联 合 国 A/CN.9/WG.IV/WP.86

大 会

Distr.: Limited
18 August 2000
Chinese
Original: English

电子商务工作组
第三十七届会议
2000 年 9 月 18 日至 29 日，维也纳

电子签字

贸易法委员会电子签字统一规则颁布指南草案

秘书处的说明

1. 根据委员会第二十九届会议（1996 年）[1] 和第三十届会议（1997 年）[2] 作出的决定，电子商务工作组第三十一至三十六届会议专门拟订了《贸易法委员会电子签字统一规则》草案（以下简称“统一规则”）。这几届会议的报告载于 A/CN.9/437、446、454、457、465 和 467 号文件。在拟订统一规则时，工作组注意到，似宜在评注中对统一规则作进一步的补充说明。按照在拟订《贸易法委员会电子商务示范法》时采取的方式，关于统一规则草案应附带一份指南从而协助各国颁布和实施统一规则的建议，获得了普遍支持。这份指南的许多部分可以摘自统一规则的准备工作文件，对统一规则的其他使用者也将起到帮助作用。

2. 工作组在其第三十六届会议上以秘书处编写的说明(A/CN.9/WG.IV/WP.84)为基础，讨论了电子签字的问题。经讨论后，工作组通过了统一规则第 1 和第 3—11 条草案的实质内容，并把这些条款转交一个起草小组，以确保统一规则各项条款之间的统一性。工作组请秘书处就所通过的条文编写一份颁布指南草案。工作组建议在其今后的一届会议上连同颁布指南一起审查统一规则的第 2 和第 13 条草案，这项建议仍有待于委员会核准。[3]

3. 委员会在其第三十三届会议（2000 年 6 月至 7 月）上注意到，工作组第三十六届会议通过了统一规则第 1 和第 3—11 条草案的案文。据指出，由于工作组决定从统一规则草案中删除关于增强式电子签字的概念，所以有些问题仍有待澄清。有人表示关切，认为视工作组将对第 2 和第 13 条草案所作的决定而定，条款草案的其余部分可能还需重新讨论，以避免造成统一规则制定的标准对可确保高度安全性的电子签字和可能在电子通信中使用的、并不打算具有重大法律效力的低价值证书将同样适用的局面。

4. 经讨论后，委员会对工作组作出的努力和在拟订统一规则方面取得进展表示赞赏。敦促工作组在其第三十七届会议上完成其关于统一规则的工作，并对拟由秘书处编写的颁布指南草案进行审查。[4]

5. 本说明附件中载有秘书处编写的指南草案第一部分和第二部分第一章。第二部分第二章载于 A/CN.9/WG.IV/WP.86/Add.1 号文件。

附件

贸易法委员会电子签字统一规则

及其

颁布指南

2001 年

目 录

第一部分

贸易法委员会电子签字统一规则（2001 年）

贸易法委员会电子签字统一规则（2001 年）第 1 和第 3－11 条草案

（2000 年 2 月 14 日至 25 日在纽约举行的贸易法委员会电子商务工作组
第三十六届会议通过的《贸易法委员会电子签字统一规则》）

第 1 条. 适用范围

本规则适用于商务**活动过程中*电子签字的使用，并不凌驾于旨在保护消费者的任何法律规则之上。

* 委员会建议意欲扩大本规则适用范围的国家采用下列案文：

“本规则适用于电子签字的使用，但下列情况除外：[…]。”

** 对“商务”一词应作广义解释，使其包括不论是契约型或非契约型的一切商务性质的关系所引起的种种事项。商务性质的关系包括但不限于下列交易：供应或交换货物或服务的任何贸易交易；分销协议；商务代表或代理；客帐代理；租赁；工厂建造；咨询；工程设计；许可贸易；投资；融资；银行业务；保险；开发协议或特许；合营或其他形式的工业或商务合作；空中、海上、铁路或公路的客货运输。

第 3 条. 签字技术的平等对待

除第 5 条外，本规则任何条款的适用概不排斥、限制或剥夺可生成满足本规则第 6(1)条所述要求或符合适用法律要求的电子签字的任何方法的法律效力。

第 4 条. 解释

(1) 对本规则作出解释时，应考虑到其国际渊源以及在电子商务中促进其统一适用和遵守诚信的必要性。

(2) 对于由本规则管辖的事项而在本规则内并未明文规定解决办法的问题，应按本规则所依据的一般原则解决。

第 5 条. 经由协议的改动

本规则可经由协议而加以删减或改变其效力，除非根据颁布国法律[或本规则另有规定]，协议无效或不具有效力。

第 6 条. 符合签字要求

(1) 凡法律规定要求有某人的签字时，如果根据各种情况，包括根据任何有关协议，使用电子签字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，则对于该数据电文而言，即满足了该项签字要求。

(2) 无论第(1)款提及的要求是否作为一项义务，或者法律只规定了没有签字的后果，第(1)款均适用。

(3) 就满足第(1)款所述要求而言，符合下列条件的电子签字视作可靠的电子签字：

(a) 创作电子签字的手段在其使用的范围内与签字人而不是还与其他任何人相关联；

(b) 创作电子签字的手段在签字时处于签字人而不是还处于其他任何人的控制之中；

(c) 凡在签字后对电子签字的任何篡改均可被觉察；

(d) 如签字的法律要求目的是对签字涉及的信息的完整性提供保证，凡在签字后对该信息的任何篡改均可被觉察。

(4) 第(3)款并不限制任何人下列任何方面的能力：

(a) 为满足第(1)款所述要求的目的，以任何其他方式确立某一电子签字的可靠性；

(b) 举出某一电子签字不可靠的证据。

(5) 本条规定不适用于下列情形：[…]

第 7 条. 第 6 条的满足

(1) [颁布国指定的任何主管个人、公共或私人机关或机构]可确定哪些电子签字满足第 6 条的规定。

(2) 依照第(1)款作出的任何决定应与公认的国际标准相一致。

(3) 本条中任何规定概不影响国际私法规则的适用。

第 8 条. 签字人的行为

(1) 各签字人应当做到如下：

(a) 采取合理的防范措施，避免他人擅自使用其签字装置；

(b) 在发生下列情况时，毫无任何不适当的迟延，向签字人按合理预计可能依赖电子签字或提供电子签字辅助服务的任何人员发出通知：

㈠ 签字人知悉签字装置已经失密；或

㈡ 签字人知悉的情况引起签字装置可能已经失密的很大风险；

(c) 在使用证书支持电子签字时，采取合理的谨慎措施，确保签字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。

(2) 签字人应对未能满足第(1)款的要求而承担责任。

第 9 条. 验证服务供应商的行为

(1) 验证服务供应商应当做到如下：

(a) 按其所作出的关于其政策和做法的表述行事；

(b) 采取合理的谨慎措施，确保其作出的有关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：

㈠ 验证服务供应商的身份；

㈡ 证书中所指明的人在签字时拥有对签字装置的控制；

㈢ 在证书签发之日或之前签字装置运作正常；

(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：

㈠ 用以鉴别签字人的方法；

㈡ 对签字装置或证书的可能用途或使用金额上的任何限制；

㈢ 签字装置运作正常和未发生失密；

㈣ 对验证服务供应商规定的责任范围或程度的任何限制；

㈤ 是否存在签字人发出关于签字装置已经失密的通知的途径；

㈥ 是否提供了及时的撤销服务；

(e) 提供签字人发出关于签字装置已经失密的通知的途径，并确保提供及时的撤销服务；

(f) 使用可信赖的系统、程序和人力资源提供其服务。

(2) 验证服务供应商应对未能满足第(1)款的要求而承担责任。

[第 10 条. 可信赖性

在确定验证服务供应商使用的任何系统、程序和人力资源是否可信赖以及在何种程度上可信赖时，应当注意下列因素：

(a) 财力和人力资源，包括是否存在资产；

(b) 硬件和软件系统的质量；

(c) 证书及其申请书的处理程序和记录的保留；

(d) 是否可向证书中指明的签字人和潜在的依赖方提供信息；

(e) 由独立机构进行审计的经常性和审计的范围；

(f) 国家、鉴定机构或验证服务供应商是否有关于上述条件遵守情况或上述条件是否存在的声明；

(g) 其他任何有关因素。]

第 11 条. 依赖方的行为

依赖方对其未能做到如下应当负法律后果：

(a) 采取合理的步骤核查电子签字的可靠性；或

(b) 在电子签字有证书支持时，采取合理的步骤：

㈠ 核查证书的有效性或证书的吊销或撤销；以及

㈡ 遵守对证书的任何限制。

第二部分

贸易法委员会电子签字统一规则颁布指南（2001 年）

本指南的宗旨

1. 在编拟和通过《贸易法委员会电子签字统一规则》（在本手册中也称作“统一规则”）时，联合国国际贸易法委员会（贸易法委员会）铭记，如果向政府执行部门和立法人员提供有关背景说明资料，帮助他们使用统一规则，那么统一规则将成为各国增订本国立法使之达到现代化的一个更加有效的工具。委员会还注意到，一些不太熟悉统一规则中所述那类通信技术的国家，也可使用统一规则。本指南的许多内容取自统一规则准备工作文件，本指南也是为了帮助统一规则的其他使用者，例如法官、仲裁员、从业人员和学术界人士。这些资料也可能有助于各国考虑哪些条款可能应该改动，以适合需要作出这种改动的任何特定国情。在编拟统一规则时，曾设想统一规则草案还将附有这样一份指南。例如，曾决定有些问题不在统一规则中处理，而是在指南中处理，以便向颁布统一规则的国家提供指导。本指南中所载的内容是为了说明为什么列入统一规则条文作为旨在实现统一规则目标的法规文书的基本核心内容。

2. 本颁布指南是秘书处根据贸易法委员会 2001 年第三十四届会议结束时提出的要求编写的。委员会第三十四届会议通过了统一规则，而电子商务工作组则进行了筹备工作，本指南就是以委员会该届会议的审议情况和各项决定以及电子商务工作组的讨论情况为基础编写的。

第一章. 统一规则简介

一. 统一规则的宗旨和来历

A. 旨宗

3. 作为手写签字和其他传统认证程序的替代，电子认证技术的日益普遍使用，表明需要有一项专门的法律框架，以减少因使用这类现代技术（可统称为“电子签字”）而可能产生的法律效力上的不确定性。各国对电子签字可能采取不同的立法处理方式，这就有要求有统一的立法规则，对这种本质上的国际现象制订基本规则。在这方面，法律上（以及技术上）的通用性至关重要。

4. 统一规则建立在《贸易法委员会电子商务示范法》（本手册中也称作“示范法”）第 7 条关于在电子环境中履行签字功能的基本原则基础上，旨在协助各国建立现代化、协调和公正的立法框架，更加有效地解决电子签字问题。统一规则是对示范法的一点补充，但却是重要的补充，其中列出了可用以衡量电子签字技术可靠性的实际标准。另外，统一规则还将这种技术可靠性与特定电子签字可能应有的法律效力联系在一起。统一规则对示范法作出了实质性的补充，采取了可预先确定（或在实际使用前评定）某项电子签字技术法律效力的方式，因此，统一规则意在增进对电子签字的了解，使人们更加确信在具有法律效力的交易中某些电子签字技术是可以依赖的。另外，对于可能涉及使用电子签字的当事各方（即签字人、依赖方和第三方服务商），统一规则还制订了一套基本行为守则，并附带适当的灵活性，从而可有助于在电子网络空间中形成更加协调的商业惯例。

5. 统一规则的目的包括授权或便利使用电子签字，对书面文件的使用者和计算机信息的使用者给予同等待遇，这些目标对于增进国际贸易中的经济效率至关重要。颁布国通过将统一规则（和示范法）规定的程序纳入本国立法，使当事方在有些情况下可选用电子通信手段，将可相宜地创造一种不偏重任何手段的环境。

B. 背景

6. 统一规则是贸易法委员会通过的一系列国际文书中向前又迈出的一步，这些文书或专门着重于电子商务的需要，或在拟订时牢记现代通信手段的需要。在第一类情况下，专门针对电子商务的文书包括《电子资金划拨法律指南》（1987 年）、《贸易法委员会国际贷记划拨示范法》（1992 年）和《贸易法委员会电子商务示范法》（1996 年和 1998 年）。第二类包括贸易法委员会 1978 年以来通过的所有国际公约和其他法律文书，所有这些公约和文书都促进减少繁琐的手续，并载有关于“书面”的定义，意在将非物质化的通信包括在内。

7. 在电子商务领域，贸易法委员会最具体（可能也是最著名）的文书是《贸易法委员会电子商务示范法》。示范法于九十年代初开始编拟，其原因是诸如电子邮件和电子数据交换等现代通信手段更加广泛用于进行国际贸易交易。人们认识到，新技术迅速发展，并且随着信息高速公路和因特网等技术支持手段的更加普及而将进一步发展。但是，以非书面电文的形式传递具有法律效力的资料却受到在这些电文的使用方面存在的法律障碍的限制，或受到这些电文法律效力或有效性不确定的限制。为了推动现代通信手段的更广泛使用，贸易法委员会编写了示范法。示范法的目的是向各国立法人员提供一套国际公认的规则，指出如何可消除一些此类法律障碍，以及如何可为已逐渐称作“电子商务”的交易方式创造一种更加可靠的法律环境。

8. 一些国家关于资料传递和储存的现行立法不充分或已过时，因为其中未考虑到使用电子商务手段。贸易法委员会关于制订电子商务示范立法的决定就是针对这种情况作出的。在有些情况下，现行立法对使用现代通信手段仍然实行或意味着限制，例如规定必须使用“书面”、“经签字的”或“原始”文件。关于“书面”、“经签字的”和“原始”文件的概念，示范法采用了一种功能上等同的做法。

9. 在编拟示范法时，有些国家已通过了处理电子商务某些方面的具体规定。但是，尚没有关于整个电子商务的立法。这可能造成非传统书面文件形式所载的信息在法律性质和有效性方面的不确定性。另外，虽然在电子数据交换和电子邮件日益普及的所有国家都需要有健全的法律和惯例，但许多国家也感觉对传真和电传等通信技术也有此必要性。

10. 示范法还有助于克服国家一级立法不足所形成的某些贸易障碍从而造成的缺点，其中很大部分是与使用现代通信技术相关的。在很大程度上，各国关于使用这类通信技术的法律制度相异，有些还不明确，所以仍可能促成对商家可能进入国际市场的程度的限制。

11. 另外，在国际一级，现有的一些国际公约和其他国际文书可能对使用电子商务构成法律障碍，例如规定某些文件或合同条款必须以书面形式作成，所以示范法在这些情况下还可作为对这些公约和文书的一个解释工具。在这些国际文书的缔约国之间，采用示范法作为解释规则可有助于确认电子商务的用途，并消除谈判一项有关国际文书议定书的必要性。

C. 历史

12. 在通过了《贸易法委员会电子商务示范法》之后，委员会第二十九届会议（1996年）决定将电子签字和验证局问题列在其议程上。要求电子商务工作组审查拟订这些题目的统一规则的适宜性和可行性。会议一致认为，将要编拟的统一规则应涉及下列问题：验证程序的法律依据，包括新出现的数字认证和验证技术；验证程序的可适用性；在使用验证技术时使用者、服务商和第三方的风险和责任划分；使用登记处而涉及的特定验证问题；以提及方式纳入。[5]

13. 委员会第三十届会议（1997 年）收到工作组第三十一届会议的工作报告（A/CN.9/437）。工作组向委员会指出，工作组已就努力协调这一领域立法的重要性和必要性达成了共识。虽然尚未就这项工作的形式和内容作出最后决定，但工作组已得出初步结论，认为至少就数字签字和验证局问题，以及如有可能还就有关的事项，着手拟订统一规则草案是可行的。工作组回顾说，除数字签字和验证局问题外，电子商务领域今后的工作还需要讨论：有别于公用钥匙加密的其他技术方法问题；第三方服务商履行职能的一般问题；以及电子立约问题（A/CN.9/437，第 156－157 段）。委员会核可了工作组达成的结论，并委托工作组编拟关于数字签字和验证局法律问题的统一规则。

14. 关于统一规则的具体范围和形式，委员会普遍一致认为，在工作的这个早期阶段无法作出决定。据认为，虽然似宜将注意力重点放在数字签字的问题上，因为公用钥匙加密在新出现的电子商务活动中显然起主要作用，但统一规则应与示范法采取的不偏重任何手段的方式相一致。因此，统一规则不应抑制使用其他认证技术。另外，关于公用钥匙加密，统一规则还可能需要顾及各种保密程度，并承认数字签字中与所提供的各类服务相应的各种法律效力和赔偿责任限度。关于验证局，虽然委员会承认市场驱动的标准的重要性，但普遍认为，工作组似宜设想制订一套验证局应达到的最低限度标准，尤其是在希望获得跨界认证时，验证局应达到的最低限度标准。[6]

15. 工作组第三十二届会议在秘书处编写的一份说明（A/CN.9/WG.IV/WP.73）基础上开始编拟统一规则。

16. 委员会第三十一届会议（1998 年）收到工作组第三十二届会议的工作报告（A/CN.9/446）。委员会注意到，工作组第三十一届和第三十二届会议都遇到明显的困难，难以就数字签字和其他电子签字的更加普及使用而产生的新的法律问题达成共识。另外还注意到，关于如何可在国际公认的法律框架内解决这些问题，仍有待于达成协商一致。但是，委员会普遍一致认为，迄今为止所取得的进展表明，电子签字统一规则草案正在逐渐形成一个可行的构架。

17. 委员会第三十届会议重申了其关于编拟这些统一规则的可行性而作出的决定，并表示相信，工作组第三十三届会议可在秘书处编写的订正草案（A/CN.9/WG.IV/WP.76）基础上取得更多的进展。在当时的讨论中，委员会满意地注意到，工作组已逐渐被普遍确认作为就电子商务法律问题交换意见和拟订这些问题解决方法的一个特别重要的国际论坛。[7]

18. 工作组第三十三届（1998 年）和第三十四届（1999 年）会议在秘书处编写的三份说明（A/CN.9/WG.IV/WP.76 和 A/CN.9/WG.IV/WP.79 和 80）基础上继续修订统一规则。这两届会议的报告分别载于 A/CN.9/454 号和 457 号文件。

19. 委员会第三十二届会议（1999 年）收到工作组第三十三届（1998 年 6 月至 7 月）

和第三十四届（1992 年 2 月）会议的工作报告（A/CN.9/454 和 457）。委员会对工作组在编拟统一规则中所作出的努力表示赞赏。虽然普遍认为这两届会议在理解电子签字法律问题上取得了重大进展，但也认为工作组面临着重重困难，难以就统一规则所应依据的立法政策建立共识。

20. 一种意见认为，工作组目前采取的做法不足以反映灵活使用电子签字和其他认证技术的商业必要性。按工作组目前的设想，统一规则将重点过分放在数字签字技术上，并在数字签字的范围内，将重点过分放在涉及第三方验证的特定应用上。因此建议，工作组关于电子签字的工作要么应局限于跨界认证所涉及的法律问题，要么全部推迟，直至市场惯例更牢固地建立起来再说。一种相关的看法是，就国际贸易而言，因使用电子签字而产生的法律问题大部分已在《贸易法委员会电子商务示范法》中得到解决。虽然在商法范围之外需要有对于电子签字某些用途的管理条例，但工作组不应卷入任何这类管理活动。

21. 普遍的意见是，工作组应在其原有授权的基础上开展工作。关于电子签字统一规则的必要性，据解释说，在许多国家，政府当局和立法当局正在制订关于电子签字问题的立法，包括建立公用钥匙基础结构或涉及密切相关事项的其他项目，这些当局希望贸易法委员会提供指导（见 A/CN.9/457，第 16 段）。关于工作组作出的把重点放在公用钥匙基础结构问题和公用钥匙基础结构术语上的决定，据回顾说，三类不同的当事方（即钥匙持有人、认证局和依赖方）之间关系的相互作用相当于一种可能的公用钥匙基础结构模式，但还可以设想其他一些模式，例如在不涉及独立的验证局情况下。将重点放在公用钥匙基础结构问题上可带来的主要好处之一是可按配对钥匙的三种功能（或作用），即钥匙的签发人（或使用人）功能、验证功能和依赖功能，方便安排统一规则的结构。普遍一致认为，这三项功能是所有公用钥匙基础结构模式所共有的。还一致认为，无论实际上这三项功能是由三个不同的实体来履行，还是其中两项功能由同一方来履行（例如，在验证局同时也是依赖方时），都应当处理这三项功能。另外，还普遍认为，将重点放在公用钥匙基础结构的典型功能上而不是放在任何特定的模式上，可能较容易在日后阶段制订一项完全不偏重任何手段的规则（同上，第 68 段）。

22. 经讨论后，委员会重申了其早些时候就拟订这些统一规则的可行性作出的决定，并表示相信，工作组今后的会议可以取得更多的进展。[8]

23. 工作组第三十五届（1999 年 9 月）和第三十六届（2000 年 2 月）会议在秘书处编写的两份说明（A/CN.9/WG.IV/WP.82 和 84）基础上继续工作。委员会第三十三届（2000 年）会议收到了工作组这两届会议的工作报告（A/CN.9/465 和 467）。委员会注意到，工作组第三十六届会议已通过了统一规则第 1 条和第 3 至 12 条草案的案文。据指出，由于工作组决定从统一规则草案中删除关于增强式电子签字的概念，所以有些问题仍有待澄清。有人表示关切，认为视工作组将对第 2 和第 13 条草案所作的决定而定，条款草案的其余部分可能还需重新讨论，以避免造成统一规则制定的标准对可确保高度安全性的电子签字和可能在电子通信中使用的、并不打算具有重大法律效力的低价值证书将同样适用的局面。

24. 经讨论后，委员会对工作组作出的努力和在编拟统一规则草案方面取得的进展表示赞赏。委员会促请工作组第三十七届会议完成关于统一规则草案的工作，并审查将由秘书处编写的颁布指南草案。[9][秘书处的说明：本节载录的统一规则历史将在委员会最后审议和通过统一规则之后补充完整，有可能更加简洁]。

二. 统一规则作为协调法律的一个工具

25. 如同示范法一样，统一规则采取法律案文的形式推荐给各国纳入本国法律。与国际公约不同，示范立法不要求颁布该立法的国家通知联合国或通知可能也颁布该立法的其他国家。但是，鼓励各国务必将颁布统一规则（或贸易法委员会拟订的任何其他示范法）的情况通报贸易法委员会秘书处。

26. 将示范立法案文纳入本国法律制度的国家，可修改或略去其中的某些条文。但就公约而言，缔约国对统一案文作出更改（通常称作“保留”）的可能性则受到很大的限制；特别是贸易法公约，通常完全禁止保留，或仅允许极个别特定的保留情况。有些国家可能希望在将统一案文颁布作为本国法之前对之进行不同的改动，在这种情况下，示范立法固有的灵活性就特别理想。当统一案文与国家法院和诉讼程序制度密切相关时，就可能特别希望进行某些改动。但是，这也意味着，通过示范立法所达到的协调程度和协调统一的确定性可能低于公约。但是，示范立法的这种相对缺点却可能因为颁布示范立法的国家可能多于加入公约的国家而得到弥补。为了达到令人满意的协调程度和确定性，建议各国在将统一规则纳入本国法律制度时，尽量少作改动。一般来说，在颁布统一规则（或示范法）时，似宜尽可能保持统一案文，以便使本国法对外国使用者来说可以尽可能做到具有透明度。

三. 关于电子签字的一般说明 [10]

A. 签字的功能

27. 《贸易法委员会电子商务示范法》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；某人认可文本出自本人之手的意图；某人同意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。统一规则与示范法第 7 条的关系在本指南下文第 67 段和第 70—75 段中作进一步讨论。

28. 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或全部功能。这类技术可统称为“电子签字”。

B. 数字签字和其他电子签字

29. 在讨论制定统一规则的可取性和可行性过程中，以及在界定此类统一规则的范围时，工作组审查了现用的或处于开发阶段的各种技术。这些技术的共同目的是提供下列手段的同等功能：(1)手写签字；(2)纸张环境下使用的其他各种认证机制(例如印章)。在电子商务领域内，同样的这些技术还可履行其他功能，这些功能由签字功能衍生物而来，但与纸张环境下的功能不完全等同。

30. 如上所述，在许多国家，政府和立法当局正在拟定关于电子签字问题的立法，包括建立公用钥匙基础结构或密切相关事项的其他项目，这些当局希望贸易法委员会提供指导(见 A/CN.9/457，第 16 段)。关于贸易法委员会作出的将重点放在公用钥匙基础

结构问题和公用钥匙基础结构术语上的决定，应该指出，三类不同的当事方（即钥匙持有人、认证局和依赖方）之间关系的相互作用相当于一种可能的公用钥匙基础结构模式，但还可以设想其他一些模式，例如在不涉及独立的验证局情况下。将重点放在公用钥匙基础结构问题上可带来的主要好处之一是可按配对钥匙的三种功能（或作用），即钥匙的签发人（或使用人）功能、验证功能和依赖功能，方便安排统一规则的结构。普遍一致认为，这三项功能是所有公用钥匙基础结构模式所共有的。还一致认为，无论实际上这三项功能是由三个不同的实体来履行，还是其中两项功能由同一方来履行（例如，在验证局同时也是依赖方时），都应当处理这三项功能。另外，还普遍认为，将重点放在公用钥匙基础结构的典型功能上而不是放在任何特定的模式上，可能较容易在日后阶段制定不偏重任何手段的规则，只要非公用钥匙基础结构电子签字技术可起到类似的功能。

1. 依靠非公用钥匙加密技术的电子签字

31. 与使用公用钥匙加密的“数字签字”一起，还存在着各种其他装置，也包括在广义的“电子签字”机制概念中，这些装置可能现已投入使用，或考虑今后使用，以期履行上述手写签字的一种或数种功能。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进行认证。在这种装置中，签字人将亲手签字，使用一支特殊的笔，书写在计算机屏幕上或数字输入板上，然后由计算机分析手写的签字并作为一组数值储存起来。这种签字可以附在数据电文之后，由收件人显示出来加以认证。这种认证体系将有一个先决条件，即手写签字的式样事先已由生物统计学装置作过分析并储存下来。

32. 贸易法委员会电子商务工作组在编拟统一规则时，关于使用依靠非公用钥匙加密技术的“签字”装置所产生的技术和法律影响，几乎没有获得任何信息。鉴于可以获得关于数字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主题的立法草案，所以贸易法委员会的工作集中于依靠公用钥匙加密的数字签字问题。

33. 但是，贸易法委员会已打算制定既促进使用数字签字也促进使用其他形式电子签字的统一规则。为此，贸易法委员会已试图在示范法高度总括性与涉及特定签字技术时可能所需的专门性之间，处理电子签字问题的法律问题。总之，统一规则与示范法不偏重任何手段的做法相一致，不得解释为不鼓励使用任何电子签字方法，无论是现已存在的方法，还是今后实施的方法。

2. 依靠公用钥匙加密的数字签字 [11]

34. 鉴于数字签字技术在一些国家日益广泛使用，以下简介可有助于那些拟定电子签字立法的国家。

(a) 技术概念和术语

㈠ 加密

35. 数字签字采用加密方法创建和核查，加密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“公用钥匙加密法”，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)。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。利用这两套钥匙的计算机设备和软件常常合起来称为“密码系统”，或更具体地称为“非对称密码系统”，其所依靠的是使用非对称算法。

36. 虽然加密法的使用是数字签字的主要特点之一，但不应将数字签字仅用于认证含有数字形式信息的电文这一事实，与为了保密而更普遍地利用加密法混为一谈。为了保密进行加密是一种用来对电子通信进行加密，以便只有电文的发件人和收件人能够看懂的方法。在若干国家中，法律限制为了保密而使用加密法，这可能是出于国防考虑的公共政策原因。不过，通过产生数字签字而利用加密法达到认证的目的，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，因为加密的数字签字可能仅仅附在未加密的电文之后。

㈡ 公用钥匙和私人钥匙

37. 用于数字签字的互补钥匙称作“私人钥匙” 和“公用钥匙”，前者仅由签字人用以创建数字签字，后者一般更广为人知，而且由依靠方用于核查数字签字。私人钥匙的用户将会保守私人钥匙的秘密。应当指出，用户个人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检索，或者理想的情况是通过生物统计识别装置，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配给他们中每个人，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。虽然配对的两套钥匙具有数学联系，但如果非对称密码系统经可靠设计和实施，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，就特别难以而且特别耗时才能断定是哪两个素数产生了新的更大的数字。[12] 这样，虽然许多人可能知道某某签字人的公用钥匙而且用它来核实签字人的签字，但他们却不能发现该签字人的私人钥匙并用它来伪造数字签字。

38. 不过，应当指出，公用钥匙加密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在开发中，例如椭圆曲线加密系统，人们常说它通过利用大大缩短的钥匙长度而提高安全度。

㈢ 散列函数

39. 除了生成配对钥匙之外，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”，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”，就几乎不可能通过了解其散列值而求出原有电文。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。

㈣ 数字签字

40. 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。

41. 典型的情况是，数字签字(电文经数字签字后的散列结果)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。

㈤ 数字签字的核查

42. 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。

43. 在下列情况下，核查软件将确认数字签字得到了“核查”：(1)签字人的私人钥匙被用于对电文进行数字签字，当签字人的公用钥匙被用于核查签字时，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；(2)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。

(b) 公用钥匙基础结构和验证服务供应商

44. 为了核查数字签字，核查人必须可以取得签字人的公用钥匙，而且相信它与签字人的私人钥匙相对应。不过，配对的公用和私人钥匙与任何人都没有内在的联系；它们只是一对数目而已。需要有一种外加的机制才能将特定的个人或实体与配对的钥匙可靠地联系起来。如果公用钥匙的加密要达到预定的目的，就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。为此，有关各方必须对发给的公用钥匙和私人钥匙高度信任。

45. 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，它们在封闭式系统上互相联系，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，用以管理它们的交易。在只涉及两方的交易中，每方只需(采用较为可靠的渠道，如信使或本身具有声音识别功能的电话系统)将各自将使用的配对钥匙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：它们彼此难得打交道，在开放的系统上联系(例如因特网上的环球通信网)，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。

46. 此外，由于公用钥匙加密是一种数学程度很高的技术，因此，所有用户必须信任公用钥匙和私人钥匙发布方的技能、知识和保密措施。[13]

47. 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。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，或对被抵赖的数字签字不得不加以反驳(常常称做“不可抵赖性”问题)。

48. 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”（在统一规则中选用了“认证服务供应商”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。

㈠ 公用钥匙基础结构

49. 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窜改，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；(3)如果获准使用可用于保密性加密的公用和私人钥匙技术，可信任发布加密钥匙的该实体留存或重新制作这类钥匙；(4)不同的加密系统具有通用性。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)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)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；(7)核实最终用户的标识并向它们提供服务；(8)提供关于不可抵赖性的服务；(9)提供时间标记服务；(10)在获准使用加密钥匙时，管理用于保密性加密的加密钥匙。

50. 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；[14] (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(即未经窜改)；(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。

51. 公用钥匙基础结构的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，这些公共政策问题在目前阶段留给各国自行处理可能更好。[15] 在这一方面，如考虑建立公用钥匙基础结构，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布配对加密钥匙，或者是否此类配对钥匙可由用户自己发布；(3)验证配对加密钥匙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)如允许某个实体充当验证局，这一程度是否应当由国家明确授权或颁发“许可证”，或者当允许验证局在无具体授权的条件下运作时，是否也可使用其他的方法控制验证局的质量；(5)应在多大程度上授权加密法用于保密目的；(6)政府机构是否应当保留通过“钥匙托管”或其他形式等机制获取加密信息的权利。统一规则不涉及这些问题。

㈡ 验证服务供应商

52. 为使配对钥匙与未来的签字人联系起来，验证服务供应商（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，而且对应的电文经数字签字后未被改动过。

53. 为了保证证书的内容和来源的真实性，验证局对证书加上数字签字。签发证书的验证局在证书上的数字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该验证局的公用钥匙来核查(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。在每种情况下，签发证书的验证局在用以核查验证局数字签字的另一证书的操作期间，必须对自己的证书加上数字签字。

54. 与电文相应的数字签字，不管是配对钥匙持有人为了认证电文而创建的，还是验证局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，因为这是能否查验数字签字的一个条件。

55. 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。

56. 证书一旦签发，可能证明并不可靠，例如持有人向验证局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，验证局(按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局所知收到按不可靠证书核查数字签字的人。

57. 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。另一些国家认为，证书服务应由私营部门公开竞争。不管验证局由公共机构运作还是由私营部门的服务商运作，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“相互验证”。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。

58. 在涉及多种保密政策时，对于相互验证或连套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。

59. 验证局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，但任何验证局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局实行的责任制度，即验证局应持续不断地执行总局或上级验证局的政策和保密要求，或任何其他适用的要求。

60. 在编拟统一规则时，下列因素被认为是评估验证局可信性时应予考虑的可能因素：(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索偿的情况下，基本的交易完成后许多年，验证局仍可能被要求出示证书证据或解密钥匙)；(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)有应急计划(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)责任的限度；(14)保险；(15)与其他验证局的通用性；(16)废止程序 (在加密钥匙可能遗失或失密的情况下)。

(c) 数字签字程序小结

61. 数字签字的使用通常涉及下列过程，由签字人执行或由数字签字电文的收件人执行：

(1) 用户生成或被给予独有的配对加密钥匙；

(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”。数字签字创建时利用从签字电文和给定私人钥匙中求出的并为此二者所独有的散列结果。为使散列结果安全保密，必须使通过任何其他电文和私人钥匙的结合产生同样数字签字的可能性小到可忽略不计；

(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文本。数字签字由加密的电文摘要组成；

(5) 发送人一般将其数字签字附在电文之后；

(6) 发送人利用电子手段将数字签字和(未加密或加密的)电文发给收件人；

(7) 收件人利用发件人的公用钥匙核查发件人的数字签字。利用发件人公用钥匙所作的核查，证明电文完全来自发件人；

(8) 收件人也创建电文的“电文摘要”，利用同样的保密散列算法进行；

(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。电文经数字签字后，即使有一点改动，收件人产生的电文摘要也会与发件人产生的电文摘要不同；

(10) 收件人从验证局(或者经由电文的发端人)取得证书，证书确认发件人电文上的数字签字。验证局一般是受信赖的第三方，在数字签字系统中负责管理验证工作。证书载有发件人的公用钥匙和姓名(可能还有其他信息)，经由验证局数字签字。

四. 统一规则的主要特点

A. 统一规则的立法性质

62. 编拟统一规则时所依据的设想是，统一规则应直接来自示范法第 7 条，并应当视作一种方法，对“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这一概念，加以详细的说明（见 A/CN.9/WG.IV/WP.71，第 49 段）。

63. 提出了统一规则草案可采取何种形式的问题，并强调了考虑形式与内容之间关系的重要性。关于可能采取何种形式，提出了各种不同的方法，其中包括合同规则、立法条款或供考虑颁布电子签字立法的国家使用的指南。作为一个工作设想，一致同意应将统一规则制订成附有评注的立法规则，而不仅仅是指南（见 A/CN.9/437，第 27 段；A/CN.9/446，第 25 段；A/CN.9/457，第 51 和 72 段）。

B. 与《贸易法委员会电子商务示范法》的关系

1. 统一规则作为一项单独的法律文书

64. 本来也可扩大示范法将统一规则纳入其中，例如作为示范法新的第三部分。为了明确表明统一规则可单独或结合示范法一起颁布，最后决定统一规则应编拟成一份单独的法律文书（见 A/CN.9/465，第 37 段）。这项决定主要是因为在最后核定统一规则时，示范法已在一些国家得到成功实施，还有许多国家也正在考虑予以通过。扩大示范法可能会破坏其原有版本所取得的成功，因为可能暗示需要通过增补而对该文本加以改进。另外，编拟新版的示范法可能会在那些最近已通过示范法的国家中造成混乱。

2. 统一规则与示范法完全一致

65. 在起草统一规则时，已作出了一切努力，确保与示范法实质内容和术语保持一致（A/CN.9/465，第 37 段）。统一规则中转载了示范法的一般性条款。这些是示范法的第 1 条（使用范围）、第 2(a)、(c)和(e)条（“数据电文”、“发端人”和“收件人”的定义）、第 3 条（解释）、第 4 条（经由协议的改动）和第 7 条（签字）。

66. 统一规则以示范法为基础，尤其要反映如下几点：不偏重任何手段的原则；不歧视在功能上等同传统书面文件概念和惯例的做法；对当事自主权的广泛依赖（A/CN.9/WG.IV/WP.84，第 16 段）。统一规则的目的是既作为“在开放”环境（即各当事方在未事先达成协议的情况下进行电子通信）下的最低限度标准，又作为在“封闭”环境（即各当事方在利用电子手段进行通信时，均受预先制定的合同规则和程序的制约）下的缺省规则。

3. 与示范法第 7 条的关系

67. 在编拟统一规则时，有人表示认为，统一规则第 6 条案文中提及示范法第 7 条应被解释为将统一规则的范围限定于使用电子签字满足关于某些文件必须签字才能生效的强制性法律要求的情形。根据这种看法，因为对用于商业交易的文件，法律载有的这类要求很少，所以统一规则的范围非常狭窄。针对上述看法，普遍认为，对第 6 条草案（和示范法第 7 条）的这种解释与委员会在《示范法颁布指南》第 68 段中所采用

的“法律”一词的解释不一致，在颁布指南中，“‘法律’一词应理解为不仅包括成文法规条例，而且也包括法院产生的法律和其他程序法”。事实上，示范法第 7 条和统一规则第 6 条的范围都特别广，因为商业交易中使用的大多数文件在实践中都可能面对提供书面证明程序的法律要求（A/CN.9/465，第 67 段）。

C. 拟由技术条例及合同加以补充的“框架”规则

68. 作为《贸易法委员会电子商务示范法》的一个补充，统一规则旨在规定基本原则，为使用电子签字提供便利。但是，作为一个“框架”，统一规则本身并没有规定（在使用者之间合同安排以外的）为在颁布国采用这些技术而可能必要的所有细则。另外，正如本指南所指出，统一规则并不打算将电子签字在使用上所涉及的每一方面都包括在内。因此，颁布国似宜发布适当的条例，为统一规则批准的程序填补程序上的细节，并考虑到颁布国（可能正在变化中的）具体国情，不损害统一规则的各项目标。建议颁布国如果决定发布这种条例，应特别注意保持电子系统使用者在系统运作中的灵活性的必要性。

69. 应该指出，统一规则中考虑到的电子签字技术，除提出在执行技术条例时可能需要加以解决的程序事项之外，还可能提出某些法律问题，这些问题的答案不一定将在统一规则中找到，而是要在其他法律中才能找到。这些其他法律例如可包括使用的行政法、合同法、刑事法和司法程序法，统一规则并不打算讨论这些法律。

D. 对电子签字法律效力增加的确定性

70. 关于承认电子签字在功能上等同手写签字，示范法第 7 条规定了灵活的标准。统一规则的主要特点之一就是增加这项标准在操作上的确定性。

示范法第 7 条规定如下：

“(1) 如法律要求要有一个人签字，则对于一项数据电文而言，倘若情况如下，即满足了该项要求：

(a) 使用了一种方法，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，以及

(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。

“(2) 无论本条第(1)款所述要求是否采取一项义务的形式，也无论法律是不是仅仅规定了无签字时的后果，该款均将适用。

“(3) 本条的规定不适用于下述情况：[…]。”

71. 第 7 条是以承认在书面环境下签字的功能为基础的。在编拟示范法时，考虑了签字的下列功能：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。另据指出，签字还可以履行其他各种功能，这依所签署的文件的性质而定。例如，签字可以证实某一方接受已签署合同内容约束的意图；某人认可文本出自本人之手的意图；某人同意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。

72. 为了确保需要认证的电文不会仅仅因为其未经书面文件特有的认证方式加以认证

而被否定法律价值，第 7 条采取了一种全面的方式。第 7 条规定了一些总的条件，在这些条件下，数据电文将视作得到充分可信的认证，并在目前构成电子商务障碍的签字要求面前行之有效。第 7 条侧重于签字的两项基本功能，即鉴定文件的作者和证实作者认可了该文件的内容。第(1)(a)款规定了一项原则，即在电子环境下，如果某种方法可鉴定数据电文的发端人并证实发端人认可了该数据电文的内容，这种方法即履行了签字的基本法律功能。

73. 第(1)(b)款对根据第(1)(a)款采用的签定方法而将达到的可靠程度规定了灵活性原则。按照第(1)(a)款规定所采用的方法，根据各种情况看，包括根据数据电文的发端人与收件人之间的任何协议，应是可靠的，而且适宜于生成或传递该数据电文所要达到的目的。

74. 在决定根据第(1)款所采用的方法是否适宜时，可予考虑的各种法律、技术及商业因素包括：(a)每一当事方所用设备的先进程度；(2)他们所从事的贸易活动的性质；(3)当事方之间进行商业交易的频度；(4)交易的种类和数额；(5)在特定的法规环境下签字要求的功能；(6)通信系统的能力；(7)是否遵行由中间人提出的认证程序；(8)可由中间人提供的各种核证程序；(9)是否遵行贸易惯例和做法；(10)有无防范未经授权而发出电文的保险机制；(11)数据电文所含信息的重要性和价值；(12)利用其他鉴别方法的可能性和实施费用；(13)有关行业或领域在商定该鉴别方法时以及在数据电文被传递时，对于该鉴别方法的接受或不接受程度；(14)任何其他有关因素。（《贸易法委员会电子商务示范法颁布指南》，第 53 和 56—58 段）。

75. 在示范法第 7(1)(b)所载的灵活标准基础上，统一规则第 6 和第 7 条制订了一项机制，通过这项机制，符合技术可靠性客观标准的电子签字可因为其法律效力得到预先确定而从中受益。统一规则的效用是承认两类电子签字。第一类也是范围较广的一类，是示范法第 7 条所述的电子签字，即可用以达到对手写签字的法律要求的任何“方法”。这种等同于手写签字的“方法”的法律效力取决于在实际适用者面前其“可靠性”的表现。第二类也是范围较窄的一类，是统一规则提出的电子签字，即可能为国家机构、私人开证实体或当事各方本身承认符合统一规则制订的技术可靠性标准的电子签字方法，这种承认的优点是在这类电子签字技术（有时称作“增强式”、“可靠”或“合格”的电子签字）的使用者实际使用电子签字技术之前，即可为他们带来确定性。

E. 有关各方的基本行为守则

76. 统一规则并未详细论述可能涉及电子签字系统运作的当事各方的赔偿责任问题。这些问题留待统一规则以外的适用法处理。但是，统一规则制订了这些当事方（即签字人、依赖方和验证服务供应商）行为的评定标准。

77. 关于签字人，统一规则详细阐述了基本原则，即签字人对其电子签字装置应采取合理的谨慎措施。签字人还应采取合理的防范措施，避免他人擅自使用该签字装置。在签字人知悉或理应知悉该签字装置已经失密的情况下，签字人应毫无任何不适当的延迟，向根据合理预计可能依赖电子签字或提供电子签字服务的任何人发出通知。在使用证书支持电子签字时，签字人还应采取合理的谨慎措施，确保签字人就证书而作出的所有重大表述均精确无误和完整无缺。

78. 依赖方应采取合理的步骤核查电子签字的可靠性。在电子签字有证书支持时，依赖方应采取合理的步骤核查证书的有效性或证书的吊销或撤销情况，并遵守对证书的任何限制。

79. 证书服务供应商的一般义务是使用可信赖的系统、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。另外，验证服务供应商还应采取合理的谨慎措施，确保其作出的关于证书的所有重大表述均精确无误和完整无缺。在证书中，供应商应提供基本资料，使依赖方能够鉴定供应商的身份。供应商还应表明：(1)证书中所指明的人在签字时拥有对签字装置的控制；(2)在证书签发之日或之前签字装置运作正常。在与依赖方的交往中，证书服务供应商还应提供关于下列方面的附加信息：(1)用以鉴别签字人的方法；(2)对签字装置或证书的可能用途或使用金额上的任何限制；(3)签字装置的运作状况；(4)对验证服务供应商责任范围或程度的任何限制；(5)是否存在签字人发出关于签字装置已经失密的通知的途径；(6)是否提供及时的撤销服务。

80. 对于评估证书服务供应商使用的系统、程序和人力资源的可信赖度，统一规则作为示例列举了其中一些因素。

F. 不偏重任何技术的框架

81. 鉴于技术革新的速度，统一规则对电子签字给予了法律上的承认，无论所采取的技术是什么（例如利用非对称加密法的数字签字或生物计量法）。

五. 贸易法委员会提供的协助

A. 起草立法方面的协助

82. 贸易法委员会秘书处在其培训和协助活动的范围内向各国提供技术咨询，协助根据《贸易法委员会电子签字统一规则》制订立法。凡考虑根据贸易法委员会其他示范法制订立法或考虑加入贸易法委员会制订的其中一项国际贸易法公约的国家政府，也得到同样的协助。

83. 关于统一规则和贸易法委员会制定的其他示范法和公约的进一步资料，可按下述地址向秘书处索取：

International Trade Law Branch, Office of Legal Affairs
United Nations
Vienna International Centre
P.O. Box 500
A-1400, Vienna, Austria
电话： (+43-1) 26060-4060 or 4061
传真： (+43-1) 26060-5813
电子邮件： uncitral@uncitral.org
网页： http://www.uncitral.org

B. 关于以统一规则为基础的立法的说明资料

84. 秘书处欢迎对统一规则和指南提出意见，并欢迎提供关于以统一规则为基础颁布的立法的资料介绍。统一规则一旦颁布后，将收入法规判例法资料系统，该系统用于收集和传播与贸易法委员会制订的公约和示范法相关的判例法的资料，目的是促进各国了解贸易法委员会制定的法规，并为这些法规的统一解释和适用提供便利。秘书处以联合国六种正式语文出版案例判决的摘要，并在收到复制费用的情况下，提供这些

摘要的详细判案资料。秘书处的文件（A/CN.9/SER.C/GUIDE/1）和贸易法委员会的上述网页上所登载的一份使用者指南中对这套系统作了说明。

———————

注

[1] 《大会正式记录，第五十一届会议，补编第 17 号》（A/51/17），第 223—224 段。

[2] 同上，《第五十二届会议，补编第 17 号》（A/52/17），第 249—251 段。

[3] A/CN.9/467，第 18—20 段。

[4] 《大会正式记录，第五十五届会议，补编第 17 号》（A/55/17），第 380—383 段。

[5] 《大会正式记录，第五十一届会议，补编第 17 号》（A/51/17），第 223—224 段。

[6] 同上，《第五十二届会议，补编第 17 号》（A/52/17），第 249—251 段。

[7] 同上，《第五十三届会议，补编第 17 号》（A/53/17），第 207—211 段。

[8] 同上，《第五十四届会议，补编第 17 号》（A/54/17），第 308—314 段。

[9] 同上，《第五十五届会议，补编第 17 号》（A/55/17），第 380—383 段。

[10] 本节取自 A/CN.9/WG.IV/WP.71 号文件，第一部分。

[11] 本节中有关数字签字系统运作的说明有许多内容以《美国律师协会数字签字指导原则》第 8 至 17 页为基础。

[12] 某些现行的标准，如《美国律师协会数字签字指导原则》，提及“计算上不可行”概念，用以描述该过程预定的不可逆性，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。“计算上不可行”是一个相对的概念，它基于所保护的数据的价值、保护数据所需的计算费用、数据需要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(《美国律师协会数字签字指导原则》第 9 页，注 23)。

[13] 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验证人提供。

[14] 政府是否应当拥有留存或重新创建保密性私人钥匙的技术能力，这个问题可在总局当局的层面上处理。

[15] 不过，从相互证明的角度看，全球通用的必要性要求各国建立的公用钥匙基础结构应能互相沟通。