联 合 国 A/CN.9/493

大 会

Distr.: General
17 May 2001
Chinese
Original: English

联合国国际贸易法委员会
第三十四届会议
2001 年 6 月 25 日至 7 月 13 日，维也纳

电子签字

贸易法委员会电子签字示范法颁布指南草案

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三十七届会议专门拟订了《贸易法委员会电子签字示范法》草案（以下简称“示范法”、“示范法草案”或“新示范法”）。这几届会议的报告载于 A/CN.9/437、446、454、457、465、467 和 483 号文件。在拟订示范法时，工作组注意到，似宜在评注中对示范法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，关于新示范法应附带一份指南从而协助各国颁布和实施示范法的建议，获得了普遍支持。这份指南的许多部分可以摘自示范法的准备工作文件，对示范法的其他使用者也将起到帮助作用。

2. 工作组在其第三十七届会议上完成了示范法条款草案的编拟工作并以秘书处编写的说明（A/CN.9/WG.IV/WP.86 和 Add.1）为基础讨论了颁布指南草案。请秘书处在考虑到本届会议上提出的各种意见、建议和关切考虑的基础上，拟订一份颁布指南草案的订正本，其中应反映工作组作出的各项决定。由于时间不够，工作组未完成对颁布指南草案的审议（见 A/CN.9/483，第 23 和第 145－152 段）。据商定，工作组应在第三十八届会议上留出一些时间，完成这个议程项目。据指出，示范法草案连同颁布指南草案一起，将提交定于 2001 年 6 月 25 日至 7 月 13 日在维也纳举行的委员会第三十四届会议审查和通过。

3. 工作组第三十八届会议（2001 年 3 月，纽约）在秘书处编写的一份订正草案(A/CN.9/WG.IV/WP.88)基础上，审查了《贸易法委员会电子签字示范法颁布指南草案》。工作组关于指南草案的讨论情况和决定，载于该届会议的报告(A/CN.9/484)。已请秘书处根据这些讨论情况和决定编写一份指南订正本(A/CN.9/484，第 19 段)。秘书处编写的指南草案订正本现附于本说明之后。

附件

贸易法委员会电子签字示范法

及其

颁布指南
2001 年

目 录

大会决议.....

第一部分

贸易法委员会电子签字示范法（2001 年）

序言

页 次

第 1 条. 适用范围..... 5
第 2 条. 定义..... 5
第 3 条. 签字技术的平等对待 5
第 4 条. 解释..... 6
第 5 条. 经由协议的改动 6
第 6 条. 符合签字要求 6
第 7 条. 第 6 条的满足 6
第 8 条. 签字人的行为 7
第 9 条. 验证服务商的行为 7
第 10 条. 可信赖性..... 8
第 11 条. 依赖方的行为 8
第 12 条. 对外国证书和电子签字的承认 8

第二部分

贸易法委员会电子签字示范法颁布指南（2001 年）

段 次 页 次

本指南的宗旨..... 1－2 9
第一章. 示范法简介..... 3－85 9
一. 示范法的宗旨和来历 ..... 3－25 9
A. 宗旨..... 3－5 9
B. 背景..... 6－11 10
C. 来历..... 12－25 11
二. 示范法作为协调法律的一个工具 ..... 26－28 13
三. 关于电子签字的一般说明 ..... 29－62 14
A. 签字的功能 ..... 29－30 14
B. 数字签字和其他电子签字 ..... 31－62 14
1. 依靠非公用钥匙加密技术的电子签字..... 33－34 15

	段 次	页 次
2. 依靠公用钥匙加密的数字签字	35－62	15
(a) 技术概念和术语	36－44	15
㈠ 加密	36－37	15
㈡ 公用钥匙和私人钥匙	38－39	16
㈢ 散列函数	40	16
㈣ 数字签字	41－42	16
㈤ 数字签字的核查	43－44	17
(b) 公用钥匙基础结构和验证服务商	45－61	17
㈠ 公用钥匙基础结构	50－52	18
㈡ 验证服务商	53－61	18
(c) 数字签字程序小结	62	20
四. 示范法的主要特点	63－82	20
A. 示范法的立法性质	63－64	20
B. 与《贸易法委员会电子商务示范法》的关系	65－68	21
1. 新示范法作为一项单独的法律文书	65	21
2. 新示范法与《贸易法委员会电子商务示范法》完全一致	66－67	21
3. 与《贸易法委员会电子商务示范法》第 7 条的关系	68	21
C. 拟由技术条例及合同加以补充的“框架”规则	69－70	22
D. 对电子签字法律效力增加的确定性	71－76	22
E. 有关各方的基本行为守则	77－81	23
F. 不偏重任何技术的框架	82	24
G. 不歧视外国电子签字	83	24
五. 贸易法委员会秘书处提供的协助	84－86	24
A. 起草立法方面的协助	84－85	24
B. 关于以示范法为基础的立法的说明资料	86	25
第二章. 逐条说明	87－160	25
标题	87	25
第 1 条. 适用范围	87－92	25
第 2 条. 定义	93－106	27
第 3 条. 签字技术的平等对待	107	30
第 4 条. 解释	108－110	31
第 5 条. 经由协议的改动	111－114	32
第 6 条. 符合签字要求	115－131	33
第 7 条. 第 6 条的满足	132－136	37
第 8 条. 签字人的行为	137－141	38
第 9 条. 验证服务商的行为	142－146	39
第 10 条. 可信赖性	147	41
第 11 条. 依赖方的行为	148－151	42
第 12 条. 对外国证书和电子签字的承认	152－160	43

第一部分

贸易法委员会电子签字示范法（2001 年）

（经 2000 年 9 月 18 日至 29 日在维也纳举行的贸易法委员会电子商务工作组第三十七届会议核准）

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 2 条. 定义

在本法中：

(a) “电子签字”系指在数据电文中，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字人和表明签字人认可数据电文所含信息；

(b) “证书”系指确认签字人与签字制作数据之间关系的某一数据电文或其他记录；

(c) “数据电文”系指经由电子手段、光学手段或类似手段生成、发送、接收或储存的信息，这些手段包括但不限于电子数据交换、电子邮件、电报、电传或传真；

(d) “签字人”系指持有签字制作数据的人，代表本人或所代表的人行事；

(e) “验证服务商”系指签发证书和可能提供与电子签字有关的其他服务的人。

(f) “依赖方”系指可能根据某一证书或电子签字行事的人。

第 3 条. 签字技术的平等对待

除第 5 条外，本法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) 对本法作出解释时，应考虑到其国际渊源以及促进其统一适用和遵守诚信的必要性。

(2) 对于由本法管辖的事项而在本法内未明文规定解决办法的问题，应按本法所依据的一般原则解决。

第 5 条. 经由协议的改动

本法的规定可经由协议而加以删减或改变其效力，除非根据适用法律，该协议无效或不具有效力。

第 6 条. 符合签字要求

(1) 凡法律规定要求有一人的签字时，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) 签字制作数据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) 签字制作数据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) 如签字制作数据可用于制作具有法律效力的签字，各签字人应当做到如下：

(a) 采取合理的谨慎措施，避免他人擅自使用其签字制作数据；

(b) 在发生下列情况时，毫无任何不应有的迟延，向按签字人合理预计可能依赖电子签字或提供支持电子签字服务的任何人员发出通知：

㈠ 签字人知悉签字制作数据已经失密；或

㈡ 签字人知悉签字制作数据很有可能已经失密的情况；

(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. 验证服务商的行为

(1) 如验证服务商提供服务，支持可用作具有法律效力的签字而使用的电子签字，验证服务商应当做到如下：

(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：

㈠ 验证服务商的身份；

㈡ 证书中所指明的签字人在签发证书时拥有对签字制作数据的控制；

㈢ 在证书签发之日或之前签字制作数据有效；

(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 签字制作数据或证书的可能用途或使用金额上的任何限制；

㈢ 签字制作数据有效，且未发生失密；

㈣ 验证服务商规定的责任范围或程度上的任何限制；

㈤ 是否存在签字人依照第 8(1)(b)条发出通知的途径；

㈥ 是否开设及时的撤销服务；

(e) 在开设 d㈤项所述服务的情况下，提供签字人依照第 8(1)(b)条发出通知的途径，在开设 d㈥项所述服务的情况下，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) 验证服务商应对其未能满足第(1)款的要求而承担责任。

第 10 条. 可信赖性

为第 9(1)(f)条之目的，在确定验证服务商使用的任何系统、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 12 条. 对外国证书和电子签字的承认

(1) 在确定某一证书或某一电子签字是否具有法律效力或在多大程度上具有法律效力时，不得考虑：

(a) 签发证书或制作或使用电子签字的地理位置；或

(b) 签发人或签字人营业地的地理位置。

(2) 在[颁布国]境外签发的证书，如具有基本等同的可靠性，则在[该颁布国]境内具有与在[该颁布国]境内签发的证书同样的法律效力。

(3) 在[颁布国]境外制作或使用的电子签字，如具有基本等同的可靠性，则在[该颁布国]境内具有与在[该颁布国]境内制作或使用的电子签字同样的法律效力。

(4) 在确定某一证书或某一电子签字是否为第(2)款或第(3)款之目的而具有基本等同的可靠性时，应当考虑到公认的国际标准或其他任何有关的因素。

(5) 如当事各方之间议定使用某些类别的电子签字或证书，即使有第(2)款、第(3)款和第(4)款的规定，仍应承认该协议足以成为跨国境承认的依据，除非根据适用法律该协议无效或不具有效力。

第二部分

贸易法委员会电子签字示范法颁布指南（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示范法》（在本手册中又称作“示范法”或“新示范法”）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，那么示范法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，一些不太熟悉示范法中所述那类通信技术的国家，也可使用示范法。本指南的许多内容取自示范法准备工作文件，本指南也是为了帮助示范法的其他使用者，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。在编拟示范法时，曾设想示范法草案还将附有这样一份指南。例如，曾决定有些问题不在示范法中处理，而是在指南中处理，以便向颁布示范法的国家提供指导。本指南中所载的内容是为了说明为什么列入示范法条文作为旨在实现示范法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示范法，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。[3]

第一章. 示范法简介

一. 示范法的宗旨和来历

A. 宗旨

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，法律上的协调一致和技术上的通用性是一项适当的目标。

4. 示范法建立在《贸易法委员会电子商务示范法》（为避免引起混乱，本手册中始终用其全称）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。示范法是对《贸易法委员会电子商务示范法》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，示范法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。示范法对《贸易法委员会电子商务示范法》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，示范法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），示范法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. 示范法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。颁布国通过将示范法（和《贸易法委员会电子商务示范法》）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。这种也在《贸易法委员会电子商务示范法》中采用的不偏重任何手段的方法，是为了原则上规定适用于生成、储存或传递信息的所有实际情况，无论该信息可能附载于何种介质手段（见《贸易法委员会电子商务示范法颁布指南》，第 24 段）。《贸易法委员会电子商务示范法》中使用的“不偏重任何手段的环境”这句话，反映了对纸张介质附载的信息和电子手段传递或储存的信息实行一视同仁的原则。新示范法也同样反映了对电子手段传递或储存信息而可能采用的各种技术的一视同仁原则，这项原则常常称作“不偏重任何技术”(A/CN.9/484，第 23 段)。

B. 背景

6. 示范法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，贸易法委员会最著名的文书是《贸易法委员会电子商务示范法》。该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《贸易法委员会电子商务示范法》。《贸易法委员会电子商务示范法》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，《贸易法委员会电子商务示范法》采用了一种基于功能等同的做法。“功能等同的做法”是根据对传统纸张形式要求的用途和功能的分析而来的，以确定如何可通过电子商务技术实现这些用途或功能（见《贸易法委员会电子商务示范法颁布指南》，第 15-18 段）。

9. 在编拟《贸易法委员会电子商务示范法》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。根据《贸易法委员会电子商务示范法》第 2(b)

条，电子数据交换的定义是“电子计算机之间使用某种商定标准来规定信息结构的信息电子传输”。

10. 《贸易法委员会电子商务示范法》还有助于克服国家一级立法不完备造成国际贸易障碍而带来的缺点，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《贸易法委员会电子商务示范法》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《贸易法委员会电子商务示范法》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. 来历

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示范法的适宜性和可行性。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。[3]

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. 关于统一规则的确切范围和形式，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《贸易法委员会电子商务示范法》采取的不偏重任何手段的方式相一致。因此，统一规则不应限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。[4]

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（后来作为示范法通过）。

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，工作组已被逐渐普遍承认是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。[5]

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）收到工作组这两届会议的工作报告（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，但也看到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。按工作组当时的设想，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。[6]

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。[7]

25. 工作组在第三十七届会议（2000 年 9 月）上完成了统一规则的拟订工作。此届会议的报告载于 A/CN.9/483 号文件中。工作组还讨论了颁布指南草案。请秘书处在考虑到本届会议上提出的各种意见、建议和关切的基础上拟订一份颁布指南草案订正本，其中应反映工作组作出的决定。由于时间不够，工作组未完成对颁布指南草案的审议。据商定，工作组应在第三十八届会议上留出一些时间，以完成这个议程项目的工作。据指出，统一规则（采用《贸易法委员会电子签字示范法》草案的形式）连同颁布指南草案，将一并提交委员会第三十四届会议（2001 年）审查和通过。[秘书处的说明：本节论及示范法的来历，尚需在委员会最后审议和通过示范法之后完成]。

二. 示范法作为协调法律的一个工具

26. 如同《贸易法委员会电子商务示范法》一样，新示范法采取法律案文的形式推荐给各国纳入本国法律。新示范法并非旨在干预国际私法规则的正常运作（见下文，第 136 段）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，鼓励各国务必向贸易法委员会秘书处通报颁布新示范法（或贸易法委员会拟订的任何其他示范法）。

27. 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，建议各国在将示范法纳入本国法律制度时，尽量少作改动，并适当考虑其基本原则，包括不偏重任何技术，本国和外国电子签字一视同仁，当事方自主权和示范法的国际渊源。一般来说，在颁布新示范法（或“《贸易法委员会电子商务示范法》”）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和不陌生。

28. 应当注意的是，有些国家认为与使用电子签字有关的法律问题已经由《贸易法委员会电子商务示范法》解决，在这一新的领域中的市场做法更加完善之前不打算采用关于电子签字的进一步规则。然而，同时颁布新示范法和《贸易法委员会电子商务示范法》的国家可以指望得到额外的益处。对于本国的政府机构和立法机构正在拟订关于电子签字问题、包括关于建立公用钥匙基础结构的法规的国家来说，示范法的某些条文作为一种考虑到公用钥匙基础结构问题及其术语而拟订的国际文书可以提供指

导。对于所有国家来说，示范法提供了一套可在公用钥匙基础结构模式之外采用的基本规则，因为这些规则设想到任何种类电子签字可能涉及的两种不同功能（即制作和依赖电子签字）之间的相互作用和某些种类电子签字涉及的第三种功能（即验证电子签字）。这三种功能都应论及，而不论其事实上是否由三个或更多个单独的实体来完成（例如，不同实体彼此间分别完成验证功能的不同方面），也不论其中的两项功能是否由同一人来完成（例如，验证功能由一依赖方完成）。因此，示范法为依赖于独立验证局的公用钥匙基础结构系统和电子签字过程中不涉及此种独立第三方的电子签字系统提供了共同基础。无论是哪种情形，新示范法都给电子签字的法律效力增加了确定性，而又不会限制《贸易法委员会电子商务示范法》第 7 条中所体现的灵活标准的运用（见下文第 67 和第 70 至 75 段）。

三. 关于电子签字的一般说明 [8]

A. 签字的功能

29. 《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《贸易法委员会电子商务示范法》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。示范法与《贸易法委员会电子商务示范法》第 7 条的关系在本指南下文第 65 和 67 段以及第 70—75 段中作进一步讨论。

30. 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

31. 在讨论制定新示范法的可取性和可行性过程中，以及在界定电子签字统一规则的范围时，贸易法委员会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。

32. 如上所述（见第 21 和第 28 段），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，但市场上已通用其他一些模式，（例如不涉及独立验证局的情况）。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电子签字的三种功能（或作用），即按签字人的功能、验证功能和依赖功能而方便地安排示范法的结构。其中两项功能是所有公用钥匙基础结构模式所共有的（即制作和依赖

电子签字）。第三种功能是许多公用钥匙基础结构模式都涉及的（即验证电子签字）。无论实际上这三项功能是否由三个以上不同的实体来履行（例如，不同实体彼此间分别完成验证功能的不同方面），还是其中两项功能是否由同一方来履行（例如，在验证服务商同时也是依赖方时），都应当处理这三项功能。只要非公用钥匙基础结构电子签字技术可满足类似的功能，将重点放在公用钥匙基础结构环境中完成的功能上而不是放在任何特定的模式上，可能较容易制定完全不偏重任何手段的规则。

1. 依靠非公用钥匙加密技术的电子签字

33. 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。其他技术包括使用个人识别码、手写签字的数字版以及其他方法，如点击“OK框”。

34. 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法规。为此，贸易法委员会已试图在《贸易法委员会电子商务示范法》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，新示范法与《贸易法委员会电子商务示范法》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 [9]

35. 鉴于数字签字技术在一些国家日益广泛使用，以下简介可能有帮助。

(a) 技术概念和术语

㈠ 加密

36. 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。

37. 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

38. 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。[10] 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。

39. 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

40. 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

41. 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。

42. 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，就无法操作了。

㈤ 数字签字的核查

43. 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。

44. 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商

45. 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使形形色色的个人可以使用，其中许多人并不为签字人所认识，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有某种程度的信任。

46. 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。

47. 此外，由于公用钥匙密码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。[11]

48. 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。此类声明的形式和法律效力由颁布国的法律管辖。例如，可通过在官方公报或公共当局承认的“正宗”文件上发表声明来确立将电子签字归属于某一特定签字人的推定（见 A/CN.9/484，第 36 段）。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署名的签字人不利，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(常在电子签字的“不可抵赖性”环境下提到的一个问题)。

49. 对其中一些问题的一种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“验证服务商”（在示范法中选用了“认证服务提供商”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。其他解决办法例如可包括由依赖方签发的证书。

㈠ 公用钥匙基础结构

50. 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)使用的密码技术是可靠的。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密码钥匙；(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；(9)在获准使用密码钥匙时，管理用于保密性加密的密码钥匙。

51. 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；[12] (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。

52. 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)验证配对密码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服务商，这一过程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密码法用于保密目的；(6)政府当局是否应当拥有通过“钥匙托管”或其他形式等机制获取加密信息的权利。示范法不涉及这些问题。

㈡ 验证服务商

53. 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，则在技术上提供了某种程度的保证，即数字签字是由签字人所创建的，而且散列函数中使用的电文部分（以及因而对应的电文）经数字签字后未被改动过。

54. 为了保证证书的内容和来源的真实性，验证服务商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(这另一个验证服务商可以是上级机构，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，签发证书的验证服务商在用以核查验证服务商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。

55. 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，因为这是能否查验数字签字的一个条件。

56. 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。

57. 证书一旦签发，可能证明并不可靠，例如持有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，验证服务商(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，验证服务商可能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。

58. 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，不止有一个验证服务商工作。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。

59. 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。

60. 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

商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。

61. 在编拟统一规则时，下列因素被认为是评估验证服务商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)验证服务商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 (在密码钥匙可能遗失或失密的情况下)。

(c) 数字签字程序小结

62. 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密码钥匙；

(2) 签字人在计算机上起草电文(例如，采用电子邮件电文的形式)；

(3) 签字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；

(4) 签字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) 签字人一般将其数字签字附在电文之后；

(6) 签字人利用电子手段将数字签字和(未加密或已加密的)电文发给依赖方；

(7) 依赖方利用签字人的公用钥匙核查签字人的数字签字。利用签字人公用钥匙所作的核查可提供某种程度的技术保证，确保电文完全来自签字人；

(8) 依赖方也创建电文的“电文摘要”，利用同样的保密散列算法进行；

(9) 依赖方对比两种电文摘要。如果二者一样，则依赖方知道电文经签字后未作改动。电文经数字签字后，即使有一丁点改动，依赖方产生的电文摘要也会与签字人产生的电文摘要不同；

(10) 依赖方从验证服务商(包括通过签字人或以其他方式)取得证书，证书确认签字人电文上的数字签字（见 A/CN.9/484，第 44 段）。证书载有签字人的公用钥匙和姓名(可能还有其他信息)，并经由验证服务商数字签字。

四. 示范法的主要特点

A. 示范法的立法性质

63. 编拟示范法时所依据的设想是，示范法应直接来自《贸易法委员会电子商务示范法》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）。

64. 提出了该文书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，一致同意应将示范法案文制订成附有评注的一套立法规则，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）。该案文最后作为示范法通过（A/CN.9/483，第 137－138 段）。

B. 与《贸易法委员会电子商务示范法》的关系

1. 新示范法作为一项单独的法律文书

65. 本来也可扩大《贸易法委员会电子商务示范法》将新的条文纳入其中，例如构成《贸易法委员会电子商务示范法》新的第三部分。为了明确表明示范法可单独或结合《贸易法委员会电子商务示范法》一起颁布，最后决定新示范法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新示范法时，《贸易法委员会电子商务示范法》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《贸易法委员会电子商务示范法》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《贸易法委员会电子商务示范法》可能会在那些最近已通过《贸易法委员会电子商务示范法》的国家中造成混乱。

2. 新示范法与《贸易法委员会电子商务示范法》完全一致

66. 在起草新示范法时，已作出了一切努力，确保与《贸易法委员会电子商务示范法》实质内容和术语保持一致（A/CN.9/465，第 37 段）。新的文书中转载了《贸易法委员会电子商务示范法》的一般性条款。这些是《贸易法委员会电子商务示范法》的第 1 条（适用范围）、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）。

67. 新示范法以《贸易法委员会电子商务示范法》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；对当事方自主权的广泛依赖（A/CN.9/WG.IV/WP.84，第 16 段）。其目的是既作为在“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，又酌情作为在“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）下的示范合同规定或缺省规则。

3. 与《贸易法委员会电子商务示范法》第 7 条的关系

68. 在编拟新示范法时，有人表示认为，新示范法第 6 条案文中提及《贸易法委员会电子商务示范法》第 7 条应被解释为将新示范法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，大多数国家的法律载有的这类要求很少，所以新示范法的范围非常狭窄。针对上述看法，普遍认为，对第 6 条草案（和《贸易法委员会电子商务示范法》第 7 条）的这种解释与委员会在《贸易法委员会电子商务示范法颁布指南》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，《贸易法委员会电子商务示范法》第 7 条和新示范法第 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

69. 作为《贸易法委员会电子商务示范法》的一个补充，新示范法旨在规定基本原则，为使用电子签字提供便利。但是，作为一个“框架”，示范法本身并没有规定（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，示范法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，为示范法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，不损害示范法的各项目标。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。商业惯例长期以来都依赖自愿性技术标准程序。此类技术标准构成了产品规格、工程和设计标准以及未来产品研究与开发共识的基础。为了确保此项商业惯例所依赖的灵活性、促进为通用性提供便利的公开标准和支持跨界承认的目标（如第 12 条所述），各国似宜适当顾及国家条例已载入或批准的任何规格同自愿性技术标准程序之间的关系。

70. 应该指出，示范法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示范法中找到，而是要在其他法律中才能找到。这些其他法律例如可包括适用的行政法、合同法、侵权赔偿法、刑事法和司法程序法，示范法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

71. 关于承认电子签字在功能上等同手写签字，《贸易法委员会电子商务示范法》第 7 条规定了灵活的标准。新示范法的主要特点之一就是增加这项标准在操作上的确定性。《贸易法委员会电子商务示范法》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：[…]。”

72. 正如上文第 29 段所述，第 7 条是以承认在书面环境下签字的功能为基础的。

73. 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。

74. 第(1)(b)款对根据第(1)(a)款采用的鉴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。

75. 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）。

76. 在《贸易法委员会电子商务示范法》第 7(1)(b)所载的灵活标准基础上，新示范法第 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。示范法按关于承认电子签字在功能上等同于手写签字这个问题上实现确定性的时间，确立了两种不同的制度。第一种也是范围较广的一种制度，是《贸易法委员会电子商务示范法》第 7 条所述的电子签字，这种制度承认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。第二种也是范围较窄的一种制度，是示范法提出的电子签字，这种制度设想采用可能为国家机构、经正式认可的私人实体或当事各方本身承认符合示范法所定技术可靠性标准的电子签字方法（见 A/CN.9/484，第 49 段）。这种承认的优点是在这类电子签字技术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

77. 示范法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。这些问题留待示范法以外的适用法处理。但是，示范法制订了这些当事方（即签字人、依赖方和验证服务商）行为的评定标准。

78. 关于签字人，示范法详细阐述了基本原则，即签字人对其电子签字制作数据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制作数据。数字签字本身并不保证实际操作签字的人是签字人。数字签字充其量只是保证该签字归属于签字人（见 A/CN.9/484，第 50 段）。在签字人知悉或理应知悉该签字制作数据已经失密的情况下，签字人应毫无任何不应有的延迟，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。

79. 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。

80. 验证服务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。其中还应表明：(1)证书中所指明的签字人在证书签发时拥有对签字制作数据的控制；(2)在证书签发之日或之前签字制作数据运作正常。为了依赖方的利益，验证服务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)对签字制作数据的或证书的可能用途或使用金额上的任何限制；(3)签字制作数据的运作状况；(4)对验证服务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制作数据已经失密的通知的途径；(6)是否提供及时的撤销服务。

81. 对于评估证书服务提供商使用的系统、程序和人力资源的可信赖度，示范法作为示例列举了其中一些因素。

F. 不偏重任何技术的框架

82. 鉴于技术革新的速度，示范法规定了电子签字的法律承认标准，而不论所采用的是何种技术（例如，利用非对称加密法的数字签字；生物计量法（能够通过人的自然特征鉴别个人，例如通过手形或面部几何学、读取指纹、声明识别或视网膜扫描等）；对称密码法；使用个人识别码；通过签字人持有的智能卡或其他装置，使用“令牌”作为认证数据电文的一种方式；手写签字的数字式样；签字动态法以及诸如点击“OK框”等其他方法）。所列各种技术可合并使用，以减少系统性风险（见 A/CN.9/484，第 52 段）。

G. 不歧视外国电子签字

83. 示范法确立了一项基本原则，即来源地本身绝对不应成为外国证书或电子签字是否应被承认在颁布国可具有法律效力及法律效力程度的一个决定因素（见 A/CN.9/484，第 53 段）。决定证书或电子签字是否可具有法律效力或法律效力的程度，不应取决于证书或电子签字的签发地（见 A/CN.9/483，第 27 段）。而是应取决于其技术可靠性。这一基本原则在第 12 条中作了详细阐述（见下文，第 152-160 段）。

五. 贸易法委员会秘书处提供的协助

A. 起草立法方面的协助

84. 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示范法》制订立法。凡考虑根据贸易法委员会其他示范法（即《贸易法委员会国际商事仲裁示范法》、《贸易法委员会国际贷记划拨示范法》、《贸易法委员会货物、工程和服务采购示范法》、《贸易法委员会电子商务示范法》以及《贸易法委员会跨国界破产示范法》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。

85. 关于贸易法委员会制定的示范法及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
主页网址： http://www.uncitral.org

B. 关于以示范法为基础的立法的说明资料

86. 秘书处欢迎对示范法和指南提出意见，并欢迎提供关于以示范法为基础颁布的立法的资料介绍。示范法一旦颁布后，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。

第二章. 逐条说明

标题

“示范法”

87. 这份文书在整个编写过程中，始终被设想为是对《贸易法委员会电子商务示范法》的一个补充，因此，应与《贸易法委员会电子商务示范法》的一个补充，因此，应与《贸易法委员会电子商务示范法》同样对待，并具有与《贸易法委员会电子商务示范法》同样的法律性质。

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。

概论

88. 第 1 条的目的是阐明示范法的适用范围。示范法中所采用的方法是在原则上涵盖使用电子签字的所有实际场合，不论所采用的具体电子签字或认证技术如何。在拟订示范法时，工作组认为，如果限制示范法的范围，将任何形式或手段排除在外，则有可能造成实际困难，并且违背规定真正“不偏重任何手段的”和“不偏重任何技术的”规则的宗旨。在拟订示范法过程中，贸易法委员会电子商务工作组虽然意识到“数字签字”，即通过采用双钥加密技术获得的那些电子签字，是一项特别普及的技术，但仍然遵守了不偏重任何技术的原则（见 A/CN.9/484，第 54 段）。

脚注[**]

89. 工作组认为，示范法中应指明，其重点在于商务领域中遇到的各类情形，而且示范法是以贸易和金融关系为背景编拟的。为此原因，第 1 条提及“商务活动”，并在脚注[**]中指明了其含义。为了统一一致的原因，这样的指明是参照《贸易法委员会国际商事仲裁示范法》第 1 条脚注的模式而来的（另作为《贸易法委员会电子商务示范法》第 1 条脚注[****]转载），对于无单独一套商法的国家来说，这样指明可能特别有用。在某些国家，法规案文中使用脚注被认为不是一种可以接受的立法方式。因此，颁布示范法的国家当局似可考虑能否将脚注中的文字列入案文的正文中。

脚注[*]

90. 示范法适用于附上了具有法律效力的电子签字的所有各类数据电文，示范法概不妨碍颁布国扩大示范法的范围，使其包括在商务领域以外使用的电子签字。例如，虽然示范法的重点并不在于电子签字的使用者与公共当局之间的关系，但示范法并非不能够适用于这类关系。脚注[*]提供了备选措词，供认为似宜将示范法范围扩大到商务领域以外的颁布国考虑使用。

消费者保护

91. 一些国家有专门保护消费者的法律可能管辖使用信息系统时所涉及的某些问题。对于这类消费者立法，如同贸易法委员会以往的文书一样（例如，《贸易法委员会国际贷记划拨示范法》和《贸易法委员会电子商务示范法》），工作组认为，应该指明在起草示范法时并未特别考虑在保护消费者方面可能产生的问题。与此同时，工作组还认为，没有理由通过一项总则将那些涉及消费者的情形排除在示范法的范围之外，尤其是视各颁布国的立法而定，示范法的规定可能非常有利于对消费者的保护。因此，第 1 条确认，凡这类保护消费者的法律均可优先于示范法的规定。如果立法人员对示范法是否可为本国的消费者交易带来有益的影响这一点得出不同的结论，可考虑将消费者排除在颁布示范法的该项立法的适用范围之外。哪些个人或法人将被视作“消费者”，这个问题留待示范法以外的适用法律处理。

电子签字在国际和国内贸易中的使用

92. 建议尽可能扩大示范法的适用范围。如排除示范法的适用，将其范围局限于电子签字在国际上的使用，应特别小心谨慎，因为可以认为这种限制将不能充分达到示范法的目标。另外，示范法中也规定了各种程序，可以在必要时对电子签字的使用作一定的限制（例如为公共政策的目的），这也减少了限制示范法范围的必要性。示范法提供的法律确定性对国内和国际贸易都是必要的。对国内使用的电子签字和国际贸易交易中使用的电子签字区别对待，可能导致对使用电子签字的双重管辖制度，从而造成对使用这种技术的严重障碍（见 A/CN.9/484，第 55 段）。

贸易法委员会文件参考资料

A/CN.9/484，第 54—55 段；
A/CN.9/WG.IV/WP.88，附件，第 87—91 段；
A/CN.9/467，第 22—24 段；
A/CN.9/WG.IV/WP.84，第 22 段；
A/CN.9/465，第 36—42 段；
A/CN.9/WG.IV/WP.82，第 21 段；
A/CN.9/457，第 53—64 段。

第 2 条. 定义

在本法中：

(a) “电子签字”系指在数据电文中，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字人和表明签字人认可数据电文所含信息；

(b) “证书”系指确认签字人与签字制作数据之间关系的某一数据电文或其他记录；

(c) “数据电文”系指经由电子手段、光学手段或类似手段生成、发送、接收或储存的信息，这些手段包括但不限于电子数据交换、电子邮件、电报、电传或传真；

(d) “签字人”系指持有签字制作数据的人，代表本人或所代表的人行事；

(e) “验证服务商”系指签发证书和可能提供与电子签字有关的其他服务的人。

(f) “依赖方”系指可能根据某一证书或电子签字行事的人。

“电子签字”的定义

功能上等同于手写签字的电子签字

93. “电子签字”的概念意在包括具有法律效力的手写签字的所有传统用途和鉴别签字人，而签字的意图则只不过是各种法律制度中各种“签字”手段最基本的共同特点。在

编写《贸易法委员会电子商务示范法》第 7 条时，已经讨论过手写签字的这些功能。因此，将电子签字界定为能够表明认可信息，这主要是为了确定一个技术先决条件，以便承认某项技术手段能够等同于手写签字。通常称作“电子签字”的技术手段除用于制作具有法律效力的签字之外，还可用于其他目的，而上述定义并没有忽视这一事实。定义只是表明了示范法的重点在于使用电子签字作为功能上等同于手写签字的手段（A/CN.9/483，第 62 段）。

电子签字其他可能的用途

94. 应对“签字”的法律概念和“电子签字”的技术概念加以区别，电子签字这个固定术语中所包括的做法不一定涉及制作具有法律效力的签字。在编写示范法时，认为应提醒使用者注意，使用同一种技术工具既可以用于制作具有法律效力的签字，也可以用于其他认证或鉴别职能，从而可能造成混淆（同上）。

“证书”的定义

定义的必要性

95. 某些种类电子签字中使用的和示范法所界定的“证书”一词，不外乎是指某人用以确认某些事实的文件，与这个一般含义没有什么不同。唯一区别是证书采用的是电子形式，而不是书面形式(见 A/CN.9/484，第 56 段)。但是，并不是所有法律制度中，或甚至所有语言中都可能有“证书”的一般概念，所以认为宜在示范法中列入其定义（见 A/CN.9/483，第 65 段）。

证书的用途

96. 证书的用途是承认、表明或确认签字制作数据与签字人之间的联系。这种联系在生成签字制作数据时产生（同上，第 67 段）。

“签字制作数据”

97. 在非数字签字的电子签字中，“签字制作数据”一词是为了指在制作电子签字过程中用以提供所产生的电子签字与签字人本人之间可靠联系的那些秘密钥匙、编码或其他要素（见 A/CN.9/484，第 57 段）。例如在以生物鉴别装置为基础的电子签字中，基本要素是生物鉴别标志，例如指纹或视网膜扫描数据。这一术语的定义中仅包括为确保签字过程质量而应加以保密的那些核心要素，对于那些虽然可能有助于签字过程但既使公开也不会影响所形成的电子签字的可靠性的任何其他要素，则不包括在内。而在依靠非对称密码技术的数字签字情况下，可称作“与签字人相关联的”核心操作要素就是密码配对钥匙。在数字签字中，公用钥匙和私人钥匙都与签字人本人相关联。由于在数字签字的情况下，证书的首要目的是确认公共钥匙与签字人之间的联系（见上文第 53-56 段和第 62(10)段，所以还必须验证公用钥匙也属于签字人。虽然“签字制作数据”这一术语仅包括私人钥匙，但应该指出，为了避免疑虑，在数字签字的情况下，第 2(b)条中“证书”的定义应理解为包括确认签字人与签字人公用钥匙之间的联系。这一术语中不包括的其他内容还有经电子签字的案文，尽管在签字（通过散列函数或其他方式）制作过程中，案文也起重要的作用。第 6 条表示的设想是，签字制作数据应与签字人而不是还与其他人相关联（见 A/CN.9/483，第 75 段）。

“数据电文”的定义

98. “数据电文”的定义取自《贸易法委员会电子商务示范法》第 2 条，这是一个广泛的概念，包括网上商务在内的电子商务环境下生成的所有电文（同上，第 69 段）。“数据电文”的概念并不局限于通信，而是还意在包括计算机生成的并非用于通信的记录。因此，“数据”的概念包括“记录”的概念。

99. 这里提到的“类似手段”一词是为了反映《示范法》不仅打算适用于现有的通信技术，而且打算适用于未来可能预料的技术发展。“数据电文”的定义的目的是要包含基本上以无纸形式生成、储存或传递的各类电文。为此目的，提及“类似手段”意在包括可用于履行定义中所列各种手段同样功能的所有信息传递和储存手段，尽管“电子”传递手段和“光学”传递手段严格地说可能并不相似。就示范法而言，“类似”一词意为“功能上等同”。

100. “数据电文”的定义还意在适用于撤销或修订的情况。一项数据电文假定具有固定的信息内容，但可以通过另一数据电文加以撤销或修订（《贸易法委员会电子商务示范法颁布指南》，第 30—32 段）。

“签字人”的定义

“人”

101. 与《贸易法委员会电子商务示范法》所采取的做法相一致，新示范法中凡提到“人”这个字均应理解为包括各种类型的人或实体，无论是自然人、法人团体还是其他法人均包括在内（A/CN.9/483，第 86 段）。

“代表所代表的人”

102. 对于利用现代技术提供的可能性来说，参照手写签字的做法可能并不总是适当的。例如，在纸张环境下，严格地说，法人不可能成为以其名义拟定的文件的签字人，因为只有自然人才能制作真实的手写签字。但是，电子签字可被设想是由公司或其他法人实体（包括政府和其他公共当局在内）完成的，在要求采取人为行动的某些情况下，实际进行签字的人的身份对制作签字的用途可能毫不相关（同上，第 85 段）。

103. 然而，在示范法中，签字人的概念不能与实际制作电子签字的人或实体相分离，因为示范法规定的签字人的一些具体义务在逻辑上与对签字制作数据的实际控制相关。但是，为了将签字人代表他人签字的情况包括在内，“签字人”的定义中保留了“或所代表的人”一语。“委托他人”制作电子签字的人在多大程度上受电子签字的约束，这个问题应根据签字人和签字委托人作为一方与依赖方作为另一方这两者之间法律关系的适当管辖法律来解决。这个问题以及与基本交易相关的其他问题，包括代理问题和在签字人未能遵守第 8 条规定的义务时应由谁承担最后责任（是签字人还是签字人的委托人）等其他问题，不属于示范法的范畴（同上，第 86—87 段）。

“验证服务商”的定义

104. 就示范法而言，所界定的验证服务商至少必须提供验证服务，如有可能，还连带提供其他服务（同上，第 100 段）。

105. 对于验证服务商从事的提供验证服务是作为其主要活动还是作为一项附属业务，是经常性还是偶尔为之，是直接提供的还是通过分包商提供的，示范法并不加以区分。定义包括凡在示范法范畴内（即“在商业活动中”）提供验证服务的所有实体。但是，鉴于示范法适用范围上的这种限制，为内部目的而不是为商业目的签发证书的实体将不属于第 2 条界定的“验证服务商”的范畴（同上，第 94—99 段）。

“依赖方”的定义

106. “依赖方”的定义是为了确保在示范法中匀称整齐地列出电子签字系统在操作上所涉及的各当事方的定义（同上，第 107 段）。就该定义而言，“行事”一词应作广义的解释，不仅包括作为，也包括不作为（同上，第 108 段）。

贸易法委员会文件参考资料

A/CN.9/484，第 56—57 段；
A/CN.9/WG.IV/WP.88，附件，第 92—105 段；
A/CN.9/483，第 59—109 段；
A/CN.9/WG.IV/WP.84，第 23—36 段；
A/CN.9/465，第 42 段；
A/CN.9/WG.IV/WP.82，第 22—33 段；
A/CN.9/457，第 22-47 段；第 66—67 段；第 89 段；第 109 段；
A/CN.9/WG.IV/WP.80，第 7—10 段；
A/CN.9/WG.IV/WP.79，第 21 段；
A/CN.9/454，第 20 段；
A/CN.9/WG.IV/WP.76，第 16—20 段；
A/CN.9/446，第 22—46 段（第 1 条草案）、第 62—70 段（第 4 条草案）、第 113—131 段（第 8 条草案）、第 132—133 段（第 9 条草案）；
A/CN.9/WG.IV/WP.73，第 16—27 段、第 37—38 段、第 50—57 段和第 58—60 段；
A/CN.9/437，第 29—50 段和第 90—113 段（A、B 和 C 条草案）；
A/CN.9/WG.IV/WP.71，第 52—60 段。

第 3 条. 签字技术的平等对待

除第 5 条外，本法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。

不偏重任何技术

107. 第 3 条所载的根本原则是不歧视任何电子签字方法，即所有技术在是否满足第 6 条的要求方面都被给予同样的机会。因此，如果符合示范法第 6(1)条规定的基本要求，或符合适用的法律规定的任何其他要求，电子签字的电文与手写签字的书面文件之间，或各种电子签字的电文之间，将同等对待。这类要求可能例如规定在某些指定的场合下使用一种特定的签字技术，或可能制定了高于或低于《贸易法委员会电子商务示范法》第 7 条（和示范法第 6 条）规定的一项标准。不歧视的基本原则旨在普遍适用。

但是应该指出，这一原则并不是为了影响第 5 条确认的合同自由。因此，在当事方彼此之间并在法律允许的限度内，当事各方仍可保留合同自由，可经由协议排除某些电子签字技术的使用。通过规定“本规则的适用概不排斥、限制或剥夺可生成电子签字的任何方法的法律效力”，第 3 条仅仅表明某项电子签字所采用的形式不能作为否定该签字法律效力的唯一理由。但是，也不应将第 3 条错误地解释为确立了任何特定签字技术或任何电子签字信息的法律有效性。

贸易法委员会文件参考资料

A/CN.9/WG.IV/WP.88，附件，第 106 段；
A/CN.9/467，第 25－32 段；
A/CN.9/WG.IV/WP.84，第 37 段；
A/CN.9/465，第 43－48 段；
A/CN.9/WG.IV/WP.82，第 34 段；
A/CN.9/457，第 53－64 段。

第 4 条. 解释

(1) 对本法作出解释时，应考虑到其国际渊源以及促进其统一适用和遵守诚信的必要性。

(2) 对于由本法管辖的事项而在本法内未明文规定解决办法的问题，应按本法所依据的一般原则解决。

渊源

108. 第 4 条是受《联合国国际货物销售合同公约》第 7 条的启发并从《贸易法委员会电子商务示范法》第 3 条转载而来的。其用意是作为仲裁庭、法院和其他国家当局或当地行政当局在解释示范法时的指南。第 4 条的预期效用是限制统一案文纳入当地立法之后只能以当地法律概念为准作为解释的范围。

第(1)款

109. 第(1)款的目的是提请可能被要求适用示范法的任何人注意，示范法的条款（或示范法的实施文书的条款）虽然被颁布作为本国立法的一部分，因而具有本国特性，但在解释时应考虑到其国际渊源，以确保所有颁布国在示范法解释上的统一性。

第(2)款

110. 在示范法所依据的一般原则中，可适用的原则试列举一二如下：(1)促进各国之间和各国内部的电子商务；(2)确立通过新信息技术手段达成的交易的有效性；(3)以不偏重任何技术的方式促进和鼓励采用一般的新信息技术，特别是电子签字；(4)促进法律的统一性；(5)支持商务活动。虽然示范法的总体宗旨是促进电子签字的使用，但绝对不应将之解释为强制规定电子签字的使用。

贸易法委员会文件参考资料

A/CN.9/WG.IV/WP.88，附件，第 107－109 段；
A/CN.9/467，第 33－35 段；
A/CN.9/WG.IV/WP.84，第 38 段；
A/CN.9/465，第 49－50 段；
A/CN.9/WG.IV/WP.82，第 35 段。

第 5 条. 经由协议的改动

本法的规定可经由协议而加以删减或改变其效力，除非根据适用法律，该协议无效或不具有效力。

尊重适用法

111. 作出决定开展示范法编拟工作的基本前提是承认实际上主要在合同中寻求对使用现代通信技术而引起的法律困难的解决办法。因此，示范法意在支持当事方自主权原则。但是，使用的法律可能对该原则的适用规定了限制。对第 5 条不应错误地解释为允许当事各方删减强制性规则，例如为公共政策原则而通过的规则。第 5 条也不应解释为鼓励各国制定强制性立法从而在电子签字方面限制当事方自主权的效力，或邀请各国限制当事方彼此之间就其通信的形式要求问题达成协议的自由。

112. 当事方自主权原则对示范法广泛适用，因为示范法中不载有任何强制性规定。这原则也适用于第 13(1)条的情形。因此，虽然颁布国的法院或负责实施示范法的当局不应当仅以某一外国证书签发的地点为由而拒绝承认该证书的法律效力或宣布其无效，但第 13(1)条并不限制商务交易的当事方可自行商定使用来自某一特定地点的证书（A/CN.9/483，第 112 段）。

明示或暗示的协议

113. 关于当事方自主权原则在第 5 条中的表现方式，工作组在拟订示范法时普遍承认，经由协议的改动可以是明示的，也可以是暗示的。第 5 条的措词与《联合国国际货物销售合同公约》第 6 条保持一致(A/CN.9/467，第 38 段)。

双边或多边协议

114. 第 5 条不仅旨在适用于数据电文发件人与收件人之间的关系，而且还适用于涉及中间人的关系。因此，示范法的规定可通过当事方之间双边或多边协议或当事方商定的系统规则加以改动。一般来说，适用法将把当事方自主权限定于当事方之间产生的权利与义务范围内，以避免对第三方权利与义务造成任何影响。

贸易法委员会文件参考资料

A/CN.9/WG.IV/WP.88，附件，第 110－113 段；
A/CN.9/467，第 36－43 段；
A/CN.9/WG.IV/WP.84，第 39－40 段；

A/CN.9/465，第 51－61 段；
A/CN.9/WG.IV/WP.82，第 36－40 段；
A/CN.9/457，第 53－64 段。

第 6 条. 符合签字要求

(1) 凡法律规定要求有一人的签字时，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) 签字制作数据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) 签字制作数据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 6 条的重要性

115. 第 6 条是示范法的核心条款之一。第 6 条是为了在《贸易法委员会电子商务示范法》第 7 条的基础上更进一步，对如何可达到第 7(1)(b)条规定的可靠性检验标准提供指南。在解释第 6 条时，切记该条款的目的是确保如果使用手写签字会带来任何法律后果，那么使用可靠的电子签字也应带来同样的后果。

第(1)、(2)和(5)款

116. 第 6 条第(1)、(2)和(5)款分别转载了《贸易法委员会电子商务示范法》第 7(1)(b)、7(2)和 7(3)条。根据《贸易法委员会电子商务示范法》第 7(1)(a)条的启发而提出的措词已载入第 2(a)条“电子签字”的定义。

“身份”和“鉴别”的概念

117. 工作组商定，为界定示范法中的“电子签字”，“鉴别”一词的范围可比仅仅鉴别签字人姓名更广些。身份或鉴别的概念包括以姓名或其他方式将之与其他任何人区别开来，可指称其他重要的特征，例如职位或职权，可与姓名并用，或不提姓名。在此基础上，对身份和其他重要的特征不必加以区分，也不必将示范法局限于仅使用列有签字持有人姓名的身份证件的情形(A/CN.9/467，第 56－58 段)。

示范法的效力随技术可靠性程度变化

118. 在拟订示范法时，有人表示认为，（要么通过提及“增强式电子签字”的概念，要么通过直接提及确立某项签字技术的技术可靠性标准，）第 6 条的双重目的应是确立：(1)使用经确认可靠的电子签字技术将具有法律效力；(2)反过来说，使用可靠性不高的技术将无这种法律效力。但是普遍认为，对于可能的各种电子签字技术，可能还需要加以细分，因为示范法应避免歧视任何电子签字形式，即使该形式在某种场合下可能看来不够精致和安全。因此，为根据《贸易法委员会电子商务示范法》第 7(1)(a)条对数据电文加以签字而采用的任何电子签字技术，只要从所有情形来看，包括根据当事方之间的任何协议都认为足够可靠，那么便可能产生法律效力。但是，根据《贸易法委员会电子商务示范法》第 7 条，关于什么构成适合具体情形的可靠签字方法，可能只能是在使用电子签字很长时间之后由法院来决定，或由事后再作尝试的其他人员来决定。对比之下，新示范法将更有利于那些无论使用场合都被认为特别可靠的某些技术。这是第(3)款的目的，该款将（通过推定或一项实质性规则）在使用任何这类电子签字技术时或之前（事先）建立明确性，指明使用公认的技术将产生与手写签字相同的法律效力。因此，就使用某些特别可靠的电子签字方式而将产生的法律效力而言，如果新示范法要达到其目标，提供比《贸易法委员会电子商务示范法》更直接的确定性，那么第(3)款就是一项根本性规定（见 A/CN.9/465，第 64 段）。

推定或实质性规则

119. 关于使用第 2 条界定的电子签字后而产生的法律效力，为了提供确定性，第(3)款明确规定了电子签字的某些技术特点综合产生的法律效力（见 A/CN.9/484，第 58 段）。至于如何确定这些法律效力，颁布国应该根据各自的民事诉讼法和商务程序法，自行通过推定或通过直接认定签字的某些技术特点与法律效力之间的联系（见 A/CN.9/467，第 61－62 段）。

签字人的意图

120. 如果签字人使用电子签字技术核准经电子签字的信息，但没有明显的意图表明将接受其法律约束力，那么对这种情况是否应产生法律效力，仍有疑问。在任何此种情形下，《贸易法委员会电子商务示范法》第 7(1)(a)条所述的第二项功能没有实现，因为没有“意图表明对数据电文中所含的信息的任何认可”。示范法中所采取的做法是在电子环境中应具有与使用手写签字同样的法律后果。因此，通过在信息之后加上签字（无论是手写签字还是电子签字），签字人都应被推定认可了其身份与该信息之间的联系。这种联系是否应产生法律效力（合同效力或其他效力），将取决于所签字的信息的性质，以及根据示范法以外适用的法律加以评估的任何其他情形。在这种情况下，示范法并非意在干涉关于合同或义务的一般法律（见 A/CN.9/465，第 65 段）。

技术可靠性的标准

121. 第(3)款(a)至(d)项是为了表明电子签字技术可靠性的客观标准。(a)项着重于签字制作数据的客观特征，即必须“与签字人而不是还与其他任何人相关联”。从技术角度来看，签字制作数据可以单独与签字人“相关联”，而本身并不是“独一无二的”。用于制作签字的数据与签字人之间的关联是必不可少的因素(A/CN.9/467,第 63 段)。虽然某些电子签字制作数据可能是许多使用者共享的，例如公司的若干工作人员共同使用公司的签字制作数据，但这种数据必须能够在每个电子签字中毫无含糊地鉴别出其使用者。

签字人对签字数据的唯一控制

122. (b)款述及的是使用签字制作数据的情形。签字制作数据在使用时必须处于签字人的唯一控制之中。关于签字人的唯一控制这个概念，一个问题是签字人是否将保留其授权另一人的能力，以便该人可代表其使用签字数据。出现这种情形的场合是公司中使用的签字数据，公司实体将是签字人，但需要若干人才能代表其签字（A/CN.9/467,第 66 段）。另一个例子可见于商业应用，例如签字数据存在于网络上，并且能够供若干人使用。在这种情况下，按推定网络将与某个实体相关，该实体将是签字人并保持对签字制作数据的控制。如果不是这样，签字数据可普遍得到，那么这一签字数据就不应包括在示范法的范围内（A/CN.9/467,第 67 段）。如一把钥匙由一人以上按“组合式钥匙”或其他“共享秘密”的方法操作，则提及“签字人”系一并指这些人（A/CN.9/483，第 152 段）。

代理

123. (a)和(b)项加在一起可确保在任何特定时候，主要在签字时，签字制作数据只能由一人使用，而不是还可由其他人使用（见上文，第 103 段）。代理或授权使用签字制作数据的问题在“签字人”的定义中阐述(A/CN.9/467，第 68 段)。

完整性

124. (c)和(d)项述及电子签字完整性和经电子签字的信息的完整性问题。可以将两项规定合在一起强调这样的观念，即当文件附有签字时，文件的完整性和签字的完整性密切相关，难以想象二者缺一的情形。但是，工作组决定示范法应采用《贸易法委员会电子商务示范法》第 7 条与第 8 条之间所作的区别处理方式。虽然有些技术可同时提供认证（《贸易法委员会电子商务示范法》第 7 条）和完整性（《贸易法委员会电子商务示范法》第 8 条），但这些概念可被视作不同的法律概念，而且可以作这样的处理。由于手写签字并不能担保经签字的文件的完整性，也不能担保对文件的任何改动将可被觉察，所以功能上的等同这一做法要求这些概念不应集中在一项规定中论述。第(3)(c)款的目的是规定所应达到的标准，以便表明某种电子签字方法非常可靠，足以满足法律对签字的要求。这项法律要求可以在不必表明整个文件完整性的情况下得到满足（见 A/CN.9/467，第 72—80 段）。

125. 在有些国家中，关于使用手写签字的现有法律规则不对签字的完整性与经签字的信息的完整性加以区分，(d)款主要就是为了在这些国家中使用的。而在其他国家，(d)款形成的签字将可能比手写签字更为可靠，从而超出与签字在功能上等同的概念。在

某些法域，(d)款的效用可能是形成一种在功能上与原始文件等同的形式（见A/CN.9/484，第62段）。

对电文一部分的电子签字

126. 在(d)项中，指明了签字与经签字的信息之间的必要关联，以避免暗含电子签字仅可适用于数据电文全部内容的意思。事实上，在许多情况下，经签字的信息将仅仅是数据电文中所含的信息的一部分。例如，电子签字可能仅涉及所传递的电文的附带信息。

经由协议的改动

127. 有些适用的法律承认当事各方可在任何有关的协定中自由规定其彼此之间对某种签字技术将视作手写签字的一种可靠同等方式。第(3)款并非意在限制第5条和任何此种法律的适用。

128. 第(4)(a)款是为了给商业活动提供一个法律依据，使许多商业当事方能够在此基础上就电子签字的使用问题通过合同调整彼此之间的关系（见A/CN.9/484，第63段）。

提出某个电子签字不可靠性的证据的可能性

129. 第(4)(b)款是为了指明，示范法并不限制可能存在的对第(3)款设想的推定加以否定的任何可能性（见A/CN.9/484，第63段）。

排除在第6条范围之外

130. 第(5)款所载的原则是颁布国可将示范法立法中拟加以规定的某些情况排除在第6条适用范围之外。特别是根据所确立的正式要求手写签字的场合，颁布国可能希望特别将某些种类的情况排除在外。可以考虑特别排除在外的例如包括依照颁布国的国际条约义务规定而要求的手续和超出颁布国的权利之外无法通过法规加以改变的那些情况和法律领域。

131. 列入第(5)款是为了增强示范法的可接受性。这一款确认应由颁布国具体指明拟加以排除的情况，这种方法将可更好地照顾到各国的国情差异。但是，应该指出，如果利用第(5)款确立广泛的例外情况，示范法的目标将不能实现，因此，应避免利用第(5)款在这方面所提供的机会。如果将许多情况排除在第6条的范围之外，将会产生对电子签字发展的不必要的障碍，因为示范法所载的是预计将可普遍适用的一些非常基本的原则和做法（见A/CN.9/484，第63段）。

贸易法委员会文件参考资料

A/CN.9/484，第58—63段
A/CN.9/WG.IV/WP.88，附件，第114—126段；
A/CN.9/467，第44—87段；
A/CN.9/WG.IV/WP.84，第41—47段；
A/CN.9/465，第62—82段；

A/CN.9/WG.IV/WP.82，第 42－44 段；
A/CN.9/457，第 48－52 段；
A/CN.9/WG.IV/WP.80，第 11－12 段。

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。

电子签字地位的预先确定

132. 颁布国可建立或承认对电子签字的使用确立其效力或以其他方式验证其质量的任何实体，第 7 条所述的就是颁布国在这方面的作用。如同第 6 条一样，第 7 条的指导思想是，为了促进电子商务的发展，商务当事方在使用电子签字技术时而不是将争端提交法院时，需要有确定性和可预见性。如果某项签字技术可满足高度可靠性和安全性的要求，就应该有对可靠性和安全性的技术特性进行评估的方法，这种签字技术也应相应地获得某种形式的承认。

第 7 条的宗旨

133. 第 7 条的宗旨是阐明，颁布国可指定一个机关或机构，这个机关或机构将有权对哪种特定技术可从第 6 条的规则中受益而作出决定。第 7 条并不是各国可以或必须按其目前形式加以颁布的一项授权条款。但是，其用意是传达一个明确的意思，即只要根据国际标准确定哪种电子签字技术符合第 6 条的可靠性标准，便可达到确定性和可预见性的目的。第 7 条不应解释成规定了使用某些种类签字技术的强制性法律效力，或将技术的使用范围局限于经确定符合第 6 条可靠性要求的那些技术。例如，当事各方应可自由地使用虽未经确定是否符合第 6 条要求但当事方彼此之间已商定加以使用的那些技术。当事各方也应可以自由地在法院或仲裁庭上表明所选用的签字方法的确符合第 6 条的要求，即使事先未经过如此确定。

第(1)款

134. 第(1)款阐明，对使用电子签字可确立其效力或以其他方式验证其质量的任何实体，不一定非得是国家机构不可。第(1)款不应理解为向各国提出了关于签字技术获得承认的唯一方法的建议，而应理解为指出了各国希望采用这种方法时所应适用的限制条件。

第(2)款

135. 关于第(2)款，“标准”的概念不应局限于例如国际标准化组织（标准化组织）和因特网工程工作队制定的标准，或局限于其他技术标准。“标准”一词应作广义的理解，包括业界惯例和商业习惯及国际商会、在标准化组织统一领导下运作的各区域认证机构、万维网集团等国际组织制定的文书（见 A/CN.9/484，第 66 段），以及贸易法委员会本身的著作（包括本示范法和《贸易法委员会电子商务示范法》在内）。可能

缺乏有关的标准，但这不应妨碍主管个人或机构如第(1)款所述加以确定。关于所提到的“公认”标准，对于什么构成“公认”和谁需要获得这种公认可能提出疑问（见A/CN.9/465，第 94 段）。这个问题在第 12 条下讨论（见下文，第 159 段）。

第(3)款

136. 第(3)款旨在充分阐明，第 7 条的目的并不是为了干预国际私法规则的正常运作（见A/CN.9/467，第 94 段）。如果没有这项规定，第 7 条可能被错误地理解为鼓励各颁布国以不符合第(1)款所述有关个人或机构制定的规则为由而对外国电子签字加以歧视。

贸易法委员会文件参考资料

A/CN.9/484，第 64－66 段；
A/CN.9/WG.IV/WP.88，附件，第 127－131 段；
A/CN.9/467，第 90－95 段；
A/CN.9/WG.IV/WP.84，第 49－51 段；
A/CN.9/465，第 90－98 段；
A/CN.9/WG.IV/WP.82，第 46 段。
A/CN.9/457，第 48－52 段；
A/CN.9/WG.IV/WP.80，第 15 段。

第 8 条. 签字人的行为

(1) 如签字制作数据可用于制作具有法律效力的签字，各签字人应当做到如下：

(a) 采取合理的谨慎措施，避免他人擅自使用其签字制作数据；

(b) 在发生下列情况时，毫无任何不应有的迟延，向按签字人合理预计可能依赖电子签字或提供支持电子签字服务的任何人员发出通知：

㈠ 签字人知悉签字制作数据已经失密；或

㈡ 签字人知悉签字制作数据很有可能已经失密的情况；

(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。

标题

137. 按最初的计划，第 8 条（和第 9 及第 11 条）将载有关于各有关当事方（签字人、依赖方和任何验证服务商）义务和责任的规则。但是，对电子商务技术和商务方面产生影响的迅速变化，以及在某些国家电子商务领域实行自律目前所起的作用，使工作组难以就这些规则的内容达成协商一致。所起草的这些条款是为了体现当事各方最低限度的“行为守则”。正如在关于验证服务商的第 9 条下所指出（见下文，第 144 段），示范法并不要求签字人达到与电子签字或证书的使用目的无合理关系的过度审慎或可

信赖度（见 A/CN.9/484，第 67 段）。因此，示范法主张将第 8 和第 9 条中阐明的义务与制作具有法律重要性的电子签字联系在一起的处理办法(A/CN.9/483，第 117 段)。签字人不遵守第(1)款时应负责任的原则载于第(2)款；不遵守该行为守则时这种责任的范围留待示范法以外的适用法律处理。

第(1)款

138. (a)项和(b)项普遍适用于所有电子签字，而(c)项仅适用于有证书支持的那些电子签字。特别是第(1)(a)款的义务，即采取合理防范措施避免他人擅自使用签字制作数据的义务，构成一项基本义务，这项义务例如已普遍载于关于使用信用卡的协议中。根据第(1)款通过的政策，这一义务也应适用于可用以表示具有法律效力的意图的任何电子签字制作数据。但是，第 5 条关于经由协议的改动的规定，允许就认为不适当或可导致意图之外后果的方面而对第 8 条制定的标准加以改动。

139. 第(1)(b)款提及“按签字人合理预计可能依赖电子签字或提供电子签字辅助服务的人员”的概念。视所采用的技术而定，这种“依赖方”可能不仅仅是意图依赖签字的某个人，而且也是其他一些人员，例如验证服务商、证书撤销服务提供商和任何其他有关当事方。

140. 第(1)(c)款适用于以证书支持签字装置的情形。“证书的周期”意在作广义的解释，包括从申请证书或创建证书开始，到证书期满或撤销证书为止的整个期间。

第(2)款

141. 第(2)款并未指明责任的后果或限度，这两方面都留待国内法处理。但是，第(2)款即使将责任的后果留待国内法处理，也有助于向颁布国发出一个明确的信号，即所负的责任应与未能满足第(1)款规定的义务相联系。第(2)款是以工作组第三十五届会议达成的结论为基础的，该结论是，可能很难就签字人的责任而可能产生的后果达成协商一致。根据现有法律，这类后果轻重不一，从签字人在法律上受电文内容的约束到损失赔偿责任不等，视使用电子签字的场合而定。因此，第(2)款仅仅制定了签字人应对未能满足(1)款要求而承担责任的原则，而将如何处理这种责任产生的法律后果问题交由示范法以外各颁布国的适用法律处理(A/CN.9/465，第 108 段)。

贸易法委员会文件参考资料

A/CN.9/484，第 67－69 段；
A/CN.9/WG.IV/WP.88，附件，第 132－136 段；
A/CN.9/467，第 96－104 段；
A/CN.9/WG.IV/WP.84，第 52－53 段；
A/CN.9/465，第 99－108 段；
A/CN.9/WG.IV/WP.82，第 50－55 段；
A/CN.9/457，第 65－98 段；
A/CN.9/WG.IV/WP.80，第 18－19 段。

第 9 条. 验证服务商的行为

(1) 如验证服务商提供服务，支持可用作具有法律效力的签字而使用的电子

签字，验证服务商应当做到如下：

(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：

㈠ 验证服务商的身份；

㈡ 证书中所指明的签字人在签发证书时拥有对签字制作数据的控制；

㈢ 在证书签发之日或之前签字制作数据有效；

(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 签字制作数据或证书的可能用途或使用金额上的任何限制；

㈢ 签字制作数据有效，且未发生失密；

㈣ 验证服务商规定的责任范围或程度上的任何限制；

㈤ 是否存在签字人依照第 8(1)(b)条发出通知的途径；

㈥ 是否开设及时的撤销服务；

(e) 在开设 d㈤项所述服务的情况下，提供签字人依照第 8(1)(b)条发出通知的途径，在开设 d㈥项所述服务的情况下，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) 验证服务商应对其未能满足第(1)款的要求而承担责任。

第(1)款

142. (a)项列出了一条基本原则，即验证服务商应遵守其所作的表述和承诺，例如在验证惯例声明或任何其他种类的政策声明中所作的表述和承诺。

143. (c)项界定了根据示范法任何证书的基本内容及其核心效用。应该指出，在数字签字的情况下，还必须可以查明签字人与公用钥匙以及与私人钥匙之间的关联(A/CN.9/484，第 71 段)。(d)项列出了应载入证书或以其他方式向依赖方提供或使之可及的、与该证书有关的附加内容。(e)项并非意在适用于交易证书等证书，因为这些是一次性的证书，或低风险应用的低额证书，这两种证书可能都不会遭受撤销。

144. 可能有人认为，可以合理地期望任何验证服务商，而不仅仅是签发“高价值”证书的提供商，均会遵守第 9 条草案规定的责任和义务。但是，示范法并不要求签字人或验证服务商达到与电子签字或证书的使用目的无合理关系的过度审慎或可信赖度。因此，示范法主张将第 8 和第 9 条中阐明的义务与制作具有法律重要性的电子签字联系在一起的办法（A/CN.9/483，第 117 段）。示范法将第 9 条的范围局限于那些提供验证服务以支持可用作具有法律效力的签字而使用的电子签字的广泛一系列情形，但

这样做的意图并不是为了创造签字的一些新型法律效力（同上，第 119 段）。

第(2)款

145. 第(2)款把如何确定责任后果留给国内法去处理（见 A/CN.9/484，第 73 段）。第(2)款需以适用的国内法规则为准，作者的用意并非在于将之解释为一项绝对责任规则。第(2)款的效用并不是预期将把验证服务商可证明例如无过错或无造成失误的过错这种情况排除在外。

146. 第 9 条最初的草案还载有另一款，其中阐述了第(2)款规定的责任后果。在编写示范法时，有人指出验证服务供应商的责任问题通过大致措词如第(2)款的一项规定将无法充分阐明。虽然第(2)款可指明一项适用于签字人的适当原则，但可能不足以充分阐明第 9 条所涵盖的专业和商业活动。弥补这种不足的一项可能方法本来可以是在示范法的案文中列出对验证服务商未能满足第(1)款要求而造成的任何损失进行评估时应考虑的各种因素。但最后决定，本指南中应将这些因素作为示例列举一二。在评估验证服务商的责任时，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)是否存在限制验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，应侧重于验证服务商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(A/CN.9/484，第 74 段)。

贸易法委员会文件参考资料

A/CN.9/484，第 70—74 段；
A/CN.9/WG.IV/WP.88，附件，第 137—141 段；
A/CN.9/483，第 114—127 段；
A/CN.9/467，第 105—129 段；
A/CN.9/WG.IV/WP.84，第 55—60 段；
A/CN.9/465，第 123—142 段（第 12 条草案）；
A/CN.9/WG.IV/WP.82，第 59—68 段；
A/CN.9/457，第 108—119 段；
A/CN.9/WG.IV/WP.80，第 22—24 段。

第 10 条. 可信赖性

为第 9(1)(f)条之目的，在确定验证服务商使用的任何系统、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。

“可信赖性”概念的灵活性

147. 当初在起草时，第 10 条曾作为第 9 条的一部分。虽然这部分后来成了单独的一条，但其主要用意是帮助说明第 9(1)(f)条中“可依赖的系统、程序和人力资源”的概念。第 10 条列举了在确定可信赖性时应考虑的部分因素。列出这些因素的用意是提供关于可依赖性的一种灵活概念，其内容可能会因制作证书时对证书的不同期望而异。

贸易法委员会文件参考资料

A/CN.9/WG.IV/WP.88，附件，第 142 段；
A/CN.9/483，第 128－133 段；
A/CN.9/467，第 114－119 段。

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。

依赖的合理性

148. 第 11 条反映的概念是，打算依赖电子签字的当事方应当切记根据具体情况这种依赖是否合理以及在何种程度上合理的问题。第 11 条并不是为了论述电子签字有效性的问题，这个问题在第 6 条中论述，并且不应当取决于依赖方的行为。电子签字有效性的问题应该与依赖方如果依赖不符合第 6 条所列标准的签字是否合理的问题区别开来。

消费者问题

149. 虽然第 11 条可能把责任放在依赖方身上，特别是当依赖方是消费者时，但可以回顾到，示范法的用意并非凌驾于关于保护消费者的任何规则之上。不过，示范法可发挥有益的作用，使包括依赖方在内的各有关当事方了解在电子签字方面应达到的合理行为标准。另外，制定一项有依赖方据以通过方便可及的手段核查签字可靠性的行为标准，可被看作是任何公用钥匙的基础结构系统发展的必要条件。

“依赖方”的概念

150.“依赖方”的概念与其定义相一致，意在包括可能依赖电子签字的任何当事方。

因此，视具体情况而定，“依赖方”可能是无论是否与签字人或验证服务商有合同关系的任何人。甚至还可以设想，验证服务商或签字人本人也可能成为“依赖方”。但是，“依赖方”的这种广义概念不应造成证书用户有义务核查其从验证服务商处购买的证书的有效性。

未能遵守第 11 条的要求

151. 关于规定依赖方应作为一项一般义务核查电子签字或证书是否有效这样做可能产生的影响，在依赖方未能遵守第 11 条的要求时将出现问题。如果依赖方未能遵守这些要求，在合理核查未能显示出签字或证书无效的情况下，不应不准许依赖方使用该签字或证书。第11条的规定并不是为了要求遵守限制或核查依赖方无法方便获取的信息。这种情况可能需要由示范法以外的适用法律处理。总体来说，依赖方不遵守第 11 条各项要求的后果由示范法以外的适用法律处理(A/CN.9/484，第 75 段)。

贸易法委员会文件参考资料

A/CN.9/484，第 75 段；
A/CN.9/WG.IV/WP.88，附件，第 143—146 段；
A/CN.9/467，第 130—143 段；
A/CN.9/WG.IV/WP.84，第 61—63 段；
A/CN.9/465，第 109—122 段（第 10 和 11 条草案）；
A/CN.9/WG.IV/WP.82，第 56—58 段（第 10 和 11 条草案）；
A/CN.9/457，第 99—107 段；
A/CN.9/WG.IV/WP.80，第 20—21 段。

第 12 条. 对外国证书和电子签字的承认

(1) 在确定某一证书或某一电子签字是否具有法律效力或在多大程度上具有法律效力时，不得考虑：

(a) 签发证书或制作或使用电子签字的地理位置；或

(b) 签发人或签字人营业地的地理位置。

(2) 在[颁布国]境外签发的证书，如具有基本等同的可靠性，则在[该颁布国]境内具有与在[该颁布国]境内签发的证书同样的法律效力。

(3) 在[颁布国]境外制作或使用的电子签字，如具有基本等同的可靠性，则在[该颁布国]境内具有与在[该颁布国]境内制作或使用的电子签字同样的法律效力。

(4) 在确定某一证书或某一电子签字是否为第(2)款或第(3)款之目的而具有基本等同的可靠性时，应当考虑到公认的国际标准或其他任何有关的因素。

(5) 如当事各方之间议定使用某些类别的电子签字或证书，即使有第(2)款、第(3)款和第(4)款的规定，仍应承认该协议足以成为跨国境承认的依据，除非根据适用法律该协议无效或不具有效力。

不歧视的一般规则

152. 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字是否能够具有法律效力或能够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字是否能够具有法律效力或能够具有多大法律效力，不应当取决于签发该证书或该电子签字的地点（见 A/CN.9/483，第 27 段），而应取决于其技术上的可靠性。

“基本等同的可靠性”

153. 第(2)款是为了提供对于跨国境承认证书的一般标准，没有这些标准，验证服务供应商将可能面临必须在多个法域中获取许可证的不合理负担。为此目的，按照颁布国依照示范法规定的可靠性要求检验外国证书的可靠性，第(2)款规定了外国证书技术上等同性的基本限度（同上，第 31 段）。这一标准将无论证书或签字来源地法域实行的验证办法的性质而一概适用（同上，第 29 段）。

可靠性的程度因法域而异

154. 通过提及“基本等同的可靠性”这一核心概念，第(2)款承认在各法域的要求之间可能存在着显著的差异。第(2)款所使用的等同性要求并不意味着外国证书的可靠程度应当与国内证书的可靠程度完全一致（同上，第 32 段）。

可靠性的程度在同一法域内的差异

155. 另外，还应该指出，实际上，验证服务供应商根据其客户打算使用证书的用途而签发不同可靠程度的证书。视各自的可靠程度，证书和电子签字可能会在本国和国外产生不同的法律效力。例如在某些国家，甚至有时称作“低额”或“低价值”的证书也可能在某些情况下（例如在当事方通过合同方式商定使用这类文书时）产生法律效力（见 A/CN.9/484，第 77 段）。因此，在运用第(2)款使用的等同性概念时，应牢记所要确立的等同性是功能上可作比较的证书之间的等同性。但是，示范法并不试图在不同法域不同验证服务供应商签发的不同种类证书之间确立一种对应的关系。示范法在拟定上已考虑到各种不同种类证书之间可能有一种等级关系。实际上，法院或仲裁庭在需要就外国证书的法律效力作出决定时，通常将根据每一证书的具体情况加以考虑，并尽量将该证书与颁布国中对应关系最接近的那一等级等同起来（同上，第 33 段）。

证书和其他种类电子签字的同等对待

156. 关于电子签字，第(3)款规定了与第(2)款对证书规定的同样规则（同上，第 41 段）。

承认符合外国法律的某种法律效力

157. 第(2)和第(3)款专门论述了在评估外国证书或电子签字的可靠性时应采用的跨国界可靠性检验标准。但是，在编写示范法时，考虑到当颁布国确信签字或证书的来源地法域的法律提供了一个充分的可靠性标准时，颁布国可能认为没有必要对具体的签字采用可靠性标准。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字的可靠性（同上，第 39 和 42 段）。

在评估外国证书和签字的基本等同性时应考虑的因素

158. 在编写示范法时，第(4)款最初罗列了在确定证书或电子签字就第(2)或第(3)款而言是否具有基本等同的可靠性时而应考虑的一系列因素。后来发现其中大部分因素已列入第 6、第 9 和第 10 条。在第 12 条中重复指出这些因素将是多余的。第(4)款是示范法中提及这些有关标准的适当条款，据认为，如果其中指出参见其他条款，而且还增列对跨国境承认特别重要的其他一些标准，那么将会造成措词过于复杂（特别见A/CN.9/483，第 43－49 段）。最后，第(4)款的措词成为非特指的“任何有关因素”，其中第 6、第 9 和第 10 条所列的用以评估本国证书和电子签字的因素特别重要。另外，事实上，评估外国证书的等同性与评估第 9 和第 10 条规定的验证服务商的可信赖程度略有不同，第(4)款正是由此产生的。为此，第(4)款中增加了“公认的国际标准”一语。

公认的国际标准

159. “公认的国际标准”的概念应作广义的解释，既包括国际技术和商业标准（即市场驱动的标准），也包括政府机构或政府间机构采用的标准和规范（同上，第 49 段）。“公认的国际标准”可以是对公认的技术、法律或商业惯例的阐述，无论是由公共部门还是由私营部门（或同时由这两类部门）拟定而成，属规范性质或解释性质，并经公认可在国际上适用。这些标准的形式可以为要求、建议、准则、行为守则或对最佳做法或规范的阐述”（同上，第 101－104）。

承认有关当事方之间的协议

160. 第(5)款规定承认有关当事各方之间就使用某些种类电子签字或证书而达成的协议足以构成（这些当事方之间）跨国境承认这种商定的签字或证书的依据（同上，第 54 段）。应该指出，第(5)款与第 5 条相一致，并非为了排除任何强制性法律，特别是颁布国可能希望在适用法律中保留的关于手写签字的任何强制性规定（同上，第 113 段）。当事各方之间可以根据合同规定而商定，彼此之间承认可使用某些电子签字或证书（在当事方可能谋求使这些签字或证书获得法律承认的某些或所有国家中，这些签字或证书可能被视作外国签字或外国证书），而这些签字或证书不受第(2)、第(3)和第(4)款规定的基本等同性检验，第(5)款正是为落实这些合同规定所需的。第(5)款并不影响第三方的法律地位（同上，第 56 段）。

贸易法委员会文件参考资料

A/CN.9/484，第 76－78 段；
A/CN.9/WG.IV/WP.88，附件，第 147－155 段；
A/CN.9/483，第 25－58 段（第 12 条）；
A/CN.9/WG.IV/WP.84，第 61－68 段（第 13 条草案）；
A/CN.9/465，第 21-35 段；
A/CN.9/WG.IV/WP.82，第 69－71 段；
A/CN.9/454，第 173 段；
A/CN.9/446，第 196－207 段（第 19 条草案）；
A/CN.9/WG.IV/WP.73，第 75 段；
A/CN.9/437，第 74－89 段（第一条草案）；
A/CN.9/WG.IV/WP.71，第 73－75 段。

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] 《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。

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

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

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

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

[8] 本节取自 A/CN.9/WG.IV/WP.71 号文件，第一部分。

[9] 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。

[10] 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)。

[11] 在公用和私人的密码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。

[12] 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。

[13] 不过，从相互验证的角度看，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。