联合国 A

大会

Distr.
LIMITED

A/CN.9/WG.IV/WP.73
12 December 1997
CHINESE
ORIGINAL: ENGLISH

联合国国际贸易法委员会
电子商业工作组
第三十二届会议
1998年1月19日至30日，维也纳

电子签字统一规则草案

秘书处的说明

目　　录

目　录(续)

导　言

1. 委员会第二十九届会议（ 1996 年）决定将数字签字和验证当局问题列入其议程．请电子商业工作组研究制订上述专题的统一规则的可取性和可行性．会议一致认为，工作组第三十一届会议将要进行的工作，可包括制订有关上述专题某些方面的规则草案．会议请工作组向委员会提供充分的基本要素，以便就将要制订的统一规则范围做出明智的决定．至于工作组更加明确的任务，会议一致认为要制订的统一规则应当涉及如下问题：支持验证方法的法律依据，包括正兴起的数字认证和验证技术；验证方法的可适用性；在使用验证技术方面，用户、提供者和第三方之间风险与责任的分配；利用登记簿进行验证的具体问题；以及以提及方式列入条款．[1]

2. 委员会第三十届会议（ 1997 年）收到了工作组有关其第三十一届会议工作情况的报告（ A/CN.9/437 ）．至于制订有关数字签字和验证局问题的统一规则的可取性和可行性，工作组向委员会说明，它已就逐步统一该领域法律的重要性和必要性达成了共识．尽管该工作组尚未就此项工作的形式和内容做出明确决定，但它已初步得出结论认为，至少就数字签字和验证局问题以及在可能的情况下，就有关事项制订统一规则草案是可行的．工作组忆及，除数字签字和验证局问题外，或许还需研究电子商业领域今后的工作：公用钥匙加密技术替代问题；第三方服务提供者履行职能的一般问题；以及电子订约问题（ A/CN.9/437，第 156 - 157 段）．关于以提及方式列入条款的问题，工作组得出结论认为，秘书处需要作进一步研究，因为各种基本问题已众所周知，而且格式之争与服从合同的诸多方面显然需要留待适用的本国法律予以解决，其原因包括如消费者保护和其他公共政策考虑．工作组认为，在其下届会议开始举行时，应当将此问题作为其议程上的第一个实质性项目加以审议（ A/CN.9/437,第 155 段）．

3. 委员会对工作组第三十一届会议已完成的工作表示赞赏，并认可了工作组得出的结论，它委托工作组制订有关数字签字和验证局法律问题的统一规则（以下简称“统一规则”）．

4. 关于统一规则的切确范围和格式，委员会普遍认为，在目前工作这一初期阶段已不能做出任何决定．它认为，虽然鉴于公用钥匙加密法在正形成的电子商业惯例中所发挥的明显主导作用，工作组不妨将注意力适当集中在数字签字问题上，但是统一规则应符合《贸易法委员会电子商业示范法》采取的不偏重任何手段的方法，而且不应妨碍采用其他认证技术．此外，在处理公用钥匙加密法的过程中，统一规则或许需要考虑不同的安全程度，并承认在数字签字情况下与提供的各类服务相对应的不同法律效力和责任程度．关于验证局，尽管委员会确认了市场驱动标准的价值，但普遍认为，工作组可适当地制订一套要求验证局达到的一套最低限度标准，在谋求跨境验证时尤其应当如此．

5. 作为将在电子商业领域今后工作范围内审议的另一个项目，有人建议工作组在后一阶段讨论因特网上管辖权、适用法律和争端解决的问题．委员会获悉， 1997 年 6 月在海牙国际私法会议主持下，举行了一次有关在因特网上管辖权和适用法律问题的学术讨论会．委员会还获悉，经合发组织 1997 年 11 月召开的一次国际会议将试图研拟有关

国家政府、政府间组织、非政府组织和私营部门团体对电子商业问题采取的协调方法。委员会希望秘书处能参加上述两项活动，并就此提出报告。[2]

6. 此项说明载有为可能列入统一规则而将予以审议的订正条款草案。这些条款涉及数字签字、其他电子签字、验证局和有关的法律问题。制订条款所依据的是工作组第三十一届会议报告所载该届会议的审议和决定（A/CN.9/437），以及上文转载的委员会第三十届会议的审议和决定。这些条款草案尤其以工作组通过的这样一项初步假定为依据，即工作组在数字签字领域的工作将采取法律规定形式（A/CN.9/437，第 27 段）。这些条款还旨在反映工作组上届会议做出的如下决定，即可行的数字签字领域的统一规则应从《贸易法委员会电子商业示范法》（以下简称“示范法”）第 7 条衍生出，并应认为这类条款确定了一种方式，按此方式，可以利用一种可靠办法“鉴别某人”，并“表明该人核准”数据电文所载资料。更笼统地讲，对《示范法》、统一规则和关于以提及方式列入条款的可行规则之间的关系（见 A/CN.9/437,第 151 - 155 段）做出最后决定之前，条款草案准备与《示范法》所表述的原则和所使用的术语一致（A/CN.9/437,第 26 段）。

7. 本说明未涉及因特网上管辖权、适用法律和争端解决问题、电子环境下合同的订立和履行，或须由工作组今后届会审议的任何其他问题。将向工作组提交一项口头报告，介绍 1997 年 6 月在海牙国际私法会议主持下，就因特网上管辖权和适用法律问题举办的学术讨论会以及 1997 年 11 月经合发组织举行的国际会议（见上文第 5 段）。

8. 在编写本说明的过程中，秘书处得到了一些专家，包括秘书处邀请的专家及有关政府和国际组织指定专家给予的帮助。

一、 一般说明

9. 正如本说明第二部分所载条款草案表明的那样，统一规则的目的，是促进在国际商业交易中更多采用电子签字。这些条款草案借鉴了一些国家已经生效或现正编写的多种法律文书，目的在于通过提供一套标准，防止适用于电子商业的法律规则不一致。在还为其规定了若干基本规则的验证局的可能协助下，根据这些标准可确认数字签字和其他电子签字的法律效力。

10. 统一规则侧重商业交易的私法方面，因此不打算解决在日益更多采用电子签字方面可能产生的一切问题。尤其是，统一规则不涉及国家立法机关在建立电子签字综合法律框架时可能需要考虑的公共政策、行政法、消费法或刑法等方面的问题。

11. 根据《示范法》，统一规则尤其要反映如下几点：不偏重任何手段的原则；不应歧视功能等同的传统纸本概念和做法的方法；以及对当事方自主权的广泛依赖。统一规则的目的是既作为在“开放”环境（即各当事方在未事先达成协议的情况下进行电子通信）下的最低限度标准，又作为在“封闭”环境（即在利用电子手段进行通信时，各当事方均受预先制订的合同规则和程序的约束）下的缺省规则。

二、 关于数字签字、其他电子签字、验证局和有关法律问题的条款草案

第一章. 适用范围和一般规定

12. 在审议拟列入统一规则的条款草案时，工作组似宜更加一般地审议统一规则与《示范法》之间的关系。尤其是，工作组似宜对以下问题向委员会提出建议，即数字签字统一规则是应构成一项单独的法律文书，还是应纳入《示范法》扩充文本，例如，作为《示范法》新的第三部分。

13. 有人认为，如果将统一规则作为一项单独文书或作为《示范法》的补充进行编拟，则须纳入《示范法》如下各条内容的条款：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”定义），第3条（解释），第7条（签字），和第13条（数据电文的归属）。尽管本说明未转载这些条文，但应注意到，秘书处已根据关于这类条款将构成统一规则一部分的假设，编拟了统一规则条款草案。关于统一规则的适用范围，应当牢记，根据《示范法》第1条规定，尽管涉及消费者的交易不是统一规则的焦点，但仍将包括在适用范围之内，除非立法国适用于消费者交易的法律与统一规则有抵触（见A/CN.9/WG.IV/WP.71,第49 - 50段）。

14. 关于当事方自主权问题，仅提及《示范法》第4条（经由协议的改动），不足以提供一种令人满意的解决办法，因为第4条确定了《示范法》中两类规定之间的区别，一类可按合同自由进行更改，另一类规定则应视为强制性规定，除非按《示范法》以外的适用法律，授权经由协议的改动。关于电子签字，由于“封闭”网络具有实际重要意义，因此有必要广泛确认当事方自主权。但是，还需考虑公共政策对合同自由的限制，包括保护消费者免受过度服从合同的法律。因此，工作组似宜根据《示范法》第4(1)条的内容，在统一规则中列入一项如下内容的条款：除统一规则或其他适用法律另有规定外，按交易各方商定的程序签发、收取或依赖的电子签字和证书依协议规定生效。此外，工作组似宜考虑制订一项有关如下内容的解释规则：在确定参照某一证书核实的一份证书、一个电子签字或一个数据电文对于某种目的是否完全可靠时，应当考虑所涉各方达成的所有有关协议、各当事方的任何行为以及任何有关的贸易惯例。

15. 除上述条款外，工作组似宜考虑，是否应有一个前言澄清统一规则的目的，即通过建立一种安全框架，并提供具有同等法律效力的书面和数字电文，促进有效利用数字通信（见A/CN.9/WG.IV/WP .71，第51段）。

第二章. 电子签字

第一节. 可靠的电子签字

第 1 条. 定义

为了这些规则的目的:

(a) "签字" 系指意欲为鉴别某人，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[意欲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[《贸易法委员会示范法》第 7 条]规定的条件所采用的]]数据电文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 系第 4 条规定的数字签字，并符合第 5 条提出的条件; 或

㈡ 截至进行此类签字时为止，利用安全程序，可以其他方式证实系某一特定个人的签字: 唯独与使用它的该人有关联;能够立即自动而客观地鉴别该人; 是按使用它的该人全权控制的方式或手段生成的;并与相关的数据电文有关,因此,一旦电文被更改，电子签字即无效; 或

㈢ [就在开展正常业务的过程中，参与生成、发送、接收、储存或以其他方式处理数据电文的各当事方之间而言]，在各当事方以前业已商定并适当应用的情况下具有商业上的合理性.

参考

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.

说明

16. 第 1 条草案旨在反映工作组第三十届会议做出的如下决定，即按照《示范法》中的不偏重任何手段的原则，统一规则不应妨碍使用任何能按《示范法》第 7 条提供 "可靠适当的方法"，取代亲笔签字和其他纸本签字的技术. 尽管统一规则可侧重数字签字，但仍应采取一种更加通用的方法，并可审议与其他电子签字技术有关的问题（见 A/CN.9/437 , 第 22 段）.

17. 根据(a)和(b)项所载 "签字" 和 "电子签字" 的定义，按对《示范法》第 7 条的理解，广义划定了统一规则范围，以涵盖可被用于提供功能等同的亲笔签字的全部技术. 应当注意到， "签字" 的定义仅以定义形式重申了《示范法》第 7(1)(a)条，它无意取代或以其他方式影响统一规则以外（如在本国立法或判例法中）可能存在的任何 "签字" 或 "亲笔签字" 的定义. 该签字定义的主要目的是用作随后的 "电子签字" 和 "可

靠电子签字”定义的依据。它也可用作在目前尚无“签字”定义的国家的一种有用的参照。

18. 第1条草案提出的三类定义（即“签字”、“电子签字”和“可靠电子签字”）旨在向工作组提供一种分析手段，并反映若干国家立法草案中众所周知的区别。但是，视统一规则的内容而定，不是所有三项定义均属必要。如果工作组决定重点强调电子签字的一种法律效力（即确认电子签字与亲笔签字功能等同），则只需审议一类“电子签字。因此，现被定义为“电子签字”和“可靠电子签字”的概念可纳入一种法律范畴，而不论将根据该法律范畴审议的技术的数量和种类如何。

19. 为划定统一规则范围所依赖的主要定义，是现已纳入标题为“可靠电子签字”的(c)项中的定义。关于定义起草事宜，可以注意到，“可靠”一词不是要表明任何特定技术都可在事实上或法律上提供绝对的安全，而只是要利用一套一旦达到就能产生某种法律效力的标准，限定电子签字较高的可信度。

20. (c)项着眼于为使用电子签字所产生的法律效力提供依据，同时打算反映工作组上届会议通过的“双重方法”。这种方法是从辩论中的两种备选方案产生的，即确定政府授权验证局的标准以及确认验证局在政府实行的公用钥匙基础结构以外行使职能的操作标准。工作组得出结论认为，这两种备选方案并非相互排斥。两种情况之间的差别可能在于使数字签字在各种情况下产生法律效力的方式。就经政府授权（或“持有许可证”）的验证局而言，它能否达到适用的操作标准，这是该验证局能否得到授权的一个先决条件，也是确认它签发的证书是否具有法律效力的一个条件。在第二种情况下，验证局在开始行使职能前无需表明它已达到操作标准。但是，如果验证局签发的证书受到质疑（如在司法争端或仲裁时），则裁决机构须通过确定该证书是否由达到此类标准的验证局签发，来评估它的可信度。（见A/CN.9/437，第48段）。

21. 除考虑到持证或非持证验证局的操作情况外，(c)项还进一步扩大了统一规则的适用范围，以涵盖不需依赖任何验证局或其他“受信赖的第三方”就能操作的认证装置。因此，有关“可靠”状况的提法有助于推行颁发许可证机制，通过此机制，立法国可确定数字签字的质量和可靠性以及可依赖其他形式电子签字的市场驱动做法。

22. 根据(c)(一)项规定，如果数字签字的应用符合立法国建立的公用钥匙基础结构，则将按统一规则推定可靠状况。在缺少这类公用钥匙基础结构的情况下，或除了这类基础结构，任何一种电子签字（即在或不在验证局或其他受信赖的第三方干预下应用的数字签字和其他电子签字）都可被认为是符合可靠状况的，但须符合最低限度要求。为了提供一种据以评估此类电子签字质量的基本标准，(c)(二)项列出了四种标准：唯独性、鉴别性、可靠性及与签字资料的联系。

23. 可靠的电子签字应是与使用的人“唯独地联系”这一要求的目的是要确保不发生合乎情理的可能，即不止一人会作出非属欺诈或其他不当行为的相同签字。唯独性的要求或许通过以生物统计学为基础的签字也能得到满足。此种签字包含签字人特有的某种属性，如指纹或视网膜扫描。就数字签字而言，这项要求也能得到满足。在这方面，签字人使用的成对钥匙随机生成，和钥匙具有足够的长度，因此，任何别人都很难生成

相同的成对钥匙。

24. 可靠的签字应能用来鉴别签字人。这并非指签字本身必须由签字人姓名组成或包括签字人姓名。通过提及其他资料来源进行鉴别就足够了。因此，例如，数字签字通过提及验证局签发的证书，就可鉴别签字人。主要要求是鉴别过程必须相对说来快捷、客观和自动。因此，例如，尽管手书签字或许能够鉴别签字人，但一般也不能快捷或自动进行，而且往往不是一种客观的测定。在诸多情况下，签字本身难以辩认。即使可辩认，最终也能鉴别谁是签字人，但是，鉴别过程的时间安排和确定性不可能总是符合电子商业要求。因此，如果没有手书签字分析专家对据称的签字人认可的签字与有关签字进行比较提供证明，手书签字不可能总是被可靠地确定为某个特定个人的签字（如果事实未得到承认或缺少签字见证人，就会出现这类情况）。在此情况下，结果不大可能是快捷或自动的，而且专家得出的结论在许多方面是主观的，而不是客观的。相比之下，在人们提款时，自动出纳机使用个人鉴别编号（ PIN ），可以自动、客观而快捷地为银行鉴别与某一特定地址和特定帐号联结的具体个人。此人不能否认提款请求上有他或她的签字（但他有可能否认签署了该提款请求，这一点是可靠性要求的主题）。

25. 除了将某人鉴别为电文签字人之外，用于签署电文的程序还必须提供十分可靠的保证：被鉴别为签字人的个人事实上就是签署了该电文的人。安全程序要求使用签字者全权控制的方式方法，这种程序可以满足此类可靠性要求。利用受信赖的第三方也可达到必要的可靠程度。可能还有另外一些方法也可实现这一要求。工作组似宜讨论其他的方法，以便能够保证达到可接受的可靠程度。

26. 可靠签字必须与所签署的数据电文联系在一起，如此，电文如被更改，签字即随之无效。这种联系可视为可靠签字的一项至关重要的要求，因为不这样，签字很有可能被从一张数据电文上删去，并被粘到另一张上。

27. (c)(一)和(二)项的目的是适用于在未预先就所签署的数据电文发端人与收件人之间的电子签字作出合同安排的情况。但是，根据《示范法》中采取的方法，统一规则可能需要重申有关数据电文认证的合同计划的有效性。因此，(c)(三)项确定了封闭系统协议的法律效力。工作组似宜讨论如下问题，即方括弧中借鉴了《示范法》用语的措词（“就开展正常业务过程中参与生成、发送、接收、储存或其他方式处理数据电文的各当事方间而言”）是否有必要将当事方自主权的效力限制在业务上使用电子签字，不包括消费者参与的交易（见 A/CN.9/437,第 24 段）。

第 2 条. 推定

(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)(三)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并不合理. 各当事方根据第 1(c)(三)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.]

参考

A/CN.9/437,第 43 、 48 和 92 段.

说明

28. 第 2 条草案重点放在从确认“可靠电子签字”的状况所产生的法律效力. 工作组上届会议讨论了利用推定处理某些电子签字问题的可能性(如验证局的责任及数字签字电文的归属)(见 A/CN.9/437, 第 58 、 70 以及 120 - 121 段).

29. 可靠电子签字概念以及从可靠电子签字状况产生的可反驳推定, 可视为能实现一种切实可行的电子商业系统的关键. 在纸本交易中, 依赖当事方可利用若干指示数字, 确定文件是否可靠以及签字是否属实. 这包括使用附有电文的纸张(有时带有水印、彩色背景、或其他可靠的指示数字)、笺头、手书签字, 或通过受信赖的第三方(如邮政局)用密封的信封传递. 但是, 就电子通信而言, 不存在这些可靠的因素. 可以进行通信的全部东西是一套在各方面都相同的电子脉冲, 而且易于复制或修改. 因此, 在许多情况下, 收件人和依赖电子通信的任何其他当事方在收到或依赖电文时, 必须了解该电文是否可靠, 它是否保存了完整的内容, 以及一旦随后发生争端下, 是否能够确定双方的事实(如确定在法庭上不否定数据电文). 为此, 就可靠签字提出的可反驳推定, 可向依赖当事方提供这类保证, 据此能够使依赖当事方放心地进行商业活动, 即如果要有可反驳推定, 他们的交易就更容易实施.

30. 应当区分第 2 条草案所作推定的效力与第 3 条所述归属的效力. 第 2 条草案中推定的目的在于在收件人利用可靠电子签字证实了电文的明显来源时, 减轻举证电子电文来源的责任. 因此, 与该签字关联的人需要证明, 尽管收件人证实可靠的电子签字, 并依赖安全程序, 但签字仍不是此人的签字. 作为确定此项推定的正当理由, 可以指出,

证明谁实际上发出了电文所必需的证据，一般掌握在与该签字关联的人的手中。例如，就数字签字而言，与该签字关联的人通常要比任何其他依赖当事方更能充分证明私人钥匙被窃、被复制、失密，或未经第三人授权被使用的情况。在通常情况下，电文收件人除了用于证明与该签字关联的人确实发送了电文的安全程序外，不会有其他证据。不过，根据第3条草案规定，如果该草案提出的要求得到满足，即使与该签字关联的当事方能够证明它未发送有关电文，也仍要对应有信赖的接收人所遭受的损失负责。

31. 根据《示范法》第7条采取的方法，第(1)款不产生如下推定，即附有可靠电子签字的数据电文构成了一种具有法律约束力的义务。该款仅仅推定，可靠电子签字是据称的签字人为签署电文而签署的。如果有证据证明附有其签字的人是差错、误述、胁迫或其他使之无效的原因的受害者，则可否定有关电文的法律效力，但提出此类问题的责任由否定数据电文法律效力的人承担。

32. 第(2)款表明，在缺少可靠电子签字的情况下，统一规则中任何规定不会改变关于电文来源的举证责任的一般证据规则。第(3)款是根据《示范法》类似条款制订的。该款旨在协助立法国根据一种合法利益的要求，从第2条草案提供的保护中排除某些情况。例如，立法国可确定，第2条草案作出的推定不适用于刑法领域。第(4)款载列了若干方法，可用来反驳第(1)款中所作的推定。工作组似宜讨论在统一规则文本中是否需要这种说明性条款，或该条款是否应在一项指南或评注的范围内加以审议。

第3条. 归属

(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[被视为电文签字人]，[受电文内容的约束]，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条(1)]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) 如果依赖当事方已从[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。

参考

A/CN.9/437，第 118 - 124 段（E 条草案）；
A/CN.9/WG.IV/WP.71，第 64 - 65 段.

说明

33. 工作组上届会议普遍认为，不应谋求在统一规则范围内重申《示范法》第 13 条规定的原则（见 A/CN.9/437，第 119 - 120 段）。但是，会议还认为，统一规则与《示范法》第 7 和 13 条之间的关系须加以澄清。为此，第(1)款备选条文 A 反映了工作组上届会议普遍接受的一项原则（A/CN.9/437，第 120 段），采用了广义的措词，以涵盖数字签字和可用于生成可靠数字签字的替代技术。

34. 备选条文 B 推定数字签字符合《示范法》第 7 条中“可靠方法”的要求。工作组似宜审议这样一个问题：此项推定是否应加以扩大，以不仅包括数字签字，而且包括使用可靠电子签字的其他实例。如果工作组想将该条款的范围限于数字签字，则须相应调换第 3 条草案的位置。

35. 工作组似宜讨论一下，是否可以利用第 3 条草案，更加准确地处理这样一个问题，即一个人何时才能对下述数据电文内容负责：该电文实际上不是由此人发送的，而且是在开放环境下传递的（即电文发端人和收件人之间（或在“系统规则”范围内）未预先就用于确定数据电文归属的程序直接达成协议）。《示范法》第 13(3)(a)条虽涉及“发端人事先同意的一项程序”的使用问题，但并未明确涉及开放环境问题。鉴于可靠电子签字所固有的高度安全性，工作组似宜考虑能否制订一项一般规则，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发端人的电文。

36. 作为此内容条款的一个实例，工作组似宜审议如下措词：

除其他适用法律另有规定外，在如下情况下，可靠电子签字可归属看来与之相关的人的签字，不论是否经过该人授权；

(a) 电子签字系某人所为，此人从据称的签字人所控制的来源取得了存取编号、代码、计算机程序或生成签字所需的其他资料，并使签字看上去就是此人的签字；

(b) 存取是在据称的签字人未能采取合理审慎做法的情况下发生的；以及

(c) 收件人因善意依赖数据电文的表面来源而受到损失。

此类措词的效力是使有关双方，即未实际签署有关电文的据称发端人与按商业上合理的安全程序善意依赖电文的收件人，都承担损失风险。只有在因据称的发端人的过失，电文上附有其签字，该发端人才要承担损失风险。在以下情况下也会出现这种问题，如签字系从据称的发端人所控制的来源获得了必要信息的某人所为，而且此类信息是在据称的发端人未能采取合理审慎做法的情况下取得的。在此情况下，如果收件人合理依赖电文，据称的发端人就要受到约束。在所有其他情况下，无论收件人如何合理依赖电文，都有遭受损失的危险。开头的措词提到了“其他适用法律”，这对从建议的规则范围内排除消费者交易或许是必要的。

第二节. 数字签字

第4条. 定义

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一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，而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.

参考

A/CN.9/437,第30 - 38段（A条草案）；

A/CN.9/WG.IV/WP.71，第18 - 45段和55 - 56段.

说明

37. 备选条文A和B之间的区别主要是起草性质上的区别.尽管备选条文B反映了工作组上届会议得出的结论（见A/CN.9/437，第32段），但备选条文A以"电子签字"的定义为基础，提供更加简洁的措辞．在这两个备选条文中，所定义的"数字签字"均未提及"验证局"或"证书"．

38. 不打算给"私人钥匙"、"公用钥匙、成对钥匙"或与公用钥匙加密法有关的其他概念下定义．尽管工作组上届会议提出了关于增加定义的建议，但在法规性质的统一规则中列入大量定义应谨慎从事，因为这样做可能有悖于许多国家的立法传统．工作组似宜讨论一下在多大程度上需要增加定义（见A/CN.9/437,第29段）．

第 5 条. 效力

(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]证书生效期间生成的，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被……签发的标准另行签发的[立法国规定，主管发给持有许可证的验证局确认的操作标准的机关或机构].

(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: [...].

参考

A/CN.9/437，第 43 、 48 和 92 段.

说明

39. 数字签字如执行得当，应能成为可靠电子签字. 但问题是要确定何时完成了数字签字的执行，如此它有资格获得可靠的地位. 根据证书可以核实的数字签字并非全部可靠，在不能确定对持有人或公用钥匙的鉴别或认证是否准确的情况下尤其如此. 确定数字签字是否可靠的主要因素包括: (1)验证局是否已对持有人进行了适当的鉴别；(2)验证局是否已对持有人公用钥匙进行了适当的认证；(3)持有人私人钥匙是否已经失密；以及(4)验证过程是否可信（如公用钥匙规则系统和所用钥匙长度是否适当）.

40. 第(1)款提出了两项基本标准，可用以确定何时数字签字才称得上可靠的电子签字. 第一项标准要求签字在有效证书有效期内生成，并根据证书所列公用钥匙加以证实. 证书有效期一般从证书签发日期算起，结束日期以期满日期、废止日期或暂停使用日期中较早者为准.

41. 第二步包括确保证书本身能够准确确定一个人就是与证书规定的公用钥匙相应的私人钥匙的持有人. 证书的可信度还可按为立法国承认的当局所规定的标准、程序和其他要求加以评估. 制订此类标准可以采取如下方法，即由第三方任命验证局，自愿发给验证局许可证，或另行要求遵守立法国通过的规则.

42. 要不然，按第(2)款规定，如果法庭或事实检验人根据证据确定，证书中申述的

信息属实，那么，证书的可信度是显而易见的．但是，在此阶段，事实检验人必须逐个确定证书是否是由对持有人进行了适当鉴别，并对持有人公用钥匙进行了认证的验证局签发的．

43. 根据工作组采取的“双重方法”，第 5 条草案的意图是为确定验证局签发的证书的可信度，提供尽可能大的回旋余地．这种灵活性特别重要，因为数字签字才开始使用，而且此种签字模式及其监管尚未得到充分发展．因此，重要的是要促进在电子商业中更多使用数字签字，同时还要制订对数字签字电文的可靠性作出推定的标准．

44. 还必须注意到，尽管第 5 条草案中有一项选择方法提出对证书的准确性作出司法裁定，但另一项选择方法作出了如下推定，即证书若是由立法国认可的验证局签发，或在其他方面符合立法国所规定的某些标准，则此证书就是准确无误的．在此情况下，不需要为取得可靠电子签字的法律地位，而对证书的准确性作出司法结论．第二项选择方法对从事电子商业的人可能有帮助，这类人在利用通信采取行动之前，会了解到此项行动是否能够实施．但是，如能证明上述认可的验证局所签发的证书事实上并不准确，也不可靠，就可以反驳有关准确性的推定．

第 6 条．法人的签字

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．如果电文也是由受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[发端人][核准了]电文的[发送的]．

参考

A/CN.9/437，第 114 - 117 段（D 条草案）；

A/CN.9/WG.IV/WP.71，第 61 - 63 段．

说明

45. 在上届会议上，普遍认为应当删除第 6 条草案．但在讨论后，工作组决定将该条放在方括弧中，供稍后一届会议进一步审议（A/CN.9/437，第 115 和 117 段）．尽管根据第 6 条草案内容作出的一项规定可能被认为不适当地干预了其他法体（如机构法以及涉及公司自然人代表权的公司法条款），但在制订统一规则的现阶段，该项规定还是有用的，它提醒人们注意，工作组或许有必要更加充分地讨论如下问题，即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．

第三节．其他电子签字

46. 由于未向秘书处提供如何根据统一规则处理除数字签字以外的认证技术的资料，因此，未制订列入本节的具体规定．工作组似宜讨论一下，这类认证技术是否应在统一规则中更加详细地予以论述．如果工作组得出结论认为，不应对此类技术作更加具

体的阐明，统一规则仍将赞同通过“签字”和“可靠电子签字”定义所载非歧视原则以及通过将视为“可靠电子签字”的任何认证技术所享有的法律地位，更多使用数字签字的替代方法。

第三章. 验证局和有关问题

第7条. 验证局

(1) 为了上述规则的目的，“验证局”系指:

(a) 由……发给许可证[认可的]，根据这些规则行事的任何人或实体[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运作条例的机关或机构]；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)A 验证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].

参考

A/CN.9/437，第39 - 50段和90 - 97段（B条草案）；

A/CN.9/WG.IV/WP.71，第18 - 45段和57 - 58段.

说明

47. 正如在第1条草案中阐明的，统一规则应当从法律上确认如下两种情况：立法国希望通过公用钥匙基础结构或其他颁发许可证计划，对验证局的运作进行监管，以及未取得许可证的验证局可按市场驱动做法标准自由运作（见上文第17 - 18段）.

48. 在涉及持有许可证的验证局问题时，第(1)款未试图规定立法国用于实施公用钥匙基础结构或为验证局的其他许可证计划的标准. 未涉及此类标准可能是因为，这种公用钥匙基础结构的公共政策部分很强，或许不太有助于按示范法规定实现国际统一. 如果工作组准备更加具体地审议在许可证计划范围内使用的标准，似宜审议评估验证局可信度时要考虑的如下因素：(1)独立性（即在基本交易中没有财务权益或其他权益）；(2)财务资源和承担赔偿损失风险的财务能力；(3)管理人员的权限、公用钥匙技术方面的专门知识以及对适当的安全程序的熟悉程度；(4)长期性（在提起诉讼和提出产权要求的情况下，基本交易结束后数年内，仍可要求验证局出示验证证明或加密钥匙）；(5)硬件和软件的批准；(6)审计线索的保留和由独立机构进行的审计；(7)有应急计划(例如“大错修复”软件或钥匙托管）；(8)人员的选拔和管理；(9)验证局本身私人钥匙的保护安排；(10)内部安全；(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)赔偿责任的限制；(14)保险；(15)与其他验证局的相互可操作性；(16)废止程

序（在加密钥匙可能遗失或失密的情况下）；(17)将验证职能与验证局可能进行的任何其他业务分开（见A/CN.9/WG.IV/WP.71，第44段和A/CN.9/437，第45段）。

49. 第(1)(b)款给“验证局”下的定义完全未提及政府授权，但提到验证局的职能是签发证书。这样一项条款与第(2)款结合，其目的还想表明以下事实，即除了签发证书外，验证局虽然还可履行其他职能和提供各种服务，但这类职能和服务不属于统一规则的适用范围，因此，在审议电子签字的法律效力时，不应予以考虑。工作组似宜讨论一下，根据第(2)款内容作出的一项主要是说明性的条款是否应成为统一规则的一部分，或是否倒不如在一项指南或评注中加以表述。

第8条. 证书

为了本规则的目的，“证书”系指如下数据电文[或其他记录],它至少能够:

(a) 确定签发证书的验证局;

(b) 命名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) 规定证书有效期[以及对公用钥匙使用范围的现有限制，如果有的话]；和

(e) 由签发证书的验证局进行（数字）签字。

参考

A/CN.9/437，第98 - 113段（C条草案）；

A/CN.9/WG.IV/WP.71，第18 - 45段和59 - 60段。

说明

50. 尽管证书可用于履行各种职能和传递统一规则范围以外的其他信息，但按统一规则说明，证书的唯一功能是将公用钥匙与特定的持有人联系起来，这种联系可以通过在证书中命名公用钥匙持有人直接进行，还可通过说明持有人的某些属性（如采购代理人有权签订定量采购合同），或说明持有人所控制的机器、装置或软件代理人间接进行。因此，例如可向公司某个雇员签发一项只规定此雇员采购权限的证书。然后，可利用此证书与贸易伙伴进行采购交易。在此情况下，某个雇员的身份并不重要，但主要问题是此雇员是否有权代表所鉴别的一个人（即雇主）行事以及雇员的采购权限。但是，无论如何都有一个称为“持有人”的人控制与证书所确定的公用钥匙相配的私人钥匙，而且根据证书核实的数字签字电文属于此人。如果此人得不到确认，则证书不能用于核实数字签字是否为某人所为。

51. 第8条草案旨在表明被工作组视为证书基本内容的各种要素，即证书应当是一份数据电文；指明验证局，载有持有人公用钥匙；指明持有人；并有验证局的数字签字（见A/CN.9/437，第101段）。至于证书是否必须采取数据电文的形式，工作组似宜讨论一下统一规则是否还应包括纸本证书。

52. 工作组上届会议决定，它有必要审议如下问题，即制订一项要求证书提供最低限度信息的强制性规则，是否违背有关数据保护的适用法律。它认为，鉴于第 8 条草案所列要素的性质，应当避免出现这种潜在冲突。

53. “证书”定义未区分有可能按“证书”标题从商业上给予的不同程度的安全。不过，在编拟统一规则时，工作组似宜记住，验证局主要签发各种类别的证书。在工作组上届会议上，人们提出各种建议，请求在统一规则中反映使用此类证书可能产生的不同程度的安全性（见 A/CN.9/437，第 20、56、138 和 145 段）。作为这种多样性的一个实例，据报告下文所列三类“证书”可在市场上获得。

54. 第一类证书证实，使用者姓名和电子函件地址是验证局所保留的登记簿或“储存库”明确记载的主题名称。这类证书主要用于在因特网上浏览或确认个人电子函件，以适当加强此种环境的安全性，而不是为了认证持有人的身份。更确切地说，这类证书是要表明，对储存库记载的不清楚的主题名称进行了简要检查，而且对电子函件地址进行了一定的核对。第一类证书所载持有人姓名被视为非经核对的信息。这类证书提供安全的程度很低。它们不用于需要提供身份证明的商业用途，而且也不应指望将它们用于这种用途。

55. 第二类证书证实，持有人在申请证书时所提供的资料与公认的消费者数据库中可存取的资料不冲突。这类证书主要用于：(1)组织间的电子函件；(2)价值低，风险小的交易；(3)个人电子函件；(4)口令的替代；(4)软件的合法性；和(5)联机订购服务。第二类证书根据一种自动的联机程序，为证实持有人身份提供一定程度的保证。

56. 第三类证书为证实持有人身份提供了重要的保证，例如要求持有人亲自面见验证局代理人，或通过适当的身份证核实其身份。必须按照验证局提出的要求，以可信的方式，生成和保存与第三类证书所载公用钥匙相配的私人钥匙。这类证书实际上用于某种电子商业用途，如电子金融、电子数据交换以及会员联机服务。第三类证书的方法是利用各种程序，取得经鉴定的个别订购者身份的证据。同第二类证书相比，这些有效程序能够提供证实申请人身份的更加可靠的保证。

57. 上述事例表明，只有第三类证书属于统一规则现有范畴。工作组似宜讨论一下，统一规则是否应当扩大范围，以涵盖较低的各类证书。在此情况下，需要就各类证书的各种法律效力，特别是验证局对低级证书的签发应负多大责任做出决定。不然，统一规则所列“证书”定义需加修改，以表明统一规则不涵盖低级证书。

第 9 条. 验证做法说明

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。

参考

A/CN.9/437,第 60 - 62、 70、 110 - 111 和 149 段（ J 条草案）；
A/CN.9/WG.IV/WP.79， 第 89 段.

说明

58. 正如证书所证明的，依赖证书的任一当事方能在多大程度上信赖一个人与公用钥匙之间的联系，这取决于若干因素．这些因素包括验证局在对成对钥匙持有人进行认证时所沿用的做法和程序、以及验证局业务方法、程序和安全控制．验证做法说明经常由现有验证局提供，这些验证局将此说明作为促使人们更加相信其所签发的证书的可靠性的主要因素之一，更概括地讲，是将此说明视为应当支配验证局与其委托人之间关系的质量和责任的标准。

59. 验证做法说明是验证局对它所奉行的政策以及它在工作中及为了支持签发、管理和废止证书而采用的做法，程序和系统的详情所作的一种说明．验证做法说明所涉专题可包括：(1)用于认证证书申请人身份的程序（在签发证书前）；(2)验证局为可靠履行生成钥匙、签发证书、废止证书、进行审计和保存档案的职能所采用的实物、程序和人员的控制措施；(3)验证局为保护其加密钥匙而采取的安全措施；和(4)任何有关的资料．这些问题对取得证书的持有人和将验证局签发的证书用作与持有人进行交易的基础的依赖当事方都至关重要。

60. 验证做法说明可采取各种形式，如涉及所有有关各方的合同，或向所有有关各方发出的公告．但是，主要内容是向依赖当事方发出的通知．验证做法说明应当成为验证局向所有依赖当事方（包括持有人）发出的，说明验证局在签发、管理和废止证书时所采用的各种做法的通知。

第 10 条. 证书签发陈述

备选条文 A

(1) 验证局签发证书，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) 据验证局所知，证书内没有删略任何已知的而且会对上述陈述具有不利影响的重要事实（如果已知的话）.

(2) 根据第(1)款，签发证书的验证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) 验证局签发证书，是要向持有人以及[善意]地和在证书有效期间依赖证书所载资料的任何人陈述:

(a) 验证局已经[办理][核可][签发]了证书，并将按如下各项，必要时管理和废止证书:

㈠ 上述规则;

㈡ 证书签发的任何其他适用的准据法律；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) 验证局已按证书或任何适用的验证做法说明申述的程度证实了持有人的身份，或在缺少验证做法说明的情况下，验证局以一种[可靠][可信]的方式证实了持有人的身份;

(c) 验证局已证实，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) 据验证局所知，除证书或任何适用的验证做法说明所规定的外，截至证书签发之日，证书所载所有其他资料均准确无误;

(e) 如果验证局公布了证书，则证书所确认的持有人已收到证书.

[(2) 如果某个验证局依照另一法域的法律签发了证书，它还要根据证书签发的准据法律，提供在其他方面适用的所有保证和陈述，如果有的话].

参考

A/CN.9/437,第 51 - 73 段（H 条草案）;

A/CN.9/WG.IV/WP.71，第 70-72 段.

说明

61. 第 10 条草案旨在反映工作组做出的如下决定，即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所产生的赔偿责任的条款（A/CN.9/437，第 55 段）. 该条草案所规定的最低限度赔偿责任标准只适用于按第 4 条草案规定，为数字签字的目的签发的证书. 统一规则草案不试图处理验证局可能从事的其他活动或服务. 此类活动或服务可能受验证局与其客户达成的合同安排制约，也可能受任何其他适用法律的制约（同上，第 71 段）.

62. 在其第三十一届会议上，工作组普遍一致认为，根据备选条文A第(1)款内容所使用的措词大部分在实质上可以接受，可作为今后讨论的基础。尽管第(1)款未明确规定一项有关赔偿责任的规则，但它确定了一项各当事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，如果与上述要求相抵触，那么它就不得被视为属于统一规则提供的任何保护或利益的范围。如果验证局被指称应承担赔偿责任，验证局就会被推定须为签发证书承担后果，除非验证局可以证明它符合第(1)款所列要求。但是，如果验证局希望承担比第(1)条所列陈述更为严格的义务，则应容许其这样做，办法是在一份验证做法说明中列入有关条款，或以其他方式作出此种规定（A/CN.9/437，第70段）。第（2）款旨在处理验证做法说明将载列此类更加严格的标准的情况。

63. 备选条文B虽是由备选条文A引出的，但它更着重强调验证局的自律。特别是，在(b)项中，验证局不保证持有人合法持有私人钥匙。相反，验证局要保证，为了将持有人与私人钥匙联系在一起，它至少遵循了其验证做法说明中提出的程序，或采用了“可靠”或“可信”的方法鉴别持有人。备选条文第(2)款表明，第(1)(a)(二)款还适用于根据另一法域的法律签发证书的情况。工作组似宜决定是在统一规则中还是在一项指南或评注中应作此澄清。

第11条. 合同责任

(1) 就签发证书的验证局与证书持有人[或与验证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，则该验证局无权限定其赔偿责任。

参考

A/CN.9/437，第51－73段（H条草案）；

A/CN.9/WG.IV/WP.71，第70－72段。

说明

64. 第(1)款重申了适用于验证局的赔偿责任制度方面的当事方自主原则。第(2)款涉及公认的免责条款问题，这类条款包括两项例外。第一项例外是根据第10条的提法确定的，该条草案旨在确定一项验证局不得违背的最低限度标准（见上文第58段）。第二项例外是根据统法社关于国际商业合同的原则（第7.1.6条）确定的，以提供一项评估免责条款的普遍接受性的统一标准。还可指出，关于限定或免除赔偿责任是“完全不

公正的”的提法表明，免责条款采用了一种灵活的方法．这一方法有可能使限定和免责条款比如果统一规则仅提及统一规则范围以外的适用法律而会出现的情况得到更加广泛的承认．

65. 第(3)款涉及验证局及其代理人的故意渎职行为将会造成损失或其他损害的情况．建议的规则的实质内容是根据许多国际运输公约使用的、以及最近在《国际法委员会国际贷记划拨示范法》第 18 条中使用的类似措词确定的．

第 12 条．验证局对依赖证书的各当事方的赔偿责任

(1) 在无相反协议的情况下，签发证书的验证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) [不是][疏忽]遵守如下程序所造成的[后果]:

㈠ 验证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，或验证局或其代理人无法采取此类措施，则该验证局不负赔偿责任．

(3) 尽管第(1)款有规定，但验证局可在证书中[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，验证局概不负赔偿责任．

(4) 尽管第(1)款有规定，但验证局可在证书中[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，验证局不负赔偿责任．

参考

A/CN.9/437，第 51 - 73 段（H 条草案）

A/CN.9/WG.IV/WP.71，第 70 - 72 段．

说明

66. 第 12 条草案旨在反映上届会议所表述的观点，即统一规则应当载有一项确定可反驳的赔偿责任推定的规则．例如，根据此规则，如果验证局对一个人作出错误的鉴别，或错误地将公用钥匙归属一个人，则应对任何受害方的损失承担责任，除非验证局能够证明，它已尽了最大努力避免此类错误．这种赔偿责任机制旨在增加对使用验证局服务的任何人的保护，但不会让验证局承担严格赔偿责任(见 A/CN.9/437，第 58 段）．

67. 在讨论第 10 条至 12 条时，工作组似宜审议验证局的赔偿责任是否应有限度和如何确定这些限度的问题（见 A/CN.9/437，第 63 - 67 段）．在上届会议上，工作组就限制验证局的赔偿责任数额可能采取的方法，对各种建议进行了讨论．一种可能的方

法是确定一个固定数额．建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、或受害方实际损失的某一百分比．但是，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，不可能作为计算赔偿责任固定数额的客观标准．再说，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，同时也与各方可能遭受的损失无关（同上，第 66 段）．至于对验证局的情况与适用于运输货物和运载旅客的国际公约所涉承运人的情况进行拟议的比较问题（同上，第 67 段），对这些案文的初步审查表明，责任限度一般是采用固定数量（如，运载旅客），并有可能根据所运货物价值确定的．工作组有必要在下届会议上，根据秘书处的进一步研究，对此问题进行审议．

第 13 条．证书的废止

(1) 在证书有效期间，如果签发证书的验证局收到如下请求或证明，则必须依照适用的验证做法说明规定的有关废止的方法和程序，或在没有这类方法和程序的情况下，立即废止证书:

(a) 收到证书所确认的持有人提出的废止请求，并证实请求废止的人就是（合法的）持有人，或是有权提出废止请求的持有人的代理人;

(b) 收到作为自然人的持有人已经死亡的可靠证明;

(c) 收到作为法人实体的持有人已经解散或已不再存在的可靠证明．

(2) 如果经证实的成对钥匙的持有人了解到私人钥匙已经遗失、失密或有被作其他方面滥用的危险，则持有人有废止相应证书的义务．如果持有人在此种情况下未能废止该证书，对于因持有人未能采取这种废止行动而使依赖电文内容的第三方遭受的任何损失，持有人应负责赔偿．

(3) 无论证书所列持有人是否同意废止，签发证书的验证局必须在了解到如下情况后立即废止证书:

(a) 证书所述重要事实是虚假的;

(b) 验证局的私人钥匙或信息系统失密影响了证书的可靠性；或

(c) 持有人的私人钥匙或信息系统失密．

(3) 在根据第(3)款废止证书后，验证局必须按照适用的验证做法说明规定的废止通知办法和程序，通知持有人和依赖当事方，或在缺少此类办法和程序的情况下，如果证书已经公布，必须立即通知持有人，并立即公布废止通知，还须在依赖当事方查询日时，另行披露废止事实．

(4) [就持有人与验证局之间而言]，废止自验证局[收到][登记]时起生效．

[(5) 就验证局与任何其他依赖当事方之间而言，废止自验证局[登记][公布]时起生效．]

参考

A/CN.9/437，第 125 - 139 段（F 条草案）；

A/CN.9/WG.IV/WP.71，第 66 - 67 段.

说明

68. 第 13 条草案旨在反映工作组上届会议所表述的各种观点，提出一项有关证书废止的缺省标准. 但是，验证局随时都能通过在其验证做法说明中规定废止程序和实施此类程序，来避免缺省标准. 就废止生效的时间，工作组拟宜决定是否应对持有人的情况与任何其他依赖当事方的情况作出区分（见 A/CN.9/437，第 130 段）.

第 14 条. 证书的暂停使用

在证书有效期间，签发证书的验证局在收到它合理地相信是证书所列持有人的人或有权代表该持有人行事的人提出的暂停使用证书请求后，必须立即按适用的验证做法说明中规定的有关暂停使用的方法和程序，或在缺少此类方法和程序的情况下，暂停使用该证书.

参考

A/CN.9/437,第 133-135 段（F 条草案）.

说明

69. 工作组在上届会议上决定，统一规则应载有一项暂停使用证书的条款（见 A/CN.9/437，第 133 - 134 段）. 关于暂停使用的生效时间，工作组似宜决定是否应按第 13 条草案第(4)和(5)款内容增加一些条款.

第 15 条. 证书登记簿

(1) 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，其中表明各项证书到期的时间或暂停使用的时间或废止的时间.

(2) 在验证局签发的任何证书废止或有效期期满之日后，登记簿应由验证局保存

备选条文 A 至少[30][10][5]年

备选条文 B ...年[立法国规定了应在登记簿中保存有关资料的时间]

备选条文 C 根据验证局在适用的验证做法说明中规定的办法和和程序保存

参考

A/CN.9/437，第 140 - 148 段（G 条草案）；

A/CN.9/WG.IV/WP.71，第 68 - 69 段.

说明

70. 在上届会议上，无人对关于在统一规则中列入一项证书登记条款的原则提出异议（见 A/CN.9/437，第 142 段）．适当保留可以广泛查阅的登记簿（有时称作“储存库”）的功用，特别是证书废止清单（ CRL ），可视为确定数字签字可信度的一个重要因素．在研究由验证局保留此类登记簿和证书废止清单的方法时，工作组拟宜审议一下，依赖当事方在可以依赖证书的效力之前，是否有义务通过查询有关登记簿或证书废止清单，证实证书的状况．

71. 更概括地讲，工作组似宜讨论一下，统一规则除确定验证局运作最低限度标准外，是否还应涉及依赖证书各当事方的权利和义务．

第 16 条. 依赖证书各当事方与验证局之间的关系

[(1) 验证局只许请求提供鉴别用户所需的资料．

(2) 根据请求，验证局应当提供有关如下内容的资料:

(a) 可以使用证书的条件;

(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、储存和传递的方法或做法;

(e) 验证局关于依赖证书各当事方所使用的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，验证局向依赖证书各当事方发出警告的条件;

(g) 验证局赔偿责任的限度;

(h) 验证局对证书使用实施的任何限制;

(i) 持有人有权对证书使用实施限制的条件．

(3) 第(1)款所列资料应在最后验证协议缔结之前提供给用户．该资料可由验证局采用验证做法说明的方式提供．

(4) 根据[提前一个月]通知，用户可终止与验证局联系的协定．此终止通知在验证局收到时即生效．

(5) 根据[提前三个月]通知，验证局可终止与验证局联系的协定．此终止通知在收到时即生效．

参考

A/CN.9/437，第 149 - 150 段（ J 条草案）；

A/CN.9/WG.IV/WP.71,第 76 段．

说明

72. 工作组在其上届会议上指出，第 15 条所列各项内容应当放在方括弧内，并由工

作组在后一阶段审议（见A/CN.9/437,第150段）.

第四章. 对外国电子签字的承认

第17. 根据此类规则提供服务的外国验证局

备选条文A (1) 如果外国[人][实体]同可成为验证局的本国实体和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局，或在无当地机构的情况下，可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 ...[立法国规定，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.

参考

A/CN.9/437,第74-89段(I条草案);
A/CN.9/WG.IV/WP.71,第73 - 75段.

说明

73. 第17条草案允许外国实体成为验证局，只是说明不应歧视外国实体的原则，只要这些实体符合为本国验证局制订的标准. 尽管该项原则会得到普遍接受，但用它来说明验证局的问题尤为重要，因为预料验证局的工作不一定非要在其工作的国家建立一个实体或其他营业场所.

第18条. 本国验证局对外国证书的认可

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...[立法国法律]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度，保证该证书细节正确无误及其有效.

参考

A/CN.9/437,第74-89段（I条草案）;
A/CN.9/WG.IV/WP.71,第73 - 75段.

说明

74. 第 18 条草案使本国验证局能够按与其自身的证书相同的程度，保证外国证书细节正确无误及其有效．在工作组上届会议上，该条所涉事项称为“交叉验证”．第 18 条草案主要载有一项条款，规定在发现外国证书有缺陷时，由本国验证局分担赔偿责任（见 A/CN.9/437,第 77 - 78 段）．

第 19 条．对外国证书的承认

(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...[立法国法律]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...[立法国法律]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，政府机构仍可规定[以公布的方式]，在利用某一特定验证局、某一类验证局或某一类证书时，必须结合向这些机构提交的电文或签字．

参考

A/CN.9/437,第 74-89 段(I 条草案);
A/CN.9/WG.IV/WP.71,第 73-75 段．

说明

75. 第 19 条草案提到了在工作组上届会议上被称为“跨界承认”的事项(见 A/CN.9/437,第 77-78 段)．第(1)和(2)款述及了可在进行任何交易(以及就签字的可靠程度发生任何争端)之前确定外国证书和签字可靠性的方法．第(3)款订立了在未预先确定外国签字和证书可靠性的情况下，对这类签字和证书进行评估的标准．第(4)款保留政府机构确定用于与其进行电子通信的程序的权利．

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．