联合国 A

大会

Distr.
GENERAL

A/CN.9/437
12 March 1997
CHINESE
ORIGINAL: ENGLISH

联合国国际贸易法委员会
第三十届会议
1997年5月12日至30日，维也纳

电子商业工作组第三十一届会议工作报告

（1997年2月18日至28日，纽约）

目　录

导 言

1. 委员会第二十九届会议(1996 年)在通过《贸易法委员会电子商业示范法》 (以下简称《示范法》)后，接着根据电子数据交换工作组第三十届会议进行的初步辩论(A/CN.9/421，第 109 至 119 段)，讨论了电子贸易领域今后的工作。一般认为，贸易法委员会应继续进行拟订法律标准的工作，使电子贸易带有可预测性，从而加强各区域的贸易。

2. 会议上就今后工作中可以讨论的议题和优先事项提出了新的建议。一项建议是，委员会应着手拟订关于数字化签字的规则。有人指出，许多国家认为，制订关于数字签字的法律，并制定承认“验证局”（以下称“验证局”）或受命就以数字方式“签字”的文件的来源和归属颁发电子证明或其它形式保证的其他人员的行动，对发展电子贸易来说是不可或缺的。有人指出，能够依赖数字化签字，对于增加合同和通过电子媒介转让商品权利或其它利益是一个关键。许多辖区正在制订关于数字化签字的新法律。据报道，这类法律的发展已经有互不统一的现象。如果委员会决定在这一领域开展工作，它将有机会协调这些新法律，或至少在数字化签字领域制订共同原则，从而为这类商业活动提供一个国际性的基本构架。

3. 不少人表示支持这项建议。不过，一般认为，如果委员会决定由电子数据交换工作组开展数字签字领域的工作，应该规定工作组的确切任务。大家还认为，鉴于贸易法委员会不可能做拟订技术标准的工作，应注意不要卷入数字签字的技术问题。有人回顾说，工作组第三十届会议曾确认可能有必要在验证局的问题上做工作，并确认这种工作很可能需要结合登记处和服务提供者的问题来进行。不过，工作组又认为，它不应就是否适宜采用任何一种特定标准的问题进行任何技术性审议(同上，第 111 段)。有人表示担心，关于数字签字的工作可能超越贸易法的领域，可能牵涉到民法或行政法的一般问题。对此，有人说，《示范法》条文也是如此，但委员会不应因为这些规则在商业关系领域之外也可能有用就不去制订这些有用的规则。

4. 根据工作组的初步辩论提出的另一项建议是，今后的工作应集中在服务提供者方面。所提到的在服务提供者方面可予审议的问题有：在没有当事方协定的情况下的最低履约标准；终端方所承担风险的范围；这类规则或协定对第三方的影响；非法经营者的行动或其他未经授权的行动所带来的风险的

分担；提供增值服务时的强制性保证(如果有的话)或其他义务的范围(同上，第 116 段)。

5. 与会者普遍认为，贸易法委员会应审议服务提供者、用户和第三方之间的关系。有人说，很重要的一点是，这项努力应着眼于拟订这一领域的商业行为的国际准则和标准，目的是支持通过电子媒介进行贸易，而不是为服务提供者建立一套规章制度，也不是制订可能使成本高得无法接受，以致电子数据交换无法在市场上适用的其他规则(同上，第 117 段)。不过，也有人认为，服务提供者这个命题太大，涉及到太多的实际情况，无法作为一个单一的工作项目来处理。一般认为，涉及服务提供者的问题宜在工作组所处理的每一个新的工作领域内来解决。

6. 还有一项建议是，委员会应着手拟订必要的新通则，以澄清如何通过电子商业履行传统的合同功能。有人说，“履约”、“交货”和其他用语在电子商业领域的含义是什么，有许多不确定性，因为在电子商业中，报价、接受和交货可以在全世界开放的计算机网络上进行。计算机上的商业以及通过互联网和其他系统进行的交易的迅速发展，已使这一问题成为优先议题。有人建议，由秘书处进行一项研究，可澄清这方面工作的范围。如果委员会在审议了研究结果之后，决定做这项工作，则一种可以选择的做法是，将这种规则放在《示范法》的“特别条款”部分。

7. 另一项建议是，委员会应集中注意以提及方式纳入条款的问题。有人回顾说，工作组已经同意，这个专题宜在有关登记处和服务提供者等问题的比较一般性的工作中来处理(同上，第 114 段)。委员会普遍同意，该问题可以在有关验证局的工作中来处理。

8. 讨论后，委员会同意，如果可以借此机会处理委员会所提议的今后工作中的其他专题，那么把数字签字和验证局的问题列入委员会议程是适当的。关于工作组更具确切的任务规定，委员会还同意，所将拟订的统一规则应处理如下的问题：验证程序的法律依据，包括新出现的数字化和认证验证技术；验证程序的适用性；在使用验证技术范围内，用户、提供者和第三方的风险和责任分担问题；用登记处提供验证的具体问题和以提及方式纳入条款的问题。

9. 委员会请秘书处对各国目前正在拟订的法律进行分析，并据此编写一份关于数字签字和服务提供者问题的背景研究报告。工作组应根据该研究报

告，审议就上述各专题拟订统一规则是否可取和可行。委员会议定，工作组第三十一届会议要做的工作可以包括拟订有关上述各专题的某些方面的规则草案。委员会请工作组向其提供足够的要素，以便有充分资料就所需拟订的统一规则的范围作出决定。鉴于《示范法》和电子贸易领域未来可能进行的工作所涉的活动范围广大，委员会决定将电子数据交换工作组更名为“电子商业工作组”。[1]

10. 电子商业工作组由委员会的所有成员国构成，于 1997 年 2 月 18 日至 28 日在纽约举行了第三十一届会议。工作组下列成员国的代表出席了会议：阿根廷、澳大利亚、奥地利、保加利亚、中国、埃及、芬兰、法国、德国、匈牙利、印度、伊朗伊斯兰共和国、意大利、日本、肯尼亚、墨西哥、波兰、俄罗斯联邦、新加坡、斯洛伐克、西班牙、泰国、乌干达、大不列颠及北爱尔兰联合王国和美利坚合众国。

11. 下列国家的观察员出席了会议：加拿大、哥伦比亚、捷克共和国、丹麦、加蓬、印度尼西亚、爱尔兰、科威特、毛里塔尼亚、蒙古、大韩民国、瑞典、瑞士和土耳其。

12. 下列国际组织的观察员出席了会议：联合国贸易和发展会议(贸发会议)、欧洲委员会、国际律师协会(律师协会)、国际商会和律师国际联合会。

13. 工作组选举出下列主席团成员：

主　席：Mads Bryde ANDERSEN 先生(丹麦)；

副主席：PANG Khang Chau 先生(新加坡)；

报告员：Piotr AUSTEN 先生(波兰)。

14. 工作组面前有下列文件：临时议程(A/CN.9/WG.IV/WP.70)和一份秘书处说明(A/CN.9/WG.IV/WP.71)。

15. 工作组通过了以下议程：

1. 选举主席团成员。
2. 通过议程。
3. 关于电子商业的法律方面问题的今后工作规划：数字签字、验证局和有关的法律问题。

---

[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。

4. 其他事项.

5. 通过报告.

一. 讨论情况和决定

16. 工作组以秘书处编写的说明(A/CN.9/WG.IV/WP.71)作为基础，讨论了数字签字、验证局的问题和有关的法律问题。工作组对这些问题的讨论情况和结论见下文第二节。工作组还对以提及方式纳入条款及今后工作等问题进行了初步讨论。这些讨论见下文第三和第四节。

二. 就数字签字统一规则拟审议的法律问题和可能制定的规则

A. 概 述

17. 在开始讨论应就数字签字统一规则审议哪些规定和有关法律问题以前，工作组就工作范围交换了意见，并审议了各国目前为处理数字签字和验证局所涉法律问题而采服的行动。

18. 工作组听取了关于各国目前为解决数字签字所涉法律问题而作出的努力的报告。 不少国家在考虑制订适当法律制度的问题，以利用可以在电子环境中发挥类似在纸本环境中的亲笔签名功能的装置。有些国家尚处在审议这个问题的初步阶段，但另一些国家据报已制订了数字签字的法律，或着手参照《示范法》制订立法。这些立法大多假定采用以公用钥匙加密法和验证局为基础的数字签字。立法的范围和周密程序各不相同，有的是制订一般法律，以便利用数字签字作为鉴别电文的一种方法，有的是较周密的立法，制订验证局运作的法律框架，甚至涉及若干有关公共政策的问题如设立公用钥匙系统所需的行政架构；为数字签字或为保密原因采用密码系统；保护消费者的问题；政府当局可否保留阅读加密信息的权力，如利用“代管钥匙”的机制。工作组还听取报告，了解了若干国际组织目前在区域一级作出的统一努力。

19. 有人认为，用于发挥相当于亲笔签名各功能的装置，如数字签字或其他形式的电子签字的法律制度，是必须解决的一个重大问题，以加强电子商业

的法律架构。普遍认为，缺乏关于数字签字和其他电子签字的法律制度会对通过电子方式进行经济交易造成障碍。还同意的是，各国考虑采取的做法和可能采取的解决办法各不相同，使这个专题成为适宜由贸易法委员会加以统一的对象。有人认为，除了提供准则，指导立法国家就数字和其他形式的电子签字建立法律架构以外，贸易法委员会不妨将工作重点放在外国验证局签发证书的承认标准的问题上。此外，贸易法委员会或许可以制订认可验证局的国际公认基本标准以促进这个进程。

20. 工作组审议了其工作应以“数字签字”(即采用“公用钥匙加密法”，又称“双钥匙加密法”的技术)为唯一重点，抑或应包括其他形式电子签字的问题。据指出，目前也有人在研制不采用公用钥匙加密法的技术，通称“电子签字”技术，以履行通常以亲笔签名发挥的功能。这些技术包括采用密码或“口令”，或生物检测识别装置，并可能与采用公用钥匙办法的数字签字制度同时存在。有人指出，在纸本环境中，不少往来事务并不需要认证和验证手续和规定。采用公用钥匙办法的数字签字据说具有高度的法律效力，但据指出，在许多不需要具有高度法律效力的情况下，其他技术可以是有用的识别和认证方法。有人认为，工作组不应给人一个错误的印象，以为工作组只重视数字签字，不鼓励采用上述其他技术。有人就这个问题的讨论指出， 采用以公用钥匙加密法为依据的数字签字不一定意味着要求获得最高度的法律效力。数字签字技术相当灵活，也可用来提供较低层次的保密，从而减少所需的费用。

21. 工作组普遍认为，电子签字统一规则的目标应该是向立法人员提供指导，说明如何在电子环境中履行各式各样的认证功能。这些功能包括在所谓“保密层级”上的各种功能，从提供最高的保密度(相当于纸本环境“公证”签字和其他验证签字)以至笔迹或签名印章等提供的低保密度。但是，电子签字领域的工作面对一个难题，如果拟订的统一规则须提供必要的指导，以执行《示范法》第 7 条所载原则，则这些规则可能要偏离其纯粹面对实务的做法，以一定的细节规定具体技术履行上述功能的办法。

22. 普遍同意的是，根据《示范法》的媒体中立原则，工作组准备拟订的统一规则不应阻止采用任何可以提供一个“ 适当可靠方法” 的技术，以作为符合《示范法》第 7 条规定的代替亲笔签名或其他纸本签字的手段。但为了便于进行审议，工作组决定以数字签字问题为其初步工作重点，因为通过立

法和法学文献，数字签字是较多人认识的技术。普遍谅解的是，讨论也可酌情从较广泛的角度出发，审议与其他电子签字技术有关的问题。

23. 关于工作范围的问题，普遍同意工作组不应涉及为保密理由采用加密的问题。这些问题极为复杂，与实行数字签字办法没有直接关系，会妨碍工作组审议工作的进展，且经由经济合作与发展组织(经合组织)等其他国际论坛审议。工作组应集中审议促进电子商业的问题。在较一般的方面，工作组同意，拟订的统一规则不应涉及执行数字签字办法时可能碰到的国家安全、公共政策、刑法或行政法问题。

24. 在工作组应否处理消费法的问题方面，提出的意见不一。一种意见认为，目前的工作不应包括消费问题而应专门探讨商业交易事项。另一种意见认为，审议的主要问题基本上与消费者无关，但拟订数字签字统一规则时也许可酌情审议消费者的交易是否需要不同标准的问题。然而，有人认为，为消费法制定特定规则可能会极其困难，因为鉴于电子通信的性质，要确定哪一方是消费者几乎是不可能的。经讨论，会议商定，工作组基本上应以商业交易为工作重点，但也会注意到其审议的事项可能对消费者交易造成的影响。

B. 数字签字的具体法律问题和条款草案

25. 关于工作组将采取的工作形式，有不同的意见。一个意见是，如果认为将由工作组拟订的关于数字签字问题及有关问题的文件应采取示范法律形式，未免言之过早。另一意见是，工作组应为其工作作出假定，决定将其今后关于数字签字问题及有关问题的工作视为《示范法》的一项增补。记得委员会第二十九届会议曾要求工作组研究应否和可否就数字签字和验证局的问题拟订统一规则。委员会同意，工作组本届会议将进行的工作可涉及拟订关于上述主题某些方面的规则草案(参看上面第 9 段)。

26. 讨论后，工作组推迟对其今后工作的形式作出决定，直至完成其对所涉实质性法律问题的审查为止。工作组还推迟审议今后这些工作与《示范法》之间的确切关系。工作组同意，在数字签字领域内可能制订的统一规则应源自《示范法》第 7 条，并应视作为在确定可以用哪一种可靠的方法来“识别某人”和“表明该人核准”一项数据电文中所载的信息。更一般而言，关于

数字签字的今后工作应与《示范法》内所载原则和使用的用语相符合。

27. 为了便于今后的讨论，工作组就其工作通过了一项初步假定，即在数字签字领域内的工作将采取法律则草案形式。不过，有人认为，工作组不妨考虑是否有必要提供附加说明，可能的方式包括加插序言部分、提供颁布统一法律规定的指导或另外拟订准则，特别是关于可能被认为不适宜统一的问题。例如，有人说，由贸易法委员会就各项有关设立公用钥匙基础结构的问题发表解释性意见可能颇具教育意义。

28. 工作组决定，工作组将根据秘书处说明(A/CN.9/WG.IV/WP.71 ，第 52-76 段) 中所载的统一条款草案进行审议。有人说，这些条款草案具初步暂定性质，普遍同意，应将对这些条款草案的审查(而非集中注意草拟个别条款)视为一个机会，以讨论数字签字统一规则可采取用的概念办法。普遍认为，工作组在讨论条款草案所提每个问题范围内可能应考虑：(a)是否有统一的必要；(b)这个问题是否已在《示范法》内获充分处理或应否拟订较详细的规定；(c)有关问题是否是数字签字的特有问题；可否在较一般性的层次上处理；(d)这个问题是否与国际贸易法、与贸易法委员会的任务规定或与其专门知识领域直接有关；(e)是否需要一项强制性规则或是否较宜由当事方自行决定。

1. 定义

29. 首先，有人表示，除了秘书处说明(A/CN.9/WG.IV/WP.71，第 52 至 60 段)中对“数字签字”、“经授权的验证局”和“证书”所载的定义草案外，工作组似应审议其他定义。建议的定义如下：“‘私人钥匙’是指成对钥匙中用于产生数字签字的钥匙”；“‘公用钥匙’是指成对钥匙中用于核实数字签字的钥匙”；“‘成对钥匙’是指非对称加密系统内的私人钥匙和与其具有数字关系的公用钥匙，其特性是公用钥匙可核实私人钥匙产生的数字签字。”工作组注意到这一建议。有人认为提出的定义有迂回循环之嫌。更一般地说，对于在制定统一法律规则时列入大量定义应谨慎从事，因为这样做会有悖于许多国家的立法传统。在讨论后，大家普遍同意似有必要在稍后阶段重新审议增加有限数目的定义的可能性。

(a) 数字签字

30. 工作组根据下列条款草案讨论了“数字签字”的定义：

"A条草案

"(1) 数字签字为一数值，附在数据电文上，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]所授权的数字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字签字能够按照[本法][本规则]经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]应为数字签字及其核查需达到的技术要求制定具体的规则。"

第(1)和第(2)款

31. 有人认为应将"数字签字"的定义扩大，不仅应包括公用钥匙加密法，而且还应包括其他种类的电子签字。然而，多数人认为试图为"数字签字"制定一个偏离其现有用途的定义是不合适的。大家同意，"数字签字"的概念范围应加以限定，只包括非对称加密法，但为包括可能在"电子签字"概念下广泛提及之其他技术，似有必要拟订其他的定义。

32. 关于第(1)款，有人建议"唯一地断定这一数值是……获得的"的措词应改为"断定这一数值只能是……获得的"。工作组决定，审议尚在早期阶段，不应着手对案文进行任何详细的重拟。大家普遍感到，就可能用于确定今后工作范围来说，第(1)和第(2)款从实质上反映出了"数字签字"这一概念。经讨论，工作组认为第(1)和第(2)款的内容基本上可以接受，但商定它可能会有必要在稍后阶段重新审议这两款的具体措词。

第(3)款

33. 对于第(3)款的目的提出了各种问题。有人认为第(3)款未能充分介绍公

用钥匙基础结构和核查数字签字等概念，而且第(3)款涉及的是“数字签字”定义以外的实质问题。有看法认为，人们会把第(3)款看作是规定核查程序为确定数字签字有效性的一项要求。建议最好是删除第(3)款，为签字的“核查”拟订一项叙述式定义。

34. 有看法表示，人们会认为第(3)款只涉及在公共当局设立的公用钥匙基础结构中使用的数字签字的有效性。有人认为目前这项规定草案行文过于拘紧，可能不承认在任何其他情况下使用的数字签字，如通过非公共当局设立的公用钥匙基础结构。会议普遍认为，最好不要影响由觉得无需得到验证局服务的当事各方之间可能 在封闭环境下进行的交易。据认为，在各国仍在考虑公用钥匙基础结构各项方案之时，不应过早在统一规则草案中作出选择，偏重任何一种公用钥匙基础结构系统，而忽视所有其他系统。

35. 有人认为，第(3)款得与《示范法》第 7 条一并理解，但这两条规定可能并不完全一致。例如，第(3)款在给“数字签字”下定义时提到“授权”的数字签字，而《示范法》第 7 条或秘书处说明（ A/CN.9/WG.IV/WP.71 ）所载 A 至 J 条草案等处则未使用授权一词。再则，《示范法》第 7 条提到使用“可靠的，对生成或传递数据电文的目的来说也是适当的”签字方法，因此承认按照数据电文的生成或传递目的，包括当事各方之间的任何协定可靠程度可以有所不同。据指出，根据《示范法》第 7 条，相互间有足够信任的交易各方可商定一种其认为符合实情的安全程度，而不必求助于验证局。从当事方角度来看，他们的基本考虑是，他们是否认为其运作系统可信可靠。据认为，有若干因素组成了当事各方适用的硬件、软件和程序的可信赖程度(例如，是否相当安全，免于侵入和滥用；是否有相当程度的可供性、可靠性和正确运作能力；是否相当适合发挥其预定功能；运作是否符合普遍接受的保密原则)。因此应由当事各方决定其需要的可靠性标准中是否应包括验证局使用的一个核查程序。反过来，第(3)款的含义是，数字签字只有在验证局协助下得到验证时方为可靠。因此，认为这比《示范法》第 7 条的限制还多。有人表示，第(3)款若要与《示范法》第 7 条相符合，就得作实质性改动。

36. 还有问题涉及第(3)款中谈到根据验证局制订的程序核查数字签字。有看法认为，提到这些程序会带来用于核查数字签字的技术说明问题和验证局适用的其他业务标准问题，或是某种情况下未遵守这些程序产生的法律后

果。不过，这些均是实质性问题，在 A 条草案的有限范围无法妥善解决。因此建议在第(3)款中删除有关核查程序的案文。

37. 工作组在考虑了不同意见后，决定删除第(3)款。经商定，在审议数字签字的法律效力问题之后，可能需要重新讨论关于公用钥匙基础结构的各种选择。

第(4)款

38. 有看法认为，在规定须由国家制订数字签字技术规则这一方面来看，第(4) 款似乎排除了非公共当局实际设立的公用钥匙基础结构。鉴于第(3)款和第(4)款之间的逻辑关系，及依照删除第(3)款的决定，工作组决定删除第(4)款。

(b) 经授权的验证局

39. 工作组根据下列条款草案讨论了“经授权的验证局”的定义:

“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) 经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) 经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，及有关通过数字签字保证的通信的其他功能。

“(5) [立法国规定，主管制定关于应由经授权的验证局履行的职能 n 的具体规则的机关或机构]，可以为应由经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。”

40. 工作组就怎样处理验证局问题进行了一般性的意见交流。有一个看法认为，目前的 B 条草案看来提出了实施公用钥匙基础结构的具体方法，但是最好还是由每个立法国自行通过这方面的规则。有人说，在建立数字签字的可信程序方面验证局也许可以发挥重大作用，但是数字签字系统在没有验证局的管理下运作并非不可能。也有人说，建立一个公法机制，使验证局据以

运作，这不一定会提高人们对数字签字的信心，而也许由民间委派的验证局或由市场机制促成的其他形式能达到更好的效果。另一种看法认为，从界定验证局的工作范围来说， B 条草案可以令人接受，因为该条内容没有约束性的规定，特别是第(2)款并没有不准立法国以不同方式建立其公用钥匙基础结构。

41. 为了审议有关验证局问题的其他可能办法，已请工作组提出通过为“验证局”下定义而可以致力达到的两个目标。一个目标可为向立法国提供咨询意见，指导它们在执行国家的公用钥匙基础结构时应当考虑什么重要的因素。有人说， B 条草案不够详细，不足以做这方面的指引。另一个目标可以是把国内建立公用钥匙基础结构的工作交由每个立法国自己执行，但在“验证局”的定义中规定每个立法国承认他国验证局所发的证明应取的标准。有人建议，如果工作组为了后一个目的想限制本统一规则草案的适用范围，则可能需要在 B 条草案之中加插一段，内容如下： “本统一规则适用于有以下特征的法律制度所发的证明。”不过，有人指出，此项建立如获通过，将需要对 B 条草案其余案文作出重大修改。另有人建议 B 条草案不规定具体的准则，其内容仅限于第(2)款的一般性条文。这方面如有更多意见，包括附有说明的、立法国可能需要考虑的准则清单，可以载入一份统一规则颁布指南中。

42. 工作组同意，关于除了每个立法国承认他国验证局所发的证明须用的准则之外，统一规则草案是否尚需要为“验证局”下定义问题，需要在稍后阶段讨论。普遍认为，虽然订立标准或准则或可帮助验证局取得其运作所必要的信任，但是可能需要区别不同的验证局的可信度（这可能与其所属的法律制度有关）此类一般性问题和某一个验证局所发的证明的可信度此类较具体的问题。

43. 有人认为，象 B 条草案所述的关于验证局职责的规定不仅是验证局制度的组成部分(如公用钥匙基础设施)。这类规定也同确定赋予数字签字以及关于或涉及使用数字签字的行为的效力有关。在这种情况下，有人建议，工作组讨论这个问题时牢记关于确定赋予数字签字的法律效力的一系列因素也许是有用的。有人提出下列因素作为工作组审议时的分析工具： (a)签字类型(按通用程度递减的次序，其中包括电子签字； 数字签字； 经验证的数字签字和经官方授权的验证局证明的数字签字)； (b)所涉当事各方(即直接合同当事方，包括验证局； 托运人和银行等第三方； 政府实体； 服务提供者和

通信公司等其他方面); (c)赋予法律效力的行为或事件(即数字签字的使用; 证书的发放, 包括未经授权的发放; 证书的到期; 证书的撤消; 赋予验证局的授权的撤消); (d)贸易法委员会在这方面的工作范围(仅是国际适用; 国际适用加上国内法的建议; 国内法的建议); (e)法律效力(即有效性; 证明发放者和证明使用者的义务; 补救办法; 赔偿责任, 包括赔偿责任的限制; 证据); (f)起草技术(即标准的制定; 达到标准的法律效力; 没有达到标准的法律效力)。工作组认为提出的一系列因素有利于它分析与验证有关的各项条款的目的和所涉及的问题。

44. 工作组在随后的讨论中审议了可否在统一规则草案中列入验证局要达到的业务标准, 不论是否经过授权。

45. 有人建议, 除了已有的规定之外, 在B条草案中应加入一些统一规则, 明确说明授权验证局运作时应考虑的标准, 或规定验证局为让其发放的证明得到法律承认所要达到的最低标准。如果统一规则草案中涉及验证局问题, 那就有必要提及这类标准。有人回顾说, 秘书处说明(A/CN.9/WG.IV/WP.71)第44段中列出了评价验证局可信度时可以考虑的若干因素。普遍认为, 如果工作组打算进一步审议这个问题, 这些因素就是良好的讨论基础。有人建议, 其中有些标准可以扩充, 以便包括管理人员的能力或把验证局的证明职能同它可能从事的任何其他业务分开等因素。

46. 有人对统一规则草案中列入验证局业务标准问题提出反对意见。有人提醒工作组, 它早些时候曾讨论政府当局在公用钥匙基础设施应用中的作用和某些国家私营实体行使证明职能无需政府事先授权的可能性(见上文第40段)。还有, 象某些商业活动领域那样, 可以考虑对经政府核准的标准采用其他可接受的替代办法, 如国际公认的商业惯例和做法或具有声望的非政府实体制订的资格标准。据认为, 按提议列入在经授权的验证局运作时要考虑的标准对于不根据政府授权而运作的验证局来说既不相关又不合适。再说, 列入任何这类标准就需要确定有能力判定任何具体验证局是否达到所述标准的实体或权威机构。这种制度会给在政府当局采用的公用钥匙基础设施范围之外运作的验证局造成困难。

47. 针对这些反对意见, 有人忆及, 为验证局运作提供可普遍接受的标准, 可能是加强数字签字可靠性的一项重要步骤。只要电子交易是在一个非公开系统内运作的双方之间进行, 而且它们认为该系统相当可靠, 则可能无需这种标准。事实上, 在这种非公开系统内运作的可依赖的合作伙伴可以不需要

验证局发放的证书。然而，为了能更广泛使用数字签字，则需使大众更加信任签字的真实性和核查签字办法的可靠性。实现该效果的重要办法之一是让大众相信，从事核查公用钥匙真实性工作的实体须达到旨在确保其可靠性的某些标准。据指出，虽然工作组不应放弃商业惯例和做法，或非政府实体在为商业活动的任何特定领域制订令人可接受的操作标准中可能发挥的作用，但目前尚未出现任何既定做法，能为验证局确定令人接受的运作标准。

48. 有人认为，目前正讨论的两项备选方案并非相互排斥，这两项方案是，为政府授权的验证局确定标准和承认在政府建立公用钥匙基础结构之外运作的验证局的操作标准。这两种情况之间的差别可能在于它们的数字签字所得到的法律效果。在政府授权的验证局情况中，验证局达到可适用的运作标准将是授权该验证局的一项前提，而对该验证局的授权则又是承认它发出的证书具有法律效力的一项条件。在第二情况中，验证局在开始运作前无需表明已达到运作标准。然而，假如它发出的证书受到质疑(如在法律争端和仲裁时)，裁决机构则需通过确定该证书是否由达到这些标准的验证局发出来评估它的可靠性。

49. 有看法认为，证明的可信性可能取决于验证局对该特定证明所采取的行动，而不是机构性因素。这种“交易性”可信性不一定取决于验证局是否获得授权，也不一定取决于国际公认的商业做法和惯例。指认为，可信性标准将取决于评估可信性的目的（如交叉验证、发放许可、确定赔偿责任）。

50. 鉴于审议仍处在早期阶段，而且对该问题出现不同的看法，因此，普遍支持以下这项提议，即工作组应保留上述提议，作为可行的工作假设，并应先审议其他密切相关的问题，如验证局的责任问题和跨境验证问题等，然后再审议那些问题。

2. 赔偿责任

51. 工作组根据下列条款草案讨论了验证局的赔偿责任:

“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，经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) 如果经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。]"

第(1)款和第(2)款

一般意见

52. 工作组讨论了所提议的验证局赔偿责任规则的范围和影响。有人指出，验证局赔偿责任包括两种不同的责任：验证局违反其运作规定所产生的"结构性"赔偿责任以及验证局在签发、暂时吊销或吊销证书方面的行动所产生的"交易性"赔偿责任。在第一种情况下，验证局辜负了公众对其的信任，应由授权的公共实体根据违章严重程度对其罚款或以其他方式予以处罚。在第二种情况下，验证局违反了对其客户的专业义务。然而，损失通常由客户的贸易伙伴承担，因为这些贸易伙伴在多数情况下与验证局没有合同关系。在这种情况下，有人问遭受损失的一方应可以直接向验证局索赔，还是仅有权要求其贸易伙伴赔偿损失，并由后者向验证局索赔。有人认为，设立使证书用户能够直接向验证局索赔的完善赔偿责任制度十分困难。

53. 有人认为，工作组也许最好避免讨论验证局赔偿责任，因为这是一个微妙而复杂的问题，无法在统一规则草案中得到完善处理。有人回顾说，在《示范法》的框架内，曾决定完全避免讨论第三方服务提供者的赔偿责任问题。有人认为，赔偿责任问题与损害问题密切相关，而后者也许不易于取得国际统一。有人请工作组考虑最好是否应该将这两个问题排除在统一规则草案之外，而由适用的国家法律处理。如果采用上述办法，则可考虑以下选择：由国家法律冲突规则确定适用于赔偿责任和损害问题的法律；起草具体的法律

冲突统一规则；或直接确定应适用何种法律冲突规则(例如，验证局注册或以其他方式经授权从业所在国的法律冲突规则)。支持这项建议的人说，根本而言，赔偿责任问题是验证局作出保证的问题，最好由订约伙伴调节，或应根据适用于其合同关系的国家法律予以确定。

54. 然而，有人表示坚决支持将关于验证局赔偿责任的条款列入统一规则草案。他们认为，赔偿责任问题极为重要，不应完全由订约各方自行调节，尤其考虑到并非所有证书用户都可能与验证局有直接合同关系。如果限制用户要求其贸易伙伴赔偿因验证局过失而造成的损害的权利，则会使验证局明知或忽略的冒名诈骗行为的受害者得不到保护。此外，缺乏关于验证局赔偿责任的统一规则可能会导致产生不可取的局面，使一些国家为吸引或促进在其境内建立验证局，只规定微不足道的赔偿责任。“验证天堂”就可能由此出现，从而可能会使贸易伙伴不愿考虑利用数字签字。这一局面将与促进电子商业的目标格格不入。不论这个专题多么困难，涉及合同赔偿责任和侵权赔偿责任这两个方面，普遍看法是，验证局赔偿责任问题应该在统一规则中得到处理。

55. 经讨论，工作组同意，统一规则草案原则上应包括关于验证局在参与数字签字机制方面的赔偿责任的规定。

赔偿责任的性质

56. 有人询问验证局赔偿责任的性质，尤其是这种责任是以过失为依据，还是把它定义为“ 严格赔偿责任”，这个概念也称为“客观赔偿责任”或“无过失赔偿责任”。有人对列入验证局负严格赔偿责任的条款提出反对意见，他们认为严格赔偿责任偏离了让个人为其本人的过失负责的侵权行为法的一般原则，这种责任在国内法中被接受仅出于罕见的公共利益原因，如针对从事危险性极高的活动的人的严格赔偿责任制度。没有任何令人信服的理由表明验证局应受严格赔偿责任制度的约束。还有，这种严格赔偿责任制度会产生不良后果，会阻碍新出现的验证局的发展，从而限制数字签字的使用范围。再者，有人指出，验证局可能向客户和公众提供不同层次的服务，从仅仅提供公用钥匙所有者和各自钥匙的名单到更符合个人需要的服务，包括保证公用钥匙及其持有者身份的可靠性。验证局承担的义务程度以及收取的费用根据所提供的服务种类而不同。考虑到这一系列服务，让所有验证局在各种设想的情况下承担同样的赔偿责任是不合理的。因此，有人建议，适用于

验证局的赔偿责任制度应根据H条草案第(1)款的备选条文以过失为依据。

57. 有人答复说，要求受害者承担确定验证局过失的负担是不公正的。鉴于验证局可望采用尖端技术和获得它们意欲得到的高度信任，验证局通常应对发放假证书造成的任何损害负责。有人指出，在某些法律系统中，一些专业类人员(如某些民法国家的公证人)有义务购买第三方赔偿责任保险或参加共同赔偿基金，以便赔偿他们的行为所伤害的当事方。有人建议，如果在许可证制度这样的机构框架内建立验证局，可以促进这种共同赔偿基金的建立。

58. 有人建议，如果不提出具体说明验证局承担责任的种种情况的规则，而在统一规则草案中列入可反驳赔偿责任推定的规则，也许会消除工作组中的意见分歧。例如，按照这项建议，如果验证局错误查证一个人或错误地把公共钥匙交给一个人，它就要对受害方的任何损失承担责任，除非验证局表明它已尽了最大努力避免错误。例如，验证局表明它遵守了统一规则规定的行为标准就可以反驳以上推定。有人指出，这种赔偿责任制度同关于产品赔偿责任的有些国内法设想的制度类似，它会增加对服务用户的保护，但不会让验证局承担严格赔偿责任。工作组欢迎这项建议，大家普遍认为它是工作组今后审议如何处理验证局赔偿责任这个难题的可行办法。

59. 工作组继而审议了可以豁免验证局工作过失的种种情况。有人建议，根据拟议的赔偿责任制度，如果验证局能表明它在查证公用钥匙持有者或履行认证职能时给予了应有的注意；如H条草案第(3)款所述，错误由用户自己的过失造成；或错误归咎于验证局不能控制的情况，则验证局的赔偿责任应予免除。大家普遍认为，按这些思路考虑的豁免情况可以接受。

<u>验证做法说明和各方的自主权</u>

60. 有人认为，在审议赔偿责任问题时，必须铭记用户与验证局的相互期望和利益。验证局应当公布其验证做法说明，除其他以外，通知用户它用于查明公用钥匙持有者的方法和程序。用户应合理地确定此项文件。此外，用户在利用证书之前，有义务查明证书目前是否有效(例如，证书没有废止) 。最后，用户应根据掌握的资料，合理行事。关于有人提出用户如何核实证件是否有效的问题，有人答复说，可请验证局维持有效证书的数据库，有些验证局已经在这样做，这样，有关方面就可以进入数据库以核实证书的有效性。有人在答复这一提议时认为，尽管也许有必要鼓励用户用心核实证书，

但是核实证书真伪和有效性的首要责任还在验证局，在让用户承担义务之前须十分小心，这样做也许会使他们共同承担责任。在多数情况下，用户通常都无法弄清关于证书是否有效的一些因素，例如验证局利用的验证程序，或公用钥匙持有者是否也同时持有相应的私人钥匙。将其中任何责任转嫁到用户是不合理的。

61. 工作组讨论了验证做法说明的作用及其在限制或确定验证局承担的赔偿责任范围方面可发挥多大作用。为了保护用户的利益，可要求验证局根据其公布的验证实践说明中的相应条款，公开这类赔偿责任的范围。从技术角度出发，利用验证局服务的个人可以电子形式得到验证实践说明。有人认为，要求得到验证局服务的一方因利用了这一服务而应接受验证实践说明条款的制约。各方之间达成的合约安排应比其他来源的规则得到优先考虑，在此方面，必须确保执行这些条款和条件。不过，有人认为，象赔偿责任限度这样对依靠验证局的当事方来说非常重要的规定，应当列入证书本身而不是仅仅列入证书所提及的某项文件，无论这项文件如何易于取得。

62. 工作组普遍认为，在为验证局制定赔偿责任机制时，应适当考虑维护各方自主权的必要性。但是有人有保留地认为，验证局有可能利用验证实践说明或验证局印发的任何其他文件中所载的免除赔偿责任条款或解除条款，逃避因本身的过失而承担的赔偿责任。有人指出，利用一项证书来核实数字签字真伪的电文收件人与验证局之间往往没有直接的法律关系，因此也无法与验证局谈判这类赔偿责任的条件。即使是与验证局之间有着相互关系的电文发送人也并非总能够谈判这些条件，在很多情况下，则采用预先确定的不可提出修改的商业条件。在一些法律制度下，单方面拒绝限制赔偿责任是违反公共政策的。如果引用这种办法，则应按照法律提出对赔偿责任的限制和免除，并应得到公共当局的核准。

赔偿责任的限度

63. 工作组审议了验证局的赔偿责任是否应该有限度和如何确定这些限度的问题。有人反对对验证局采用限定赔偿责任的做法，指出这种限度往往存在于具有某种垄断形式的活动领域，例如有些国家的邮政和电话服务业。然而，在可以公开竞争的其他活动领域，没有理由规定这种赔偿责任的限度。

64. 然而，与会者发表了各种意见，支持对验证局的赔偿责任确定某种形式的限度。人们发表了下列意见：(a)验证局是一种新出现的行业，让它们承

担无限度的赔偿责任可能妨碍其发展；(b)必须使验证局能够确定其可以承担的赔偿责任程度，这也许是一种使它们的活动得到适当保险合同的先决条件；(c)关于数字签字，验证局的作用可能仅限于发出证书，而证书本身的价值极小或无法定量。还有人进一步指出，如果发出证书，在一个公用钥匙和某一特定个人之间建立联系，那么，在各种不同的交易中，这项证书可能附加在一些信息之中，而验证局往往无法预测这些交易的总额。有人指出，在信用卡交易方面，已有分别核准每项交易的办法，因此，信用卡公司可以针对使用信用卡作交易超过预定数额的每个案例，估计发生未经核准而使用信用卡的情况时可能要承担的赔偿责任。对验证局而言，这种可能性并不存在，因为它们通常都不了解客户进行交易的条件。因此，很难参照使用数字签字进行交易的数额来确定赔偿责任的限度或上限。鉴于一份单一的证书可能与无数交易有关，验证局未必能以合理的成本获得第三方责任保险。

65. 工作组就限制验证局的赔偿责任数额可能采用的方法，对一些建议进行了讨论。一种可能的方法是如H条草案第(2)款X备选条文所建议，确定一个固定数额。提议的其他方法是在限制赔偿责任时采用用户付费的一个乘数、交易额的某一百分比、或受损失一方实际损失的某一百分比。然而，有人指出，因验证局的行为而可能造成的损失不易定量，因此不能作为计算固定赔偿责任数额的客观标准。而且，验证局提供的服务和收取的费用往往与相关的交易额没有关系，同时与各方可能遭受的损失也无关。《联合国海上货物运输公约》(《汉堡规则》)或《贸易法委员会国际贷记划拨示范法》中所载的其他限制机制适用的交易都具有可定量的因素(例如，货物价值、划拨贷记的数额)，而目前审议的案例中可能不存在这些因素。

66. 限制赔偿责任的另一种可能是将某些类别的损失、例如“间接”损失的赔偿责任排除在外。关于后一种可能，有人指出，在不同的法律系统中，“间接损失”--亦称为“ 非直接损失”--这一概念可能有不同的解释。因此，有人建议，最好具体说明验证局对这一概念中的哪几类损失不承担赔偿责任。虽然有人表示支持依照《贸易法委员会国际贷记划拨示范法》所采用的方法，拟订一种办法排除对间接损失的赔偿责任，但是，有人指出，对数字签字和验证局可能不适用这一方法。有人指出，造成损失的原因很少是发出假证书的缘故，而是第三方依赖使用这种证书的不可靠的数字签字。在这种情况下，验证局的活动可能造成的大多数损失也许被认为是“间接”或“非直接”损失。还有人建议将“可预见性”作为限制验证局赔偿责任的一项标准。

有人指出，对《联合国国际货物销售合同公约》规定适用于货物销售的赔偿责任制度是否可以作为参照因素，可能需要进一步探讨。

67. 对于提议的各种备选方法，工作组请秘书处编写一份简短的报告，说明用于限制赔偿责任的现行法律制度和方法，特别是根据国际公约适用于运输货物和运载旅客的这方面法律制度和方法。这份报告还可以审查某些国内法对在使用纸张的环境中履行为验证局所考虑的相同职能的专业类别所规定的赔偿责任制度。

赔偿责任的最低标准

68. 有人指出，在审议工作的目前阶段中，工作组仍在讨论验证局是否应要求事先得到公共实体的授权的问题。有人建议，工作组在继续审议 B 条草案过程中重新讨论这个问题的时候，也应考虑，此类公共授权实体是否将为验证局的行为承担附带责任。

69. 关于第(1)和第(2)款，工作组通过了一项临时性结论，即适用于验证局的赔偿责任制度应基于一种“双重办法”，即应确认赔偿责任可能会有不同，这要看是否有某一公共实体为验证局规定了标准或者是否只是依照私下商定的标准行事。

70. 有人建议，任何验证局在签发证书时，应承担以下所述义务：

“验证局签发证书就代表它已确认：

“(1) 该验证局已遵循这些规则的所有有关要求，并且如果验证局已公布该证书或以其他方式将证书提供给合理依靠该证书或可通过证书所列公用钥匙来核查的数字签字的任何个人，则证书中所列的持证者已经接受证书；

“(2) 证书所指明的持证者持有与证书所列公用钥匙相对应的私人钥匙；

“(3) 持证者的公用钥匙和私人钥匙是同时起作用的一对钥匙；

“(4) 证书中的所有资料均正确无误，除非验证局在证书(或证书说明内容)中注明某一资料的准确性尚未查证；

“以及

“(5) 据验证局所知，证书内没有删略任何已知的而且会不利地影响以上所作证明的实质性事实。”

会议普遍认为，所建议的措词大部分在实质上可以接受作为今后讨论的基

础，因为它规定了一个各方不得以私下协议背离的最低标准。特别是，限制验证局赔偿责任的任何条款如果与上述要求相冲突，那么它就不得视为属于统一规则提供的任何保护或利益范围。一旦有人声称验证局应承担赔偿责任，那么将会假定验证局须为签发证书承担后果，除非验证局可以证明它已按照上述要求行事。但是，如果验证局希望承担比上述所列内容更为严格的责任，则应容许这样做，其方法是在一份验证说明书中列入有关条款或以其他方式作出此种规定。

71. 工作组同意，上述最低标准应适用于 A 条草案所定义的数字签字有关证书的签发。普遍同意，统一规则草案不应牵涉到验证局可能从事的其他活动或服务。此类活动和服务可能受验证局与其客户之间某种契约安排的制约，也可能受其他有关法律(如有关豁免赔偿责任条款可容许程度的强制性法律规则)的制约。

第(3)和第(4)款

72. 工作组认为第(3)和第(4)款的实质内容一般可以接受，以作为今后讨论的基础。对于第(3)款，一般认为，虽然在拟订 H 条草案的订正案文时，也许需要考虑到追究遭受损失一方过失的原则，但第(3)款所载的具体规定也许已不再有必要，因为工作组已作出决定，对验证局适用的赔偿责任制度不应仅基于疏忽过失。对于第(4)款，工作组决定将“用户因此遭受的”改为“ 因此造成的”，以此将该条规定扩大适用于任何有关方面所遭受的损失。

73. 经讨论，工作组请秘书处参考以上审议情况和决定，草拟一份订正的 H 条草案。

3. 跨境验证问题

74. 工作组根据下列条款草案讨论了跨境验证问题:

“I 条草案

“(1) 外国验证局签发的证书可用于数字签字，其条件与受[本法][本规则]管辖的数字签字相同，条件是这种证书得到一个经授权的验证局的承认，而且该经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) ……[立法国规定的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。”

75. 在工作组开始审议跨境验证问题之前，有人提醒工作组，根据贸易法委员会交给工作组的任务，它将就编写数字签字、验证局和相关问题的统一规则的可取性和可行性问题向贸易法委员会提供咨询意见（见上文第 9 段）。这项任务并不要求工作组在目前阶段把案文草案定稿，提交贸易法委员会第三十届会议审议。

76. 有人还提醒工作组，它以前在 B 条草案范围内讨论验证局的作用时，尤其是在验证局营业是否需要政府核准问题上有不同意见（见上文第 40-50 段）。工作组普遍认为，工作组在审议了验证局赔偿责任和跨境验证问题之后应能更深入讨论这个问题。同时有人指出，关于 B 条草案所提问题的决定也会对统一规则草案所设想的跨境验证制度产生影响。

77. 普遍认为，第(1)和第(2)款从某些不同的角度说明了国内验证局签发的证书和外国证书之间的关系。第(1)款使国内验证局能在与其本身的证书相同的程度上保证外国证书细节正确无误及其有效。根据第(2)款规定，立法国主管向验证局授权的机关或机构被获准可按所规定的条件承认外国验证局签发的证书。有人建议，第(1)款所涉事项可以称为“交叉验证”，而第(2)款所涉情况可以更精确地称为“跨境承认”。分别处理这些不同的问题可能更好。

78. 有人认为，根据统一规则草案，第(1)和第(2)款是针对将来外国证书制度的两种不同选择。有人支持这两种中的每种选择。不过，大家普遍认为，这两种选择不必当作相互排斥的条款。虽然有人支持把第(1)和第(2)款的内容分别列为两条，但是另有人提出，它们各自的适用范围值得进一步审议。有人指出，第(1)款主要规定在发现外国证书有瑕疵时应如何向本国验证局分配拟由 H 条草案所得出的赔偿责任。然而，第(2)款则不涉及赔偿责任问题，它涉及外国证书可能直接产生的法律效力问题，例如在把争端提交立法国法院裁判的情况下外国证书要作为根据。这些法律效力不一定因为存在第(1)款规定的保证而受到肯定或影响。

79. 鉴于工作组决定在统一规则草案中不仅处理公共实体许可的验证局的问题，而且还处理“市场导向的验证局”的问题（见上文第 48-50 段），所以，大家普遍认为第 I 条草案应规定这两种验证局签发的外国证书的承认问题。

80. 有人建议，工作组还应审议可以承认外国证书的条件问题。这些条件可以采用政府要求的形式，或由国内验证局和外国验证局间的安排加以规定。

有人解释了验证局之间进行这种安排的可行办法。有人回顾说，公用钥匙基础设施常常基于不同的权力等级制度。在这些等级制度内似乎可能产生交叉验证的两个阶段。在初步阶段，交叉验证可望完全留给“基层当局”进行（即证明使用成对钥匙的技术和做法并对验证分局进行注册的权力机构）。在后一阶段，随着该行业的发展，预计在“基层”当局管辖下的验证分局也能直接参与保证外国验证局所签发的证书正确无误。然而，工作组编写交叉验证问题的规则时，应考虑一种可能性，那就是，尤其对于安全程度最低的数字签字，外国证书可能需要在验证局之间尚无具体协议的情况下加以执行。因此，有人提议可能需要制定关于承认在这种情况下所签发的外国数字签字的默认标准。

81. 有人指出，列入有关跨境承认问题的条款是朝提高证书可信度方面迈出的重大步骤。不过，工作组还须认真审议这种跨境验证或承认的方法和程序。有人指出，在评估外国证书是否可信时，附有此证书的数字签字电文的接收人应考虑下列这些问题，例如:签发此证书的验证局是否被授权在海外活动；该验证局的数字签字能否证明并非伪造；是否可对该验证局诉诸法律手段；是否承认该数字签字可产生法律效果；数字签字能否用来对抗签字人。

82. 从这一角度出发，有人进一步指出，交叉验证基本上可提供四种不同程度的可信度。其中最高一层是，国内验证局应使用外国证书一方的要求，根据其宣称的对签发证书的程序的了解，为证书的内容提供担保，从而为证书中的任何错误或其他瑕疵承担全部赔偿责任。其次的一层是，国内验证局根据所收到的有关该外国验证局可信度的资料，为一项外国证书的内容提供担保。再低的一层是，国内验证局只限于承诺为该外国验证局的可信度提供担保，但不为外国证书的内容承担任何赔偿责任。最低的一层是，国内验证局在核实了公用钥匙和数字签字之后，只为此外国验证局的身份提供担保。有人建议工作组在制定交叉验证或承认外国证书的条款时，应注意电文接收人想要得到的放心程度。

83. 在此方面，有人将担保一份外国证书是否正确无误和有效的验证局的立场与担保一家外国银行签发的信用证的一家金融机构的立场相比较。信用证的受益人是否接受这一信用证取决于签发该信用证的外国银行是否可信以及该信用证在受益人国家是否可予强制执行等因素。在某些情况下，受益人可能坚持让一家地方银行提供副署担保。信用证受益人在考虑到愿意承担的

风险程度之后，便可决定交易的足够安全程度。同样，例如，涉及到使用一项外国证书的交易的一方在了解到签发证书的是一家信誉良好的外国验证局以后会感到满意，因此认为没有必要再让国内一个验证局提供担保。有人担心I条草案可能会被理解为不鼓励或阻止使用未经国内一个验证局担保的证书，即使有些交易的各方都认为完全有理由对较低程度的安全或法律保证保持信心。重要的是应确保I条草案能够灵活处理交叉验证和跨境承认的问题。

84. 关于上文所述将验证局的作用与信用证交易中的银行的作用相比较的问题，大家普遍认为，在制定承认证书的统一规则时，应铭记，数字签字不仅可用来转让权利，也可用来转让义务，例如在一项数字签字附有一张转让债务通知的情况下。因此，根据所涉交易种类，可能有必要让数字签字接收人或发送人承担因利用数字签字而产生的风险。

85. 关于交叉验证和承认的可能范围，有人指出，从某种程度上来说，一个验证局的职能类似于某些法律制度下的一名公证人的职能。在一些法律制度下，某种交易确实需要一名公证人或履行相同职能的另一名官员来核证某些事实（例如，其中一方的身份）或交易的内容（例如，各方的签字或一份文件的真伪）。但是在不同的法律制度下，须由一名公证人进行这类核证的交易则各有不同，因此试图对基本交易的手续要求提出一个各国统一的办法是不可行的。

86. 有人认为，对外国证书的承认往往以对等方式给予，因此，这种承认的根据源自双边或多边国际协定。有人对于在统一规则草案中提及对等原则持保留态度，因为在不同的法律制度下，“对等”一词的含义各不相同。对于提及双边或多边国际协定的建议，反应不一。支持这项建议的人指出，提及双边或多边国际协定将表明，统一规则草案不影响各国在区域经济一体化或合作协定等框架内承担的国际义务。但是，也有人指出，不必特别提及这类协定，因为第(1)款中的任何规定都不妨碍各立法国通过这类协定进行交叉验证或承认外国证书。还有人建议，工作组不用在I条草案中提及国际协定，而应考虑就承认外国证书拟订实质性规则。有人说，应避免在I条中提及双边或多边国际协定，除非：(a)工作组得出结论，认为就承认一事制定协调一致的规则是行不通的；或(b)提及的协定对外国证书的承认比统一规则草案所订的承认更为有利。

87. 有人指出，第(1)和第(2)款载列了供立法国选择的两种不同方案，选择何

种方案取决于验证局的营业是否需要政府事先批准。但是，有人表示担心，如果将第(1)款与规定在立法国境内设立验证局必须得到事先核准的 B 条草案对照着看，(1)款可解读为允许承认尚未根据国内规则核准营业的外国验证局签发的证书，同时却否认该立法国内未获必要授权的国内验证局所签发的证书具有法律效力。在这方面，有人质问，I 条草案的目的是否为让已获政府授权的验证局可以使未获授权的其他验证局所签发的证书具有法律价值，不论其为国内的或外国的验证局。如果这就是该条要达到的目的，则 I 条草案可能需要根据工作组将对 B 条草案作出的决定加以修改。

88. 关于第(1)款提供的担保，有人指出，以列入一款一般规定而不以增加比较详细的条款的方式来处理这一问题，对一些法律制度来说可能会有困难，因为验证局提供的担保在不同国家可能大不相同。如果验证局提供的担保没有共同基础，那么国内验证局很难对在外国签发的证书承担责任。

89. 与会者在审议了在工作组中所发表的各种不同的意见后普遍认为，在统一规则草案中阐明跨境验证问题是适宜的。虽然人们认为 I 条草案所反映的各项原则大致是可以接受的，但工作组在审议的初期就拟订有关这些问题的详细条款，尚为时过早。请秘书处拟订经修改的 I 条草案，其中应考虑到上述审议情况，而且必须将政府授权的和未经政府授权的验证局都包括在内。请秘书处区别承认数字签字和证书与承认验证局两者的条件和效力，并且提出适当的建议，如有可能，提出各有差异的变式案文，以处理上述各种不同的问题。

1. 定义（续）

(b) 经授权的验证局（续）

90. 工作组结束初步审议H条草案和I条草案内的赔偿责任和交叉验证问题之后，又重新审查 B 条草案中就“验证局”的定义所引起的各项问题（见上文第 40-49 段）。有人回顾说，为使本条包含纯属私营的验证局的情况和在验证局获准运作之前应得到许可证或得到公共当局授权的情况，工作组曾暂时决定采用“双重办法”（见上文第 48-50 段），其中建议扩大“验证局”的定义，使其能包容这两种情况。在这方面，有人建议工作组不妨考虑是否可能将“验证局”改为“验证实体”，以避免验证工作可能必须交由公共当局执行的含义。虽然有人支持这项建议，但工作组指出，“验证局”已在公

共和私有实体被广泛采用。有人敦促工作组在选用名称方面应谨慎从事，以免与新出现的验证工作不符。

91. 有人指出， B 条草案中的现有案文已对验证局的各个方面作出了规定。虽然有些条款，例如第(3)款，纯属定义性质，但其他各款，例如第(4)款则对验证局进行的工作有更详细的规定和说明。因此，有人建议 B 条草案可能需要细分为不同的条文，分别对验证局的定义和功能作出规定。普遍认为，在改订 B 条案文时，除提到验证局进行的加盖时间标记的工作外，也可提到验证局在执行有关数字签字的主要工作之外的“附属”工作，例如签发成对钥匙、维持名册、保存记录等服务。然而，普遍赞同，在规定这些附属服务的范围时，不应超过 A 条草案“数字签字”中所规定的统一规则的范围。

92. 为在适用于立法国颁发许可证或经授权的验证局的法律机制和适用于未获授权的验证局的法律机制之间作出分别，有人建议统一规则草案应载明经授权的验证局签发的证书可能产生的具体法律效力。在答复关于未经授权的验证局签发的证书可能产生的法律效力的问题时，有人建议这项问题不妨以提及《示范法》第 7 条的方式加以解决。有人虽然支持这项提案，但认为不妨由统一规则对纯属私有的验证局所签发的证书的法律效力作出明文规定。另有人建议，经授权的验证局和未经授权的验证局之间的划分不妨以这两类验证局所进行的不同功能为依据。与会者普遍认为，这些问题可能值得工作组在今后的会议中进一步审议。

93. 在讨论第(3)款时，有人指出案文中提到“自然人和法人的……钥匙”是否已对在没有直接人为干预下向电子设备签发编密钥匙或这些设备使用编密钥匙的情况提供足够的指导。工作组回顾，这项问题曾在制订《示范法》时加以讨论，当时大家普遍认为这项问题可能需要在以后审议签发数字签字的问题时进一步讨论。

94. 关于订正的 B 条草案可能采用的结构，有人提请工作组注意《示范法》所采用的方法，即依靠法律规则和颁布这些规则的指南这两者的结合。采用这种方法就有可能对法律规则作出更详细的解释和说明，有助于立法人员未来对这些规则的审议。有人建议同样的办法也应用于统一规则，尤其在制订验证局进行的各项功能的规定时不妨在立法指南中列入解释性材料。工作组虽推迟对统一规则的最后形式作出决定，但认为这项建议作为一项工作假设可以普遍接受。

95. 经讨论，工作组决定 B 条草案的现行案文应分列两条，分别对“验证局”扩大后的定义和验证局执行的功能作出规定。工作组决定，“验证局”的一般性定义应以 B 条草案第(3)款的案文为依据。工作组同意，在提到“自然人和法人”时应提及“ 电子设备”来加以补充，并应在工作组未来审议前放在方括号内。除“验证局”的一般性定义外，订正后的定义条文可依据 B 条草案第(1)款，应载有“经颁发许可证的”、“经授权的”或“经认可的”验证局的定义。至于 B 条草案第(2)款和第(5)款中所载的要素则应反映在与“经授权的”验证局的定义相应的统一规则草案的立法指南中。

96. 普遍同意对验证局的各种功能作出规定的另一条案文可以 B 条草案第(4)款为依据。还同意未来有关验证局功能的条文的范围可适当扩大，把其他功能亦包括在内。为此，可从现行立法、指导方针和目前使用的或为通过验证局的规定而正在审议的示范合同中提取组成要素。至于起草问题，普遍认为第(4)款中“通过数字签字保证的通信”的案文可能需要修正，以避免对验证局使用的保密方法的可接受性给予特殊含义。

97. 工作组要求秘书处根据上述审议和决定编写 B 条订正草案。

(c) 证书

98. 工作组根据下列条款草案讨论了证书的定义:

“C 条草案

“经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;

(d) 验证局的名称、地址或营业地点;

(e) 用户的公用编密钥匙;

(f) 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字签字的收件人;

(g) 证书的序号; 以及

(h) 证书的[签发日期和截止日期][有效期]。”

99. 首先，有人提请工作组注意，在审议“验证局”的定义时，工作组已同

意，作为一项工作假定，采取一种灵活处理方式，其范围涉及由政府授权的验证局签发的或在政府所操作的公用钥匙基础结构范围以外运作的验证局签发的证书，但在目前阶段这两种方式都不会排除。根据该项工作假定， C 条草案开首语中“授权”两字应予删除。

100. 对 C 条草案的用语，特别是在提到成对编密钥匙中的私人钥匙持有人时关于“用户”一词的使用，与会者作了一般性评论。有人认为，该词会与电文收件人混同，因为电文收件人可被视为证书“用户”，或核实数字签字所用公用钥匙的“用户”。有人提出其他用语，其中包括“成对钥匙拥有人”、“证书持有人”、“私人钥匙持有人”等。大家同意，秘书处应审查 C 条草案和统一规则其余各项条款的用语，并拟订避免采用含糊不清词句的建议。

101. 普遍认为， C 条草案应于提及“证书”必须包含的内容以前确定“证书”一词的定义。有人建议按下列方式下定义:“证书是一份指明其验证局、载有用户公用钥匙以及列明用户姓名并有验证局的数字签字的称为证书的数据电文”。按照另一项建议，定义应以秘书长说明内所载的证书要点为根据，其中称证书是一份电子记录，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（ A/CN.9/WG.IV/WP.71 ，第 36 段）。有人认为，后一项建议所提出的定义大体上可以接受。但这样的一个定义应指明，如果证书系以电子通信方式递交，验证局应在证书上以数字方式签字，以保证证书在其内容和来源两个方面的可靠性。

102. 有人问， C 条草案开首语关于证书内容的“至少”两字是否意味着一项证书若不载列 C 条草案所列一切资料和数据，则按统一规则草案的意义就不视其为证书。有人回答，目前草拟的 C 条草案提到证书必须含有若干强制性组成部分，才能如统一规则所指视为一项证书。为明确起见，有人建议“证书”定义应为自成一体的条款，证书必须提供的资料应载列于另一项条款。

103. 工作组讨论了证书所应载列的资料的层次。作为一般性评论，有人建议，强制性组成部分应尽量减少，基本上应包含使证书用户能够核实数据电文所用数字签字的资料。有人担心将不必要的组成部分连同其他资料列入证书可能会无意地将若干证书排除在统一规则草案的范围之外。如果不被排除在外，这些证书可能会达到签发的目的。有人认为，必须注意，证书所载资

料与验证局为确定资料的准确性而采取的步骤是有差别的。证书所载资料越多，验证局可能要承担责任的危险性就越大。因此，有人建议，统一规则草案不应对一份证书的内容拟订最低的要求。

104. 有人根据有关验证局赔偿责任问题的讨论提出不同的方式，据理解，按照这个方式，如果错误认定一人或误以为公用钥匙属于某人，验证局应对受损方的损失承担责任，除非验证局能够证明它已竭尽全力避免错误（见上文第 58 段）。普遍认为，规定验证局应当遵守适当程序以确定资料的准确性，或者适当认定私人钥匙持有人，但却同时签发一份证书，其所载资料少于所规定的最低数量，这种让验证局避免责任的做法，对保护最终用户是毫无帮助的。

105. 有人建议，如果规定证书内容必须满足某些强制性规定，验证局将难按所指的方式随便避免责任。在这方面，应当记得，在关于验证局赔偿责任问题的讨论中，有人提出一项建议：验证局在签发一份证书时，应有责任说明它已证实证书内的若干组成要素（见上文第 70 段）。该项建议受到热烈支持。经讨论，工作组认为，此事无法在本届会议详加审议。商定根据秘书处为反映上述讨论结果而制订的备选案文尽早恢复审议这个题目。

106. 尤其关于鉴定公用钥匙持有人可能所需的数据，有人建议，第(a)、(b)和(c)项应合并成一条。在这方面，有人指出，许多国家均将诸如个人出生日期的资料视为受到保护的个人资料，可以制定具体规则对以电子手段披露这种资料实施管理。因此，有人建议，这类个人资料不应规定列入证书。在作出答复时，有人指出，在有些情况下，申请证书者可能同意公布某类个人资料或其他信息或同公布此种资料或信息的利益有关。统一规则草案不应排除这种可能性，尤其当同意披露个人资料并不违背提出此种申请或签发证书的国家的资料保护规则或公共政策时。普遍认为，数据保护问题不属于统一规则草案的范围，并且 C 条草案只需规定提供符合数据保护有关法律的足够身份证明即可。

107. 有人建议，(a)项应列入用户的“名字或身份证明”，以便包括不以用户名字而以其他证明身份方式例如帐户号证明用户身份的情况，如同在信用卡交易时使用证书的情况。有人反对这项建议，认为这可能会鼓励使用匿名电文和证书，这种情况不符合提高电子商业中法律肯定性的目标。有人要求工作组继续把私人钥匙持有人的名字作为证书的主要组成部分。

108. 为确保适当证明私人钥匙持有人的身份，有人建议，C 条草案内应增

加证明身份的组成要素，例如，在涉及自然人时增加地址，而在涉及法律实体时增加登记证号码，因为单凭个人或公司的名字并不足以证明个人或公司的身份。

109. 有人表示，数字签字在有些情况下可能限用于某类交易。例如，签字人以公司的名义签字使公司所作的交易受到约束的权力具有限制。因而，有人建议，证书内应载有关于这种限制或限度的资料，或应提到这种限制或限度的来源。在回答这项建议时，有人指出，关于数字签字可作为依据的限度范围的问题引起了一些法律难题，而这些难题并不是电子商业独有的。在书面的环境中，可能并不强制规定在手写签字时必须附带说明签字人可能拥有的权力的限度范围。有人要求工作组在数字签字问题上，不采用比适用于手写签字更严格的规定。

110. 有人提醒工作组，它曾经讨论过消费者问题和验证局的赔偿责任以及国家法律或验证局的验证做法说明中所规定的赔偿责任的可能限度或排除这种赔偿责任的情况。有人建议，验证局应指明这种限度或向用户说明能够查明这种限度的文件。有人还建议，统一规则草案应载明证书中未作这种说明可能引起的后果。同样地，有人建议，在证书有效期有限的情况下，也应以截止日期或使用期的方式在证书中提到这种限度。有人认为，为了保障证书的使用者，应向使用者提供证书合法性的资料，而且使用者也不应承担签发的证书中不附有这项说明的风险。因此，统一规则草案应载有一项指明有效期的默认案文，以用于没有这方面说明的情况。不过，有人指出，列入这项规定可被解释为验证局能选择在证书中不提及证书有效期或使用期。

111. 有人询问，根据目前的技术，验证局能向用户提供何种它能提供用户取用的服务的资料。对此有人回答说，现有技术使验证局能附加或在它们签发的证书上链接额外资料，例如验证局的验证做法说明或私人钥匙的持有人为此目的自愿提供的资料。不过，验证局客户目前使用的许多计算机系统仍然无法取用全部这类资料。除了这种技术上的困难之外，也应了解附加在证书上的有些资料可能来自于私人钥匙的持有人，并且是在它们的要求下提供的。因此，在这种情况下，应分别证书中经验证局验证的组成要素（例如，私人钥匙持有人的身份）和验证局的客户提供的并且未经验证局验证的其他组成要素（例如，公司内使用私人钥匙的限度）。验证局不应对这种未经核证的资料的正确性承担赔偿责任。

112. 与会者提出了各种看法，大致上认为在不影响验证局提供给其客户的其

他资料的情况下，验证局应说明和证明强制列入证书的资料的正确性和全面性已得到核证。

113. 工作组审议了就 C 条草案提出的意见之后，同意在本条草案中应增加“证书”的定义。证书中的强制性内容应在另一条款中作出规定，该条款也应对证书中不加附强制性案文所产生的后果作出规定。该项条款应反映(a)、(b)和(c)项中提到的组成因素（合并成一条单独的订正条款），并包括 C 条草案(d)、(e)和(h)项中提到的资料。工作组不认为(f)项中提到的资料能由验证局验证，因此同意删除此项。同意(g)项应置于方括号内，并在以后作为一项可能的备选方案审议，因为并非所有证书均可根据序列号加以确定。 C 条订正草案应明文提及关于数据保护的国内法对证书中所载资料的适用性。工作组请秘书处编写 C 条的订正草案，设法以备选案文的方式反映在工作组中表示的各种意见和达成的结论。

4. 法人和自然人的签字

114. 工作组根据下列条款草案进行了讨论:

“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证明的编密公用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字方式签字，该法人只应被视为该电文的[发端人][批准了电文的发送]。”

115. 一些代表团发表了看法，认为应该删去 D 条草案。有人说，为数字签字的目的对法人与自然人加以区分是不妥当的，因为在《示范法》中并没有作这种区分，其中“人”的概念涵盖了自然人和法人。而且，还有人说，第(2)款可能不适当地干扰代理法等其他法律，干扰涉及由自然人代表公司的公司法的规定。此外，又有人说，第(2)款内的规则看来给数字签字使用者规定了一项责任，超越了有关手写签字的现有要求。

116. 但是，有人则表示， D 条草案、特别是第(2)款有其用处。尤其是如果没有其他适用的规则对代表法人可给的有约束力的签字的形式作出具体规定，则类似第(2)款的默认规则可以对在何种情况下可以信赖据称是法人的数字签字提供有用的指导。有人表示支持保留第(2)款，但必须修改条款，

以明确说明，虽然该款提到了“被授权代表”法人“行事的自然人”，但其用意并不是要取代国内的代理法。因此，该自然人在事实上和法律上是否有权代表该法人行事的问题将由统一规则以外的有关法律规则解决。

117. 经讨论，工作组决定将 D 款草案放在方括号内，供以后一届会议进一步审议。

5. 数字签字电文的归属

118. 工作组根据下列条款草案进行了讨论:

“E 条草案

“(1) 附有发端人数字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) 附有数字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，初始电文未作改变;

“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，即如果收件人向经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止或中止;

“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。”

119. 有人表示应删除E条草案。支持这种看法的人指出，该条草案只是《示范法》第13条的一个行业特定情况，并可能由于这两条之间的可能互相作用而造成不确定性。另一种看法认为，应删除E条草案，因为它可能会使人误认为该条会干涉适用于为其使用数字签字的商业交易的法律。例如，规定数据电文发端人受“电文内容约束”的第(1)款可能会被人认为不恰当地涉及了一般合同法。

120. 普遍的看法是，E条草案的具体起草方式需要修订，但第(1)款所载原则对于确立使用数字签字的法律程序是有用的。关于此一原则应如何表达的问题，有人建议，第(1)款应根据以下不可反驳的推定重新起草，即数字签字的持有人将被认为是附有数字签字的数据电文的签字人。

121. 关于数字签字电文的归属问题是否可能可以通过推定，不论是否无法反驳，来加以处理的问题，有人建议，或许应根据可能使用数字签字的交易的种类作出进一步的区分。例如，对于长期贸易伙伴间的纯粹商业交易和对于向公共行政当局提出税务申报不应采用相同的标准。

122. 有人建议，沿着第(1)款的方式拟定的规定可能需要区分不同种类的数字签字(例如各种不同算法提供不同的安全水平，和数字签字费用上的对应差异)和使用数字签字的各种不同情况。有人建议，在修订第(1)款草案时，可以考虑到以下几种情况:数字签字是不是在各当事方间任何原有合同之外使用的;数字签字是不是在合同框架内使用的;数字签字有没有牵涉到由一个未经认可的验证局发出证明;或牵涉到由一个有执照的验证局发出证明。有人还建议，在处理欺诈个案中数字签字过程所涉及的风险水平时，应特别注意在发出成对钥匙之前发生欺诈的情况。在这种情况下，如果各方之间没有任何协议，应由收件人负起建立数字签字和发送人之间的链接的责任。如果有证明，而且该证明是恰当而有效的，那么举证之责可能会转移。另一项建议是，在处理由验证局验证过的电文时，指定某特定验证局的一方则应承担使用该验证局发出的证明所涉及的风险。

123. 有人表示怀疑，在E条草案中是否应考虑到上述所有各类情况。有人特别回顾到，在讨论责任问题时，工作组曾同意集中注意签发证明的情况。但普遍认为，在起草E条订正草案供工作组将来的届会审议时，应铭记着建议的某些或所有各类情况。

124. 经讨论，工作组同意，修订数字签字电文归属的条款对工作组今后审议

来说是必要的，而且可以沿着 E 条草案第(1)款的方式拟订这项规定。普遍认为，需要提出适当的评论以澄清 E 条和《示范法》第 7 和 13 条之间的关系。工作组要求秘书处拟定 E 条订正草案，可能可以某些变式来反映出以上的讨论。

6. 证书的废止

125. 工作组根据下列条款草案讨论了证书废止问题:

"F 条草案

"(1) 经核准的成对钥匙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) 如果经核准的成对钥匙的持有人了解到私人编密钥匙遗失、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。"

第(1)款

126. 与会者对第(1)款含义发表了一般性评论。有人指出，私人钥匙持有人应始终有权要求验证局废止证书。关于这种废止自验证局收到或登记之时生效的规定不应被解释为是对上述权利的限制。此外，关于这种废止自验证局收到或登记之时生效的规定也不应被解释为第三方在依赖证书之前有责任查明证书是否有效(如证书是否已被废止)，工作组许多成员曾反对对第三方的这种要求(见上文第 60 段)。

127. 关于这种废止开始生效的时间，大家发表了各种意见。一种意见认为，废止应从验证局登记时开始生效，因为收到的时间有时难以确定，从而导致无法断定证书失效时间。另一种意见认为，验证局应有义务在证书废止后迅速采取行动，以避免可能给私人钥匙持有人或第三方造成的损失以及在持有人废弃证书之后该证书可能被无意接受等情况下造成的损失。因此，废止证书的效力应取决于验证局采取的私人钥匙持有人无法控制的措施。

128. 有人问及证书废止的登记可能产生的效力。在这方面，有人认为，证书废止登记的概念也许不能完全满足 F 条草案的目的，因为该条除其他外，旨在确保酌情将某一证书已废止的情况通知第三方。有人指出，在一些情况

下，验证局收到关于废止的请求之后，可能需要核查这项请求是否真实，而这一程序取决于具体情况，可能会造成一些延误。因此，这种废止正式生效的适当时刻是通过将废止请求输入由验证局保持、公众可查阅的数据库或通过其他适当的公布方法公之于众的时刻。

129. 关于上述意见，有人指出，在确定证书的废止时间方面，收到废止请求的时间还是比登记的时间更加可取。然而，如果认为收到这种请求的概念不够确切，则可将收到的概念与随后由验证局采取使这种废止生效的某种行动相结合，例如公布废止或发出废止通知。

130. 为了推进就此专题进行的辩论，有人请工作组审议选择废止生效时间所涉及的一般问题以及可能受这种废止影响的各方的情况。废止生效时刻对于确定私人钥匙持有人和验证局彼此之间以及对第三方的责任至关重要。有人提议，工作组也许最好分别审议每一种情况。支持上述建议的人指出，目前第(1)款所载的每一种选择各自都有优点。就私人钥匙持有人和验证局之间的情况而言，也许应该规定废止应于验证局收到私人钥匙持有人关于废止的请求时生效。然而，就第三方而言，也许更恰当的是规定废止通知须经登记或公布方告生效。

131. 有人认为，废止的生效时间对验证局的责任有重大影响，应统一处理这两个问题。据指出，H 条草案第(4)款规定，如果经授权的验证局收到废止证书的通知，验证局应立即登记通知。如果验证局未能这样做，则应对用户因此遭受的任何损失负责。因此，如果统一规则规定证书的废止在收到之时生效，则应删除 H 条草案第(4) 款，因为验证局无须对在登记废止通知方面的过失或疏忽承担责任。但是，如果证书的废止在登记之时生效，则可能无须在 H 条第(4)款之外另立规定。

132. 针对这个意见，有人指出，无论工作组选定 F 条第(1)款目前两个选择办法的任何一个，H 条草案第(4)款内的规则都应予保留。迟登记废止请求可能对持有人或依靠一方造成一些损失，因此，还是有必要制定规则，以追究迟登记所造成的后果的责任。

133. 在这方面，有人指出，关于电子验证和认证的国际标准和准则，如国际商会在拟订中的《统一国际认证和验证程序准则》，都反映验证局须就废止证书的请求迅速采取行动的原则。但正如以前所指出，废止请求的生效可能受到一些延误，特别是在有些情况下，验证局需要进行一些核实工作，如证实代表私人钥匙持有人要求废止的人的权力。为了避免在验证局核实废止请

求期间错用证书，有人建议统一规则草案增列一条，规定验证局在私人钥匙持有人提出请求时立即暂停使用证书。据解释，与终止证书效力的废止不同，暂停使用是一项临时措施，只是在一段时间内停止证书的效力。

134. 有人赞同采用暂停使用证书的概念，以有别于完全废止证书。但建议应另立规定处理暂停使用的问题，因为暂停使用的概念和后果与废止不同。

135. 在审议了各种意见后，工作组同意，废止证书的问题是健全的数字签字法律制度的一个重要部分，工作组须作进一步审议。普遍同意处理这个主题的规定尚缺一些因素，因此请秘书处根据工作组的讨论编写一项订正规定，其中包括不同的废止生效时间所涉及的问题。另外同意订正草案应有暂停使用证书的规定。

第(2)款

136. 有人认为，本款第一句采用“义务”一词不够恰当，在该款的意义范围内，“责任”或“负责”等词较为适当。

137. 另外建议的是，除了核准成对钥匙的持有人外，验证局也应该有责任在了解到私人编密钥匙遗失、失密或有其他被误用的危险时废止相应的证书。为支持这项建议指出的是，一些关于电子验证和认证的国际标准和准则，如国际商会正在拟订中的《统一国际认证和验证程序准则》，均考虑规定这种责任。

138. 对于验证局是否有能力履行这项责任的问题，有人说现有技术使验证局可以对这些情况迅速作出反应。但是，决定需要多少时间作出反应并不单是取决于现有技术，验证局根据合同安排向其客户提供的服务水平也是一个决定因素(如验证局是否有专人处理私人钥匙的遗失、失密或误用;验证局在周末是否提供客户服务或者只有正常办公时间)。

139. 工作组注意到提出的各项意见，并同意今后审议证书的废止问题时应予考虑。

7. 证书登记簿

140. 工作组根据下列条款草案讨论了证书登记簿问题:

“G条草案

“(1) 经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，登记簿应由该验证局至少保存[10]年。”

141. 有人请工作组在关于证书登记簿的讨论中，首先审议在统一规则草案中列入关于这个问题的条款的重要性；如果对此问题的答案是肯定的话，再审议应该规定这个登记簿应有哪些内容要素和保存多长时间。

142. 虽然没有人对列入关于证书登记簿的条款提出原则性的异议，但是有人建议，工作组应该继续审议这一条款从整个统一规则草案来看是否确实有必要，以及验证局可能签发的所有不同种类的证书是否都贴切的问题。

143. 关于这种登记簿应该有怎样的结构，有人表示意见说，与其每个验证局各自保持自己的证书登记簿，倒不如由属于同一个公用钥匙基础结构的验证局保持一个中央登记簿来存放它们所签发的证书。这样一种结构的目的在于避免保持多个登记簿，一些国家目前正在考虑这样做。有人建议，工作组如果进一步研究这个可能性，也许会有好处。

144. 关于第(1)款，有人建议，没有必要在登记簿中写明证书签发的时间，因此应该删去“表明各份证书签发的时间”等字。另一项建议是，验证局应该另外保持一个废止证书的数据库，以便利各有关方面对证书的有效性进行查询。

145. 对于第(2)款所提到的保存期限有无必要和是否足够，大家表达了不同的意见。有人说，规定一个最低限度的保存期限是恰当的，目的是为了确保各有关方面能得到这种数据，在国内法对行使或执行权利或者要求履行义务订有时限的情况下尤其重要。不过，各国的国内法对不同种类的权利和义务有不同的时限。同样，它们根据公共和私人记录的不同对象而规定不同的保存期限。在这种情况下，也许更好的做法是让各国在国内法中自行规定适当的保存期限，而不是武断地规定一个不一定对所有情况都足够的期限。另外，工作组还应该考虑到把证书登记簿保存任何一段特定时限所招致的费用。视验证局所提供的服务水平和把证书存档的方法而定，要求一个验证局把某些种类的证书保存超过某个一定的时限，从成本效益来说可能不划算。如果没有这一规则对这个行业产生的实际影响的资料，就试图规定一个通用的保存期限，是并不可取的。

146. 不过，另一种意见认为，订一个记录和资料的保存期限，让有关一方能够确定其贸易伙伴的身份和他们的签字的真实性的问题，牵涉到若干公共政

策上的考虑，是工作组不应忽略的。这个问题应该在统一规则草案中处理。至于什么是适当的保存期限，有人建议，不应该完全让验证局纯粹根据费用考虑来单方面决定保存期限。而且，不应该只以保存费用作为决定因素来缩短或者废除保存期限。把它们所签发的证书存入一个公共钥匙基础结构内的同一个登记簿的验证局，可以订立某种共同分担费用的机制。

147. 有人建议，应该要求对一个登记簿内的证书作出查询的有关方面在登记簿上留下一个记号，证明曾经作过查询。根据解释，假如验证局和有关方面对于该方在依靠一份数字签字电文之前有没有核实证书的有效性发生问题的话，这种证据的存在可能会很重要。

148. 工作组注意到提出的各项意见，并请秘书处审查所提出的各种问题，拟订能反映工作组内进行的辩论情况的备选条款草案。

8. 用户与验证局的关系

149. 工作组面前有以下的条款草案：

“ 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) 与数字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。

“(3) 第(1)款中所列的信息应在缔结最后认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。]

“(4) 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。

"(5) 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。"

150. 工作组注意到，由于J条草案所处理的是用户与验证局的关系，所以它预先假定已经就若干问题作出了决定，而这些问题是工作组仍在审议的。大家同意，整个J条草案应该加上方括号，留给工作组在较后阶段加以审议。

三. 以提及方式纳入条款

151. 工作组完成了对本报告第二部分所述的数字签字统一规则拟考虑的法律问题和可能制订的规则的初步审议工作后指出，由于时间不足，本届会议无法对以提及方式纳入条款问题进行详尽的讨论。

152. 工作组忆及，以提及方式纳入条款问题在编制《示范法》各阶段工作中都简略地讨论过(见A/CN.9/406，第90和178段，和A/CN.9/407，第100-105和117段)。工作组在上一届会议大体同意，需要对电子商业范围内的以提及方式纳入条款问题进行工作。有人认为，在为数据电文中此种以提及方式纳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：(a) 提及条款应插入数据电文中；(b) 所提及的文件——例如一般期限和条件——实际上必须为参考文件可能依赖的当事方所了解的；以及(c) 所提及的文件除了为当事方了解外，还必须为其所接受。工作组大体同意，以提及方式纳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来解决较为适当(A/CN.9/421，第114段)。委员会在其第二十九届会议上大体同意，该问题可以在验证局工作的范围内处理。[2]

153. 在本届会议上，工作组大体同意，接受以提及方式纳入条款对于一般电子商业的发展非常重要。虽然这个问题也许需要在关于数字签字和验证局的工作范围内加以讨论，但是也值得在更为一般的层次上加以审议。即使在较后阶段发现宜于在数字签字范围内对以提及方式纳入条款问题设计出具体的规则，进行一般性讨论和可能地制定一套规则也是需要的。

154. 有人认为，为电子环境下以提及方式纳入条款设计出一套规则，任务可能非常艰巨，因为所涉及的问题错综复杂。以提及方式纳入条款及有关问题，例如服从契约和"格式之争"问题，在书面环境下产生了一大堆法律规

---

2 《大会正式记录，第五十一届会议，补编第17号》(A/51/17)，第222段。

则，而且并非所有有关的法律问题都解决得令人满意。这个课题本身就说明必须要平衡相互冲突的利益。一方面，需要承认当事方的自主权，而另一方面又必须限制可能滥用服从契约的行为。鉴于在以提及方式纳入条款的领域预期会碰到一些困难，有人建议应对电子商业范围内也值得进一步开展工作的其他问题给予较优先的地位。另一种看法是，对以提及方式纳入条款问题的讨论只能在秘书处对服从契约、格式之争和有关赔偿责任问题的比较法方面进一步研究的基础上进行。

155. 大多数人的看法是，秘书处无须进行进一步研究，因为根本问题已经是众所周知，而且很明显格式之争和服从契约的许多方面问题将需留待适用的国内法来解决，因为这里涉及例如消费者的保护和其他公共政策考虑等因素。经讨论，工作组决定这个问题应在下一届会议开始时作为议程上的第一个实质性项目来处理。

四. 今后的工作

156. 工作组忆及，委员会曾要求它研究编制关于数字签字和验证局问题的统一规则的适宜性和可行性。工作组在本届会议结束时认为，其提交委员会的报告应指出它已就统一这个领域的法律的工作的重要性和需要达成共识。虽然它还未就这类工作的形式和内容作出有力的决定，但是它已初步得出结论认为，对数字签字问题编制统一规则草案是可行的。

157. 在讨论今后的工作时，工作组忆及，除了数字签字和验证局的问题外，电子商业领域今后的工作还需要讨论：公用钥匙加密的技术性备选办法问题；第三方服务提供者履行职能的一般问题；以及电子立约问题（见A/51/17，第219-221段）。