联 合 国 A

大 会

Distr.
GENERAL

A/CN.9/WG.IV/WP.71
31 December 1996
CHINESE
ORIGINAL: ENGLISH

联合国国际贸易法委员会
电子商业工作组
第三十一届会议
1997 年 2 月 18 日至 28 日，纽约

电子商业问题今后工作的规划: 数码式签字、验证局和有关法律问题

秘书长的说明

目 录

目　录（续）

目　　录（续）

导　言

1．在《贸易法委员会电子商业示范法》通过以后，委员会根据电子数据交换工作组在其第三十届会议上进行的初步讨论（A/CN.9/421，第109-119段），在委员会第二十九届会议上讨论了电子商业领域今后的工作。人们普遍认为，贸易法委员会应继续工作，编制能够给电子商业带来可预测性，从而加强各地区贸易的法律标准。

2．就未来工作可能的主题和优先事项提出了一些新的建议。其中一项建议是，委员会应着手编制关于数码式签字的规则。有人说，数码式签字法的制定，连同确认“核准当局”（以下称为“验证局”）的行动或授权就数码式“签字”的电文的来源和归属签发电子证书或其他形式保证的其他个人的行动的法律，在许多国家被认为是发展电子商业必不可少的条件。有人指出，依靠数码签字的能力将是通过电子媒介发展订立合同业多及转让货物权利或其他权益的关键。在若干法域内，目前已在制定管理数码式签字的新的法律。据报告称，这种法律的发展已经互不统一。如果委员会决定开展这一领域的工作，它将有机会协调这些新的法律，或至少确立电子签字领域的共同原则，从而为这种商业活动提供一个国际基础结构。

3．相当多的人表示支持这项建议。不过，人们普遍感到，如果委员会决定通过其电子数据交换工作组开展数码式签字领域的工作，它应当赋予工作组明确的任务。人们还感到，由于贸易法委员会不可能开始从事技术标准的制定工作，它应当注意不卷入数码式签字的技术问题。有人忆及，工作组在其第三十届会议上认识到，可能需要验证局方面的工作，而且这种工作也许需要从登记处和服务提供者的角度开展。但是，工作组也认为，它不应当着手进行关于是否适用某种标准的任何技术性工作（A/CN.9/421，第111段）。有人表示担心说，关于数码式签字的工作可能超出贸易法范围，而且还可能涉及民事法或行政法的一般问题。有人在答复时指出，《示范法》的条款也是这种情况，委员会不应当回避编制有用的规则，因为这种规则在商业关系领域之外或许也有用。

4．根据工作组初步讨论提出的另一项建议是，今后的工作应把重点放在服务提供者上。与会者提及以下各点，作为在服务提供者方面可能审议的问题：在无当事方协定情况下的履约的最低限度标准；终端当事方承担风险的范围；这种规则或协定对第三方的影响；无执照营业者行动或其他未经授权

的行动所带来的风险的分配方法；以及在提供增值服务时可能有的强制性担保或其他义务的范围（见 A/CN.9/421，第 116 段）。

5．大家普遍认为，贸易委员会审议服务提供者、用户和第三方之间的关系将是合适的。有人表示，务必应使这种工作的方向放在发展该领域商业行为的国际准则和标准，其目的是通过电子媒介支持贸易，而不是着眼于建立服务提供者的管理制度或可能给电子数据交换市场应用造成无法接受的费用的其他规则（见 A/CN.9/421，第 117 段）。不过，人们还感到，服务提供者这个专题可能范围太大，覆盖太多不同的实际情况，因而不能作为单一的工作项目处理。与会者普遍认为，关于服务提供者的问题在工作组所审议的每个新工作领域的范畴内加以处理会比较适当。

6．另有一项建议是，委员会应当开始制定新的一般性规则，这些规则需要用来澄清传统的合同功能如何能够通过电子商业来履行。有人说，在电子商业的范围内，“履约”、“交货”和其他条款的含义将有许多不确定之处，在电子商业情况下，报价和接受及产品交货可能在横跨全球的开放式计算机网络上进行。以计算机为基础的商业及在互联网络和其他系统上进行的交易的迅速增长，已使这项工作成为优先的议题。有人建议，由秘书处进行一项研究可能澄清此项工作的范围。如果委员会在对这项研究报告审议后决定进行这项工作，其中的一种选择做法将是把这些规则收入《贸易法委员会电子商业示范法》的“特别规定”部分之内。

7．还有一项建议是，委员会应当集中注意以提及方式列入条款的问题。有人回顾，工作组曾商定，这一议题将放在关于登记处和服务提供者问题这种较一般的工作范围内适当地解决（A/CN.9/421，第 114 段）。委员会普遍同意，这个问题可以在关于验证局的工作范畴内处理。

8．委员会经过讨论后认为，将数码式签字和验证局的问题列入委员会的议程是适当的，但必须借此机会处理工作组建议作为今后工作的其他议题。委员会还商定给予工作组以更明确的任务，要制定的统一规则应当处理这样的问题：支持验证过程的法律基础，包括正在出现的数码验证和核证技术；核证过程的适用性；在使用核证技术情况下用户、提供者和第三方风险和赔偿责任的分配；通过使用登记处进行核证的特别问题；以及以提及方式列入条款。

9．委员会请秘书处在对目前各国正在制定的法律进行分析的基础上，编写数码式签字和服务提供者问题的背景研究报告。工作组应在这项研究报告的

基础上审查制定关于上述问题统一规则的可取性和可行性。委员会同意，工作组第三十一届会议要进行的工作可以包括制订上述议题的某些方面的规章草案。委员会请工作组向委员会提供充分的资料，以便委员会就制定的统一规则的范围作出明智的决定。鉴于《贸易法委员会电子商业示范法》和今后电子商业领域可能的工作覆盖的活动范围很广，委员会决定电子数据交换工作组将易名为“电子商业工作组”。[1]

10．本说明载有数码式签字和有关问题的初步研究报告。它是根据《贸易法委员会电子商业示范法》编写的，同时还考虑到了若干国家最近通过的立法文本或正在制定的立法文本。而且，这项研究报告借助了其他组织的工作成果，特别是国际商会正在编写的《统一国际鉴定和验证惯例》草案和美国律师协会出版的《数码式签字指导原则》，而且反映了特设专家组会议的成果，该专家组将数码式签字领域和贸易法委员会秘书处内的有关专家召集到了一起。

11．按照最近关于更严格控制和限制联合国文件的指示，关于条款草案的解释性说明尽量简短。附加说明将来用口头方式提供。

---

[1] 《大会正式记录，第五十一届会议，补编第 17 号》（ A/51/17 ），第 216-224 段。

一、关于数码式签字的一般说明

A. 签字的功能

12. 《贸易法委员会电子商业示范法》第 7 条以承认纸张环境下签字的功能为基础。在编制《示范法》的过程中，工作组讨论了传统上由手写签字履行的下列功能：鉴定一个个人；提供该个人亲自卷入签字行为的确定性；将该个人与文件的内容联系起来。此外，人们还指出，签字还可以履行其他各种功能，这以所签署的文件的性质而定。例如，签字可以证实某一方受已签署合同内容约束的意图；某人认可文本来源的意图；某人同意由另一人编写的文件内容的意图；某人曾在某个地点的事实和时间。

13. 在电子环境下，电文的原件与复制品无法区分，它不带有手写的签字，而且也不在纸上。欺诈的潜在可能性很大，因为很容易在不被发现的情况下截获和窜改电子形式的信息，而且处理多笔交易的速度很快。目前市场上已启用或仍处于开发阶段的各种技术的目的是要提供这样的技术手段，即在电子环境下能够借助于这些手段履行被认定为手写签字所独具的某些全部功能。这类技术可统称为“电子签字”。

B. 数码式签字和其他电子签字

14. 在讨论制定数码式签字统一法律规则的可取性和可行性的过程中，以及为了帮助委员会审议此类可能的统一规则的范围，工作组可能希望审查现用的或处于开发阶段的各种技术，其目的是提供手写签字和纸张环境下使用的其他各类鉴定机制的功能等同物。

1. 依靠公开钥匙编密学以外的技术的电子签字

15. 可以回顾，与以公开钥匙编密学为基础的“数码式签字”——它构成本说明的主题——一起，还存在着各种其他的装置，常常被叫做“电子签字”机制，它们可能现已投入使用，或考虑今后使用，如期履行上述手写签字功能中的一种或数种。例如，某些技术将依靠采用以手写签字为基础的生物统计学装置的鉴定。在这种装置中，署字人将手签，使用一支特殊的笔，书写在计算机屏幕上或数字衰耗器上。然后由计算机分析手写的签字并作为一组

数值存储起来。它可以附在数据电文之后，并由收件人显示出来以供鉴定。这样一种鉴定体系将有一个先决条件，即手写签字的实例事先已经生物统计学装置分析过并存储了起来。

16．工作组可能希望讨论，它工作的范围是否应当扩展到包括一般的电子签字。这种工作将要求秘书处作补充研究，研究使用依靠非公开钥匙编密学技术的“签字”装置的技术和法律影响。鉴于可以获得关于数码式签字法律影响的足够的初步资料，而且若干国家已有关于这个专题的立法草案，本说明集中于依靠公开钥匙编密学的数码式签字的问题。

17．在讨论制定将适用于数码式签字和其他形式电子签字的统一规则的可取性和可行性的过程中，工作组可能希望考虑，贸易法委员会是否应当尝试在界于《示范法》的高层普遍性与处理某种或某几种专门技术细节的更为具体规则之间的中间层面上制订统一规则，无论如何，按照《示范法》中媒介的中立性，如果制订的统一规则集中在数码式签字上，它不应当阻止使用替代的方法。

2．依靠公开钥匙编密学的数码式签字[2]

（a）技术概念和术语

（i）编密学

18．数码式签字采用编密学建立和核查，编密学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始形态。数码式签字使用所谓的“公开钥匙编密学”，它常常依靠算法函数产生两种不同但数学上相关的“钥匙”（即利用一系列数学公式生产的大数乘以素数）。其中一种钥匙用于产生数码式签字或将数据转变为似乎不可懂的形态，另一种钥匙用来核查数码式签字或将电文还原为原始形态。利用这两种钥匙的计算机设备和软件常常合起来称为“密码体制”，或更具体地称为“非对称密码体则”，它仍依赖于使用非对称算法。

19．虽然编密学的使用是数码式签字的主要特点之一，但不应将数码式签

---

[2] 本节中数码式签字体系运作说明的众多内容以《美国律师协会数码式签字指导原则》第8至17页为基础。

字仅用来鉴定载有数码形式信息的电文这一事实，与为了保密而更普遍地利用编密学混为一谈。为了保密的加密则一种用来对电子通信进行加密，以便只有电文的发端人和收报人能够看懂的方法。在若干国家中，法律限制为了保密而使用编密学，这可是出于考虑到国防的公共政策的原因。不过，通过产生数码式签字而利用编密学达到鉴定的目的，并不一定意味着使用加密方法使任何信息在通信过程中具有保密性，因为加密的数码式签字可能仅仅附在未加密的电文之后。工作组可能希望审议关于数码式签字的可能的统一规则，应在多大程度上承认编密学用于鉴定，这种用法与它用于保密的目的是不同的。

20．利用加密技术达到保密的目的和仅仅将它用于数码式签字这两种情况可能需要不同的规则，作为对其原因的一个说明，我们认为，如果使用加密技术使电文保密，在许多情况下重要的是，应有某种方法在遗失私人钥匙的情况下还原加密的电文，如果加密的电文具有重要的法律、财务或公共责任的价值，如果正确实施，这种技术可使钥匙对的发行者能够保留或重新制作遗失的钥匙。不过，用来产生数码式签字的私人钥匙就可能没有必要留存或重新制作，而且，如果具有这样做的技术能力，就可能削弱用户和一般公众对整个体系可能具有的信心。

（ii）“公用钥匙和私人钥匙”

21．用于数码式签字的互补性钥匙被任意定名为“私人钥匙”——它只由署名人用来产生数码式签字——和“公用钥匙”——它一般更广为人知，而且由依靠方用来核实数码式签字。[3] 如果许多人需要核实署名人的数码式签字，公用钥匙必须提供或分配给他们中所有的人，例如，公布在联机储存库中或容易存取的任何其他形式的公用目录上，虽然成对的两个钥匙具有数学联系，但如果非对称密码体制可靠地设计和实施，想从对公用钥匙的了解求出私人钥匙几乎是不可能的，通过使用公用钥匙和私人钥匙加密的最常用的算法是基于大素数的一个重要特点：一旦它们相乘以得出一个新数，就几

[3] 私人钥匙的用户应该保守私人钥匙的秘密。应当指出，个别用户并不需要了解私人钥匙，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，或者理想的情况是通过生物统计识别装置，例如拇指纹识别装置来存取。

乎不可能断定是哪两个素数产生了新的更大的数。[4] 这样，虽然许多人可能知道某某署名人的公用钥匙而且用它来核实署名人的签字，但他们却不能发现该署名人的私人钥匙并用它来伪造数码式签字。

22．不过，应当指出，公用钥匙编密学的概念并不一定意味着利用上述以素数为基础的算法。其他的数学技术现正在使用或开发，例如椭圆曲线密码体制，人们常说它通过利用大大缩短的钥匙长度而提高安全度。在讨论公用钥匙编密学的问题时，工作组可能希望确认公用钥匙编密学正在国际贸易中被采用的程度。与此同时，工作组可能希望采取一种技术上中立的立场，考虑到目前的技术状况而又不排除据以制作钥匙对的计算技术的未来变化。此外，对计算机行业技术发展的这种开明的态度，将是符合贸易法委员会所作出的决定的，即贸易法委员会不可能从事技术标准的制定工作，而且应当注意不要卷入数码式签字的技术问题中去（见上文第3段）。

（iii）“散列函数”

23．除了钥匙对的产生以外，在产生和核实数码式签字时还利用另一个基本的过程，它一般称为“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的算法为基础，常被称为“电文摘要”或电文的“指印”，表现为标准长度的“散列值”或“散列结果”，它通常比电文短得多，但仍具有它明显的独特性。在使用同一散列函数时，电文的任何变动不可避免地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”——几乎不可能因了解其散列值而求出原始电文。因此，散列函数能启动产生数码式签字的软件依靠较少和可预测的数据量运作，同时仍向原始电文内容提供可靠的证据相关性，从而有效地
保证电文自以数码方式签字以来未被修改。

---

[4] 某些现行的标准如《美国律师协会数码式签字指导原则》指的是“计算的不可行性”概念，以描述该过程预期的不可逆性，即希望不可能从用户的公用钥匙求出用户的秘密私人钥匙。“计算的不可行性”是一个相对的概念，它基于所保护数据的价值、保护数据所需的计算费用、它需要加以保护的期限及攻击数据所需的成本和时间，这些因素的评估既看当前的情况，又根据未来技术进步的情况来进行（《美国律师协会数码式签字指导原则》第9页，注23）。

（ iv ）“数码式签字”

24 . 为了签署一份文件或任何其他的信息项目，署名人首先精确划定拟签署的内容的范围。拟签署的划定信息可以称为“电文”。然后。署名人软件中的散列函数计算为电文所独有的（适用于所有实际目的）散列结果。然后，署名人的软件利用署名人的私人钥匙将散列结果转变为数码式签字。所产生的数码式签字因此为电文和用来产生数码式签字的私人钥匙所独有。

25 . 典型的情况是，数码式签字（电文的数码式签字的散列结果）附在电文之后并随电文一起存储或发送。不过，它也可以作为独立的数据单元发送或存储，只要它保持与电文的可靠联系。由于数码式签字为电文所独有，如果它与其电文永久脱离联系，它就没有用了。

（ v ）数码式签字的核查

26 . 数码式签字的核查是通过参照原始电文和某一给定公用钥匙检查数码式签字的过程，从而断定数码式签字是不是利用对应于被参照公用钥匙的私人钥匙为同一电文产生的。在核查数码式签字的同时，还通过用于产生数码式签字的同一散列函数计算原始电文的新的散列结果。然后，利用公用钥匙和新的散列结果，核查人核对数码式签字是不是利用相应的私人钥匙产生的，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码式签字的原始散列结果相配对。

27 . 核查软件将确认数码式签字得到了“核查”，如果：（ 1 ）署名人的私人钥匙被用来以数码方式签署了电文，如果署名人的公用钥匙被用来核查签字，就被认为属于此种情况，因为署名人的公用钥匙将只核查采用署名人私人钥匙产生的数码式签字；以及（ 2 ）电文未经改动，如果核查人计算的散列结果与在核查过程中从数码式签字析取的散列结果相一致，就被认为属于此种情况。

（ b ）公用钥匙基础结构（ PKI ）和验证局

28 . 为了核查数码式签字，核查人必须有权获得署名人的公用钥匙，而且相信它与署名人的私人钥匙相匹配。不过，公用和私人钥匙对与任何人都没有内在的联系；它只是一对数目而已。需要有一种外加的机制将特定的个人或实体与钥匙对可靠地联系起来。如果公用钥匙的加密是为了达到预定的目的，它必须提供某种办法将钥匙发送给形形色色的个人，其中许多人并不为发送人所认识，双方没有发展成相互信任的关系。为了达到这种目的，有关各方必须对公布的公用钥匙和私人钥匙高度信任。

29 . 在这样的各方之间可能存在着所需的信任程度：它仍彼此信任，它们彼此已打过一段时间的交道，它们在闭合的系统上互相联系，它们在封闭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——管理它们的交易。在只涉及两方的交易中，每方只需将各自将使用钥匙对的公用钥匙通知（采用较为可靠的渠道如信使或密话系统）对方。然而，在下文这样的各方之间就可能不存在同样程度的信任，它们彼此难得打交道，在开放的系统上联系（例如互联网络上的环球通信网），不属于一个封闭的集团内，或者不订有贸易合伙人协议或拥有管理它们关系的其他法律。

30 . 此外，由于公用钥匙加密是一种数学程度很高的技术，因此，所有用户必须信任发行公用钥匙和私人钥匙的方面的技能、知识和保密措施。[5]

31 . 本来的署名人可以发表一则公开声明，说明应将可用某个给定的公用钥匙核查的签字作为源自该署名人的签字对待。然而，其他方面可能不愿意接受这种声明，特别是如果没有先前的合同能够有把握地证明这种公开声明的法律效力的话。如果某方信赖此种在开放系统上所作的未经证明的公开声明，它将冒疏忽大意地信任骗子或不得不驳斥虚假否认数码式签字（常常叫做“不可抵赖性”问题）的巨大风险，如果交易最终证明对自称的签名人不利的话。

32 . 这些问题的一个解决办法是利用一个或多个受到信任的第三方将认定的署名人或署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，该受信任的第三方一般称做“验局”。在若干国家中，这

---

[5] 在公用和私人的编密钥匙将由用户本身发行的情况下，这种信任度可能得由公用钥匙的证明人提供。

类验证局现正按等级组织成常常所称的公用钥匙基础结构（PKI）。

（i）公用钥匙基础结构（PKI）

33．建立公用钥匙基础结构是使人们信任下列几点的一种方法：（1）用户的公用钥匙未被窜改，而且事实上对应于该用户的私人钥匙；（2）使用的加密技术是可靠的；（3）可以信任发行编密钥匙的实体留存或重新制作可用于保密性加密的公用和私人钥匙，如果获准使用这种技术的话；（4）不同的加密体系具有相互操作性。为了使人产生上述信任，公用钥匙基础结构可以提供多种服务，其中包括：（1）管理用于数码式签字的编密钥匙；（2）证明一种公用钥匙对应于一种私人钥匙；（3）为最终用户提供钥匙；（4）决定哪些用户在系统上拥有哪些特权；（5）公布公用钥匙或证书的保密目录；（6）提供个人令牌（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制作和存储个人的私人钥匙；（7）核实最终用户的标识并向它们提供服务；（8）提供不可抵赖性服务；（9）提供时间标记服务；（10）管理用于保密性加密的加密钥匙，如果获准使用这种技术的话。

34．公用钥匙基础结构常以多层次的权力机构为基础。例如，某些国家为建立可能的公用钥匙基础结构而考虑的样板提到了下列层次：（1）一个独一无二的“根机构”，它将证明获准发行加密钥匙对或与使用这种钥匙对有关的证明的所有各方的技术和做法，并将下属的验证局记录在案；[6]（2）各种验证局，它们被置于“根”机构之下，负责证明用户的公用钥匙实际上对应于该用户的私人钥匙（即未经窜改）；以及（3）各级地方登记机构，它们被置于验证局之下，接受用户关于加密钥匙对的申请或关于与使用这种钥匙对有关的证明的申请，要求提出鉴定的证据并检查潜在用户的身分，在某些国家，设想可由公证人充当或支持地方登记机构。

35．工作组可能想一般地讨论公用钥匙基础结构的问题。不过，我们认为此类问题可能难以达成国际协调一致。公用钥匙基础结构的组织工作可能涉及各种技术问题及公共政策问题，这些问题留给各国自行处理可能更好。[7]

---

[6] 政府是否应当拥有留存或重新制作保密性私人钥匙的技术能力的问题可在根当局一级处理。

[7] 不过，从交叉证明的角度看，全球相互通用的必要性要求各国建立的公用

在这一方面，考虑建立公用钥匙基础结构的各个国家也许需要作出有关的决定，例如在下述方面：（1）公用钥匙基础结构应采用什么形式和由几级机构组成；（2）是否只有属于公用钥匙基础结构的某些机构才应被允许发行编密钥匙对，或者是否此类钥匙对可由用户自身发行；（3）证明编密钥匙对有效性的验证局是否应当是公共实体，或者说私营实体是否也可充当验证局；（4）允许某某实体充当验证局的过程是否应当由国家明确授权或颁发“许可证”，或者是否也可使用其他的方法控制验证局的质量，如果它们被允许在无具体授权的条件下运作的话；（5）应在多大程度上授权编密学可用于保密目的；以及（6）政府机构是否应当保留通过“钥匙托管”或其他形式等机制存取加密信息的权利。工作组也许想建议，上述问题不应当在委员会今后关于数码式签字的工作中加以处理。

（ii）验证局

36．为使钥匙对与未来的署名人联系起来，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“对象”，并且可以确认证书中鉴定的未来署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持有人结合在一起。如果证书的“领受者”愿意依赖证书中点名的持有人产生的数码式签字，他可以利用证书中所列的公用钥匙检查数码式签字是否采用对应的私人钥匙产生。如果这种检查获得成功，则可以保证数码式签字是由证书中点名的公用钥匙的持有人产生，并保证对应的电文自采用数码方式签字以来未改动过。

37．为了保证证书在其内容和来源两个方面的可靠性，验证局上数码方式签字。签发证书的验证局在证书上的数码式签字可以采用由另一个验证局签发的另一份证书中列出的验证局的公用钥匙检查（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，直至依赖于数码式签字的个人对其真实性确信无疑为止。在每种情况下，签发证书的验证局在用来核查验证局数码式签字的另一证书的操作期间，必须用数码方式签署自己的证书。

38．对应于电文的数码式签字，不管是钥匙对的持有人为了证实电文而产生，还是验证局为了证实它的证书而产生，一般都应当打上可靠的时间标

钥匙基础结构应能互相沟通。

记，以使检查人能够可靠地确定数码式签字是否在证书中指出的“操作期”内产生，因为这是检查数码式签字的一个条件。

39．为使公用钥匙及其与具体持有人的对应关系随时可用于核查，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，可供检索和用来检查数码式签字。依据实现的情况而定，通过让核查程序直接查询储存库获取所需证书的方式，可以自动地完成证书的检索。

40．一旦签发，一份证书可能证明不可靠，如果持有人将其身份错误地表述给验证局，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，由于私人钥匙持有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，而且验证局（应持有人的请求或甚至不经持有人的同意，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，验证局一般必须立即公布废止或中止的通知，或通知那些查询有关事项或已知他们收到了参照不可靠证书核查的数码式签字的个人。

41．据设想，验证局可由政府机构运作，或由私营部门的服务提供者运作。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。另一些国家认为，证书服务应向私营部门的竞争开放。不管验证局由公共机构运作还是由私营部门的服务提供者运作，也不管验证局是否需要获取经营许可证，典型的情况是，在公用钥匙基础结构内，不止有一个验证局工作。特别令人关注的是各种验证局之间的关系。在公用钥匙基础结构内，各个验证局可以形成层次结构，其中有些验证局只证明其他的验证局，而后者直接向用户提供服务。在此种结构中，有的验证局从属于其他的验证局。在其他可以设想的结构中，某些验证局可以与其他的验证局并起并坐地工作。在任何大规模的公用钥匙基础结构中，将可能既有下属的又有上级的验证局。无论如何，在没有国际性的公用钥匙基础结构的情况下，可能会在对外国验证局所出证书的承认方面产生若干忧虑。对外国证书的承认常被称为“交叉验证”。在此种情况下，实质上等同的验证局（或愿意对于其他验证局签发的证书承担某些风险的验证局）必须承认彼此提供的服务，以便它们各自的用户能够更有效地相互交往，而且更加信任所签发证书的可信度。

42．在涉及多种保密政策时，对于交叉验证或连销证书可能产生法律问

题。此类问题的例子可能包括确定因谁处理不当而造成了损失，以及用户应依赖谁的陈述。应当指出，某些国家考虑通过的法律规则规定，如果保密程度和政策已为用户所知而且验证局没有过失，验证局就不应负责。

43．验证局或根机构可能有责任保证，它的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，但任何验证局的可信度也可能取决于它对发证标准的执行和它对来自申请证书用户数据评估的可靠性。特别重要的是适用于任何验证局的责任制度，即它应持续不断地执行根机构或上级验证局的政策和保密要求，或任何其他适用的要求。

44．工作组在评估某个验证局的可信性时可能希望考虑下列因素：（1）独立性（即在基本的交易中没有财政利益或其他权益）；（2）财政资源和承担赔偿损失风险的财政能力；（3）公用钥匙技术方面的专门知识和对适当的保密程序的熟悉程度；（4）长期性（如在诉讼案件或产权要求的情况下，基本的交易完成后许多年，验证局仍可能被要求出示证书或脱密钥匙的证据）；（5）软硬件的批准；（6）审计线索的保留和由独立实体进行的审计；（7）应急计划的存在（例如“大错修复”软件或钥匙托管）；（8）人员的选拔和管理；（9）验证局本身私人钥匙的保护安排；（10）内部保密；（11）终止业务的安排，其中包括通知用户；（12）担保和说明（提供或不包括）；（13）责任的限制；（14）保险；（15）与其他验证局的相互可操作性；（16）废止程度（在编密钥匙可能遗失或失密的情况下）。

（c）数码式签字程序的小结

45．数码式签字的使用通常涉及下列过程，由签署人执行或由数码式签字电文的收件人执行：

(1) 用户生成或被给予唯一的编密钥匙对；

(2) 发送人在计算机上起草电文（例如，采用电子邮件电文的形式）；

(3) 发送人利用一种保密散列算法起草“电文摘要”数码式签字的生成利用从署名电文和给定私人钥匙二者求出并为此二者所独有的散列结果。为使散列结果安全保密，必须使任何其他电文和私人钥匙的结合产生同样数码式签字的可能性小到忽略不计；

(4) 发送人依靠私人钥匙给电文摘要加密。利用一种数学算法将私人钥匙应

用于电文摘要的文本。数码式签字由加密的电文摘要组成;

(5) 发送人一般将其数码式签字附在电文之后;

(6) 发送人利用电子手段将数码式签字和(本加密或加密的)电文发给收件人;

(7) 收件利用发件人的公用钥匙检查发件人的数码式签字。利用发件人公用钥匙所作的检查证明电文全部来自发件人;

(8) 收件人也产生电文的"电文摘要",利用同一保密的散列算法进行;

(9) 收件人对比两种电文摘要。如果二者一样,则收件人知道经签字后电文未作改动。电文经数码式签字后即使有一点改动,收件人产生的电文摘要也与发件人产生的电文摘要不同;

(10) 收件人从验证局取得证书(或者经由电文的发端人),它确认发件人电文上的数码式签字。验证局一般为受信赖的第三方,在数码式签字体系中负责管理验证工作。证书载有发件人的公用钥匙和姓名(以及可能另外的信息),它经验证局数码式签字。

二、数码式签字统一规则中审议的法律问题和可能的条款

A. 工作范围

46. 在决定将数码式签字和验证局问题列入其议事日程时,委员会在第二十九届会议上还同意,应利用这个问题作为一次机会,处理工作组就今后工作提出的其在议题(见上文第 8 段)。在进入数码式签字问题的讨论以前,工作组可能想讨论将其工作范围限制在数码式签字或扩大其范围以将其他的鉴定机制也包括在内的可取性和可行性,这些鉴定机制可能现已启用或不久即可开发出来用于电子商业(见上文第 15-17 段)。可以忆及,在制定《示范法》期间,工作组注意到必须以下述方式制定法律规则,即不使它们同技术发展和商业发展和某个具体阶段联系在一起,而是提供一般性的原则,可以指望这些原则经过若干年后仍能适用,而不管技术可能发生了什么变化。

47. 数码式签字现已普遍使用,而且存在着这样的风险,即各国可能对于数码式签字采取不同的立法方针,这可能表明需要制定统一的立法条款,作为此种鉴定技术的一个具体的法律框架。然而,按照在制定《示范法》时采取的媒介中立的态度,工作组可能想讨论着手制定只应用于数码式签字的统一规则是否合适,或者是否也应当起草关于其他鉴定技术的此类统一的规

则。如果工作组认为，各国自行制定不同法律的上述风险表明，制定适用于数码式签字的统一规则的必要性特别紧迫，工作组也可能想讨论如何可以起草数码式签字统一规则的有关方法，以便避免这样一种风险，即此类统一规则可能被误解为鼓励使用数码式签字而不利于相竞争的技术，这些技术也可被认为是体现在《示范法》第7条中“可靠方法”概念的可以接受的实例。

48．关于验证局，工作组也可能想考虑：在许多切实可行的情况下，商业实体作为验证局的活动只是该商业实体作为服务提供者更多种活动的一个方面。因此，工作组也许想讨论，关于验证局的统一规则在范围上是否应当仅限于制定只适用于服务提供者充当验证局的活动方面的行为规则，或者制定适用于服务提供者或电子商业中“可信任第三方”的更广泛活动的规则是否可取和可行。

B．数码式签字统一规则和一般条款的适用范围

49．本说明是根据下述假定编写的：关于数码式签字的可能规则，应当直接从《示范法》第7条得出，而且应当被视为一种方式，可为“用于鉴定”一个个人和“表明该个人同意”数据电文中所载信息的可靠方法的概念提供详细信息。在考虑有可能列入一组数码式签字统一规则的一般条款时，工作组可能想更一般地审议此种统一规则与《贸易法委员会电子商业示范法》的关系。特别是，工作组可能愿意就下述方面向委员会提出建议：数码式签字的统一规则是否应构成一个单独的法律文件，或者它们是否应纳入《示范法》扩大的版本，例如作为独立的一章收入《示范法》的第二部分。

50．不管数码式签字统一规则作为独立的文件还是作为《示范法》的补充编写，我们认为，，统一规则必须以符合《示范法》第1条（适用范围）、第2（a）、（c）及（e）条（“数据电文”、“发端人”和“收件人”的定义）、第3条（解释）、第4条（经商定更改）、第6条（书面）和第7条（签字）精神的条款为基础。这些条款未明文转载于本说明中，但应当指出，数码式签字统一规则草案是秘书处根据此类条款为统一规则的组成部分的假设制定的。在这一方面；还应当指出，符合《示范法》第2、4、6和7条精神的条款载于某些国家正在制定的数码式签字立法中，而《示范法》也在诸如《美国律师协会数码式签字指导原则》等这样的文本中被提及。

51．除了上述条款外，工作组还可能希望审议统一规则的序言是否应当澄

清统一规则的目的，即通过建立一个安全框架和给予书面签字和数码式签字在法律效力方面以相同的地位，促进数字通信的有效利用。

C．数码式签字的具体法律问题和条款草案

1．定义

52．在数码式签字和验证局领域已经实施或目前正在制定的法律、条例和指导原则，就它们所依靠的定义的条数而言，相互差别很大。根据立法国的法律传统而定，数码式签字的问题可以大多通过定义来处理，或者根本不包含任何定义。

53．按照制定《示范法》时采取的方针，工作组可能希望审议有限数目的实质性概念的定义，例如“数码式签字”、“验证局”和“证书”等。

54．工作组可能希望利用下列可能的定义作为其审议的基础。

（a）数码式签字

55．“A条草案

（1）数码式签字为一数值，它签署在数据电文上，而且使用同发端人私人编密钥匙有联系的一个已知数学步骤，使得可能唯一地断定这一数值是靠发端人的私人编密钥匙获得的。

（2）用于生成〔本法〕〔本规则〕所授权的数码式签字的数学步骤以公开加密方法为基础。在应用于数据电文时，这些数学步骤使电文发生转变，而掌握初始电文和发端人公用编密钥匙的个人能够准确地断定

（a）该转变是否是使用与发端人私人编密钥匙一致的私人编密钥匙操作的；和

（b）实施转变后，初始电文是否变动过。

（3）如果数据电文所附的数码式签字能够按照［本法］［本规则］授权的验证局规定的程序加以核查，则该签字即被认为得到了授权。

（4）［立法国的有关机构］应为数码式签字及其核查需达到的技术要求制定具体的规则。”

备注

56．按照制定《示范法》时奉行的功能方针，所建议条款的第（1）和（2）两款的重点为扼要描述公开加密方法实施的技术功能。第（3）和（4）两款反映这样一个原则，即只有用于公共当局建立的公用钥匙基础结构的情况下，数码式签字才有效。

（b）授权的验证局

57．“B条草案

（1）……[立法国规定，主管授权验证局的机关或机构]，可以依照[本法][本规则]向验证局授权。这种授权可予撤回。

（2）……[立法国规定，主管颁布关于授权验证局条例的机关或机构]，可以制定管理据以可作出此种授权的条款的规则，并且颁布关于验证局运作的条例。

（3）授权的验证局可以签发关于自然人和法人的编密钥匙的证书。

（4）授权的验证局可以提供或便利数据电文传递和接收的登记和时间标记，及有关通过数码式签字保证的通信的其他功能。

（5）……[立法国规定，主管制定关于应由授权验证局履行的职能的具体规则的机关或机构]，可以为应由授权的验证局在向各个自然人或法人签发证书方面履行的职能制定具体的规则。”

备注

58．工作组可能希望讨论拟制定的统一规则是否应当明确提及在授权验证局运作时应加考虑的标准。可以忆及，在制定《示范法》时，这类标准未列入，以便包括在《立法指南》中。

（c）证书

59．“C条草案

授权的验证局采用数据电文或其他形式签发的证书至少应表明：

（a）用户的名字[和地址或营业地点]；

（ｂ）如果用户是自然人，用户的[出生年月日][充分的身份证明]；
（ｃ）如果用户是法人，公司的名称和认定该公司的任何其他信息；
（ｅ）验证局的名称、地址或营业地点；
（ｆ）用户的公用编密钥匙；
（ｇ）任何必要的信息，表明用户的公用编密钥匙的核查情况如何提供给按照证书所作的数码式签字的收件人；
（ｈ）证书的序号；以及
（ｉ）证书的[签发日期和截止日期][有效期]。”

备注

60．某些国家正在制定的数码式签字立法草案列出了C条草案中提及的部分或全部内容，作为要求验证局签发的任何证书中必须提供的最低信息量。不过，按照工作组在编制《示范法》时所作的不参与个人数据保护问题的决定，工作组可能希望考虑，在许多国家，例如关于个人出生日期的信息将作为个人数据受到保护，而且可以制定具体的规则对通过电子手段披露这种信息实施管理。

2. 法人和自然人的签字

61. “D条草案

（1）自然人和法人同样可以获得专用于识别目的的编密公用钥匙证书。

（2）法人可以向数据电文附上已为该法人业已证明的编密私人钥匙而鉴定该份电文。如果电文也由被授权代表该法人行事的自然人以数码方式签字，该法人只应被视为该电文的[发端人][批准了电文的发送]。”

备注

62. 上述条款旨在澄清数码式签字可被用来约束法人的情况。它依赖于《示范法》第7（1）（a）条中“签字”所起的两种作用的区分，即鉴定电文的作者和表明该个人对电文中所载信息的同意。通过使用为一个自然人证明的单一钥匙，这两种功能通常将可完成，但是为法人证明的公用钥匙将只是用来保证该法人作为电文发送者的身份。因此，法人的“数码式签字”只起有限的作用。除了法人的“数码式签字”（即鉴定）之外，电文的任何批准还需要自然人的数码式签字，这种签字将既鉴定该个人，又代表法人表明批准电文内容的意向。

63. 虽然条款草案提到“被授权代表法人的自然人”，但它无意取代国内代理法。因此，自然人实际上和法律上是否有权代表法人行事的问题，留给统一规则之外的适当法律规则去处理。

3. 数码式签字数据电文的归属

64. “E条草案

（1）附有发端人数码式签字的数据电文的发端人，其受电文内容约束的情况，与电文按照适用于电文内容的法律上[手工]签署的方式存在时一样。

（2）附有数码式签字的数据电文的收件人，有资格将数据电文视为发端人的数据电文，并且根据这种假定行事，如果：

（a）为了弄清数据电文是否是发端人的数据电文，收件人将

发端人的公用钥匙正确应用于所收到的数据电文，而且通过应用发端人的公用钥匙发现：收到的数据电文是采用发端人私人编密钥匙加密的；而且通过使用发端人公用编密钥匙加密后，初始电文来作改变；

或者

（ｂ）收件人收到的数据电文产生于这样一个个人的行动，他与发端人的关系或与发端人的任何代理人的关系使该个人能够有权获得发端人的私人编密钥匙。

（３） 第（２）款不适用于：

（ａ）这样的时候，即如果收件人向授权的验证局寻求过信息，或者采取了其他合理审慎的做法，收件人知道，或应该知道，发端人的公用编密钥匙的有效期已满，或者验证局签发的证书已被废上或中止；

或者

（ｂ）如属第２（ｂ）款的情况，如果收件人采取了合理审慎的做法或利用了任何商定的程序，收件人知道或应该知道数据电文不是发端人电文的任何时候。”

备注

65．工作组可能希望讨论，数码式签字电文归属的问题是否可以通过提及《示范法》第13条简单地处理。E条草案以《示范法》第13条为蓝本，旨在说明第13条中所载的数码式签字情况下的原则。它以对数码式签字的法律效力提供确定性的需要为基础。数码式签字目前被认为是一种高度可靠的认证程序。条款草案让附有发端人数码式签字电文的发端人承担了重大的责任。可以忆及，根据《示范法》第２（ｃ）条，“发端人”意指数据电文声称由其或代表其发送的任何个人。条款草案说明，数码式签字的任何用户都必须保护其私人钥匙。这种钥匙被用来加密电文，就将造成一种无法反驳的推定：该电文是指称的发端人的电文。

4．证书的废止

66．“F条草案

（1）核准钥匙对的持有人可以废止相应的证书。废止自验证局[登记][收到]时起生效。

（2）如果核准钥匙对的持有人了解列私人编密钥匙遗失、失密或有被误用到其他方面的危险，持有人有义务废止相应的证书。如持有人在这种情况下不废止证书，对于因持有人未能采取这种废止行动而使依靠电文内容的第三方遭受的任何损失，持有人应负责赔偿。”

备注

67．工作组可能希望指出，如果数码式签字统一规则中规定，证书的废止在验证局收到时生效，H条草案（责任）第（4）款可予删除，因为不可能有验证局对废止通知登记方面的过失或疏忽负责的基础。

5．证书登记簿

68．“G条草案

（1）授权的验证局应保留一本公众可以查阅的已签发证书的电子登记簿，表明各份证书签发的时间、到期的时间或中止或废止的时间。

（2）在验证局签发的任何证书废止或有效期期满之日后，登记簿应由验证局至少保存[10]年。”

备注

69．工作组可能希望讨论，证书登记簿是否应当可以公开查阅，或者对这种登记簿的查阅是否需要限于有关方面。关于这种登记簿应保存的时间，工作组可能希望讨论，任何国家的期限是否应当作为统一的规则加以规定，这种期限的确定是否应当留给立法国负责，或者它应当没法提供一个更灵活的标准，例如表明登记簿应当可以查阅，以在每项证书的有效期内核查它们，而且直至这样一个期限——根据验证局的证书数码式签字的电文将被用来或将需要进行核实——的终止，这可能使得有必要规定几个时期，视关于限期和时效的现行法律而定。

6. 赔偿责任

70. "H条草案

（1）对于出于善意依赖验证局签发的证书的任何个人因验证局登记方面的缺点、技术故障或类似情况而遭受的任何损失，授权的验证局应负赔偿责任，[即使这种损失不是][如果这种损失是]验证局的过失所造成。

（2）X备选条文　任何单项损失的赔偿责任不应超过[金额]。……[立法国指定主管修订最大金额的机关或机构]可以每两年调整这一金额，以反映价格的变化情况。

Y备选条文　……[立法国指定主管颁布赔偿责任条例的机关或机构]可颁布关于验证局赔偿责任的条例。

（3）如果遭受损失的一方因故意或疏忽造成了这种情况，赔偿额可以减少或可以不赔。

[（4）如果授权的验证局收到了证书废止的通知，该验证局应即将此种废止进行登记。如果该验证局未能这样做，它应对用户因此遭受的损失负责。]"

备注

71. 工作组可能愿意讨论，关于责任的条款是否应当扩大范围，以包括验证局过失以外的情况。工作组也可能愿意确定，当事方自主权是否应当和在多大程度上应当适用，以允许验证局经与用户达成私下协议来控制它们应负责任的范围。

72. 工作组可能希望考虑按下精神列入"安全港"条款:

"遵守[本法][本规则]和任何适用法律或合同的验证局不对下述损失负责:

（1）由该验证局签发的证书的持有人因持有人对该证书的依赖所遭受的损失，或

（2）因依赖于该验证局签发的证书，通过参照该验证局签发的证书中所列的公用钥匙可加核实的数码式签字，或在此种证书中表述

的信息所造成的损失。”

7. 交叉验证问题

73. “I条草案

（1）外国验证局签发的证书可用于数码式签字，其条件与受[本法][本规则]管辖的数码式签字相同，条件是这种证书得到一个授权的验证局的承认，而且该授权的验证局在与其本身的证书相同的程度上保证证书细项正确无误及该证书有效。

（2）……[立法国规定，主管制定与批准外国证书有关的规则的机关或机构]，被授权批准外国证书并规定这种批准的具体规则。”

备注

74. I条草案依据这样一种概念：对外国证书的承认应在对等的基础上由一个本国验证局负责提供。在讨论交叉验证的问题时，工作组可能希望考虑，是否应当需要充分的对等，或者对于外国证书的正确性和有效性的保证，是否一定需要构成交叉验证方案组成部分的所有验证局在同一层次上提供。工作组也可能希望考虑，对于承认外国证书，是否一定需要政府的干预。

75. 作为I条草案的一个可能的备选办法，工作组可考虑某些国家在起草立法时采取的方针，根据这种方针，对外国证书的承认只能在双边或多边国际协议的基础上提供。

8. 用户与验证局的关系

76. “J条草案

（1）只允许验证局要求鉴定用户所需的信息。

（2）应法人或自然人的要求，验证局应提供关于下述方面的信息：

（a）证书可以利用的条件；

（b）与数码式签字使用有关的条件；

（c）利用验证局服务的费用；

（d）验证局关于个人信息利用、存储和交流的政策或做法；

（e）验证局关于用户通信设备的技术要求；

（ f ）在通信设备功能发生异常或故障的情况下验证局向用户报警的条件；

（ g ）验证局赔偿责任的限度；

（ h ）验证局对证书使用施加的限制；

（ i ）用户有权对证书使用施加限制的条件。

（ 2 ）第（ 1 ）款中所列的信息应在缔结最后验证协定以前提供给用户。［该信息可由验证局采用验证做法说明的方式提供］。

（ 3 ）如提前［一个月］通知，用户可以终止与验证局联系的协定。此种通知在验证局收到时生效。

（ 4 ）如提前［三个月］通知，验证局可以终止与验证局联系的协定。此种通知在收到时生效。

三、以提及方式列入条款

A．以前的讨论

77．在工作组第二十八届会议上，有人提出一项建议，要求在《贸易法委员会电子数据交换［ EDI ］及有关的数据传递手段法律事项示范法》草案中列入一项条款，其内容为保证可通过仅仅提及而列入数据记录的某些条款将被承认具有与全文列入数据记录一样的法律效力。有人指出，以提及方式将某些条款列入 EDI 电文的问题对于 EDI 用户来说是极端重要的，而且十分需要保证这种方法使用的确定性。据论证， EDI 本来就是一种以提及方式包含在内的系统，因为如不以提及方式列入有关的通信标准， EDI 电文就变得毫无意义，而且也没有多大的合同价值。会议决定，在今后的会议上，工作组将研究采用仅仅提及有关条款的方式就将这些条款列入数据电文的问题（ A/CN.9/406，第 90 和 178 段）。

78．在第二十九届会议上，工作组收到了两个关于以提及方式列入条款的条款草案的提案，一项由国际商会观察员提出（ A/CN.9/WG.IV/WP.65 ），另一项由大不列颠及北爱尔兰联合王国提出（ A/CN.9/WG.IV/WP.66 ）。普遍的看法是，这个问题列入《示范法》的时机尚不成熟，还需要作进一步的研究。有人指出，提交工作组的两项提案需要在一些问题上加以进一步的澄清，如将列入什么样的条款和在什么情况下列入等。此外，还有人指出，两项提案可能让人认为是在干预合同法的一般规则。而且，有人指出电子环境

下以提及方式列入条款的问题用不着在《示范法》中处理，因为它提出的问题与纸张环境下以提及列入条款的问题基本相同，一般合同法对此作了处理。最后，有人指出，搞一个条款区分纸张环境下与 EDI 通信环境下以提及方式列入条款的做法不符合工作组迄今为此奉行的方针，该小组旨在保证“媒介中立”。有人回答说，在从业者中有一种感觉，以提及方式列入条款的问题，在 EDI 环境下比在纸张环境下复杂，例如，因为所涉及的通信数量更大，而且如果采用数据电文的形式，以提及方式列入的条款可能更难以弄清。还可以看出，从业者需要处理电子通信条件下以提及方式列入条款的具体条款。另一种观点是，鉴于在通过 EDI 处理的特定合同关系中涉及的数据电文数量大，被人称为“格式之争”的问题特别有可能产生。工作组同意，以提及方式列入条款的问题可能需要在今后的工作中作进一步的审议（A/CN.9/407，第 100 至 105 和 117 段）。

79．在第三十届会议上，工作组普遍认为，需要进行关于 EDI 情况下以提及方式列入条款的工作。有人表示看法说，在为数据电文中此种以提及方式列入的条款制定法律规范的任何尝试中，应满足下列三个条件：（1）提及条款应插入数据电文；（2）所提及的文件——例如一般条款——实际上是针对其可能依赖参考文件的当事方所了解的；以及（3）所提及的文件除了当事方了解的以外，还必须是它可以接受的。人们普遍同意，以提及方式列入条款的课题将放在关于登记处和服务提供者问题这种较大的工作范围内适当地解决。（A/CN.9/421，第 114 段）。委员会在其第二十九届会议上普遍同意，该问题可以在验证局工作的范围内处理（A/51/17，第 222 段）。

B．关于以提及方式列入条款的统一规则的可能需求

80．以提及方式列入条款是一种简略的方式，即在一份文件中一般地提及详列在其他地方的有关条款，而不是全文复述它们。例如，在误判或缔结合同时，它使得不必再列出冗长的标准条款。这样，只要采用充分地认定有关条款并表明将它们列入的意图的办法，就能将这些条款列入提及它们的文件或数据电文。在电子环境下，以提及方式列入条款可以定义为这样一种方法：通过在一份数据电文或记录中提及另一份电文或记录（或其中所载的部分信息），使后者成为前者的组成部分，并且宣布应将后者作为前者的组成部分对待，就好像它在其中全文列明的一样。

1. 纸张环境下发展形成的传统规则

（a）以提及方式列入条款

81. 以提及方式列入条款的做法所引起的问题在纸张通信环境下已为人所知，而且在许多法律体制中存在着法律规则，规定了在一份书面文件中未全文表述的信息可以依法视为该文件组成部分的法律条件。例如，在某些条件下，对一个或多个《国际贸易术语解释通则》术语——例如“运费付至目的地”（CPT）或“运费和保险费付至目的地”（CIP）——的提及，可以列入定单或发票中，其结果是，这些国际贸易术语将被视为相应售货合同的条款之一，而用不着在任何合同单证全文说明“CPT”或“CIP”售货的实际定义。国际商会编写《国际贸易术语解释通则》的这些术语，是专门为了通过使用它们的缩略语列入合同的，因此可能有利于以提及方式列入它们。《国际贸易术语解释通则》广为人知，而且国际商会和贸易法委员会都建议使用它们。常常以提及方式列入的文本的另一个例子是国际商会编制的《跟单信用证统一惯例和做法》（UCP500）。为允许诸如UCP500这样的文本以提及方式列入合同所使用的法律推理，常常是基于这样的认识：这样一种文本在世界各地广为人们了解和接受，而且被假定为有关各方都了解。

82. 在无此种假定适用的情况下，各国法律为使以提及方式列入条款具有法律效力而规定的条件，可能涉及严格的要求，例如各方实际了解以提及方式列入的信息，或谋求对其执行的当事方甚至明确同意该信息。但是，根据有些国家的法律，使以提及方式列入条款具有法律效力的要求较为宽松。例如，对以提及方式列入条款所进行的某些传统法律测验，可能集中于以提及方式列入的条款的明晰性和以提及方式列入的信息的可存取性。

（ b ） “格式之争”

83 . 不应将以提及方式列入条款的问题与一般被人称为“格式之争”的问题混为一谈。例如，在下述情况下就可能发生格式之争：买方提出的一般合同条款以小字体印在其定单的背面，而另一组不同的合同条款又印在卖方开出的发票的背面。如果买卖双方未达成具体协议，确定以哪些条款适用于某笔合同，而且双方在其合同单证的背面传递了两组相矛盾的条款，就可能需要解决由哪些条款管理交易的不确定性的问题。在许多国家，为解决这种模棱两可的问题制定了合同法的法律规则。

2 . 电子商业环境下提出的问题

（ a ）以提及方式列入条款做法的广泛使用

84 . 以提及方式列入条款的做法对于电子数据交换（ EDI ）、电子邮件、数码式签字和其他形式的电子商业都至关重要。例如，采用标准 EDI 电文方式的通信，以及一般的电子通信，一般都采用这样的体制结构：交换的电文数量巨大，每份电文所载信息简短，而且依靠提及可从其他方面存取的信息的做法比纸张文件多得多。 EDI 和其他高度结构化和格式化的数据类型，无一例外地广泛利用以提及方式列入文件的做法，以提高数据处理的效章。在工作组的上几届会议上，有人指出， EDI 和形形色色的电子商业基本上是以提及方式列入条款的体系。实际上，如果不对以提及方式列入可能适用于 EDI 电文的有关法律、技术和行政条款、条件、款项、协议、标准、规则或指导原则的做法的有效性作出明确规定， EDI 电文的法律确定性便有可能被削弱。

85 . 关于在纸张环境下将会发生的“格式之争”的情况，应当记住，人们没有打算，甚至也没有配备有关设备让电子信息传递随每份电文传送的诸如一般印在纸张文件背面那样的一般条款。列入所有的有关条款又费钱又影响效率。它将减慢电子通信的速度，也许还会阻塞电子通信，而且，由于迫使依靠的各方将此种冗长的文本打印出来或翻阅，甚至可能降低通知的效果。因此需要制定可将此种文本视为列入电文的规则。如有可能，此种规则的目的应是在电子环境下减少纸张环境下格式之争引起的困难，或者至少应确保根据许多国家法律为解决纸张环境下的这些困难而精心制定的解决方案也

将可用于电子环境中。应当指出，制定这种规则不一定涉及改变可能产生于各国现有法律的、关于如何能解决“格式之争”情况的解决方案。

86．以提及方式将数据电文列入其他数据电文的标准，对于公用钥匙证书的使用也可能是至关重要的，因为这些证书一般为简短的记录，内容规定得很死，长短限定。不过，签发证书的授权第三方可能要求列入限制其赔偿责任的有关条款。因此，如果不以提及方式列入外部条款，商业做法中一项证书的范围、目的和效果将是模糊和不确定的。在涉及采用不同贸易做法和惯例的不同当事方的国际通信中，情况尤其如此。

87．有人在工作组上几届会议上反复指出，制定关于以提及方式将数据电文列入其他数据电文的标准，对于以计算机为基础的贸易基础结构极端重要。如果没有此种标准促进的法律确定性，以计算机为基础的交易将因列入大量的材料而变得累赘，因而使有关各方及促进交易和系统都难以应付。如果没有此种统一的标准，可能存在一种巨大的风险，即由于传统商业机制与电子商业机制之间的不同，如果把确定谋求以提及方式列入的条款可执行性的传统测验方法应用于相应的电子商业条款，这种应用可能无效。例如，对以提及方式列入条款做法的某些传统法律测验可能询问，列入的条款是否“明明白白”，它们是否载有“证明含蓄列入意图的合适的提及字眼”，或者打算的列入是否“明确和令人信服”。这类测验可能给促进电子贸易造成非故意的障碍。可能需要具体的规则，因为发通知和保证存取信息所使用的方法在纸张环境下与在电子商业环境下可能有所不同，并可能造成这样的后果：在有些法域，关于以提及方式列入条款的传统规则可能导致电子商业受到不正当的差别待遇。

（b）列入文本的可存取性

88．电子商业严重依赖于以提及方式列入条款的机制。但与此同时，通过使用电子通信，所提及信息全文的存取可能方便许多。例如，一份电文可能已嵌入了统一资源定位符（URL），它指导读者检索被查阅的文件。此种URL 定位符能够提供“超文本联系”，可使读者只要将一个指向装置（例如鼠标器）指到一个与URL 相联系的关键词上，提及的文本就将显示出来。

89．在电子环境下还可使用同一方法确保所有用户方便地存取多种文本，例如：（1）体现既定商业做法的文本（例如UCP500）；（2）管理通信

的技术标准；（3）由验证局发布的验证做法说明；以及（4）诸如某公司一般合同条款等更为具体的信息。不过，如果没有关于以提及方式将数据电文列入其他数据电文的标准，就不能有信心地依赖这些方法的法律效力。

90．电子环境下拟订关于以提及方式列入条款规则的必要性，既由于数据电文频繁提及记录在其他地方的信息，也由于获得了这样一些技术手段，它们使对这些信息的核证与在纸张环境下相比变得又快又容易。

C．可能的条款

91．在拟订关于在电子商业中以提及方式列入在内的可能条款时，工作组可能希望记住，在某些法域，为用于纸张环境下而发展的现有规则以这样一种考虑为基础：列入的条款或其他信息应恰当提请收件人或第三方（视情况而定）注意。在有这种法律规则的地方，使它们适用于各种情况可能是适当的，而不管以提及方式列入的做法是借助于EDI还是任何其他的通信类型。

92．然而，制定这样一项一般性原则似乎是可能的：它澄清以提及的方式列入条款的电子商业中是有效的，但条件是也同时明确指出，该原则不影响在下述方面可能存在的任何规则：（1）有必要把条款或其他信息的内容或地点提请拟对其适用的任何方面注意，或提供给该方；或（2）任何法律要求，即在条款能够成为合同的组成部分以前，它们应为有关方面所接受。基本的原则是，应当承认以提及方式列入条款的用法，以便信息只是列在其他地方这一事本身并不阻止该信息列入它被提及的数据电文中。

93．工作组可能希望根据下列两项备选条文重新审议以提及方式列入条款的问题。

备选条文A

除另有商定外，在一份数据电文中全文或部分地提及可以［适当］［合理］存取的条款、条件、款项、协议、标准、规则或指导原则并具有［明显］意图将它们列为内容的组成部分或者使其具有法律约束力时，应假定这些条款以提及方式列入了该数据电文。在双方之间，这类条款应在法律允许的程度上具有法律效力和约束力，就如它们在数据电文中全文申明一般。

备选条文B

（1）本条适用于一份数据电文中记录或传达的信息提及记录在其他地方的信息（“补充信息”）或只有通过提及补充信息才能完全搞清的场合。

（2）在第（4）款限制的条件下，数据电文得具有好像补充信息在数据电文中全文表达而且只有在其中提及才能查清那样的效力，如果数据电文：

（a）通过下述方法确定该补充信息：

（i）以集合名称或描述；和

（ii）以确定载有补充信息的记录和该记录的有关部分，以及在该记录不能分开获得的情况下，确定可以找到它的地方；以及

（b）明确表示或载有明确的含意，即数据电文应具有好像补充信息在数据电文中全文表达一样的效力。

（3）本条内容不影响：

（a）任何这样的法律规则，它要求适当地通知记录在其他地方的信息的内容，或可以找到这种信息的记录或地点，或者它要求记录或地点可有另一人存取或进入；或

（b）与为了缔结合同而接受报价有关的任何法律规则。