字。

(a) 技术概念和术语

(一) 加密

3. 数字签字采用加密技术创建和核查;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。数字签字使用所谓的“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)。[1] 其中一套钥匙用于产生数字签字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字或将电文还原为原有形态。[2] 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”。

---

[1] 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。

[2] 使用加密技术是数字签字的主要特征之一，但不应将用数字签字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，创建一个数字签字，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字可能仅仅是附加于一则未加密的电文之后而已。

（二）公用钥匙和私人钥匙

4. 用于数字签字的互补钥匙称作“私人钥匙”，它仅供签字人用以创建数字签字，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字。这种私人钥匙可能保留在智能卡上，或可以通过个人识别码（密码）检索，或者理想的情况是通过生物统鉴别装置，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字人的数字签字，公用钥匙就必须提供或分发给他们中每个人，具体做法，例如，在签字上附上证件，或采取其他方式确保依赖方，确保只有不得不核查签字的人才能获得有关证件。这两套成对钥匙具有数学联系，但如果为了安全，设计和实施非对称密码系统，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。[3]这样，许多人可能知道某个签字人的公用钥匙而且用它来核实签字人的签字，但却不能发现该签字人的私人钥匙并用它来伪造数字签字。

（三）散列函数

5. 除了生成密钥对之外，在创建和核实数字签字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“指印”）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”，知道电文的散列值就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字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字后未被修改。

（四）数字签字

6. 为了签署一份文件或任何其他的信息项目，签字人首先精确划定拟签字的内

[3] 某些现有的标准提及“计算无法实行”，来描述预期的进程的不可扭转性，即，希望不会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，这些因素必须在目前和未来的技术进步基础上进行评估。”（美国律师协会，《数字签字指导方针：验证局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，可在以下网页进行查阅 http://www.abanet.org/scitech/ec/isc/dsgfree.html，2007年4月5日可以使用）。

容范围。然后，签字人软件中的散列函数为拟签字的信息计算其独有的（就所有实用技术而言）的散列结果。签字人的软件接着使用签字人的私人钥匙将散列结果转变为数字签字。所产生的数字签字因此为所签字的信息和用以创建数字签字的私人钥匙所独有。典型的情况是，数字签字（用签字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。由于数字签字为电文所独有，如果与原电文永久脱离联系，就毫无用处了。

（五）数字签字的核查

7. 数字签字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字进行检查的过程，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字。在核查数字签字时，还通过用于创建数字签字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，核对数字签字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字过程中转变为数字签字的原散列结果相配对。

8. 在下列情况下，核查软件将加密的角度确认数字签字得到了“核查”：（a）用签字人的私人钥匙对电文进行数字签字，用签字人的公用钥匙核查签字时，即认为属于此种情况，因为签字人的公用钥匙将只核查采用签字人的私人钥匙创建的数字签字；（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字析取的散列结果相一致时，即认为属于此种情况。

（六）数字签字技术的其他用途

9. 如上所述，数字签字技术比只以手写签字签署文件的方式“签署”电子信件有更为广泛的用途（见第[…]段）。确实，经电子签字的证书通常用于“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。数字签字技术还可以用来“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）公用钥匙基础结构和认证服务供应商

10. 为了核查数字签字，核查人必须取得签字人的公用钥匙，而且保证它与签字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，因为签字人和经电子签字的信件接收人之间

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种程度的信任。

11. 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，可能很难证明公有钥匙的实际所有人是否真的将钥匙发给了接收人。

12. 未来的签字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字，应作为出自该签字人之手的签字对待。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字属于某个特定的签字人。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字人不利，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字的凭空否认（常在电子签字的“不可抵赖性”环境下提到的一个问题）。

13. 解决这其中某些问题的一个办法是利用一个或多个受到信任的第三方将认定的签字人或签字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，该受信任的第三方一般称做“验证局”、“验证服务商”或“验证服务供应商”（在《贸易法委员会电子签字示范法》[4] 中选用了“验证服务商”一语）。在若干国家中，这类验证局现正按等级编组成常常所称的公用钥匙基础结构。公用钥匙基础结构中的验证局可以按照等级编组成立，因为一些验证局只能证明其他的一些直接向用户提供服务的验证局。在这样的编制下，一些验证局是其他验证局的下属。在其他可能的编制下，所有的验证局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结构中，可能同时会有下级验证局和上级验证局。其他解决办法包括，例如，依赖方颁发的认证。

[4] 见注[...] [联合国出版物出售品编号 E.02.V.8]。

（一）公用钥匙基础结构

14. 建立公用钥匙基础结构是一种方法，用以使人们信任下列几点：（1）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；（2）使用的加密技术是可靠的；为令人产生上述信任，公用钥匙基础结构可以提供多种服务，其中包括：（1）管理用于数字签字的加密钥匙；（2）验证一套公用钥匙对应于一套私人钥匙；（3）为最终用户提供钥匙；（4）公布公用钥匙或证书的保密目录；（5）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创建和存储个人的私人钥匙；（6）核实最终用户的标识并向它们提供服务；（7）提供时间标记服务；以及（8）在获准使用加密钥匙时，管理用于保密性加密的加密钥匙。

15. 公用钥匙基础结构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结构而考虑的模式涉及下列层次：（1）一个独一无二的“总局”，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，并对下属的验证局进行登记；[5] （2）多个验证局，置于“总局”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）；（3）多个地方登记机构，置于验证局之下，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。

16. 在多层次权力结构内组建起来的公用钥匙基础结构是可扩缩的，因为它们只要通过“总局”与新社区的“总局”建立一种信任关系将整个新的公用钥匙基础结构社区包含在内。[6] 新社区的总局可以直接被纳入公用钥匙基础结构的接收方，从而成为该公用钥匙基础结构的下属验证服务商。新社区总局也可以成为现有公用钥匙基础结构内某一个下属验证服务商的下属验证服务商。多层次的权力结构公用钥匙基础结构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，多层次的权力结构公用钥匙基础结构的验证道路相对比较短，用户则明白应该在权力结构内验证服务商立场基础上将一个验证作何应用。但是，多层次的权力结构公用钥匙基础结构也有不利之处，主要是依赖于一个单一的信任点的缘故。如果总局被泄露，则整个多层次的权力结构公

[5] 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局一级进行解决。

[6] William T. Polk 和 Nelson E. Hastings，《桥梁验证局：连接企业间公用钥匙基础结构》，国家标准和技术研究所（2000 年 9 月），http://csrc.nist.gov/pki/documents/B2B-article.pdf，2007 年 3 月 30 日可以使用。

用钥匙基础结构也随着被泄露。此外，一些国家发觉很难选择一个单一的实体作为总局，并向所有其他的验证服务商施加多层次的权力结构。[7]

17. 所谓的“网状”公用钥匙基础结构是多层次公用钥匙基础结构的一个备选。在这一模式下，验证服务商之间以主客兼任的关系相互联系。这一模式下的所有验证服务商都可以成为信任点。一般情况下，用户会信任发布证书的验证服务商。验证服务商之间彼此发布证书，这些证书描述相互的信任关系。此种系统缺乏多层次的权力结构，意味着验证服务商不能施加管理由其他验证服务商发布的证书的条件。如果一家验证服务商欲限制向其他验证服务商提供的信任，它必须在向其同伴所发布的证书中明确说明这些限制。[8]但是，协调条件和相互承认可能是一个相当复杂的目标。

18. 第三个替代结构是“桥梁”验证服务商。这一结构可能在使各种已有公用钥匙基础结构社区相互信任彼此的证书中特别有用。与“网状”公用钥匙基础结构不同的是，“桥梁”验证服务商并不直接向用户发布证书。公用钥匙基础结构的用户也不会将“桥梁”验证服务商当作信任点，如“总”验证服务商那样。相反，“桥梁”验证服务商与不同的用户社区建立起了主客兼任的信任关系，从而使用户能够在其各自的公用钥匙基础结构内保持其自然的信任点。如果一个用户社区执行了一个多层次公用钥匙基础结构形式的信任域名，则“桥梁”验证服务商将与该公用钥匙基础结构的总局建立关系。但是，如果用户社区通过创建一个网状公用钥匙基础结构而执行了一个信任域名，则“桥梁”验证服务商将仅需与其中的一位公用钥匙基础结构验证服务商建立关系，因为此时这一服务商已经成为该公用钥匙基础结构内为了与另一公用钥匙基础结构建立“信任桥梁”的“主要”验证服务商。通过两个或两个以上与“桥梁”验证服务商有互相关系的公用钥匙基础结构将其结合起来的“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”验证服务商开展互动。[9]

（二）验证服务商

19. 为使配对钥匙与未来的签字人联系起来，验证服务商（或验证局）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字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持有人联系在一起。证书的“接收人”如果希

[7] Polk 和 Hastings （见注[6]）指出，在美国，很难在州政府中单独划出一个机构来担任联邦公用钥匙基础结构的全部授权。

[8] Polk 和 Hastings, 桥梁验证局…… （见注[5]）。

[9] “桥梁”验证服务商是最终被选为美国联邦政府成立公用钥匙基础结构系统的结构（Polk 和 Hastings，见注[6]）。这也是日本政府建设公用钥匙基础结构系统所遵循的模式。

望依赖证书中标明的持有人所创建的数字签字，可利用证书中所列的公用钥匙验查数字签字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，则可以保证数字签字是由证书中标明的公用钥匙持有人所创建的，而且散列函数中所载电文（即对应的数据电文）经数字签字后未被改动过。

20. 为了保证证书的内容和来源的真实性，验证服务商给证书加上数字签字。签发证书的验证服务商在证书上的数字签字可以采用由另一个验证服务商签发的另一份证书中列出的该验证服务商的公用钥匙来核查（这另一个验证局可以是上级机构，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，直至依赖于数字签字的个人对其真实性确信无疑为止。把数字签字记录在验证服务商签发的证书（有时被称为“总”证书）上，也是核查数字签字的可能采取的方法。[10]

21. 在每一种情况下，签发证书的验证服务商可以在另一用来核查验证服务商数字签字的证书操作期内，在其自己的证书上进行数字签字。根据一些国家的法律，对验证服务商的数字签字建立信心的一种方法是在官方公告中公布验证服务商的公用钥匙或有关总证书的某些数据（诸如“数字指印”）。

22. 与电文相应的数字签字，不管是签字人为了认证电文而创建的，还是验证服务商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，以使查验人能够可靠地确定数字签字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，未在废止列表中提及），因为这是能否查验数字签字的一个条件。

23. 为使公用钥匙及其与具体持有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字。

24. 证书一旦签发，可能证明并不可靠，例如签字人向验证服务商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足够的可靠性，但之后过段时间就可能变得不可靠了。例如，由于签字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，验证局（按签字人的请求或甚至不经签字人的同意，视情况而定）可能中止（暂时中断操作期）或废止（使永久无效）证书。在中止或废止证书以后，验证服务商一般必须立即公布关于废止或中止的通知，或通知那些查询有关事项的人或那些已由验证服务商所知收到按不可靠证书核查数字签字的人。同样地，适当时也应对验证服务商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签字的证书与向时间标记当局发布证书的验证局的证书。

[10] 《大会正式记录，第五十六届会议，补编第 17 号》和更正（A/56/17 和 Corr.3），第 279 段。

25. 验证局可由政府机构运作，或由私营部门的服务商运作。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验证局。但是，在大多数国家，验证服务或者是完全由私营部门的验证服务商运作，或者是政府运作的验证服务商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验证服务商。在一些国家，国有的验证服务商只发布公共管理部门所使用的数字签字证书。不管验证局是由公共实体还是私营部门的服务商运作，也不管验证局是否需要许可证进行运作，在公用钥匙基础结构中一般都有一个以上的验证服务商。一个特别令人关切的问题是各种验证局之间的关系（见上面第[15]-[18] 段）。

26. 验证服务商或总局可能有责任保证其政策条件持续不断地得到满足。验证局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，但任何验证服务商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验证服务商实行的责任制度，即验证服务应持续不断地执行总局或上级验证服务商的政策和保密要求，或任何其他适用的要求。同样重要的是，验证服务商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字示范法》第 9 条第 1（a）段所设想的那样。

（c）公用钥匙基础结构实施过程中的切实问题

27. 尽管拥有对数字签字技术及其运作方式的丰富知识，但是，公用钥匙基础结构和数字签字计划在实际实施的过程中面临着一些问题，使数字签字的运用水平低于原先的期望。

28. 数字签字可以作为查验在证书有效期间创建的签字的办法。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，即使密钥对未失密也是如此。因此，公用钥匙基础结构计划将需要一套数字签字管理体系来确保一段时期内提供签字。造成主要困难的风险是，即包括电子签字在内的“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，或“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。实际上，数字签字可能变得不安全，原因在于加密分析的科学进展、签字查验软件可能在长时间内不可获得或文件失去其完整性。[11] 这通常会使电子签字的长时期保留成为问题。尽管数字签字在一段时期内被认为是档案记录所必须的，但是实际经验

[11] Jean-François Blanchette，《定义电子认证：一场跨学科的旅行》，可在以下网页查阅 http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf， 2007 年 4 月 5 日访问（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。

表明，数字签字并非不会受长期风险的影响。既然在创建签字之后对记录的每一次修改都将导致签字查验的失败，那么，为将来保留一份清晰记录的操作重组（诸如“移徙”或“转换”）可能会影响签字的持久性。[12] 实际上，数字签字更多地被认为是为信息传播提供安全，而不是为了长时间地保存信息。[13] 针对这一问题的举措还未找到一个长久的解决办法。[14]

---

[12] “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）。基于公用钥匙基础结构的数字签字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，比如手写签字、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，《电子签字和受托挡案服务》，第 5 页，可在以下网页进行查阅：http://www.law.kuleuven ac.be/icri/publications/172DLM2002.pdf?2007 年 4 月 5 日访问。

[13] 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可靠记录的国际研究（InterPARES）项目，目的在于“长期保存创建的和（或）以电子形式保存的可靠记录所必须的理论和方法知识”（见 http://www.interpares.org，2007 年 4 月 5 日访问）。作为项目第一阶段一部分的可靠性问题工作队的决议报告（InterPARES 1，2001 签署）表明，“数字签字和公用钥匙基础结构（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可靠性的一种手段”（着重部分由作者标明），可在以下网页进行查阅：http://www.interpares.org/documents/atf_draft_final_report.pdf，2007 年 4 月 5 日访问。关于电子系统永久可靠记录的国际研究（InterPARES 1）项目最终报告可在以下网页查阅：http://www.interpares.org/book/index.htm. 项目 （InterPARES 2）继续实施，旨在制定并明确定义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。

[14] 例如，由信息和通讯技术标准委员会于 1999 年成立的欧洲电子签名标准化组织（EESSI），是一个关于在信息和通讯技术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字指令的执行（见注[…] [欧洲委员会正式期刊，L 13/12]）。EESSI 联合会（寻求将欧洲关于电子签字的指令转化为欧洲标准的努力）力求满足确保长期保存加密过的文件的需求，办法是通过其自身的关于电子签字格式（电子签字格式 ES 201 733, ETSI, 2000）的标准。该格式对签字测定有所区分：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使用的信息，诸如废止信息、时间戳、签字政策等等。这种信息是在最初的测定阶段收集的。这些电子签字格式的设计者担心的是由于加密强度的减弱而对签字测定所造成的安全威胁。为了防止加密强度的减弱，EESSI 签字会定期用最新的加密分析方法重新加印时间戳。关于软件寿命的问题已经在 EESSI 在 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”这一新型的将由有关机构提供的商业服务，其目的在于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，除其他外，“后向兼容性”，办法是通过维护设备和（或）仿真（见 Blanchette，《定义电子可靠性》（见注[12]））。比利时鲁汶大学法律和信息技术跨学科中心关于 EESSI 有关受托档案服务建议的后续研究，题目为《欧洲电子签字标准倡议：受托档案服务》（第 3 阶段，最后报告，2000 年 8 月 28 日），可在以下网页进行查阅 http://www.law.kuleuven.ac.be/icri/publications/91TAS- Report.pdf?where=, 2007 年 4 月 12 日访问）。EESSI 于 2004 年 10 月关闭。执行这些建议的系统目前似不再运作当中（见 Dumortier 和 Van den Eynde，《电子签字和受托档案服务》（见注[13]）。

29. 数字签字和公用钥匙基础结构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。验证服务商必须安全保存用于在其客户证书上签字的钥匙，因为外人可能会企图未经核准利用钥匙（见下面第 […]-[…]段第二部分）。此外，验证服务商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。验证服务商必须储存这一信息，以备日后之用。验证服务商必须采取必要的措施，以确保根据适用的数据保护法律查阅此种信息。[15]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

30. 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、指印、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。

31. 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，将储存在参考模板上的生物测定数据与从终端用户处收集的数据进行比较，以供查验。这样就可能表明是否实现了身份的识别或查验。[16]

32. 生物测定设备的性质包含必须给予适当考虑的独特特征。这些特征可能与选作参考的特征有所不同，它们的存在对该技术是否适合预定用途有重要影响。

33. 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。

---

[15] 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）可在以下网页查阅：http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html， 2007 年 2 月 7 日访问；《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），可在以下网页进行查阅：http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm，2007 年 2 月 7 日访问；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），可在以下网页查阅： http://193.194.138.190/html/menu3/b/71.htm，2007 年 2 月 7 日访问；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），可在以下网页查阅 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett，2007 年 2 月 7 日访问。

[16] 国际生物测定学会 （iAfB）和国际计算机安全协会（ICSA），《1999 年生物测定术语词汇》 ，可在以下网页查阅：http://www.afb.org.uk/docs/glossary.htm，2007 年 2 月 7 日访问。

34. 生物测定技术的精确性不是绝对的，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精确性。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精确性在绝大多数的商业适用中是足够的。

35. 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[17]尽管不一定明确提到生物测定，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。[18]此外，可能需要采取措施保护消费者免受因私下使用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。[19]

36. 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上可以防备未经核准查阅数据；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及披露、审核、问责和监督。[20]

37. 公认，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，特别是执法应用程度上，诸如入关查验和进出控制。

38. 商业应用程序也已开发出来，常常在需要提供控制个人的要素（生物测定技术）和个人所知要求（一般为密码或 PIN）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字特征的应用程序。基于数字的签字笔书写板记录了签字过程的运笔压力和持续时间。然后，把这些数据作为算法储

[17] 见注[15]。

[18] Paul de Hert，《生物测定技术：法律问题及意义》，欧洲联盟委员会未来技术研究所背景文件（欧洲共同体，总司联合研究中心主管，2005 年）第 13 页，可在以下网页进行查阅：http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf。

[19] 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》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））。

[20] 比如，最佳做法见“国际生物测定技术组生物隐私倡议”、“注重隐私的生物测定技术最佳做法”，可在以下网页进行查阅： http://www.bioprivacy.org。

存起来，用来与将来的签字比较。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。

39. 如果用生物测定签字替代手写签字，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不同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数据的可能性。

40. 《贸易法委员会电子签字示范法》[21]和《贸易法委员会电子商务示范法》，[22] 以及最近的联合国《国际合同使用电子通信公约》[23]规定的一般可靠性测试，可以适用于生物测定签字。为确保统一性，制定关于生物测定技术使用和管理的国际指导方针可能也是有用的。[24]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略显草率和不成熟进行认真审议。

3. 密码和混合方法

41. 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，因为在未经加密的信件传输中会有失密的风险。但是，密码和代码是各种交易，包括多数网上银行业务、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。

42. 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，供认证的签字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，可以在因特网上传输密码，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电子签字（非对称加密技术），在收到该电子签字后会生成一张 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，如同那些

---

[21] （见注[...]） [联合国出版物，出售品编号 E.02.V.8]。

[22] （见注[...]） [联合国出版物，出售品编号 E.99.V.4]。

[23] 联合国《国际合同使用电子通信公约》由联合国国际贸易法委员会第三十八届会议最后敲定（维也纳，2005 年 7 月 4 日至 15 日），后来由联合国大会于 2005 年 11 月 23 日正式通过（大会第 60/21 号决议，附件），可在以下网页进行查阅： http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html。

[24] 这些可以与载于《贸易法委员会电子签字示范法》执行指导方针中所述的可靠性标准相比较（见注 […]） [联合国出版物，出售品编号 E.02.V.8]，第 75 段。

侧重于可以阻止使用复合技术的专门技术一样。[25]技术中立规定将促进对此种混合技术办法的接受。

4. 扫描签名和原始姓名

43. 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字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字技术。

44. 在日常活动中，全世界的公司通常都满足于电子邮件往来，除了在邮件下方打上姓名、标题和地址外，未使用任何形式认证或签字。有时候会使用手写签字的传真或扫描图像，赋予更正式的外观，但这只不过是手写原件电子形式的一个副本而已。但是，在不加密电子邮件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信件原件的身份。但是，为了通信的方便、快捷和高效，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字时，必须铭记这些普遍商业做法。对电子认证和签字的严格要求，特别是采用一种特殊的技术方法，可能会在不经意间使人对每日没有使用任何认证或签字的交易的有效性和可执行性产生怀疑。反过来，这可能导致有关各方质疑其电子通信可靠性，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字要求，最终会使有关各方每天都使用，是不切实际的。最近使用电子签字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字技术的实际运用。

C. 电子身份管理*

45. 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这些服务时，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。身份和账户的增加，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。

46. 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。身份管理，对提

---

* 这一小节可以在综合参考文件最终版本中进行进一步阐述。

[25] 信息政策研究基金会应欧洲联盟委员会的要求编写的《签字指令协商汇编》，1998 年 10 月 28 日，汇编了在欧洲联盟关于电子签字指令草案协商过程中所作的答复。可在以下网页进行查阅：www.fipr.org/publications/sigdirecon.html，2007 年 4 月 12 日访问。

供商来说，益处包括提高安全性、使照章办事更简便，使商业更灵活；对用户而言，益处可能包括获取信息更方便。

47. 身份管理可以联系两种办法来描述：基于智能卡及其相关数据的传统用户使用模式（登录），用户通过智能卡和相关数据进行登录，以获取信息；以及更具创意的、基于一个为用户及其设备提供个性化服务的系统的服务模式。

48. 身份管理的用户使用办法，侧重于在一个或多个应用程序和系统中对用户认证、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机密信息不被未经核准的用户所使用。

49. 在服务模式办法下，身份管理的范围变得更为广泛，包括公司提供在线服务使用的所有资源，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。

50. 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。实际上，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。另一方面，商业应用程序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。

51. 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另一个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精确性，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。[26]现在还制定了指导方针，为遵守信任圈基础结构规定了法律要求。[27]

---

[26] 见 《关于电子政府中身份管理的方式研究：身份管理问题报告》 （欧洲联盟委员会，总司信息社会和媒体，2006 年 6 月），第 9-12 页，可在以下网页进行查阅： https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf。

[27] “图书馆联盟项目” （见 www.projectliberty.org） 是一个由全球 150 多家公司、非营利性组织和政府组织组成的联盟。它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。

52. 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动传播身份、身份联合会以及执行的通用[身份管理]框架和手段”。[28]

53. 目前还在电子政务的背景下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”倡议背景之下，启动了一项关于电子政府中身份管理的研究，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府身份管理方面找到一种协调统一办法。[29]

54. 在电子政府倡议背景下以智能卡形式发放电子签字设备正在变得日益常见。除其他外，在比利时[30]和爱沙尼亚全国范围内都已经启动了智能卡的发放。结果，除其他事项外，许多公民都以很低的费用获得了安全电子签字设备。虽然这些倡议的主要目标可能不是商业性的，但是这些设备也同样可以用于商业世界。两个适用领域的会合正在逐渐被承认。[31]

---

[28] 见 http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html。

[29] 见 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi。

[30] 见 http://eid.belgium.be/en/navigation/12000/index.html。

[31] 见，比如，《2006 年韩国因特网白皮书》 （首尔，韩国国家因特网发展局，2006 年），第 81 页，提到了《大韩民国电子签字法》对电子政府和电子商务的双重使用，可在以下网页进行查阅：http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1。