联合国 A

大会

Distr.
GENERAL

A/CN.9/446
11 February 1998
CHINESE
ORIGINAL: ENGLISH

联合国国际贸易法委员会
第三十一届会议
1998年6月1日至12日，纽约

电子商务工作组第三十二届会议工作报告
(1998年1月19日至30日，维也纳)

目　录

导言

1. 委员会在其第二十九届会议（1996 年）上决定将数字签字和验证局的问题列入议程。另外请电子商务工作组审查制定关于这些问题的统一规则的可取性和可行性。据商定，拟由工作组第三十一届会议执行的工作可包括编写关于上述问题的某些方面的规则草案。委员会请工作组为其提供足够的要素，以便就拟编写的统一规则的范围作出明达的决定。关于对工作组下达的比较确切的职权，据商定拟编写的统一规则应处理这样一些问题：支持验证过程的法律依据，包括新兴的数字认证和验证技术；验证过程的可适用性；在使用验证技术时，使用者，提供者和第三方之间风险和赔偿责任的分配；通过使用登记处验证的具体问题；以提及方式纳入。[1]

2. 在第三十届会议（1997 年）上，委员会收到了工作组第三十一届会议的工作报告(A/CN.9/437)。关于制定关于数字签字和验证局问题的统一规则的可取性和可行性，工作组向委员会表示，工作组已经就设法协调这一领域的法律的重要性和必要性达成协商一致的意见。虽然工作组尚未就此项工作的形式和内容问题作出肯定的决定，但工作组已经得出初步结论，认为至少就数字签字和验证局的问题以及可能就有关的事项制定统一规则草案是可行的。工作组回顾，在处理数字签字和验证局的问题的同时，电子商务领域中未来的工作可能还需处理下述一些问题：公用钥匙密码学的技术替代办法；第三方服务提供者履行的职责的一般问题；以及电子订约(A/CN.9/437，第 156 - 157 段）。关于以提及方式纳入条款的问题，工作组的结论是，无需由秘书处进行进一步的研究，因为基本问题已是众所周知，而且格式之争和服从契约的许多广大需留待适用的国内法来解决，因为这里涉及诸如消费者保护和其他公共政策的考虑等因素。工作组认为，这个问题应在其下届会议开始时作为议程的第一个实质性项目处理(A/CN.9/437，第 155 段）。

3. 委员会对工作组在第三十一届会议上已经完成的工作表示赞赏，赞同工作组达成的结论，并责成工作组编写关于数字签字和验证局的法律问题的统一规则（以下称“统一规则”）。

4. 关于统一规则的确切范围和形式，委员会普遍认为，目前这个阶段为时过早，还不可能作出决定。人们认为，虽然鉴于公用钥匙密码学在新兴的电子商务活动中显然发挥着支配作用，工作组可能应适当将注意力集中在数字签字的问题上，但统一规则应与《贸易法委员会电子商务示范法》（以下称《示范法》）中所采用的媒介中性办法相一致。因此，统一规则不应阻碍其他认证技术。此外，在处理公用钥匙密码学时，统一规则可能需顾及不同的安全水平，并承认相对于在数字签字的条件下提供的各类服务的各种法律效力和赔偿责任程度。关于验证局的问题，虽然委员会承认市场驱动的标准的价值，但人们普遍认为，工作组或许应设想确立一套应由验证局达到的最低限度标准，特别是如果要求进行跨境验证的话。

5. 关于拟放在电子商务领域未来工作中审议的补充项目，有人提出，工作组可能需在稍后阶段讨论管辖权、适用法律以及互联网络上解决纠纷的问题。[2]

6. 电子商务工作组由委员会的所有成员国组成，于 1998 年 1 月 19 日至 30 日在维也纳举行了第三十二届会议。工作组的下列成员国代表出席了届会：阿尔及利亚、澳大利亚、奥地利、巴西、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、墨西哥、尼日利亚、波兰、俄罗斯联邦、新加坡、斯洛伐克、西班牙、苏丹、泰国、大不列颠及北爱尔兰联合王国和美利坚合众国。

7. 下列国家的观察员出席了届会：安哥拉、白俄罗斯、波斯尼亚和黑塞哥维那、加拿大、哥伦比亚、哥斯达黎加、捷克共和国、丹麦、希腊、危地马拉、印度尼西亚、伊拉克、爱尔兰、科威特、黎巴嫩、马来西亚、摩洛哥、荷兰、巴基斯坦、巴拉圭、大韩民国、瑞典、瑞士、土耳其和乌克兰。

8. 下列国际组织的观察员出席了届会：贸发会议/世贸组织国际贸易中心、联合国贸易和发展会议（贸发会议）、联合国教育、科学及文化组织（教科文组织）、联合国工业发展组织（工发组织）、世界知识产权组织（知识产权组织）、欧洲委员会、经济合作与发展组织（经合组织）、世界贸易组织（世贸组织）、开罗国际商业仲裁区域中心、国际海事委员会（海事委员会）、国际港埠协会（港埠协会）、国际律师协会（律师协会）、国际商会、互联网络法律和政策论坛以及欧洲法律学学生国际协会。

9. 工作组选出下列主席团成员：

主席：Mads Bryde ANDERSEN 先生（丹麦）；

副主席：PANG Khang Chau（新加坡）；

报告员：Gritsana CHANGGOM（泰国）。

10. 工作组收到下列文件：临时议程(A/CN.9/WG.IV/WP.72)；秘书处为工作组第三十一届会议编写的说明，标题是“电子商业问题今后工作的规划：数码式签字、验证局和有关法律问题”(A/CN.9/WG.IV/WP.71)，这个说明归纳了工作组以往就以提及方式纳入条款的问题进行的审议；一个转载大不列颠及北爱尔兰联合王国提议的关于以提及方式纳入条款的条文草案案文和解释性说明的说明(A/CN.9/WG.IV/WP.74)；以及载有关于数码式签字、其他电子签字、验证局及有关法律问题的统一规则草案(A/CN.9/WG.IV/WP.73)。

11. 工作组通过了下列议程：

1. 选举主席团成员
2. 通过议程议程
3. 电子商务所涉法律问题：以提及方式纳入条款
4. 电子商务所涉法律问题：关于数码式签字、其他电子签字、验证局和有关法律问题的统一规则草案
5. 其他事项
6. 通过报告。

一. 审议情况和决定

12. 工作组根据秘书处的说明(A/CN.9/WG.IV/WP.71)和大不列颠及北爱尔兰联合王国的提议(A/CN.9/WG.IV/WP.74)讨论了以提及方式纳入条款的问题。工作组就这一问题进行的审议和达成的结论反映在下文第二节中。经过讨论，工作组通过了关于以提及方式纳入条款的条款草案案文。工作组请秘书处根据工作组的审议情况和讨论编写一个简短的指南，以协助各国颁布并适用这一条款草案。人们注意到，这一条款草案连同有关的颁布指南将提交 1998 年 6 月 1 日至 12 日在纽约举行的委员会第三十一届会议，以进行最后审查并可能收入《示范法》及其《颁布指南》中。

13. 工作组还根据秘书处编写的说明(A/CN.9/WG.IV/WP.73)讨论了数码式签字、其他电子签字、验证局及有关法律方面的问题。工作组就这些问题进行的审议和达成的结论反映在下文第三节中。工作组请秘书处根据这些审议和结论编写一套订正条文和可能的变式，以交由工作组今后的届会审议。

二. 以提及方式纳入

14. 工作组回顾了早些时候对“以提及方式纳入”这一问题的审议和其上届会议提议的案文草案(A/CN.9/WG.IV/WP.71，第 77-93 段)后，会议请工作组根据下文的一项拟议的条款草案(A/CN.9/WG.IV/WP.74，附件)审议电子环境下的以提及方式纳入的问题:

“(1) 当数据电文含有提及记录在他处的信息(‘进一步信息’)的文字，或当只有借助提及记录在他处的信息的文字才能充分确定数据电文的含意时，本条适用。

“(2) 在不违反第(5)款规定的情况下，如果第(3)款中的条件得到满足，数据电文所具有的效力应如同数据电文中充分表述了进一步信息时所具有的效力一样，而且数据电文中的任何提及均将构成对该电文的提及，包括所有的进一步信息。

“(3) 第(2)款中所提到的条件是，数据电文要:

“(a) 以下述方式标明进一步的信息 -

“㈠ 集体名称或说明或代号；和

“㈡ 充分列明记录和该记录的组成部分，其中应载有进一步的信息，如果该记录并非公开提供，则应列明可以找到记录的地点；如果查询手段并不明显或受到某种限制，则应标明查找的手段；和

“(b) 明文指出或明显默示数据电文所具有的效力应如同数据电文中充分表述了进一步信息时所具有的效力一样。

“(4) 第(3)款(a)项所述标明可间接作出，即提及记录在他处且含有必要标明的信息，但应满足第(3)款有关该种提及的条件。

"(5) 本条丝毫不影响-

"(a) 要求就进一步信息的内容或查找此类信息的记录或地点或手段提出充分通知或要求该地点或记录应为他人所能查找到的任何法律规则; 或

"(b) 与订约的条款的有效性包括对要约的接受有关的任何法律规则。

"(c) 规定被纳入的进一步信息的有效性或纳入程序的有效性的任何法律规则。"

15. 据指出, 条款草案意在当数据电文使用了以提及方式纳入时适用(第 1 款); 总的原则是, 所纳入的信息(不是指"条款或条件", 因为并非所有信息都构成义务)所具有的效力应如同其在数据电文中得到充分表述时所具有的效力一样(第 2 款); 以提及方式纳入的一般条件应当是清楚而准确地标明所纳入的信息(这一点对于保护消费者和其他第三方是至关重要的)、标明可查到信息的地点和手段, 并表明拟予纳入的意图(第 3 款); 在条件相同的情况下, 以提及另一信息来源间接标明信息来源应当是可以接受的(第 4 款); 适用于以书面通信提及方式纳入的任何现有法律规则应扩大到适用于电子通信(第 5 款).

16. 人们一般认为, 这是一个应予处理的问题, 因为以提及方式纳入是电子通信使用中所固有的一种方式。据指出, 在电子通信中, 大量数据出于需要而要使用以提及方式纳入(例如, 通信记录、政策声明、证书中的数字签字)。此外, 据了解, 电子环境下的以提及方式纳入可借助多种方法实现, 其中包括但不仅限于统一资源定位、目标标识符或其他在一指明地址可较易得到的记录。

17. 人们虽然都承认以提及方式纳入会造成风险, 例如就消费者而言, 但同时也有人认为, 这类做法可使消费者利用只有电子通信网才能提供的机会。据指出, 以提及方式纳入的条款的主要目标应当是平衡兼顾有关各方的利益。为了实现这一目标, 会议请工作组在审议上述条款草案的同时审议大致精神如下的条款草案:

"变式 A 除非当事方之间另有议定, 应将信息视为数据电文的构成部分, 条件是已明文指出或明显默示[而且该数据电文标明了一种可据以以合理而及时的方式查询到该项信息的程序]。这类信息在法律所许可的范围内有效。

"变式 B 不得仅以系在数据电文中以提及方式纳入为由而否认信息的法律效力。"

18. 关于变式 A, 据指出, 关系到某一条款是否能以合理的方式查找到的物质因素包括: 可得性(交存处的营业时间、存取的方便性和可接受的冗余水平); 查询费用(不包括基本通信服务费用; 如果需要收费, 收费也应当合理, 而且应与有关合同的价值成比例); 格式(为业界所普遍使用); 完整性(内容核对、发送人验证、通信误差纠正机制); 可在以后予以修正的范围(无此种修正的契约权利; 更新通知; 修正政策通知)。人们还进一步指出, 这些因素可在一以提及方式纳入的条款的颁布指南中予以列出(见下文第

23 至 24 段)。

19. 工作组接着根据上述拟议的备选条款进行了讨论。据指出，拟议的条款有着一些共同的优点。优点之一是，它们的目的都是，通过消除许多法域在处理传统的以提及方式纳入的条款是否适用于电子环境中的以提及方式纳入方面所存在的不确定性，促进电子环境中的以提及方式纳入。在这方面，有人提议采用一种不同的做法，其精神实质是不提倡在电子环境中广泛使用以提及方式纳入，以减少传统书面贸易中所谓“格式之争”的困难局面重现的风险。支持这一建议的人认为，虽然说在书面环境下出于时间、篇幅和费用的考虑有必要采用以提及方式纳入，但在电子环境中，在数据电文中完全可以简单、及时而廉价的方式反映出大量的数据。这一意见遭到了反对，反对的理由是由统一法发挥行为准则的作用是不适宜的，那样做无异于反对人们使用一种已经广泛使用而且十分重要的做法，而这种做法的采用正是电子通信环境中所固有的。

20. 据指出，上述提议的另一个好处是，它们都承认不应干涉消费者保护或其他强制性国家或国际法律(例如，附意合同的保护弱小方的规则)。据指出，第一项提议的目的是通过列举未受影响的法律规则来达到这一结果(第(5)款)；第二项提议也达到了同样的结果，因为它提到了信息“在法律所许可的范围内”具有效力(变式 A)，或者并不排斥以除了信息是以提及方式纳入的之外的理由否认信息的法律效力(变式 B)。为了明确无误地说明现有法律不受任何拟议的措辞的影响，有人建议说，任何关于以提及方式纳入的条款，均应受符合《示范法》第 1 条脚注 2 精神的用语的约束，该脚注明确指出《示范法》的原则无意于否定消费者保护法。

21. 但是，有人认为，第一项提议和第二项提案的变式 A 有一些缺点，其中之一是规定的标准太高，从而可能打乱既定的或新出现的做法。据指出，在许多惯例中，不可能满足应明文指出或明显默示打算以提及方式纳入信息或应能合理方便地查阅这些信息这种要求。列举的例子是通过提及而将包租船的主合同纳入在租船转租合同下交付的提单中，据指出，如果提出应明文指出或明显默示打算以提及方式纳入信息或应能合理方便地查阅这些信息这种要求，那么便会影响这种惯例。另一个缺点是，这些条文会在无意中干扰法律的强调性规则，并导致不公平的结果。在这方面，据指出，除第一项提议和第二项提议变式 A 所载的两个条件外，还应包括第三项要素，即以提及方式纳入的做法应得到当事各方的认可。据指出，在开放式的电子数据交换中，当事各方的认可尤为重要。

22. 对此，据答复说，第一项提议的第(5)款和第二项提议变式 A 的第二句正是为了消除这些担忧，确保以提及方式纳入的做法不会干扰既定的惯例或本国法的强制性规则。但有人认为，这些条款可能引起解释上的问题。据指出，变式 B 便没有这些缺点，因为其中只是提出了《示范法》第 5 条所载的关于不歧视的一般原则。普遍承认，变式 B 意味着，以提及方式纳入将只有在法律许可的范围内有效。在这个基础上工作组普遍同意变式 B 更加可取。

23. 作为起草上的措词问题，据建议，变式 B 应与《示范法》第 5 条的措词相应，从而不仅提及法律效力，还提及有效性和可施行性。关于以提及方式纳入的规定的位

置，据建议，鉴于这个问题涉及整个电子商务而不仅仅是数字签字，所以其位置应是添加在《示范法》中作为第5条之二。为协助《示范法》使用者和立法人员解释关于以提及方式纳入的规定，另据建议，关于以提及方式纳入的规定，其背景和说明应列入《示范法颁布指南》。与会者建议，《指南》中可指明一些因素，各国也许希望依据这些因素采用扩大范围的关于以提及方式纳入的规定。这些因素可从第一项提议和第二项提议变式A的案文中启发而来。这项建议被认为基本可以接受。但有人告诫说，这样的做法可能与《示范法》第5条的做法不符。据认为，不应将上述因素作为《示范法》有关条款的替代案文提出。普遍认为，在起草《颁布指南》关于以提及方式纳入的部分时，应注意避免在无意中指出除在书面方式贸易中已经适用的限制之外，对电子商务以提及方式纳入的做法也应实行限制。

24. 经讨论，工作组通过了变式B，决定将其提交委员会审查，也可能作为《示范法》第5条之二列入。工作组还请秘书处编写一份解释性说明附在《示范法颁布指南》之后。

三. 审议电子签字统一规则草案

第一章. 适用范围和一般规定

25. 工作组一般认为，统一规则与《示范法》之间的关系（尤其是数字签字统一规则究竟应作为一份单独的法律文书还是并入《示范法》扩大版的问题），将需要在后一阶段加以澄清。虽然一致认为现阶段无法作出决定，但工作组确认其工作设想说，统一规则应：作为法律条文草案来拟定；总体上与《示范法》条文一致；以某种方式围绕《示范法》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）和第7条（签字）的精神纳入条款。

26. 关于统一规则的适用范围，据认为，应使其仅限于数字签字而不包括其他认证技术。对此，有人在答复时回顾说，工作组上届会议在作出其初步结论认为着手拟定数字签字是可行的时候，还商定除了数字签字和验证局的问题外，电子商务领域的工作可能还需要讨论公用钥匙加密的备选技术方法问题(A/CN.9/437，第156 - 157段）。另据回顾说，委员会第三十届会议认为，虽然鉴于公用钥匙加密在兴起的电子商务做法中显然起着突出的作用，因而工作组似宜将其重点放在数字签字问题上，但统一规则应与《示范法》中采用的不偏重任何媒体的行文方式一致（见上文第4段）。经讨论，工作组确认其决定，即在着重编拟关于数字签字技术的具体规定时，工作组还应从其中摘选一些适用于一般情况的规则，以便照顾到其他认证技术。

第二章. 电子签字

第一节. 可靠的电子签字

第 1 条. 定义

27. 工作组审议的第 1 条草案案文如下:

"在这些规则中:

"(a) "签字"系指意在为鉴别某人和表明该人核准附有签字的资料，而由此人[或代表此人]所使用的任何符号或所采用的任何安全程序;

"(b) "电子签字"系指[意在为鉴别某人和表明该人核准数据电文内容]，[而由此人[或代表此人]采用的[以及为满足[《贸易法委员会电子商务示范法》第 7 条]规定的条件所采用的]]在数据电文中以电子形式所载或所附或在逻辑上与数据电文有关的[签字][数据];

"(c) "可靠的电子签字"系指如下电子签字

"㈠ 第 4 条规定的数字签字，并符合第 5 条规定的条件; 或

"㈡ 截至进行该签字之时，可另行利用安全程序证实确系某一特定个人的签字，这种程序: 唯独与其使用者相关联;能够立即、自动而客观地鉴别该人; 系以其使用者全权控制的方式或手段生成;并与相关的数据电文相联系,一旦电文被更改，电子签字即告无效; 或

"㈢ [对于正常业务过程中涉及数据电文生成、发送、接收、储存或以其他方式处理的当事各方之间而言]，是经当事各方先前商定的，在实际情况下是商业上合理的，并且经由当事各方正确使用。"

一般性评论

28. 据指出，第 1 条草案所载的规定，其用意不仅是作为定义，也是作为界定统一规则范围的一种手段。虽然据指出《示范法》也采用了同样起草方法，但人们一般认为，工作组在审议统一规则范围时，可能需要重新查看第 1 条草案。

(a)项

29. 会议普遍认为，(a)项应予删除。虽然在统一规则中列入以《示范法》第 7 条为基础的"签字"定义对目前无"签字"定义的国家可提供有益的指导，但据指出，统一规则不必有这样的定义。支持删除者提出的一条理由是，列入一条关于"签字"的包罗万象的定义对于(a)项所载规定可能与本国现有定义发生冲突的国家来说，还可能影响文书的可接受性。

(b)项

30. 会议普遍认为，(b)项的措词应借鉴《示范法》第7条的案文。为此，或可在(b)项中全文转载该条，或可通过提及“《示范法》第7条规定的条件”。经讨论，工作组认为后一措词更为可取。作为行文上的一个问题，人们一般认为应使用“数据”一词，而不是“签字”一词。

(c)项：一般性评论

31. 据认为，将电子签字限定为“可靠的”也许不妥。某项技术是否“可靠”并非定义问题，而是应参照所用技术的具体情况加以确定的事实问题。使用“可靠的”一词受到批评的另一理由是，该词提出的是一项主观标准，而且暗指此类范围之外的签字有着固有的不可靠性。对此，据答复指出，虽然可能需要以更好的措词替代关于“可靠的”签字这一词语，但在统一规则中，这一词语的使用只是作为一种手段限定某类特定质量的电子签字，因为这种特定质量，这些电子签字可附带特定的法律效力。至于使用“可靠的”一词是否会确立一种主观的标准，据指出，认证技术并不是在真空中发展的。将会有通过条例或通过自愿的本行业惯例而实施的标准来评估任何特定技术的可靠程度。经讨论，工作组决定在如下设想基础上进一步审议：使用某一类别(暂时称作“可靠的”)来指称统一规则将使其具有某些法律效力的一系列技术。

32. 据认为，对于五花八门的认证技术赋以同样的法律效力是不适宜的，因为据说其中既有具有固有可靠性的(例如数字签字)，也有具有固有的不可靠性的认证技术(例如当事各方可能商定的某些认证技术)。对此，据答复指出，(c)项正是为了确立可放在与其他技术同等地位上的最可靠的一类数字签字，但这些其他技术必须符合(c)㈡项规定的严格标准。关于(c)㈢项，可考虑将其列入关于当事方自主权的另一条规定中。会议一致认为，在审议完关于这些定义的法律效力的条文之后，可能还需要重新讨论这些定义。

(c)㈠项

33. 据认为，(c)㈠项的实质内容基本上可以接受。但有人认为，(c)㈠项提及的第5条草案的要求并不充分确保数字签字的质量同可靠电子签字一样。据建议，需要在审议第5条草案时再次讨论这个问题。

(c)㈡项

34. 有人表示关切说，(c)㈡项下的举证责任要求太高，以致第2(1)条草案的推定对使用非数字式电子签字的情况几乎毫无意义。据答复指出，(c)㈡项和第2条草案是为了达到不同的目的。但人们一般认为，在将由秘书处编拟的统一规则修订草案中，可能需要对(c)㈡项与第2条草案之间的关系加以澄清。

35. 人们普遍认为，(c)㈡项的实质内容对保证统一规则不偏重任何媒体至关重要。据认为，由于(c)㈡项的目的是规定某项技术应达到的某些标准从而适用第2条草案载列的推定，所以该技术的使用是否带有签字的意图并不重要。因此，已建议删去“可另行

证实确系某一特定个人的签字”一语。

36. 对(c)㈡项的具体措词还提出了其他建议。一项建议是，“立即”和“自动”等语应予删除。据指出，“立即”和“自动”鉴别某人并非大多数认证技术(包括某些数字签字技术)使用过程中所固有的现象，而且这与认证程序的可靠性和经电子签字后的数据的完整性并无明显关系。另一项建议是，“安全程序”一语，可以“或若干安全程序并用”一语作为补充。经讨论，这些建议获得工作组的通过。

(b)㈢项

37. 有人提出删去㈢项。据指出，将“可靠的电子签字”的地位给予任何可能由当事各方商定的程序，可能会造成使用任何可靠程度低的程序来产生法律效率的危险。关于这个问题表示了这样的看法：目前唯一“可靠的”认证方法是数字签字方法。对此有人提出，作为一个订约自由的问题，当事各方应当自由地商定，它们之间可以依靠一种较之于(c)㈡项中说明的那种电子签字的可靠程度低的认证方法；它们还可以对使用这种认证方法附加第2条草案所阐明的推定。另据认为，签字方法的“商业上的合理性”的提法意在提供一种保障，以免借当事方自主权无限制地承认可能不可靠的认证方法。然而，对于依靠“商业上的合理性”概念来提供这种保障，有人提出应当慎重。在一些国家中，仅仅凭“商业上的”当事方已商定某种程序这一事实，就足以将此种程序解释为“商业上合理的”。作为一个起草问题，有人对使用“商业上合理的”一词与《示范法》第7条中所使用的措词之间可能不一致提出疑问。虽然工作组回顾，在《贸易法委员会国际贷记划拨示范法》第5条中使用了“商业上合理的”一词，但工作组认为或许有必要适当改写一下，以避免作出上述解释。有人提出，或许有必要在(c)㈢中提到由当事各方明文规定所商定的方法将根据第2条草案具有可靠的电子签字的效力。会上还提出，应当保留(c)㈢项中的“各当事方之间”一词而不加方括号。

38. 对于当事方是否可援引(c)㈢项以偏离关于某些法律行为方式的强制性法律规则，人们提出了问题。据指出，这种解释是不能接受的，因为在以书面为基础的环境下并不存在此种订约自由。虽然普遍看法是，在有些国家的法律中，私人协定是不能偏离某些强制性形式要求的，但此种强制性形式的要求一般适用于范围极窄的几类交易，而对于这些交易，或许可以通过明文将其排除在有关当事方自主权的总则范围之外来解决。

39. 讨论的重点是，以何种方式在《统一规则》中述及当事方自主权。有人回顾，单是提到《示范法》中的第4条(经由协议的改动)可能不足以提供一种令人满意的解决办法，因为第4条确定了那些《示范法》中可以经由合同自由改动的条文与那些除非《示范法》以外的适用法律允许经由协议改动否则均应视为强制性的条文之间的区别。关于电子签字，鉴于“封闭的”网络的实际重要性，对当事方自主权给予广泛的承认是必要的。然而，可能还需考虑到对订约自由作出的公共政策限制，包括保护消费者不受范围过广的服从性合同的影响的法律。有人建议，《统一规则》应当按《示范法》第4(1)条的思路加入一条规定，其大意是：除《统一规则》或其他适用法律另有规定者，对电子

签字以及按某项协议当事各方商定的程序签发、接收或依靠的证书，可以给予该协定所具体说明的效力。另外还提出，工作组似应考虑确定这样一条解释规则，其大意是：在确定证书、电子签字或参照证书核证的数据电文是否就某一具体目的而言足以可靠时，涉及当事各方的一切有关协议、当事各方之间的任何行为方式，以及任何有关的贸易惯例均应考虑在内。

40. 作为一个备选办法，已请工作组审议拟议的新条款，案文如下：

"(1) 在法律要求某人签字的情况下，如系下列情形，则通过电子签字即符合这一要求：

"(a) 使用电子签字已由交易当事各方商定，或

"(b) 电子签字对于使用电子签字之目的适当而且可靠。

"(2) 在确定电子签字对于某一具体目的是否适当可靠时，应将当事各方的任何行为方式以及任何有关的贸易惯例均考虑在内。

41. 在拟议的新条款的基础上，讨论继续进行。据指出，拟议的案文旨在确立并扩大《示范法》第7条所依循的办法。有人特别指出：第(1)(a)款旨在使当事各方能够确定它们希望在其商业交易中使用的电子签字的类型；第(1)(a)款是受到《示范法》第7(1)(b)条的启发；第(2)款则试图对第(1)(b)款做出解释。有人认为，如果把拟议的新条款纳入《统一规则》中，则《统一规则》第2条草案第(2)款便无必要而可予删去。

42. 对这项建议普遍表示反对，根据是，这项建议在几个方面显然与《示范法》第7条相悖，其中包括：它未能纳入识别身份和核准的要素，因此，对签字的指称，按《示范法》来看并非签字；它允许当事各方偏离与签字有关的强制性法律规则，从而推翻了按《示范法》第7(2)条可确定对签字的义务或在无签字时确定法律后果的规则；它未能按《示范法》第7(3)条的思路列入一条规定，该条允许各国在某些情形下(如可转让票据)排除第7条的适用。

43. 普遍认为，拟议的新条款的主要不利之处在于，它与《示范法》第7条不同，而且与书面环境下适用的规则相抵触的是，它允许当事各方偏离强制性法律规则。因此，拟议的新条款会无意导致破坏《示范法》以及与签字有关的国内法，不适当地影响到第三方的权利。另外，对下述观点普遍表示支持：拟议的新条款不必要地重复了《统一规则》第1条草案中载列的内容。

44. 为了使拟议的新条款与《示范法》第7条相一致并解决上述各种缺陷，提出了一些建议。一项建议是，提到签字的基本特点，即那些与识别某人身份和核准电文内容有关的特点，办法是，在拟议新条款的第(1)款开头语的结尾处加入下述用语："系该人的签字和"。另一项建议将适用法律置于优先地位，在第(1)(a)款的开头加入下述用语："在不违反有关法律规定的情况下"。还有一项建议是，按《示范法》第7条，应当用"和"而不是用"或"来连接(a)项和(b)项。还有人提出，对于新条款第(2)款所说明的考虑到当事各方的行为和有关的贸易惯例，应当是允许这样做，而不是规定必须这样做，把"应"字改为"可"字即可。另一项建议是，应当在拟议的新条款中引入《示范法》第7(2)和(3)条的基本要素。

45. 下述观点为人们普遍同意：工作组不应重新起草拟议的新条款，而应设法就《统一规则》应在多大程度上顾及当事方自主权的问题确定基本原则。普遍意见是，《统一规则》通常不应把当事方自主权限制在当事方之间。人们还同意，工作组的努力应当着眼于确定哪些种类的交易(以及在数字签字情形下，哪些种类的证书)意味着可靠程度高，为此按有些国家的现行法律可能需受强制性规则的约束。关于有可能干涉当事方自主权的法律形式要求，普遍看法是，不妨在目的是提供证据(而这种证据可能需受当事方自主权的限制)的签字要求与那些为了有效性目的而规定的形式要求(一般来说这是强制性的)之间加以区别，或许有所帮助。

46. 经过讨论，工作组决定请秘书处编写第 1 条订正草案，其中应反映出上述审议和决定。

第 2 条. 推定

47. 工作组审议的第 2 条草案案文如下：

“(1) 关于利用可靠电子签字认证的数据电文，有人以反证推定：

“(a) 数据电文自签署可靠的电子签字以来未更改；

“(b) 可靠的电子签字是与之相关的人的签字；以及

“(c) 可靠的电子签字是该人为签署数据电文而签署的。

“(2) 关于利用电子签字，而不是可靠电子签字手段认证的数据电文，这些规则中的任何规定均不影响有关数据电文或电子签字可靠性和完整性举证责任的现行法律规则或举证规则。

“(3) 本条中的各项规定不适用于如下各项：[…]。

“[(4) 可通过如下各种证据对第(1)款中的推定进行反驳：

“(a) 证明由于技术进步、实施安全程序的方法或其他原因，用于证实电子签字的安全程序不被公认为可信的；

“(b) 证明各当事方间根据第 1(c)㈢条商定的安全程序未以可信的方式实施；或

“(c) 依赖当事方知道与表明依赖安全程序有关的事实的证据不合理。各当事方根据第 1(c)㈢条商定的安全程序在商业上的合理性，要根据各当事方在商定采用安全程序时此种程序的目的和商业境况来确定，其中包括交易的性质、各当事方的复杂程度、一方或双方进行的类似交易的数量、向一方提供的，但被该方拒绝的替代方法利用率、替代程序的费用以及类似交易中通用的程序。]”

48. 虽然认为应当在《统一规则》中反映出媒体中性的原则，办法是承认对借助于非数字方法使用电子签字所附加的法律效力，但工作组还是决定暂停对第 2 条草案的审议，直到工作组完成对《统一规则》其余条款草案的审查。

第 3 条. 归属

49. 工作组审议的第 3 条草案案文如下:

"(1) 备选条文 A 根据[《贸易法委员会电子商业示范法》第 13 条], 附有发端人可靠电子签字的数据电文发端人[受电文内容的约束][被视为电文签字人]; 如同电文按照适用于电文内容的法律[手工]签署的方式存在时一样。

备选条文 B 就私人钥匙持有人与依赖使用经核证的相配公用钥匙可以[证实][认证]数字签字的任何第三方之间而言, 数字签字[被推定为持有人的签字][符合[《贸易法委员会电子商业示范法》第 7(1)条]提出的条件].

"(2) 第(1)款不适用于如下情况:

"(a) [发端人][持有人]能够证实, [可靠电子签字][私人钥匙]未经授权被使用, 而且证实[发端人][持有人]虽采取了合理审慎的做法, 却未能避免此种使用; 或

"(b) 依赖当事方如果已向[发端人][验证局]那里了解到情况, 或另行采取了合理审慎的做法, 就会知道或应当知道, [可靠的电子][数字]签字不是[发端人][私人钥匙持有人]的签字。"

一般性评论

50. 工作组首先审议了第 3 条草案的宗旨和范围及其与《示范法》第 7 和 13 条的关系。

51. 对于本条草案是否仅应论述可靠电子签字(或数字签字)的归属, 还是也应述及名义签字人对依赖当事方的赔偿责任问题, 与会者发表了不同的意见。一种观点是, 第 3 条草案应旨在将签字与名义签字人联系起来和确保数据电文的完整性。另一种观点是, 第 3 条草案的主要目的应是鼓励使用数字签字, 对名义签字人未采取合理审慎做法以避免其签字被擅自使用而使依赖当事方遭受损失的赔偿责任加以适当的划分(见下文第 58 段)。普遍看法是两个问题都应述及。在这方面, 有人提请注意对赔偿责任问题须审慎处理, 因为论述该问题可能与《示范法》遵循的做法不符, 根据该示范法, 合同事项由示范法以外的适用法律处理。对此有人指出, 统一规则根据的是一种有所不同的做法, 其中已经论及了验证局的责任。经讨论, 工作组同意考虑论及这两个问题, 也许可分为两款条文(见下文第 55 和 60 段)。

52. 关于第 3 条草案的范围, 据认为, 应局限于数字签字, 所以第 3 条草案应相应地改换顺序。支持这种观点者指出, 数字签字众所周知, 广为应用, 所以值得给予优先。另据指出, 数字签字的归属问题至关重要, 需要与其他类型的电子签字的归属问题分别处理。另一种观点是, 第 3 条草案制定的规则应同时适用于数字签字和其他电子签字。普遍意见是, 第 3 条草案阐述的问题, 在用词上应尽可能使用不针对特定技术手段的中

性词语，以便包括广泛的各种电子签字。

53. 关于第 3 条草案与《示范法》第 7 和 13 条之间的关系，据指出，第 7 条论述的是签字的要求，第 13 条论述的是电文的归属。有人关切地表示，第 3 条草案可能不过是重述了示范法第 13 条的规定而已。对此有人答复说，第 3 条草案论述的是有别于数据电文归属的电子签字归属问题，在发生名义签字人签字被擅自使用和即使他采取了合理审慎做法也无法避免这种擅自使用的情况时，向名义签字人提供保护。

第(1)款

54. 两种备选条文都得到了支持。赞同备选条文 A 者指出，其措词采用了媒体中性做法，因此适用于国际贸易中使用的各种技术。在这方面，据指出，对某种特定技术的应用方法也应确保中性(例如数字签字，无论有无证书)。据指出，要做到这种应用上的中性处理，这就是通过制订一项一般规则，规定合理依赖可靠电子签字的数据电文收件人有权将该电文视为名义签字人的电文(见 A/CN.9/WG.IV/WP.73，第 35-36 段)。支持备选条文 B 者指出，其重点适当放在数字签字上，与其他种类的电子签字相比，数字签字众所周知，使用广泛。

55. 但是，备选条文 A 和 B 都因为将两个不同问题，即归属问题和责任问题，混为一谈而受到批评。另外，与会者还对这两个备选条文表示了一些关切和发表了意见。关于备选条文 A，据指出：起句的措词不够明确；使用“发端人”一词不妥，原因有几条，其中包括数据电文的签字人不一定必须是其发端人；“受……内容的约束”等词语关系到义务的一般法则，而并非仅仅关系到电子签字对名义签字人的归属问题；提及适用法律应指适用于整个数据电文而不只是适用于其内容的法律。

56. 关于备选条文 B，据指出：为了避免否定统一规则中例如关于失密的私人钥匙的其他条款所列出的例外情况，备选条文 B 的句首应增加内容大致如下的文字：“根据第……和……条的规定”；按照《示范法》第 13 条的做法，应提及对授权使用数字签字作实际核证，而不是仅提及私人钥匙持有人对这种使用加以核证的能力；为避免即使证书已被废止但数字签字仍可被归属于名义签字人的情形，应采用内容大致如下的文字：“有效证书中所含的私人钥匙”；不应提及《示范法》第 7 条，因为该条论述的是签字的要求，而不是签字的归属问题。

第(2)款

57. 虽然工作组一致认为第(2)款总的来说是可以接受的，但有人关切地表示使用“合理审慎”一词可能会引起不确定性。为了处理这一关切，提出了一些建议。一项建议是，如果名义签字人不能证明该签字是被擅自使用的，则该签名应归属该名义签字人。另一项建议是，如果名义签字人此外还不能证明他不能避免擅自使用，则该签字应视作为该名义签字人的签字，而不必提及任何关于“合理审慎”的概念。这两项建议都遭到反对，理由是它们将不适当地增加名义签字人的责任。

关于新的第3款的建议

58. 为了处理对第3条草案所表示的关切并假设可靠电子签字的归属问题已经在《统一规则》的第2条草案中得到了充分的处理，有人建议第三条草案的重点应当转移到名义签字人的赔偿责任问题上来，因而第3条应当大致如下:

"(1) 就私人钥匙持有人与依赖数字签字的任何人之间而言，该持有人不受未经其签字的电文的约束。

"(2) 如果钥匙持有人未采取合理审慎的做法来防止依赖当事方依赖数字签字的擅自使用，他有责任赔偿依赖当事方所受到的损害。依赖当事方只有在他曾向验证局了解过情况或另行采取了合理审慎的做法以查明该电子签字并非该持有人的签字时，才有权获得这种赔偿。"

59. 虽然普遍认为所提议的文字正确地区分了签字的归属和擅自使用签字所造成的损害的责任(或赔偿责任)，但据指出它并未充分处理对变式A和B提出的关切。此外，据指出，它将举证责任转移到了依赖当事方，使之不得不证明他采取了合理审慎的做法来证明该签字是名义签字人的签字。与会者普遍认为最好是采取一种媒体中性做法，而且归属和责任性问题应当分别处理。

60. 为了反映这一做法，有人请工作组审议文字大致如下的一个替代案文:

"可靠电子签字的归属

"就名义签字人与依赖当事方而言，该名义签字人的签字视为可靠电子签字，除非该名义签字人能够证明该可靠电子签字被擅自使用。

"可靠电子签字的赔偿责任

"如果可靠电子签字被擅自使用而名义签字人并未采取合理审慎的做法来防止收件人依赖这样的电文，名义签字人应负责支付赔偿金赔偿依赖当事方所受到的损害，除非该依赖当事方未曾向某一有关第三方索取信息或者他通过其他方式知道或应当知道该签字并非名义签字人的签字。"

61. 经讨论，工作组请秘书处在《统一规则》修订草案中反映这些拟议的备选案文，供工作组今后一届会议进一步审议。一些代表团对拟议案文与其国内法之间可能互相干扰表示担心。

第二节. 数字签字

第4条. 定义

62. 工作组审议的第4条草案案文如下:

"为了上述规则的目的，

"备选条文A '数字签字'系指一种电子签字，由利用电文摘要功能和非对称加密系统变换数据电文组成，以使掌握初始未变换数据电文

和签字人公用钥匙的任何人都能准确地断定:

"(a) 该变换是否是使用与签字人公用钥匙相配的签字人私人钥匙生成的; 和

"(b) 实施变换后, 初始电文是否改动过。

"备选条文 B "(a) '数字签字'系指一数值, 它签署在数据电文上, 而且使用同发端人私人加密钥匙有联系的一个已知数学步骤, 使得可以断定这一数值是唯一靠发端人的私人钥匙获得的;

"(b) 用于生成本规则规定的数字签字的数学步骤是以公用钥匙加密方法为基础的。在应用于数据电文时, 这些数学步骤使电文发生变换, 使掌握初始电文和发端人公用钥匙的一个人能够准确地断定:

"(1) 该变换是否是使用与发端人公用钥匙相配的私人钥匙操作的; 和

"(2) 实施变换后, 初始电文是否改动过。"

63. 虽然备选条文 A 和 B 都受到了一些支持, 但这两个条文都没有为工作组所通过。

64. 支持备选条文 A 者说, 就备选条文 A 着重的是电子签字的产生而不提及任何特定技术而言, 它有充分的灵活性来包括各种不同类型的数字签字。然而, 有人关切地表示, 备选条文 A 没有认识到执行公用钥匙基础结构的不同方式(例如依靠或不依靠电文摘要功能)和通过使用电子签字得到执行的不同功能(例如确定签字人的功能("可靠签字"), 确定数据电文完整性的功能("可靠记录")或这两个功能的结合)。在讨论中提出, 为了确保跨国承认数据签字和证书的各种不同类型, 工作组应当考虑拟定一项公约而不是在示范法中增添某些规定的设想(见下文第 212 段)。

65. 针对上述关切, 有人指出, 在关于"数字签字"的定义中列入鉴定签字人和核证数据完整性的要素是一种公认的做法。此外, 有人指出, 此种旨在确定在功能上等同于书面签字的做法是与示范法所采取的做法相一致的。再者, 有人说, 要处理数字签字的所有类型可能要求过高, 将会推迟在迫切需要订立条例以避免因在国家立法中采用不同的做法而造成法律不协调这一领域取得进展。对此, 有人指出, 既然变式 A 将数字签字界定为一种电子签字, 则该词只限于指那些意在功能上等同于书面签字的公共钥匙加密应用, 而变式 B 的涉面广泛, 足以涵盖各种形式的数字签字技术, 包括那些目的不是起签字的等同功能的形式。

66. 赞同备选条文 B 的人指出, 就这一条文的范围而言, 它具有较大的确定性, 因为它使用了更多的技术用语并具体提到了公用钥匙加密方法, 据说这构成了一种普遍使用的技术。与此同时, 有人关切地表示备选条文 B 局限性太大, 因为它依赖某一数学程序来产生数字签字, 因而有可能排除今后也许会使目前采用的程序变得过时的技术发展。有人提议可能需要在该规定草案中提及"最新水平的数学程序"。

67. 备选条文 A 和 B 遭到反对的原因是这两款条文都不妥当地通过提及"数据电

文的变换”来定义“数字签字”。有人解释说，通过使用一种算法来处理电文后所改变的不是整个电文而仅仅是其数字表示形式。为了处理这个问题，有人提议采用大致如下的文字:

“数字签字是(使用非对称密码技术)对数据电文数字表示形式的加密变换，以使具有该数据电文和有关公用钥匙的任何人能够确定:

68. 支持该拟议条文者说，由于没有提及签字人的私人钥匙，它处理了确保用于确定签字人之外的其他目的的数字签字将为本统一规则所涉及这一必要性。另据指出，由于没有提及电文摘要功能，上述拟议条文将涵盖通过不同程序产生的数字签字。

69. 讨论期间有人提议，仅为比较目的，工作组应当考虑通过一个技术定义，其文字可以沿用国际标准化组织(标准化组织)1988 年通过的如下一条案文: “数据电文: 一数据单位的附属数据或加密转换，以使该数据单位的收件人能够证明该数据单位的来源和完整性和防止收件人等伪造”(ISO 7498/2)。另一建议认为，应将标准化组织的定义纳入统一规则。虽然与会者同意标准化组织的定义表示了一种技术方法，但工作组中普遍怀疑这项定义对统一规则来说是否适宜。

70. 经讨论，工作组普遍认为在它审查完统一规则的实质性条款和对这些条款的范围做出结论之前应当保留对“数字签字”的定义作出决定。具体地说，“数字签字”的定义也许会取决于统一规则是否仅仅涉及以在电子环境中重复国际贸易交易中传统上通过使用书面签字而履行的职能为目的的计算机技术的使用，还是统一规则的范围可以扩大到包括“数字签字”的其他用途。会议请秘书处根据上述提议(见上文第 6 段)并考虑到所发表的意见，以备选条文 A 和 B 为基础编写替代草案，供工作组今后某一届会议进一步审议这个事项。

第 5 条. 效力

71. 工作组审议的第 5 条草案案文如下:

“(1) 在以下情况下，如果全部数据电文或其任何部分是以数字签字签署的，则就此部分电文而言，该数字签字被视为可靠电子签字:

“(a) 数字签字是在[有效]证书发生效力期内生成的，并依据证书所列公用钥匙得到证实; 和

“(b) 证书被视为对一个人身份的公用钥匙完全具有约束力，

因为:

“㈠ 证书是由持有许可证[被认可]的验证局签发的[立法国规定主管发给验证局许可证并颁布持有许可证的验证局操作条例的机关或机构]; 或

“㈡ 证书是由验证局根据[立法国规定主管对持有许可证的验证局发布公认操作标准的机关或机构]发布的标准另行签发的。

“(2) 在数据电文全部或任何部分是以不符合第(1)款要求的数字签字签署的

情况下，如果有充分证据证明，证书对持有人身份的公用钥匙具有约束力，则就此部分电文而言，该数字签字应被视为可靠电子签字。

“(3)本条中的各项规定不适用于以下情况：[……]。”

一般性评论

72. 与会者一开始便普遍承认，将需要根据对统一规则范围作出的决定而由工作组对第5条草案的实质内容作进一步的讨论。特别是，第5条草案将直接取决于统一规则将来是否会使用“可靠电子签字”这一概念。对于数字签字，使用证书后所附带产生的法律效力还将取决于第8条草案对“证书”的定义。如果统一规则仅仅涉及国际贸易交易中使用数字签字的用意是为了签署(即指明签字人并将签字人与所签署的资料联系起来)这种情况，那么将证书的功能局限于把一对钥匙与一个人的身份联系在一起是可以令人接受的。在这种情况下，应指明统一规则只涉及一种特别的证书(“身份证书”)，特别是因为电子商务中还可能使用其他类型的证书，例如，为了确定一个人的受权级别(“授权证书”)。有人表示，第5条应同时包括身份证书和授权证书。在讨论这个问题时有人建议，第5条草案应提及核证数据电文所载资料完整性的证书。对此有人答复说，虽然核证数据的完整性是电子签字过程中使用证书的一个重要结果，但它并非证书本身的一个特征要素。

73. 经讨论，工作组决定继续审议第5条草案。但是，普遍认为在工作组完成其对统一规则实质性条文的审查之后，还需要重新开展对本条的讨论。

标题

74. 普遍所持的看法是，第5条草案的标题说明性不够，可能引起误解。会议决定标题应改为大致如下：“附带证书的数字签字”。

第(1)款

起首句

75. 与会者对这样的观点表示支持，即第5条草案中不必提及“可靠电子签字”的概念，应改成提及示范法第7条载明的各项条件。对此有人答复说，这样提及示范法第7条会不适当地限制第5条草案的范围，预先假定存在着对签字的法律要求，并需要在电子环境中加以满足。第5条草案的目的更广，直接旨在提供数字签字法律效力的确定性，无论是否存在对签字的特别要求，只要符合某些技术标准即可。

76. 经讨论，工作组决定，应保留提及“可靠电子签字”和提及示范法第7条所载条件的词语，作为工作组今后会议进一步审议的备选措词。第5条草案的起首句应大致如下：“在以下情况下，对于全部数据电文或其任何部分，如由数字签字确定了发端人，则该数字签字[是可靠的电子签字][满足了贸易法委员会电子商业示范法第7条规定的条件]：”。

(a)项

77. (a)项的实质性内容被认为基本上可以接受。为了更好地反映数字签字程序的必要可信度，会议决定应添加“可靠地”一词，修饰数字签字的生成和依据证书所列公用钥匙对数字签字的核证。会议还决定，条文草案中关于证书有效性的词语应予保留，但去掉方括号。

(b)项

78. 关于(b)㈠项，与会者普遍认为，在一项处理国家将对公用钥匙基础设施采用条例办法的条文中，“持有许可证”或“已登记的”这样的用词比“被…认可”更可取。关于(b)㈡项，据认为应当删去这一条文，因为第5条草案的范围应当限于使用由持有立法国许可证的验证局签发的证书。然而，普遍看法是，还是应当提及行业标准和从业人员为确保此种标准的可靠性而制定的机制。会议普遍认为，这种提法对于反映工作组上届会议上对数字签字和公用钥匙基础设施所采取的“双重办法”是必要的。按照这种办法，以行业为基础的标准将随政府条例一道得到承认。据指出，在有些国家，政府当局可能不希望参与数字签字安全标准的制定。对此有人指出，第5条草案不仅应当提到“安全标准”，而且应当更为广泛地把行业可能制定的各类标准包括进去。

79. 关于提及公认的行业标准问题，有人提出，不妨参照联合国国际货物销售合同公约第9(2)条的措词，其中提到“…双方当事人已知道或理应知道的惯例，而这种惯例，在国际贸易上，已为有关特定贸易所涉同类合同的当事人所广泛知道并为他们所经常遵守”。然而，普遍认为，“商业上适宜且国际公认的标准”这样的提法更为妥当。

80. 考虑到上述讨论，会议同意按下述措词改写(b)项供今后讨论:

“(b) 证书因下述情况而使公用钥匙受某人身份的约束:

㈠ 证书是由持有许可证的验证局签发的[立法国规定主管发给验证局许可证并颁布持有许可证的验证局操作条例的机关或机构]; 或

㈡ 证书是由经负责的认可机构适用商业上适宜且国际上公认的标准而认可的验证局签发，这些标准应包括验证局的技术的可信性、做法以及其他有关的特点。[立法国规定主管颁布持有许可证的验证局的公认操作标准的机关或机构] …可公布与本款相符的机构或标准的非专属性一览表;或

㈢ 证书是根据商业上适宜且国际公认的标准另行签发的。”

第(2)款

81. 与会者对(2)款表示了一些关切。一种关切是，鉴于有第2条草案，第(2)款可能是多余的，后者阐明了对于“可靠电子签字”的地位所附加的法律假设。对此有人指出，第(2)款对于在数字签字与统一规则的其他规定(如关于“可靠电子签字的赔偿责任”的第3条草案）之间建立联系是必要的，这是因为，这种数字签字虽然未正式满足第(1)款所载的要求，但仍然有可能被(法院等)承认使公用钥匙受持有人的约束。对此有人认

为，不妨在第3条草案中加入“虽有第5条的规定”这样的措词。

82. 另一项关切是，第(2)款为承认未在其他方面满足第(1)款所规定的要求的数字签字确定了过低的标准。按现在的措词，第(2)款可能导致把“可靠”地位给予那些借助于不可靠程序的数字签字，钥匙长度不足即为此种不可靠程序的一例。对此有人指出，固然可能有必要在第5条草案或在“可靠电子签字”的定义中补充提及技术程序的可信性，但按第(2)款的措词订立一条规定对于保留下述可能性是必要的：允许当事各方在法院或在仲裁庭上证明，他们所使用的数字签字是可靠的，即便是在第(1)款范围之外使用，仍足以获得法律效力。然而，有人表示关切，认为根据第2和3条草案，给予“可靠的”地位制造了推定情况，从而转移了侵权行为的责任。据说，在使用签字前提及而不是在后期由一法院对无怀疑的当事方规定明确的规则和标准，此种严重后果应是可以明确的。

83. 对于如何提及第(2)款中载明的一般证据规则，提出了各种意见。一种观点是，第(2)款的范围应当更广，不仅包括使用证书的情形，而且还包括使用数字签字或任何其他电子签字的任何其他情形。按照这种意见，应当把提及“证书”的文字从第(2)款中删去，移到涉及一般电子签字的章节中。另一种观点是，第(2)款的范围应当更窄一些，而且只有当数字签字是在证书的有效期内产生时才能适用这条规定。按这一观点，第(2)款中载明的规则应当按下述措词成为第(1)(b)款的一部分：

“㈣ 充分证据表明，证书准确地使公用钥匙受持有人身份的约束。”

84. 经讨论，工作组未就第(2)款中载列的规定的范围和位置达成协商一致的意见。工作组请秘书处编写一项订正规定草案，列出反映第(2)款讨论情况的备选条文，供工作组今后某一届会议审议。

第6条. 法人的签字

85. 工作组审议的第6条草案案文如下：

“[法人通过在电文上注明证实该法人的加密公用钥匙，就可鉴别数据电文。如果电文也是由授权代表该法人行事的自然人以数字签字签署的，则该法人只能被认为是电文的[发端人][核准了]电文的[发送]。”

86. 有人回顾在工作组上一届会议上普遍认为应当删去第6条草案。把它放在方括号内是为了提醒工作组注意，工作组或许有必要更为充分地讨论一下，统一规则应在多大程度上确认“电子代理人”为自动认证数据电文所进行的活动。工作组决定，需在稍后阶段讨论“电子代理人”的问题。但决定删去第6条草案，因为该条会被看作是不适当地干预其他法律体系（如代理法和涉及自然人代表公司的公司法规定）。

第三节. 其他电子签字

87. 普遍同意，在就有关“签字”和“可靠的电子签字”的定义中包含的(和通过

对符合条件可称作“可靠的电子签字”的任何认证技术承认的法律地位体现的)非歧视原则是否也应以处理非数字签字认证技术的更具体的条款来表述这一问题作出决定前，第三节应保留在统一规则中。

88. 为了向工作组提供更多的关于数字签字和各种其他认证技术如何运作的情况，作了若干技术性专题介绍。现将这些专题介绍概述如下(第…段至…段)。

89. 有人回顾指出，可靠的电子商务要求，交易当事方应有能力彼此认证。在许多电子交易的情况中(如在因特网上购物)，传统的认证方法不是无有就是不可靠。此种电子认证可靠方法的需要已超出了商务要求而扩展到数字世界的几乎每种交易。

90. 据指出，为满足这些需要，目前可有大量的解决办法。这些解决办法既有技术因素，也有方法因素。虽然着眼点大都往往放在不同的技术方法上，但不应低估电子认证解决办法所基于的方法或商业模式的作用。除了许多不同的技术方法以外，市场也已提供了多种实施这些技术的方法。此种解决方法的多样性反映了在数字环境下提出的许多不同解决办法所要求的不同类型认证。随着这一环境的发展，将需要新的认证解决办法。

91. 认证方法可依对认证的特征的着眼点来分类。有人把三个基本特征类型概述为：(1)“你知道的事物”；(2)“你的身份”；(3)“你所拥有的物”。许多解决办法综合使用这三种特征。

92. 第一类(“你知道的事物”)是认证某些个人最常用的特征之一。密令、密令短语和个人身份号码属于这一类。大多数计算机系统向拥有有效密令的人提供密令选择办法，使之可检索资料。例如，自动检索银行帐户信息要求用户知道与检索的帐户有关的正确类别。另一种该类认证依据只有某一具体人可能才知道的个人情况。例如，在某些法域，在有人建立银行帐户时，银行通常要求提供开立帐户人母亲的婚前姓氏。以后可利用此一资料认证帐户持有人。虽然目前广泛利用此类认证方法，但它有许多弱点。第一，通常要求相互知道的情况不是秘密的，就是难于得到的。第二，要求当事方有事先存在的关系，彼此可“共享”相互知道的秘密内容(如，密令、个人身份号码或母亲的婚前姓氏)。

93. 第二类认证方法(“你的身份”)，常常被称为生物统计学。这一方法利用个人的天生特性作认证。在生物统计学中使用的某些天生特性包括：指纹、视网膜、虹膜、手印、声纹和手写签字。因为所有这些特性每个人都是独特不一样的，所以它们是一种绝妙的认证方法。如果可将关于这些特性的信息公诸于众，此种认证便不需要有事先存在的关系。此外，这些方法往往可提供有力的认证方法，因为操纵或篡改作假是非常困难的。这些方法的一个不足之处是实施起来代价较高，因为这些方法需要某种硬件用来获取有关特征的信息。关于此类某些应用的另一问题是用于收集生物统计学信息资料的装置。在某些情况下，此种装置被认为是强人之难(例如，视网膜扫描器要求使用者把眼睛贴到一个目镜上(利用红光对视网膜扫描)。在其他情况下，认证扫描取得的信息可泄漏个人不愿公诸于众的个人健康信息资料(例如，从虹膜异常可诊断某些健康状况，因此，虽然虹膜扫描在身体上不是那么强人之难，但某些人认为是对人身进行侵犯)。

最后，如果使用状况“反常”(如手指上有伤口裂口的指纹)，某些此类装置便不总是可靠的。然而，生物统计学解决办法仍广泛被认为是最有力的认证方法之一，当前正被用于实践。有人举出某国的例子，该国移民归化机构正测试手印技术方法以加速护照控制，还举出一些保险公司的例子，一些保险公司正利用签字生物统计学在索赔受理过程中对个人进行认证。)

94. 第三类认证方法（“你所拥有的物”）被认为是在电子认证中最活跃领域之一。这个“物”可是有形的（如问答器），或可是一种信息（如密钥）。问答器类似于只在硬件中实施的“你知道的事物“类中使用的共享密秘方法。这一方法要求给予有关个人一个独特而且只供该个人使用的装置。如果某人试图利用一种服务，主人系统便要求该人证明自己的身份（通常采用用户名称的方法），然后，该系统根据它拥有的关于已分配给该人的独特装置的信息，提出一数字询问。然后，被询问人将该数字键入作出数字答复的装置。然后，可将该数字回答键入装置持有者正想进入的系统。主人系统“知道”，对于它向该人提出的数字询问只有一种可接受的回答。因此，如果该人键入了适当的数字回答，主人系统便“知道”想进入系统的人便是该人所声称的人。该类装置常用于认证寻求远距离进入计算机系统的人。某一银行还用于称作“浏览联机定题检索银行业务”的一个家中办理银行业务试办项目，因为它可使个人从任何机器上的任何浏览器查阅银行帐户。这一应用显示了该方法的优点之一。虽然目前它的确要求一种硬件组件，但它不像芯片所要求的那样，要求一个系统改变。

95. 第三类的另一小类包括使用数字签字。数字签字技术的重要方面是利用一个人密钥以生成一数字签字，并使用一个人密钥认证该数字签字。用于生成数字签字的个人密钥可储存于一硬磁盘上或一智能卡上，使用人对之必须严加保密。公用钥匙被广泛传播。使用数字签字技术已有若干不同范例，每一范例都有一种对接收数字签字的人提供可信性的不同方法。

96. 第一类方法之一是建立一种个人和公用钥匙名录。根据这一模式，收到数字签字单证的人从受信赖的名录中查找公用钥匙以核查单证签署人的公用钥匙。据报，若干应用目前使用这一模式。

97. 源于基于名录方法的另一办法依靠利用数字证书。数字证书是经由一受信赖的实体数字签署的电子证书。当一单证经数字签署时，便附上一份签署人的数字证书。数字证书载有有关个人和个人公共钥匙的信息资料。当接收人收到电文和数字证书时，接收人使用数字证书中的公用钥匙对电文进行认证.

98. 数字证书的一种普通用法利用一种标准(ISO X.509)，可使利用一系列的受信赖的实体对当事方进行认证。这一方法往往称作信用卡模式，因为它反映了基于信用卡行业的商业模式。例如，一商人可能不了解一客户，但他愿意接受某种卡作为支付手段，因为他知道，该卡是由一银行(银行的名字往往写在卡上)发给顾客的，该银行受权由信用卡公司签发该卡。即使该商人不知道发卡银行，他也可相信该客户，因为他知道，该客户业经银行认证，而银行业经信用卡公司认证。同样，X.509 信用系统允许数字证书由可经证书接收人核查的一系列受信赖的实体(称作“证书当局”)认证。在这一信托树

的最后的证书当局称作根。因此，X.509 方法中的数字签署单证包括发送签署人数字证书和所有与被信赖的信托系列机构有关的辅助数字证书。在这一模式下，接收人可核查整个信托树而不必核查联机名录。这一方法被认为特别适于使彼此没有什么接触或以前没有接触的大多数人能相互进行信托通信。这一方法的优点之一，能够将许多证书同最后信托的根联系起来，也是其弱点之一。如果此根受到损害，根上面的一切便都不可靠了。

99. 使用数字证书的另一变化方式通常被称作信托网模式。在这种模式中，没有证书当局。数字证书由个人产生。没有信托根。个人决定信赖谁和信赖的程度。这一模式旨在供有经常接触的少量用户使用，但难于大规模实施。然而，这一模式目前正在许多环境下被使用。

100. 据说，理解 X.509 数字证书用法的一个重要考虑是对身份的历史偏爱。因为 X.509 标准源于 X.500 名录，自然它注重于把公共钥匙同个人的身份联系起来。据说，这种对身份的偏爱搞乱了许多关于数字签字用法的公共政策问题。虽然很明显，某些数字证书认证一个人的身份，但同样明显的是，其他数字证书有认证身份之外的作用。数字证书还可用来认证一个人的权利或关系而不必对该人的身份作任何说明。在许多情况下，个人身份是不必要的，甚至是不受欢迎的。有许多仅可用于某些职能的特殊用途证书，就像一个人信用卡不可用认证该人的身份和一个人的护照不可用于购物一样。从身份角度来考虑问题的倾向虽然合乎逻辑，但可严重限制这种技术的应用。如果使用数字签字的每一应用都需要满足严格的普通用途身份证的要求，那么，这种技术付诸使用便会非常困难和昂贵。重要的是要记住，可能有广泛一系列认证要求，而技术是足以可以灵活地满足所有这些要求的。

101. 当许多信用卡公司决定在像因特网这样的公共网络上开供电子商务使用的可靠方法时，它们确定了三个基本商业目标：解决方法必须是安全可靠的；解决方法必须是对一切希望开发符合界定议定书的产品的技术供应商都开放的；所有实施必须是可共同操作的。对支付行业来说，“安全可靠”具有下列三个要素：(1)支付信息的保密，包括客户的帐号；(2)订货信息的完整；(3)交易当事方的认证。为了提供必要水准的“安全”，定了“可靠电子交易”协议。该协议使用了数字签字(基于 X.509 模式)以起到使数据完整和对当事方认证的作用。

102. 对可靠电子交易协议作了简短说明。消费者如果决定使用可靠电子交易来进行可靠的电子商务，首先需要获得已通过可靠电子交易根基证书当局规定的达标程序的软件。这套软件生成一对钥匙和一项申请，由消费者发往签发准备使用的付款卡的实体。软件将公用钥匙放在证书申请中，并提示消费者提供鉴别资料，以便金融机构可以证实证书申请者是经授权这样做的。这项申请通过因特网发给金融机构。如果申请被接受，金融机构便在消费者的证书上进行数字签字，并通过因特网发还给消费者。消费者的软件将这一数字证书储存在消费者的计算机内。获得证书只需操作一次这一申请程序即可。

103. 消费者然后便开始在网上联机购物，并可使用符合可靠电子交易要求的软件开

始进行与供应商的可靠交易。在交易的初期阶段，消费者的软件请求供应商的认证资料。通过证实供应商发送的所有数字签字和数字证书，软件对供应商加以认证。如果在认证过程的任何一个环节出现失误，计算机便对消费者提出警告。然后消费者挑选将购买的货物或服务，选择付款方法，并开始交易。消费者软件将付款资料与订货资料区分开来。付款资料经严格的加密程序进行加密，从而只有供应商的金融机构才能对付款资料进行解密。订购资料中指明将要订购什么和交易的其他细节，这些资料与加密的付款资料经数字签字后发给供应商。当供应商收到这项电文时，便将加密的付款资料划分开来，对这项新的电文进行数字签字，然后发给其金融机构。金融机构将证实供应商的数字签字，对付款资料进行解密，然后提交付款资料通过现有的付款基础设施进行处理。金融机构对授权答复进行数字签字并发给供应商。然后供应商再将经过数字签字的答复发给消费者。如果交易获得授权，供货商便完成了订货单的要求。

104. 据指出，可靠电子交易可表明在对电文和当事方进行认证时对数字签字技术的依赖。但是，应当注意，可靠电子交易证书并非身份证，并不对任何人的身份加以认证，也不能用于此项功能，正如与证书相联系的政策声明中所明确指出的那样。可靠电子交易证书仅仅是认证一把公用钥匙对一个帐号的关系。可靠电子交易使用电子签字技术增加交易的安全性，但并不是鉴别某一个人。另外，对于消费者或供应商证书，可靠电子交易并不使用证书撤销单(“CRL”)。在可靠电子交易商业模式环境下，不需要这些清单。仍需要通过现有的付款基础设施对交易加以授权，所以增加一个持卡人证书撤销单并不带来任何益处，但对建设和维持系统来说，则增加了大量费用。

105. 据指出，“可靠电子交易”是为了表明：(1)数字签字和证书的非身份鉴别用途；(2)由无许可证的市场性验证当局签发证书；(3)在当事各方已通过协议确定了其权利和责任的系统中签发证书；(4)在有些情况下，依赖当事方(根据经由消费者电子签字的资料完成了付款的银行)可以是证书的签发者。“可靠电子交易”只不过是数字签字技术应用的一个实例。据指出，在今后的岁月里将会有其他许多用途，而且这些用途将以尚待出现的技术和商业模式为基础。

106. 工作组对所作的介绍表示赞赏。会议普遍认为，示范说明正在应用或考虑应用的技术有助于更好地理解《统一规则》中需要处理的法律问题。工作组希望在其今后的会议上可对数字签字和其他认证技术的发展动态进行进一步的专题介绍。

第三章. 验证当局及有关问题

第 7 条. 验证当局

107. 经工作组审议的第 7 条草案案文如下：

(1) 为了上述规则的目的，“验证当局”系指：

(a) 由……[立法国规定主管发给验证当局许可证并颁布持有许可证的验证当局运作条例的机关或机构]发给许可证[认可的]，根据这些规则行

事的任何人或实体，或

(b) 作为其正常业务的一部分，负责签发与数字签字用加密钥匙有关的证书的任何人或实体。

[(2) 验证当局可以提供或便利数据电文传递和接收的登记与时间标记，以及有关通过数字签字保证的通信的其他功能]。

第(1)款

108. 有人认为，第(1)款过多地强调了验证当局职能由独立第三方(常称“受托第三方)行使的情形，而这并不是可设想到的唯一的一种情形。据指出，在数字签字做法方面，当事方越来越多地依靠自我验证(或相互验证)制度，所涉及的仅为数字签字电文的发端人和收件人。因此，应当将“验证当局”的定义扩大到包括所有类型的做法。据建议，应以“在其营业过程中”一语取代第(2)款中“作为其正常业务的一部分”一语。人们认为这一建议一般可以接受。

109. 还有一项建议是，除“验证当局”的定义之外，工作组可能还需要解决“登记当局”的定义。虽然没有人支持这项建议，但会议一般认为这一问题可能需要在后一阶段进一步予以讨论。

110. 另一项建议是删去(a)项，因为该项仅仅针对(b)项所涉及的大类的一个子集。第(2)款中“作为其正常业务的一部分”一语应由“在其营业过程中”或“在其营运过程中”一语予以取代。支持这一建议者指出，在统一规则中对“持有许可证的验证当局”的任何提及都可能被解释为鼓励立法国确定许可证制度，而这同工作组在其上届会议上采用的“双重办法”可能是背道而驰的(见 A/CN.9/437，第 69 段)。另外还指出，删去(a)项可在保留必要的灵活性的同时恰到好处地将统一规则的重点放在为了国际贸易交易目的使用数字签字方面，而不是放在为行政管理目的使用数字签字。但普遍的意见却是应当保留(a)项的实质内容。据指出，在某些场合，持有许可证的验证当局可能并不经营“业务”。而且，由于持有许可证的验证当局不同于纯属私人经营业务的验证当局，有理由将可能对这两种类型的验证当局产生影响的不同的法律制度表现出来。所指出的这类不同的一个例子是，可适用于私人运营的验证当局的反托拉斯立法便可能不适用于行事公共职能的验证当局。另外，即使(b)项中所载条款中包含了(a)项中的类别，(a)项仍是有其作用的，因为该项可适应那些打算依靠某种许可证制度的国家的需要，从而可以保持统一规则的中立性。

111. 考虑到上述讨论，会议决定，第(1)款应按下述精神予以改写以便今后讨论：

“(1) 为本规则的目的，“验证当局”系指在其营业过程中从事发放与用于数字签字的加密钥匙有关的许可证工作的个人或实体。

“(2) 第(1)款不得违反要求验证当局持有许可证、得到认可或以法律中所规定的方式运营的任何适用法律的规定。”

第(2)款

112. 有些人支持保留第(2)款。据认为，对第(2)款所列举的各项功能，还应通过明确提及其他功能予以补充，例如证书的制作、管理、吊销和撤消等，以便更好地说明验证当局提供的各种辅助服务同构成验证当局主要活动的数字签字系统的运作之间的联系。但普遍的意见却是应当删去第(2)款，而其实质内容则可在后一阶段予以审议，以确定是否可在工作组最终决定编写立法指南时将其列入指南之中。

第 8 条. 证书

113. 工作组审议的第 8 条草案案文如下:

"在本规则中，"证书"系指至少具备以下内容的数据电文[或其他记录]:

"(a) 确定签发证书的验证当局;

"(b) 指定或确定证书持有人或持有人所控制的装置或电子代理人;

"(c) 包含与持有人所控制的私人钥匙相配的公用钥匙;

"(d) 规定数据电文的有效期[以及对公用钥匙使用范围的现有限制，如果有的话]; 和

"(e) 经签发证书的验证当局作了[数字]签字。"

一般性评论

114. 会议一般认为第 8 条草案应分为两部分(或分写成两条)，前部分载列对统一规则拟涉及的证书而下的一般定义，后部分则基本按照(a)至(e)项列出这种证书的最起码内容。据指出，这样做可适当扩大统一规则的范围，否则如果所有要素都列在第 8 条下作为"证书"定义的一部分，局限性会较大。

"证书"的定义

115. 首先，会议一致同意，对证书使用技术定义可能不妥，因为这样的定义在今后可能需加以修订，以反映需要和技术的变化。工作组接着审议了"证书"的一种定义，其措词大致如下: "在本规则中，"证书"系指验证当局为了确定拥有私人钥匙的个人或实体而发的一份数据电文或其他记录"。

116. 据指出，这一定义只包括身份证书，而将各种广泛使用和可能需要获得承认的证书置于统一规则的范围之外。在这方面，与会者发表了不同的意见。一种观点是，统一规则中只应包括身份证书。另一种观点是，也应包括其他种类的证书(例如授权证书)。虽然有些人对这一观点表示支持，但也有人表示关切，认为如果也包括其他证书，那么涉及验证当局的陈述及因此而承担的责任的有关条文便将需要确定不同的法律制度，以涵盖所签发的各种证书，而这对工作组来说可能会造成要求过高。

117. 在措词问题上，据建议，为了包括各种证书，可拟定一项一般性定义以包括所有各类证书，而在随后的条文中写明各类证书的最低限度内容。为了体现这种做法，提

出了大致如下的措词: “在本规则中, “证书”系指一份数据电文, 可按其中所含公共钥匙对相配的数据电文加以核证”。然后, 对于每一种证书, 将需要制定一项规则, 规定其用途, 例如大致措词如下: “身份证书是为了提供身份证明”。另据建议, 为了反映证书可履行不同功能这一看法, 需要对定义加以修改, 以提及数据电文“……其用意是核证某人的身份或其他重要特征”。据进一步建议, 应使用“确认”、“确定”或其他类似的词语代替“核证”一词, 因为后者有时会有特定的技术含义。

118. 对后一个拟议定义作了重点讨论。关于身份证书定义的具体措词, 与会者提出了不少建议。一项建议是应避免提及“其他记录”。支持这一建议者指出, 在统一规则中提及“记录”可能会造成对示范法第2(a)条的解释问题。对此, 有人答复说, 这样提及“记录”将有助于避免在统一规则是否包括纯书面形式的证书方面造成任何不确定性。另一项建议是, 为了避免对当事方的主观意图提出解释问题, “为了确定……”等词语应改成“它确定……”。

119. 上述建议措词遭到反对, 理由是这种措词会使验证当局得以通过不确定证书发给何人而逃避责任。因此, 应添加大致如下的词语: “……其用意是确定……”。还有一项建议是, “个人”一词应改成“主体”, 这是在实践中广泛使用的行业术语, 对于证书的主体不是一个人而是一个“装置或电子代理人”的情况, 可适当涵盖。这项建议遭到反对, 理由是: 如果使用“主体”一词, 便需要通过提及“人”来予以界定; 无论如何, 任何“装置或电子代理人”总是由人控制的。而且“主体”一词将与示范法以及贸易法委员会其他文书中使用的术语不相吻合。虽然提及一个“人”是可以令人接受的, 但据指出, 应表明这个词系指证书的主体, 而且也包括“实体”。至于提及“实体”, 据一致认为, 在工作组对“装置”或电子代理人是否可成为证书主体这个问题作出最后决定之前可先予以保留。还有一项建议是, “私人钥匙”应改成“一对钥匙”。

120. 经讨论, 工作组决定应按照如下大致措词重拟定义:

“[身份]证书

“在本规则中, [身份]‘证书’系指一份数据电文或其他记录, 由验证当局签发, 其用意是确认持有一对特定钥匙的个人或实体的身份[或其他重要特征]”。

121. 会议一致认为, 方括号中的“身份”和“其他重要特征”这两个词语将使工作组在日后阶段可以审议是否应包括身份证书以外的其他种类证书这一问题。

关于身份证书最低限度内容的规定

122. 工作组接着将注意力转向(a)至(e)项, 重点审查了这几项是否准确说明了身份证书最低限度内容的问题。

一般性评论

123. 普遍认为, 在条文中列出一项证书的最低限度内容的实际目的是, 订立验证当局为履行其职责, 避免因未将所有必要的内容列入证书而对造成的损失负赔偿责任所必

须满足的标准。普遍认为，在澄清验证当局的赔偿责任问题以及需将哪类证书包括进去的问题之前，无法对证书的最低限度内容作出最后决定。工作组假定初步交换意见可能会有助于以后阶段重新进行讨论，因而决定着手审议(a)至(e)项。

124. 在讨论中提出了这样的问题：不符合第 8 条草案中规定的最低限度要求的证书是否应视为无效证书；第 8 条草案是否应当起缺省规则的作用，以便证书在当事各方同意的情况下即为有效。就后一种情形而言，有人提出应在第 8 条草案中按第 5(2)条草案的措词加入一条规则。

起始部分

125. 虽然同意可以用纯书面形式签发证书，但对使用“或其他记录”一词是否妥当提出了疑问(见上文第 118 段)。

(a)项

126. 会议认为(a)项的实质性内容基本上可以接受。

(b)项

127. 有人指出，使用“持有人”一词产生了这样的疑问：究竟是指向其签发证书者，还是指持有并依赖证书副本者。另据指出，使用“持有人”一词造成不确定性，因为第 8 条草案中使用该词时指的既是持有证书者又是持有有关的一对钥匙者。虽然有人提出，出于上述理由使用“主体”一词更为可取，但工作组普遍倾向于使用“人”(见上文第 119 段)一词。但是，工作组决定，这两个词都应留在方括号内，以便今后进一步审议这一事项。关于“装置或电子代理人”的提法，据说这种用法会引起不确定性，因此决定在工作组进一步审议这一事项之前将这些用词放在方括号内(见上文第 119 段)。

(c)项

128. 会议认为(c)项的实质性内容基本上可以接受。关于“持有人”一词，决定将其改为“主体”和“人”并放在方括号内(见上文第 127 段)。

(d)项

129. 普遍认为，有效期是证书的最关键的要素之一。关于对证书范围的提法以及目前对此作出的任何限制，有人提出将其删去或至少对其进行修改，以具体说明可以提及方式将证书的范围和对此作出的任何限制纳入证书。支持这一建议的人提出，可能无法将所有限制列入证书。另据认为，这种提法可能无意中造成验证当局因未能将所有可能的限制列入证书而负赔偿责任。这项建议遭到反对，理由是，证书的范围和对此作出的任何限制均为至关重要的内容，证书的功能和完整性均需以此为根据才能加以评估。另据指出，提及证书的范围以及对其作出的任何限制，可顾及需表明证书会起不同作用的必要性。因此，建议把这种提法包括在新的(f)项中，放入方括号内，以备工作组进一步

审议这一事项。除这一修正外，工作组核准了(d)项的实质性内容。

(e)项

130. 虽然普遍认为验证当局的签字是证书的基本内容之一，但对这一签字是否必须是数字签字则提出了不同看法。一种看法是，签字应当是数字签字，以确保证书的完整性。另一种意见是，如果验证当局的签字是加密的，各依赖方可能无法确定这是某一验证当局的签字，而这个签字本应表明其打算受证书的约束。另据指出，如果验证当局的签字并非依循某种透明程序的结果，则该证书可能归于无效。工作组一致认为，有必要确保验证当局的签字是可靠的，其程序也应当是透明的。因此，决定保留“数字”一词，去掉方括号，并加上“或其他可靠的”一词，以便解决对“数字”一词表示的关切。

新的(g)项

131. 据建议，验证当局所采用的算法应当作为证书的最低限度内容之一列出。支持这一建议的人提出，算法对于确保识别签字人的身份以及数据电文的完整性必不可少。反对意见的依据是，如果需提及有关的算法，证书才能有效，那么验证当局不在证书中列出这种算法即可逃避赔偿责任。有人提出，确保数据的完整性固然必要，但要取得这一结果，更好的办法可能是在数字签字的定义中列出数据完整性的要素。相反的观点是，不在证书中列入所使用的算法将使验证当局对未能签发有效的证书负赔偿责任。经讨论，工作组决定在第 8 条草案中提及所适用的规则，放入方括号内，以便在今后的届会上进一步审议这一事项。

第 9 条. 验证做法说明

132. 工作组审议的第 9 条草案案文如下:

> “为了上述规则的目的，‘验证做法说明’系指验证局公布的、具体说明验证局签发或办理证书等所采用的做法说明。”

133. 工作组注意到，第 9 条草案与统一规则其他条文中所述及的一些问题有关，如证书签发陈述问题(第 10 条草案)和验证当局的赔偿责任(第 12 条草案)问题，并决定将第 9 条草案的审议推迟到工作组完成对统一规则的审议后进行。

第 10 条. 证书签发陈述

134. 工作组审议的第 10 条草案的案文如下:

“备选条文 A

“(1) 验证当局签发证书，是要向合理依赖证书或证书所列公用钥匙可证实的数字签字的任何人陈述:

"(a) 验证当局在签发证书时遵守了此规则的所有适用要求,并且如果验证当局已公布证书或以其他方式将证书提供给依赖者，则该证书所列[以及合法持有相应私人钥匙的]持有人已经接受证书。

"(b) 证书所确认的持有人[合法地]持有与证书所列公用钥匙相配的私人钥匙;

"(c) 持有人的公用钥匙与私人钥匙是同时起作用的成对钥匙;

"(d) 截至证书签发之日，证书所载全部资料均正确无误，除非验证当局在证书中[或以提及方式在证书内列入一项说明]申明，特定资料的准确性尚未证实；和

"(e) 据验证当局所知，证书内没有删略任何已知的任何一旦得知便会对上述陈述具有不利影响的重要事实。

"(2) 根据第(1)款，签发证书的验证当局向合理依赖证书或证书所列公用钥匙可证实的数字签字的任何人陈述，验证当局根据[以提及的方式列入证书的，或]依赖当事方已收到通知的任何适用的验证做法说明，签发了证书。

备选条文 B

"(1) 验证当局签发证书，是要在证书有效期间[本着诚意]向持有人和依赖证书所载资料的任何人陈述:

"(a) 验证当局已经[办理][核可][签发]证书，并将在必要时按如下各项管理和废止证书:

㈠ 本规则;

㈡ 管束证书签发的任何其他适用法律；和

㈢ 在证书中申明或以提及方式列入证书的,或有关个人已收到通知的任何适用的验证做法说明，如果有的话;

"(b) 验证当局已按证书或任何适用的验证做法说明申述的范围证实了持有人的身份，或在无验证做法说明的情况下由验证当局以一种[可靠][可信]的方式证实了持有人的身份;

"(c) 验证当局已证实，申请证书的该人持有与证书所列公用钥匙相配的私人钥匙;

"(d) 据验证当局所知，除证书或任何适用的验证做法说明所规定之外，截至证书签发之日，证书所载所有其他资料均准确无误;

"(e) 如果验证当局公布了证书，证书所确定的持有人即为接受了该证书。

"[(2) 如果某个验证当局签发了须受另一法域的法律管束的证书，该当局也是作出了其他适用于管制证书签发的法律的所有保证和陈述。"

135. 有人建议说，条文草案的标题可改为"证书签发的程序"之类的提法。据指出，

第 10 条草案一开始便提出了用以衡量验证当局的赔偿责任的标准，该条同第 12 条草案密切相关，因为第 12 条草案规定是对该标准的认可。会议结合备选条文 A 重点讨论了是否应将第(1)款(a)至(e)项所列陈述视为强制性要求（即当事方不能经协议予以减损的最低限度标准）或视为“缺省”。关于“缺省规则”可能的含意，在讨论中几次将“缺省”规则的特点归结为“填补空白”规则(即只有在无相反协定情况下才具有约束力的补充性要求)或当事方之间没有任何契约的情况下才适用。

136. 主张将第(1)款变成一项缺省规则的人指出，需要有灵活的规则来保证对即将出现的技术变革的适应；对所有的验证当局都规定很高的赔偿责任标准的结果只能是妨碍业界的发展，并会鼓励较不可靠的验证当局进入市场；对可靠性低的证书规定最低限度标准有可能对在各种重要情况下在全球使用这类证书构成限制。一般来说，证书持有者和依赖当事方对证书内容的期望，应当仅靠提及验证当局在其验证做法说明中所承诺的内容或在证书中陈述的内容来确定；对证书采用强制性最低限度标准有可能使统一规则脱离主要市场的商务惯例。因此，验证当局的赔偿责任应仅靠提及验证当局已同意承担的义务来确定。据说，这样做可提供为适应市场上现有的五花八门的证书的情况所需的灵活性。下面是对第 10 条草案进行改写的建议，可同第 12 条草案合并：

“(1) 验证当局应在证书中明确说明自己提供何种服务。如果不在证书中表明验证当局的义务，即应认为验证当局已保证钥匙持有人的身份。

“(2) 如果验证当局未能履行证书中所说明的服务或在保证钥匙持有人身份方面失职，即对依赖当事方负有损害赔偿责任。

“(3) 验证当局可通过在证书中明确列明拒赔事项来限制其对损害的赔偿责任。

“(4) 本条须受验证当局与依赖当事方之间相反协议的管束。”

137. 这一提案遭到反对，理由是，在某些法律制度中，一方面界定可据以承认证书的法律地位的标准，另一方面又规定可采用拒赔条款否定这些标准中的基本内容，这未免有前后矛盾之嫌。另外还指出，依赖当事方与验证当局之间通常并无契约关系。对此，有人认为，澄清“依赖当事方”概念是否包括证书中所列成对钥匙持有人可能会有帮助。还有人认为，证书的篇幅可能十分有限，难以再在其中列入“明确拒赔事项”。对此，有人指出，就证书应有内容规定最低限度标准是符合缩短证书本身篇幅的精神的。

138. 有人支持将备选案文第(1)款保留作为一项最低限度标准，从而按此标准，当事各方不得通过私下协议减除义务，为此，据回顾说，工作组上届会议已就这一点明确作出了一项决定(见 A/CN.9/437，第 70 - 71 段)。另外，据指出，确立最低限度要求而同时保护证书持有人和其他依赖当事方，还将增强数字签字办法的可信赖度和商业上的可接受性，从而也有利于验证当局。有人提出反对意见，认为确立最低限度标准将会对验证当局造成难以负担的义务。对此，据答复指出，第 10 条的目的并不是对验证当局规定任何义务，而只是对某些证书界定特定的法律制度——如果符合某些要求，这些证书便够格享有特定的法律地位。验证当局依然可不受限制地提供质量较低的证书，不过这类证书将不会产生同样的法律后果。主张保留最低限度标准者认为，第 12 条草案规定的赔偿责任限额对于验证当局接受第 10 条草案的强制性要求将可起到适当的平衡作

用。在这方面，发言者列举了海洋运输业类似的赔偿责任制度，在海运方面，不受约束的市场力量错综复杂，在历史上曾造成整个局面扑朔迷离，以致阻碍当事各方达成海运交易，从而需要在这一领域尽早缔结诸如《海牙规则》之类的国际文书。

139. 据建议，限制规定的范围，确定第 10 条草案将可适用的特定类别的证书（例如为高额交易而签发的身份证书），也许可以使人们更易于接受制定强制性标准。另据建议，采用一种减弱式的强制性标准，可能有助于使人们接受将第 10 条草案适用于更广泛的证书。为了将这两项建议结合起来，据提议，只应保留第(1)款的(a)、(d)和(e)项作为最低限度标准。虽然一般都支持在继续讨论时列入这一提案，但又普遍认为，对于一些问题，还需要作进一步的澄清。

140. 需要澄清的一个问题是减弱式强制性标准具体将适用于哪些种类的证书。一种观点认为，减弱式标准应只适用于有限种类的高度安全的身份证书。有人支持这样一种意见：带有高度法律确定性的证书则需要有更加严格的标准。特别是，如果证书是为了提供具有法律约束性的签字，那么对于证书与成对钥匙的持有人身份之间的联系，便将需要提供进一步的保证。但也有人支持这样一种意见：(a)、(d)和(e)项项下的拟议最低标准已经减弱了许多而可以使其适用于广泛的证书。

141. 需要进一步澄清的另一个问题是，拟议的第(1)款案文与统一规则关于证书的鉴别功能的其他条文是否相互一致。据回顾说，对数字签字而言，证书的主要功能是鉴别成对钥匙的持有人，这是其中一个原因，说明为什么早些时候有人建议工作组把注意力放在“身份”证书的概念上。如果拟议的减弱式标准获得通过，验证当局便不再需要对持有人的身份作出任何陈述，而仅仅是保证验证当局本身制定的程序已得到遵守即可。虽然据承认这一过程会间接导致对配对钥匙的持有人的鉴别，但据建议，可进一步考虑在统一规则中保留关于直接（或“确凿”）鉴别持有人身份的(b)和(c)项的实质内容，也许可将其作为第 2 条草案的一部分。

142. 经讨论，人们一般认为，虽然说提出的(a)、(d)和(e)项被认为是为“身份”证书确定标准的，但经讨论后，一般的看法是，将这样一种有限的标准适用于广泛的各种证书可能更为适宜。人们还认为应进一步考虑如何列明鉴别功能，可在第 10 条草案中，或在统一规则更靠前部分中，作为少数几类证书的一项基本功能，因为对于这类证书，要求有高度的法律可靠性。会议一致认为，这个问题将需要在今后的会议上进一步讨论。在对这个问题进一步讨论之前，(a)、(d)和(c)项将保留于第(1)款中，并应将(b)和(c)项置于方括号之内。据建议，从备选案文 B 第(1)(b)款中抽出的备选措词，可能需要置于第(1)款的方括号之内，以供工作组今后的会议审议。关于(d)项，普遍认为，只有(b)和(c)项都成为第(1)款的一部分时，验证当局对证书所载资料准确性可能不予负责的申明这段文字才可予以接受。

143. 关于第(2)款，人们一般认为，关于验证当局应遵守在其验证做法声明中所作的承诺这一原则应予保留。

144. 为反映上述讨论，有人建议将第 10 条草案订正如下：

“证书一经签发，即应认为：

(a) 签发证书的人或实体已遵守了统一规则的一切适用要求;

[(b) 在签发证书时，私人钥匙即为持有人的钥匙，并且与证书所列公用钥匙相配对;]

[(c) 持有人的公用钥匙与私人钥匙是同时起作用的成对钥匙;]

(d) 截至证书签发之日，证书所载全部资料均准确无误[,除非验证当局在证书中申明，特定资料的准确性尚未证实];

(e) 据验证当局所知，证书内没有删略任何已知的、但如知道后会对上述陈述具有不利影响的重要事实; 和

[(f) 如果验证当局已公布了验证做法声明，证书便是由验证当局按该验证做法声明而签发的。”

145. 经讨论后，工作组请秘书处拟定一份第 10 条修正稿及可能的备选案文，以反映上述的讨论结果。

第 11 条. 合同责任

146. 工作组审议的第 11 条草案案文如下:

“(1) 就签发证书的验证当局与证书持有人[或与验证当局建有合同关系的其他任何一方]之间而言，各当事方的权利和义务由其达成的协议确定。

“(2) 根据第 10 条规定，因证书所列资料的缺陷、技术故障或类似情况而遭受的任何损失，验证当局可通过协议，使自己免负赔偿责任。但是，如果对合同责任的免除或限定完全是不公正的，则限定或免除验证当局赔偿责任的条款不得援引，同时还要考虑到合同的目的。

“(3) 如果证明验证当局的作为或不作为所造成的损失系蓄意或轻率造成损害所致，而且它知道可能会造成损害，则该验证当局无权限定其赔偿责任。”

147. 据指出，第(1)款重申了关于适用于验证当局责任制度的当事方自主原则。此外，还指出，第(2)款涉及免责问题，对于该款，除有两点例外以外，一般都说是可以接受的。第一点例外系由于提及第 10 条草案所致，该条旨在规定一个不应允许验证当局减免的最低限度标准。第二点例外系由于关于国际商业合同的统法社原则（第 7.1.6 条）所引起，该原则试图为评价免责条款的普遍可接受性提供一个统一标准。此外，还指出，第(3)款涉及验证当局或其代理人的故意不端行为造成损失或其他损害的情况（系借鉴《贸易法委员会国际信贷划拨示范法》第 18 条）。

148. 工作组审议了是否应保留第 11 条草案作为统一规则的一部分的第一个问题。支持删去的人说，该条所涉及的事项留待合同和适用法律处理更好。特别是，认为第(1)款是多余的，因为它只谈及当事方自主原则，而《示范法》第 4 条已涉及当事方自主原则问题; 第(2)和(3)款与有关可能难于统一的事项的国家法律相冲突。此外，还指出，第 10 条草案全面涉及了该事项。虽然认为把合同责任的一些问题留待合同和统一规则以外的适用法律来处理是一可接受的备选方法，但普遍认为，应设法就此一重要事项取

得一定程度的统一。

149. 关于可取得这一结果的方法问题，人们提出了若干建议。一种建议是，保留目前措词的第 11 条草案。支持这一建议的人说，虽然第(1)款可能看起来是在谈显而易见的道理，但第(2)款所提出的却是非常重要的原则，即不能通过免责条款免掉合同的核心义务。此外，还指出，第(3)款是必要的，它不仅涉及合同关系，而且也涉及非合同关系。

150. 另一建议是在第(1)款中提及当事方不能商定“严重不公平”条件而删去第(2)和(3)款。虽然有的表示赞同删去第(2)和(3)款，但也有人出于若干原因而反对该建议，反对理由包括：使用“严重不公平”词语不合适，因为许多法律制度不熟悉这一词语；该词语旨在保护弱方的目的应留待其他法律（如保护消费者法）去解决；删去第(2)和(3)款可无意中导致允许当事方废弃合同的核心效力或免除为蓄意不轨行为承担责任。

151. 一个有关的建议是，在第(1)款“义务”一语后插入“及对权利和义务的任何限制”和“根据可适用的法律”等语，并删去第(2)和(3)款。支持该建议者说，这种处理方法最终会成为一种基于当事方自主原则和可适用法律的可接受的一般性陈述。然而据指出，如果采取该处理方法，可能会出现不统一。

152. 另一项建议是，用一个规定应要求验证当局达到的最低限度标准应是证书做法说明中提出的那些标准的条款来取代第 11 条草案。有人反对这一建议，认为这将取代了合同和第 10 条草案作为量测验证当局责任参照点提出的最低限度标准。然而，有人认为，该建议可为第 10 条草案的最低限度标准可能不适用的可靠度低的证书提供一条适当的规则。

153. 在讨论中，提出了若干行文性的建议。关于第(1)款，一种建议认为，在方括号中提及“任何一方”太笼统含糊，应改为提及“任何依赖当事方”。另一建议认为，对第(1)款应作修改，以便明确该款并非旨在使各当事方之间的关系只受其协议约束，因为那会使各当事方商定第(2)和(3)所载的免责条款权利例外失去意义。关于第(2)款，有人建议，在“损失”一词之前增加“与证书有关的”一语，第(2)款第一句中的其他部分可予删去。

154. 经过讨论，工作组未能就第 11 条草案的具体措词达成协议，工作组请秘书处根据讨论中人们提出的各种意见起草备选案文供今后届会审议。

第 12 条. 验证当局对依赖证书的各当事方的赔偿责任

155. 工作组审议的第 12 条草案案文如下：

“(1) 在无相反协议的情况下，签发证书的验证当局因如下过失而对合理依赖证书的任何人负有赔偿责任：

“(a) [违反根据第 10 条作出的保证][因疏忽误述证书所述资料的正确性]；

“(b) 收到废止证书的通知后，立即对废止证书进行登记；和

“(c) [不][疏忽]遵守如下程序所造成的[后果]：

"㈠ 验证当局公布的验证做法说明规定的任何程序；或

"㈡ 适用法律规定的任何程序。

"(2) 尽管第(1)款有规定，但如果验证当局能够证明它或它的代理人已为避免证书出现差错采取了一切必要措施，或验证当局或其代理人无法采取此类措施，则该验证当局不负赔偿责任。

"(3) 尽管第(1)款有规定，但验证当局可在证书中[或以其他方式]限定使用证书的目的。对于为任何其他目的使用证书所产生的损失，验证当局概不负赔偿责任。

"(4)尽管第(1)款有规定，但验证当局可在证书中[或以其他方式]限定证书对其有效的交易价值。对超出此价值限度所造成的损失，验证当局不负赔偿责任。"

一般性评论

156. 与会者普遍支持按第 12 条草案的精神订立一条关于验证当局对依赖证书的各当事方的赔偿责任的规定。然而，普遍认为，这样一条规定的范围应当以验证当局保证钥匙持有人的身份和该钥匙持有人签署的数据电文的完整性这类情况为限。这样做将便利某些需要较高安全标准的做法，同时又不对可能不适宜采用如此高的安全和赔偿责任标准的其他做法产生不利影响。

157. 但有人对是否能够或应当建立一个适当的赔偿责任制度表示某种怀疑。据说，如果不同时对提供核证服务所涉风险作出合理的定量规定，采用这样一种赔偿责任制度会阻碍验证做法，因为验证当局将会冒某种风险但对此又不能获得保险。此外有人指出，这样一种赔偿责任制度也许并不必要，因为在没有特定制度的情况下，侵权行为法律的一般原则将适用。但有人指出，在某些验证当局的赔偿责任并未得到具体规定的法域，原则上说验证当局将不对依赖当事方负赔偿责任。另据指出，鉴于下述一些原因将这一事项留给适用法处理并不妥当：许多法域中存在的不确定性会对电子商务的发展产生消极影响；缺乏任何赔偿责任会无意中使商务当事方不能利用验证当局提供的服务；如何确定适用法律会提出许多难题。至于工作产物的形式，有人表示实施统一赔偿责任制度的方式，公约可能比示范法更有效(见下文第 212 段)。

158. 经讨论，工作组决定应当作出一切努力在统一规则中处理验证当局对依赖当事方的赔偿责任问题，并开始详细审议第 12 条草案。据建议，工作组似宜在以后讨论第 12 条草案时列入对关于依赖当事方所造成的损失的性质和可预见性的审议。

第(1)款

起始部分

159. 与会者对起始部分的开头语是否应当保留发表了不同的看法。一种看法认为，如果第 10 条草案订立了验证当局必须满足的最低限度标准，这开头语应当删除。另一种观点认为，这一开头语是有用的而且应当予以保留，因为它们使当事方得以谈判他们

的赔偿责任。对此有人答复说，当事各方不能谈判，因为第 12 条草案处理的是一般并无协议情况下的侵权行为赔偿责任。但有人指出，闭路通信系统中的依赖当事方通常与验证当局有某种类型的协议。此外，据指出，验证当局和钥匙持有者之间达成的赔偿责任条件可以纳入钥匙持有人与依赖当事方之间的合同中。

160. 大多数与会者的意见是所提及的是例外情况，不应当让这类情况破坏第 12 条草案的主要目的，即管制验证当局对第三方的侵权行为赔偿责任。因此提议如有必要处理验证当局与其客户或依赖当事方之间可能存在的相反协议，可以在第 12 条草案末尾加入适当的文字。

第(a)至(c)项

161. 有人指出，(a)和(c)项中放在第二组方括号内的文字反映了严格赔偿制度这一原则，应当删除。有人关切地表示，使用“误述”概念可能会造成不确定性，因为虽然它在某些法律制度中有特定含义，但在另外一些法律制度中却并不为人所知。有人提议以“误陈”一语作为变通。

第(2)款

162. 与会者对关于疏忽的举证责任应当由验证当局还是应当由依赖当事方承担的问题发表了不同的看法。一种看法是，依赖当事方应当负举证责任。支持这一观点者说，依赖当事方能够证明是否有疏忽，因为关于验证当局是否满足了第 10 条草案订立的审慎标准的证据对依赖当事方来说是不难获得的。此外据指出，只有当工作组采用严格赔偿责任这一原则时，将举证责任移到验证当局身上才将是适宜的。另一种观点认为，虽然赔偿责任以是否有疏忽为依据，但应由验证当局负举证责任，因为任何有关证据都将置于验证当局的控制之下。据指出，特别当证书提及的不是钥匙持有人的身份而是验证当局为确定钥匙持有人身份所采用的程序时就是这种情况。

第(3)和第(4)款

163. 与会者对第(3)和第(4)款中体现的限制验证当局的赔偿责任的原则表示支持。但有人表示，只有对以验证当局的严格赔偿责任为基础的制度来说而不是对以疏忽为基础的赔偿责任制度来说，赔偿责任的限度才是适宜的。

164. 至于可以采用的限度类型，有人说，每一项交易规定一个货币限度的做法并不能充分保护验证当局，特别是在对“身份证书”的情况下，因为身份证书可以不受赔偿责任限度的影响在某一非常短的时间内多次使用，而无法确定赔偿责任限度是否已经超过。因而有人建议，在第 12 条草案中应当列入一条采用赔偿责任总限度的规定，其文字大致可以是：“验证当局可以在证书中或以其他方法规定一个该证书的总价值数额，作为对该证书有效期内所有依赖事例的赔偿责任限度。不管对该证书提出多少次索赔，验证当局对损害所负的赔偿责任不应超过该总限度”。但有人认为，赔偿责任总限度可能并不可行，因为依赖当事方在现有技术应用情况下无法知道是否已超过某一限度。

对新的第 12 条草案的提议

165. 为了解决上面表示的关切，对第 12 条草案的替代案文提出了一些建议。一项建议是第 12 条草案应按下文改写:

"(1) 如果验证当局签发证书但以下述方式疏忽，则它对合理依赖证书的任何人负有赔偿责任:

"(a) 在证书中提供不一致的资料;

"(b) 未能在意识到需废止[或吊销]证书时随即[通知或]公布废止[或吊销]证书[; 或

"(c) 未能依循验证当局所公布的并且已通知依赖人的验证做法说明中的程序].

"(2) 验证当局可以在证书中[或他处]说明对使用证书的目的所做的限制，验证当局不对因证书用于任何其他目的而造成的损害负赔偿责任。

"(3) 验证当局可在证书中[或他处]说明证书对之有效的交易的价值的限度，验证当局不对超出这一限度的损害负赔偿责任。

["(4) 如果而且只有当验证当局与依赖证书者之间的协议中有相反规定，本条第(1)款不适用。"]

166. 另一项建议是第 12 条草案应按下述方式修改:

"(1) 除非验证当局证明验证当局或其代理人已采取一切合理的措施来避免证书出错，否则验证当局因如下过失而对合理依赖该验证当局签发的证书的任何人负赔偿责任:

[插入(a)至(c)项]

"(2) 尽管第(1)款有规定，但对证书的依赖，只要与该证书所载资料相抵，即为不合理。"

167. 虽然第一项提议引起一定的兴趣，但工作组重点讨论了第二项提议。据指出，第(1)款的意图是根据合理依赖的原则来确定对证书中的差错的赔偿责任，避免任何提到陈述和疏忽之处。另据认为，第(2)款旨在允许验证当局在证书中阐明检验依赖证书的合理性的标准。据解释，第(2)款并非要提供一个详尽无遗的一览表，列出所有不合理的依赖证书的情形。虽然第(1)和第(2)款作为今后讨论的依据基本上是可以接受的，但有人表示了一些关切并提出了建议。

新的第(1)款

168. 一项关切是，实际上，验证当局几乎无法以讲求成本和时间效益的方式来采取"一切合理的措施"。为处理这一关切提出了一些建议。一项建议是，用"商业上"一词替代"一切"。支持这项建议的人指出，"商业上合理的措施"这种提法可反映出在具体情况下哪些做法是行得通的。另据认为，这种措词与贸易法委员会的其他法律文本中所使用的术语将是一致的(例如，贸易法委员会国际贷记划拨示范法第 5(2)(a)条)。反对意见的理由是，这样会产生不确定性，因为对于什么是"商业上合理的"并没有普遍

的共识可言。还有人提出把“一切”一词干脆删去。对此提出反对意见，理由是，这样会无意中不适当地降低应由验证当局达到的谨慎行事的标准。还有一项建议是，应当采用示范法第 7(1)(b)条中使用的措词。

169. 另一个关切是，第(1)款未能解决验证当局签发证书出错的问题。针对这一担心，有人提出，在第(1)款“证书”之后加上“或在签发证书时”一词。据指出，第(2)款中还应包括证书废止一览表或类似的一览表中载列的资料。

170. 一致认为，在确定验证做法说明的作用问题之前，(c)项应当放在方括号内。

新的第(2)款

171. 有人提出，作为起草问题，应当删去开头语并在第(1)款的开头处加入“在不违反第(2)款的情况下”字样。有人关切地表示，第(2)款可能事与愿违，过份地限制对依赖证书的合理性提出质疑的理由。另一个关切是，第(2)款可能未包括这样一种情形：在一项价值过高的交易中依赖了证书，因为价值可能未包括在“资料”一词的含意中。为了解决这些关切，有人提出，应当把第 12 条草案的第(3)和第(4)款列作不合理地依赖证书的例子。本着同样的思路，有人提出，或许可以列出其他类似的例子，例如，在哪些情形下验证当局可以在证书中说明哪些指定的当事方或哪类当事方可以依赖该证书。还提出，如果损失是验证当局蓄意造成或肆意妄为造成的，则验证当局不能援用赔偿责任限度。

172. 另一种关切是，如果提及在证书中“载列的”资料，那么第(2)款可能无意中导致需列入证书中的资料数量的不适当的增加。为了解决这一关切，有人提出，应当允许以提及方式将这一资料纳入证书。反对意见的理由是，使第三方的权利受纳入验证当局与钥匙持有人之间的协议中的条件的限制，是不公平的，因为这些条件可能甚至不会轻易地提供给第三方。

173. 经讨论，工作组决定按下文改写第 12 条草案：

> “(1) 在不违反第(2)款的情况下，除非验证当局证明，验证当局或其代理人已经为避免证书中[或签发证书时]出现差错而采取了[一切合理的][商业上合理的]措施，[而且这种措施从所有情形来看都与签发证书的目的相宜]，否则验证当局因如下过失而对合理依赖该验证当局签发的证书的任何人负赔偿责任：
>
> “(a) 证书中有差错；[或]
>
> “(b) 它超出了证书对之有效的价值；或
>
> “(c) […]。”

据认为，第 12 条草案应只适用于签发身份证书的验证当局。

第 13 至 16 条

174. 因为缺乏足够的时间，工作组将其对第 13 至 16 条草案的审议推迟到今后的会议。据认为，这些条款草案应只适用于签发身份证书的验证当局。另一种观点是，工作

组应考虑统一规则是否只适用于身份证书，或是适用于任何其他种类的证书。

第四章. 对外国电子签字的承认

第 17 条. 根据此类规则提供服务的外国验证当局

175. 工作组审议的第 17 条草案案文如下:

"备选条文 A (1) 如果外国[人][实体]同可成为验证当局的本国实体和个人一样符合相同的客观标准，并采取相同的程序，就可成为当地的验证当局，或可在无当地机构的情况下从另一个国家提供验证服务。

(2) 备选条文 X 第(1)款所述规则不适用于如下方面[…]。

备选条文 Y 第(1)款所述规则可有一些例外，但以不影响国家安全要求为限。

"备选条文 B …[颁布国指明主管制订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。"

一般性评论

176. 关于第四章的标题，有人说在其中提及对外国电子签字的承认不妥，因为该章涉及的是外国验证当局提供服务(即第 17 条草案)、本国验证当局对外国证书的认可(即第 18 条草案)和对外国证书的承认(即第 19 条草案)。工作组对一些为更清楚地在本章标题中反映其中所涉及的主题而提出的建议进行了简短的审议(例如"证书的跨境承认"、"对电子签字和证书的承认"、"对外国验证当局和证书的承认")。不过，人们一般认为，对第四章以何种标题为宜的审议应等到工作组更详尽地讨论了证书的法律效力后再进行。

177. 关于第 17 条草案中提议的两项备选条文，人们一般认为，备选条文 B 规定由一个经颁布国指定的机关来规定核准外国证书的具体规则，这一条文不能作为制订统一规则的依据。人们一致认为，备选条文 B 应予删去，工作组应将重点放在对备选条文 A 的审议上。

第 17 条草案的范围

178. 据指出，第 17 条草案有两项目标: 首先，承认外国验证当局根据其中所规定的条件成为当地验证局的权利; 其次，条文给予外国验证当局以在无当地机构的情况下在颁布国提供服务的权利。第 17 条草案涉及贸易政策的问题，即颁布国在多大程度上放弃对外国验证当局机构的限制和对外国验证当局提供服务的限制的问题。有人建议说，工作组应当将其工作重点放在有关外国证书的法律效力和证书持有者与验证当局间的关系之类的示范条款的制订上。不少人发言支持这一意见。据认为，贸易政策问题属

于其他论坛的范围，在统一规则草案中予以处理并不适宜。

179. 有人在针对这些意见作答时指出，第 17 条草案允许外国实体成为当地验证当局，这只是指出了在外国实体符合为本国验证当局所规定的标准的情况下不得对其歧视的原则。这一原则就验证当局而言是尤为适切的，因为它们可能会在不一定在经营国设立机构或其他营业点的情况下经营。还进一步指出，贸易法委员会电子商务示范法本身便涉及了一系列可被视为事关贸易政策问题的跨境问题。

180. 在听取了各种意见之后，为了推动对统一规则草案的审议，工作组进而讨论了对第 17 条草案的若干修正，但并不影响就第 17 条草案实质所作的各种保留。

第(1)款

181. 有人问第(1)款是否仅考虑对那些按照某一机关或外国政府机构的核准从事经营的验证当局的承认。针对这一问题所作的答复说，从目前的行文看，第(1)款并不涉及验证当局须有外国政府核准的问题。但是，也有人认为，象第 17 条草案这样的规定应当以符合立法要求的某种许可证制度为基础。

182. 有人认为，第(1)款所引起的某些问题，其根源在于该款过份强调了对验证当局本身的承认，而没有强调验证当局签发将在颁布国使用的证书的能力。而且，“同可成为验证当局的实体和个人一样符合相同的客观标准并采取相同的程序”一语可能会对新技术的使用构成障碍，因为据认为，该款为阻止对那些按照技术上同颁布国所遵循程序相比更先进的程序行事的外国验证当局的承认留下了口实。有人建议将现有行文改为提及颁布国验证当局应予达到的“客观标准”似乎更为可取。或者将“并采取相同的程序”一语置于方括号内。

183. 关于外国验证当局应符合的条件，据指出，第(1)款的目的是要确保这些条件同适用于本国验证当局的那些条件基本相同。因此建议改写第(1)款，其大意是：对外国验证当局的承认应受颁布国法律的管辖。关于外国验证当局应予达到的标准的定义问题，可由工作组在日后阶段予以审议。此类修正将进一步明确这样的一点：承认还应受在颁布国取得的任何除外条款的管束，这样就没有必要再保留第(1)款中的任何备选条文了。所提议的案文如下：

“在不违反颁布国法律的前提下，外国[人][实体]可：

“(a) 成为在当地设立的验证当局，或

“(b) 在无当地机构的情况下提供验证服务，条件是其同可成为验证当局的本国实体和个人一样符合相同的客观标准并采取相同的程序。”

184. 有人针对该提案指出，提及国内法并不是一种令人满意的解决办法，因为颁布国的法律可能载有会破坏第 17 条草案精神的歧视性规定。而且，提议的修正还引起了这样的问题：颁布国由谁来决定外国验证当局同国内实体和个人一样符合相同的客观标准并采取相同的程序，以及以何种手段作出这种决定。

185. 有人认为，从现有行文看，第(1)款似乎意味着，外国验证当局不仅需要根据其本国法律获得核准，而且还需符合颁布国的要求。据认为，这样的规则可能会起到不应

有的限制作用，不利于促进电子商务。有人针对后一种意见提议说，第(1)款的含义可通过将其按照下述精神改写为一项非歧视规则而加以澄清：

"(1) 如果外国[人][实体]同可成为验证当局的本国实体和个人一样符合相同的客观标准并采取相同的程序，即不得仅以其是外方为由拒绝其成为当地验证当局或提供验证服务的权利。"

186. 这项提案遭到反对，理由是提议的非歧视规则引起了同就第 17 条草案的范围发表一般评述时提出的一般性关切类型相同的关切(见上文第 178-180 段)。

187. 在审议了各项提案后，考虑到所发表的各种不同意见，工作组认为需要有更多的时间就第(1)款所涉问题进行磋商。已请秘书处提出一份第 17 条草案的订正案文，其中可附有反映上述讨论的各种备选条文，以供工作组在日后阶段进行审议。

第(2)款

188. 关于第(2)款所列两段除外性备选条文，有人认为备选条文 X 可提供一种限制第(1)款范围的开放性机制。根据这一意见，如果允许任何例外，允许的理由只能是如备选条文 Y 中所规定的国家安全。不过，人们一般都倾向于只保留备选条文 X 。根据这种意见，对第(1)款的一般规则的例外将由颁布国予以规定。虽然说备选条文 Y 有着将可能的例外限制在那些与国家安全有关的方面的优点，但有人认为国家可能会希望在其立法中根据公共政策列入其他一些可作为例外的理由。

第 18 条. 本国验证局对外国证书的认可

189. 工作组审议的第 18 条草案案文如下：

"外国验证局签发的证书可用于数字签字，其条件与受本规则制约的证书相同，但这种证书要得到根据…[颁布国法律]运作的验证局承认，而且该验证局按与其本身的证书相同的程序，保证该证书细节正确无误及其有效。"

190. 作为一般性评论，有人说，列入关于跨国界承认问题的规定是朝着提高证书可信度迈出的一大步。据说，在商业上使用证书的做法越来越多，对这种新技术的信任会通过遵守国际标准而得到加强。工作组应当考虑委任按照国际标准运作的验证当局的国际机制。有人对将拟议中的议题列入工作组稍后阶段拟讨论的事项之中表示支持。但据指出，该拟议中的议题不仅仅与第 18 条草案提出的事项有关，例如工作组可以在重新审议证书的登记时讨论这个问题。

191. 关于第 18 条草案，据指出，该条所载规则的目的仅仅是要使本国验证当局能够如同对自己的证书一样保证外国证书细节正确并保证该外国证书有效。有了第 18 条草案，当外国证书被发现有缺陷时赔偿责任将由提供这种保证的本国验证当局承担。然而，存在着根据第 18 条草案作出的保证并非是承认某一由外国验证当局签发的、在其他方面满足第 19 条草案所载条件的证书的必要条件。有人认为，由于提供第 18 条草案所涉及的保证仅仅是自愿的，第 18 条草案并非必要，可以删除。有人还认为，统一规

则草案应当让颁布国来决定本国验证当局是否可以和根据什么条件对外国验证当局签发的证书提供这种保证。可以视最后通过的文书的性质而定，在立法指南或随同的解释性说明中提及第 18 条草案意指的这类保证的签发问题。

192. 有人提请工作组注意曾在其第三十一届会议上讨论过本国验证当局可对外国验证当局提供的不同等级的可信度。据指出，这些等级从最高等级一直到最低等级不等。在最高可信度等级中，本国验证当局应依赖外国证书的当事方的要求，根据它宣布的对导致签发该证书的程序的了解，保证该证书的内容，从而对该证书中的任何差错或其他缺陷承担完全赔偿责任，而在最低可信度等级中，本国验证当局仅仅根据对其公共钥匙和数字签字的核证，来保证外国验证当局的身份(见 A/CN.9/437，第 81-82 段)。据认为，这些不同的可信度等级并未在第 18 条草案中得到充分的反映，如要保留该条规定，应明确规定它并不排除完全保证外国验证当局签发的证书的正确性和有效性之外的其他安排。

193. 针对上述意见有人指出，第 18 条草案的一个有益用途是，它允许证书的流通和跨国界使用，而不要求有关于承认证书的双边和多边国际协定，而为了提供第 19 条草案所述的承认，有些国家可能考虑需要这种协定。另外，鉴于工作组曾决定在统一规则中不仅涉及由政府实体授予许可证的验证当局，而且还涉及在政府许可证制度范围以外运作的验证当局(见 A/CN.9/437，第 48-50 段)，因此第 18 条草案还有一个好处，即在出现不可能自动获得第 19 条草案所述的承认时，允许采取商业解决办法。在这方面有人建议，第 18 条草案的范围可以通过按下列文字重新措词而得到澄清:

> “根据按…[颁布国法律]运作的验证当局提供的有关保证，外国验证当局签发的证书可用于数字签字，其条件与受本规则制约的证书相同。”

194. 有人表示支持在统一规则草案中保留一条授权本国验证当局对外国验证当局签发的证书提供保证的规定。这样一条规定可以第 18 条草案为基础，同时考虑到在工作组会议上提出的建议。然而据指出，第 18 条草案目前在第四章中的位置并不妥当，因为该条规定并不涉及对在国外签发的证书的承认问题。

195. 经审议，工作组同意在方括号中保留第 18 条草案连同提议的修订，并请秘书处考虑到与会者已经发表的观点编拟该条的备选案文，供工作组今后审议。

第 19 条. 对外国证书的承认

196. 工作组审议的第 19 条草案案文如下:

> “(1) 如果外国验证局的做法至少达到根据本规则要求验证局所应达到的可靠性，就应承认该外国验证局签发的证书与根据...[颁布国法律]运作的验证局所签发的证书具有同等法律效力。[此项确认可通过一项公布的国家决定或有关国家间达成的双边或多边协定进行。]
>
> “(2) 符合另一国有关数字或其他电子签字的法律的签字和记录，被确认为与符合本规则的签字和记录具有同等法律效力。但该国法律要求此种签字

和记录的可靠程度至少与根据...[颁布国法律]进行的记录和签字所须达到的可靠程度相同。[此项确认可通过一项公布的国家决定或与其他国家达成的双边或多边协定进行。]

"(3) 如果从所有情况看，证书可靠适当，适合签发证书的目的，则采用外国验证局签发的证书核实的数字签字应[由法院或其他事实检验人]宣布有效。

"(4) 尽管有上述条款,政府机构仍可[以公布的方式]规定，必须结合向其提交的电文或签字，使用某一特定验证局、某一类验证局或某一类证书。"

第(1)和第(2)款

197. 据指出，第(1)和第(2)款处理的是在做成任何交易(和在对某一签字的可靠性等级产生争执)之前就可以确定外国证书和签字的可靠性的方式。为此目的，第(1)和第(2)款订立了颁布国为了承认外国验证当局签发的证书以及符合另一国法律的签字和记录而可以使用的检验规则。

198. 与会者对第(1)和第(2)款中的承认的范围提出了一些问题。关于第(1)款，有人认为，外国验证当局签发的证书与根据颁布国规则运作的验证当局签发的证书两者之间的法律等同性概念并不十分清楚。据指出，"承认"一词，如在国际私法中通常使用的那样，意味着需要对在另外一个法域作出的行动给予法律效力。然而，这个概念不能在第(1)款的情况中使用，因为证书是一种文书，它所载列的事实陈述仅仅起到了声明性功能。再则，第(1)和第(2)款都意指颁布国应当适用本国法律来确定外国验证当局签发的证书的可靠性以及符合另一国法律的签字和记录。因此，据说，第(1)和第(2)款并不与国际私法的一般原则相符，因为根据这种一般原则，境外行为的有效性应当根据完成该行为的所在法域的适用法加以处理。此外，据指出，示范法第 13 条和统一规则第 3 和第 5 条草案已经为数据电文的归属和电子签字可靠性的确定订立了规则。

199. 针对以上意见有人答复指出，第(1)和第(2)款对要求使用特定级别的证书以为履行某些交易提供较高程度的可靠性的国家管制制度来说起着有益的作用。在具有这种管制制度的颁布国，第(1)款为承认由外国验证当局签发的、用于不需要特定级别证书的交易的证书提供了最低限度的标准。同样，第(2)款为这些颁布国提供了一条缺省规则，该规则假设符合另一国法律的签字和记录是有效的，被认为对所有根据颁布国法律不必提出更高要求的情况提供了合理的可靠程度。有人促请工作组不要让适用于外国证书的最低限度标准问题完全留给颁布国的法律冲突规则来处理。

200. 工作组讨论了对第(1)和第(2)款可能作出的修正，以便解决人们表示的关切。有人特别认为，第(1)和第(2)款可合并按以下文字重新措词作为一条不歧视规则:

"由外国验证当局签发的证书不得以系由外国验证当局签发为由而得不到与本国验证当局签发的证书相同的承认。"

201. 但是，有人反对拟议中的否定性措词，因为它没有规定以什么标准来给予承认。再则，据指出，拟议中的不歧视规则可能会引起如对第 17 条草案提出的相同的保

留(见上文第 185-186 段)。

202. 经审议，会议普遍认为，订立一条实质性规则，为在做成任何交易之前就确立外国证书和签字的可靠性提供一种方法将是可取的。工作组请秘书处编拟第(1)和第(2)款修订案文，包括将这两款规定合二为一的案文，连同将与会者所发表的意见考虑在内所可能订立的变式。

第(3)款

203. 据指出，第(3)款的目的是要建立一个标准，据以在没有事先确定外国签字和证书的可靠性的情况下评估其可靠性。然而，据认为，这条规定，如按现有措词，可能并不需要，因为它仅仅陈述了这样一条原则，即当对一个签字的真伪和由一外国验证当局签发的证书的可靠性产生争执时，颁布国法院必须给予这种签字或证书以与有关情况相宜的证据效力。

204. 针对以上看法有人指出，受贸易法委员会电子商业示范法第 7 条启发制定的第(3)款为颁布国法院评估外国证书的可靠性提供了有益的指导。鉴于采用统一规则的国家可能不一定将示范法第 7 条纳入其国内立法，在统一规则草案中陈述这一重要原则是可取的。为了更明确地陈述其目的，有人建议第(3)款可按如下文字重新措词:

> “如果从所有情况看，证书可靠适当，适合签发证书的目的，则采用外国验证当局签发的证书核实的数字签字不得[由法院或其他事实检验人]宣布无效。”

205. 经审议，工作组决定应当保留第(3)款的实质内容供工作组以后阶段进一步审议。

第(4)款

206. 有人对是否有必要制订第(4)款这样一条规定提出了质疑，因为该条保留了政府机构确定在与其进行电子通信时使用的程序的权利。一方面，有人关切地表示，第(4)款可能会具有并不可取的限制性含义，可能会被解释成政府机构以外的个人或实体没有结合他们所收到的电文或签字选择自己希望使用的特定验证当局、某一类验证当局或某一类证书的权利。这样一种情况被视为与示范法各条款中所确立的当事方自主权原则不相吻合。另一方面，如果第(4)款的目的是要为政府机构确立一项特权，则这条规定可能需要进一步完善。因为可以把它解释为在政府机构没有明确指出结合向它们提交的电文和签字它们希望使用哪一特定验证当局、哪一类验证当局或哪一类证书时，政府机构有义务接受任何类别的验证当局和证书。

207. 会议普遍认为，不仅仅应当承认政府机构，而且还应当承认商业交易或其他交易的当事各方都有权利结合他们所收到的电文或签字选择所希望使用的特定验证当局、某一类验证当局或某一类证书。工作组请秘书处重新拟订第(4)款以便反映这一谅解，并决定在以后阶段审议修订后的条款的适当位置。

四. 工作的协调

208. 工作组听取了关于联合国教育、科学及文化组织（教科文组织）和联合国贸易和发展会议（贸发会议）在电子商务领域开展的工作的发言。

209. 据指出，教科文组织在其第二十九届大会上接受了着手编拟关于电脑空间的使用的国际法律文本这一任务。在这方面，据表示，教科文组织和贸易法委员会有必要在电子商务领域共同作出努力。据指出，指导这些努力的应当是促进电子商务的必要性，以使电子商务既能造福于发达国家和发展中国家，同时又将保证基本人权，包括隐私权。据强调，数据电文对其发端人的归属、数据电文的完整性和电子商务所涉当事方的责任性等问题应当是工作组关于数字签字和其他电子签字工作的核心。

210. 关于贸发会议的工作的发言指出，全球贸易点网络已经建立，其目的是协助发展中国家努力受惠于电子通信领域的发展。另外据宣布，贸发会议正在组织一个电子商务领域设备制造商、软件生产商和服务提供商的展览（1998 年 11 月 8 日至 13 日，里昂）。据指出，该展览将包括一系列与电子商务有关的广泛问题的讲座。

211. 工作组注意到了这些发言，并欢迎有关组织参加其工作。会议请秘书处继续监测其他国际组织在电子商务法律问题上的动态，并向工作组报告这些动态。

五. 今后的工作

212. 在本届会议结束时，有人提议，工作组似宜对以示范法和统一规则的各项规定为基础编拟一项国际公约作初步考虑。据认为，这个议题可能在工作组下一届会议上以有关代表团可能提出的更加详细的提议为基础作为一个议程项目加以讨论。但是，工作组的初步结论是，无论如何应当将编拟公约视作为一个与统一规则的编拟和示范法的任何其他增添分列的项目。在对统一规则的形式作出最后决定之前，关于在以后阶段编拟一项公约的建议不应当转移工作组目前的任务，即集中精力编拟关于数字签字和其他电子签字的统一规则草案，也不应当改变工作组目前的工作假设，即统一规则将采取法律规定草案的形式。大家一致理解，编拟这项公约草案的可能性不应当被用来重新提出已在示范法中得到解决的问题，因为那样做可能会对促进这项已经取得成功的文书的使用产生消极影响。

213. 据指出，工作组下一届会议定于 1998 年 6 月 29 日至 7 月 10 日在纽约举行，但尚需由委员会第三十一届会议（1998 年 6 月 1 日至 12 日，纽约）确认。

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。