



联合国国际贸易法委员会
电子商务工作组
第三十五届会议
1999年9月6日至17日，维也纳

电子签字统一规则草案

秘书处的说明

目 录

	段 次	页 次
导言	1—12	2
一. 一般说明.....	13—20	3
二. 电子签字条文草案.....	21—71	4
第 1 条. 适用范围.....	21	4
第 2 条. 定义.....	22—33	5
第 3 条. [不歧视][不偏重某一技术].....	34	9
第 4 条. 解释.....	35	10
第 5 条. 经由协议的改动.....	36—40	10
第 6 条. [符合签字要求][推定签字].....	42—44	11
第 7 条. [推定原件].....	45	13
第 8 条. [强化]电子签字的确定.....	46	13
第 9 条. 签字持有人[责任][义务].....	50—55	14
第 10 条. 对强化电子签字的依赖.....		18
第 11 条. 对证书的依赖.....	56—58	18
第 12 条. 信息验证人的[责任][义务].....	59—68	20
第 13 条. 对外国证书和签字的承认.....	69—71	30

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局问题列入其议程。委员会请电子商务工作组审查就这些议题编写统一规则的可取性和可行性。会议议定，拟编写的统一规则应处理下列各项问题：支持验证过程的法律根据，包括正在出现的数字认证和验证技术；验证过程的适用性；使用验证技术情况下的用户、提供者和第三方的风险和赔偿责任分配；通过使用登记处进行验证的特殊问题；和以提及方式纳入条款。¹
2. 委员会第三十届会议（1997 年）收到了工作组第三十一届会议的报告（A/CN.9/437）。工作组向委员会表明，它已就努力实现这方面的法律协调的重要性和必要性达成了协商一致意见。工作组虽然尚未就这一工作的形式和内容作出明确决定，但已得出初步结论认为，至少就数字签字和验证局问题，以及可能时还就有关问题进行统一规则的编写工作是可行的。工作组回顾说，在处理数字签字和验证局问题的同时，电子商务方面的未来工作可能也需要解决：公共钥匙加密的技术替代问题；第三方服务提供者所履行职能的一般性问题；以及电子订约问题（A/CN.9/437，第 156-157 页）。
3. 委员会核可了工作组达成的结论，并委托工作组编写与数字签字和验证局法律问题有关的统一规则（下称“统一规则”）。关于统一规则的确切范围和形式，委员会总的认为，在目前这一过程的早期阶段尚不能作出决定。有人认为，虽然说考虑到公共钥匙加密在新出现的电子商务实践中显然发挥着主要作用，工作组将注意力放在数字签字问题上也许是适宜的，但统一规则应当同《贸易法委员会电子商业示范法》（《示范法》）中的不偏重任何媒体的方针相一致。因此，统一规则不应妨碍其他认证技术的使用。而且，在处理公共钥匙加密问题时，统一规则可能需要照顾到不同层级的安全，并要承认与数字签字环境下各种类型的服务相应的各种法律效力和赔偿责任水平。关于验证局问题，虽然委员会承认以市场为驱动的标准的价值，但又普遍认为，工作组似宜设想确立一组应由验证局达到的最低标准，特别是在寻求跨境验证的情况下。²
4. 工作组第三十二届会议着手根据秘书处编写的一份说明（A/CN.9/WG.IV/WP.73）编写统一规则。
5. 委员会第三十一届会议（1998 年）收到了工作组第三十二届会议的工作报告（A/CN.9/446）。委员会注意到，工作组在整个第三十一届和第三十二届会议期间都遇到了明显的困难，难以就数字签字和其他电子签字日益普遍使用而引起的新的法律问题达成共同理解。委员会还注意到，关于如何在国际公认的法律框架内解决这些问题，尚待寻求协商一致的意见。然而，委员会总的认为，迄今所取得的进展表明，电子签字统一规则草案正在逐步形成一种可行的结构。委员会重申其第三十一届会议作出的关于拟订这类统一规则可行性的决定，并表示坚信工作组第三十三届会议可在秘书处编写的订正草案的基础上取得更大的进展。根据上述讨论，委员会满意地注意到工作组已被普遍看作是就有关电子商务所涉法律问题交换意见并拟订这类问题的解决方案的一个极为重要的国际论坛。³
6. 在其第三十二届会议上，委员会收到了工作组第三十三届（1998 年 7 月）和第三十四届（1999 年 2 月）会议的工作报告（A/CN.9/454 和 457）。委员会对工作组在编拟电子签字统一规则草案方面完成的工作表示赞赏。尽管普遍认为这两届会议在对电子签字的法律问题的理解方面取得了很大进展，但仍然感到，工作组在统一规则应以何种立法政策为依据方面仍难以达成共识。
7. 一种意见认为，工作组目前采取的做法并没有充分反映出商务中对使用电子签字和其他认证技术的灵活性的需要。根据工作组目前的设想，统一规则过份侧重于数字签字技术，而在数字签字范围内，又过于注重涉及第三方验证的某一特定应用。因此，建议工作组在电子签字上的工作要么只局限于跨境验证方面的法律问题，要么干脆推延到市场惯例更好地确立起来后再说。与此相关的一种意见是，为了进行国际贸易，由于使用电子签字而引起的法律问题多数都已经在《贸易法委员会电子商业示范法》中得到了解决。对于电子签字的某些应用，也许应当在商法范围之外订立法规，工作组不应卷入任何此种法规的规范活动。
8. 广泛一致的意见是，工作组应继续在其原来授权任务的基础上进行工作（见上文第 3 段）。关于电子签字统一规则的必要性，据解释，在许多国家，政府或立法当局目前正在就电子签字问题制定法规，包括建立公共钥匙基础设施或涉及密切相关事项的其他项目，它们期待着得到贸易法委员会的指导（见 A/CN.9/457，第 16

段)。关于工作组作出的侧重公共钥匙基础设施问题及公共钥匙基础设施术语的决定，据回顾，明显有区别的三类当事方（钥匙持有人、验证局和依赖方）之间相互关系和作用相应于一个可能的公共钥匙基础设施模式，但仍可设想其他模式，例如，并不涉及独立验证局的情况。侧重于公共钥匙基础设施问题的主要好处之一是，便于按照成对钥匙的三种功能（或作用）来设计统一规则的结构，这三种功能分别为：钥匙签发人（或订户）功能、验证功能和依赖功能。普遍认为这三种功能是所有公共钥匙基础设施模式所共有的。还一致认为，处理这三种功能时，应不论其事实上是否分别由三个单独实体来履行，还是由同一人来发挥其中两种功能（例如，验证局同时也是依赖方）。此外，大家广泛认为，只侧重于公共钥匙基础设施特有的功能而不侧重任何特定模式也许会在稍后阶段更容易编拟出一个完全不偏重任何媒体的规则（同上，第 68 段）。

9. 经讨论，委员会重申其先前作出的关于编拟此种统一规则的可行性的决定（见上文第 3 和 5 段），并表示相信，工作组会在以后各届会议中取得更大进展。

10. 本说明载列了根据上文所述工作组的讨论和决定以及委员会第三十二届会议的讨论和决定编写的订正条文草案。它是用来反映工作组第三十四届会议所作出的决定。新修订的条文用下划线表示。

11. 根据适用的有关更加严格控制 and 限制联合国文件的指示，对条款草案作了尽可能简明扼要的解釋性说明。本届会议上将口头作出附加说明。

国家立法和其他文书参考资料

12. 为了提供资料 and 进行比较，在一些条文中在本标题下以小字体载列了一些国家的立法和其他文书参考资料。所列入的国家立法参考资料是秘书处知道的而且能获得供参考的那些法规。所列入的其他文书参考资料是一些由国际组织订立的文书或众所周知、能普遍能获得的那些文书。所用的简称是指下列立法和文书：

- 德国 1997 年数字签字法（信息和通信服务法令，第 3 条，1997 年 6 月 13 日批准；1997 年 8 月 1 日生效）；
- 伊利诺伊 美国，1998 年电子商务安全法令（1997 年伊利诺伊州议院法案 3180； 5 Ill. Comp.Srat. 175，1998 年 8 月颁布）；
- 明尼苏达 美国，电子认证法令（明尼苏达州法规第 325 号，1997 年 5 月颁布）；
- 密苏里 美国，1998 年数字签字法令（1998 年 SB 680，1998 年 7 月颁布）；
- 新加坡 1998 年电子交易法令，1998 年法令第 25 号；
- 美国律师协会指导原则 美国律师协会，科学技术科，“数字签字指导原则”，1996 年；
- 欧委会指令草案 欧洲议会和欧洲联盟委员会关于电子签字共同框架的指令草案，1999 年 (7015/99)；
- 数字式受保通用法 国际商会，“国际数字式受保商务通用法”，1997 年。

一. 一般性说明

13. 正如本说明第二部分所载条款草案所表明的那样，统一规则旨在促进在国际商务活动中进一步使用电子签字。这些条款草案借鉴了在一些国家已经生效或现正编写的诸多法律文书，通过提出一套标准据以在验证局的可能协助下确认数字签字和其他电子签字的法律效力，从而防止适用于电子商务的法律规则出现不一致的情况。关于验证局，另规定了若干规则。

14. 统一规则侧重商业交易的私法方面，而不力求解决在进一步使用电子签字的情况下产生的所有问题。特别是，统一规则不涉及国家立法者在制订电子签字综合法律框架时可能需考虑的公共政策、行政法、消费者保护法或刑法等方面。

15. 根据《示范法》，统一规则尤其要反映如下几点：不偏重任何媒体的原则；不歧视功能等同的传统书面票据的概念和做法；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(即各当事方在利用电子手段进行通信时，均受预先制订的合同规则和程序的制约)下的缺省规则。

16. 在审议拟列入统一规则的条款草案时，工作组似宜更加全面地考虑统一规则与《示范法》之间的关系。本统一规则草案是以它们将构成一项单独的法律文书为基础编拟的。增加了两条新条文以反映《示范法》所载的条款——第 1 条(适用范围)和第 4 条(解释)。涉及消费者的交易没有专门排除在统一规则的适用范围之外，但在第 1 条草案案文中列入了《示范法》的脚注，用以澄清统一规则无意推翻国家法律中关于保护消费者问题的任何规定。

17. 工作组似宜考虑，序言部分是否应明确统一规则的目的，即通过建立一种安全框架并使书面电文和数字电文具有同等法律效力而促进电子通信的有效运用。

18. 工作组第三十三届会议对使用“强化”或“可靠”一词来描述可提供比一般“电子签字”具有更高度可靠性的签字技术的做法是否妥当表示怀疑(A/CN.9/454, 第 29 段)。工作组认为，在没有更合适的术语情况下，应保留“强化”这个词。在第三十四届会议上(A/CN.9/457, 第 39 段)，据认为，一旦明确了处理两类电子签字的目的，特别是两类电子签字的法律效力之后，对“强化电子签字”的定义可能需要结合统一规则的总体结构重新加以审议。有人建议，只有当统一规则要提供一种与手书签字的特定用途同等的功能时，才来处理提供高度可靠性的电子签字问题，这是合理的。由于要在国际上这样做可能特别困难，而对国际商务交易来说又意义不大，可能需要进一步澄清使用“强化电子签字”与单单使用“电子签字”相比预期将得到的额外好处。

19. 鉴于对是否需要“强化电子签字”这一类别的讨论情况，本统一规则订正草案列入了一个替代做法供工作组讨论。在第 2(b)条草案中，“强化电子签字”的定义加上了方括号。在第 2 条下面列入了关于可能如何修订该项定义的说明。第 6、7 和 8 条草案载列了该项定义的有关部分以作为替代性的实质性条款。这一替代做法的目的是协助工作组确定是否应当不提及电子签字和强化电子签字这两种签字，这样，统一规则将仅处理一种电子签字类型。关于具体建议的说明放在各有关条文后。

20. 本统一规则订正草案扩大了它的适用范围，超出了对形式有法律要求或法律对不满足某些条件(例如签字或原件)规定了后果这些情形。为此，统一规则的范围可能要比《示范法》的范围大，虽然第 6 条草案确实包括了《示范法》第 7 条的形式要求。工作组适宜考虑统一规则这一比较大的适用范围。

二. 电子签字条文草案

第 1 条. 适用范围

本规则适用于商务*关系中使用的电子签字，它不得凌驾于任何旨在保护消费者的法律之上。

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

A/CN.9/457, 第 53—64 段。

说明

21. 第 1 条草案最初是在工作组第三十四届会议上作为一条关于当事方自主权的条文的第 1 款提出的(E 条草案, A/CN.9/457, 第 55 和 60 段)。由于这项规定更适当地处理了统一规则的范围问题, 所以在本草案中将它放在“适用范围”标题下单立一条。如工作组商定的那样(A/CN.9/457, 第 64 段), 第 1 条草案包括一个脚注, 脚注重复了《电子商业示范法》第 1 条中的“商务”的定义, 第 1 条草案还采用了《示范法》中脚注**关于保护消费者的措辞。本条中加入了“在…中使用的电子签字”, 以便更精确地界定统一规则的主题事项。

第 2 条. 定义

就本规则条文而言:

(a) “电子签字”系指[在数据电文中, 以电子形式所含、所附或在逻辑上与数据电文有联系的数据, 和][与数据电文有关系的任何方法], 它可用于鉴别与数据电文有关的签字持有人和表明此人认可数据电文所含信息;

[(b) “强化电子签字”系指一种电子签字, 对于这种电子签字, 通过使用一种[安全程序][方法]可以表明该签字:]

(一) [就其使用目的而言][在其使用范围内], 对签字持有人而言是独一无二的;

(二) [不是由任何其他入而是]由签字持有人或以签字持有人单独掌握的方法所制造并附于数据电文中;

[(三) 其制造及与有关数据电文的连接方式对电文的完整性提供可靠的保证:]

(c) “证书”系指由信息验证人签发的某一数据电文或其他记录, 用以确定持有[一对]特定[钥匙][签字装置]的个人或实体的身份;

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

(e) “签字持有人”[装置持有人][钥匙持有人][订户][签字装置持有人][签字人] [签署人]系指由本人或委托他人制造强化电子签字并把此种签字附于某一数据电文之内的个人;

(f) “信息验证人”系指在其业务范围内为促成使用[强化]电子签字而从事[提供鉴别服务] [验证信息]的个人或实体。

贸易法委员会文件参考资料

A/CN.9/457, 第 22—47、66—67、89、109 段;

A/CN.9/WG.IV/WP.80, 第 7—10 段;

A/CN.9/WG.IV/WP.79, 第 21 段;

A/CN.9/454, 第 20 段;

A/CN.9/WG.IV/WP.76, 第 16—20 段;

A/CN.9/446, 第 27—46 段 (第 1 条草案)、第 62—70 段 (第 4 条草案)、第 113—131 段 (第 8 条草案)、第 132—133 段 (第 9 条草案) ;

A/CN.9/WG.IV/WP.73, 第 16—27、37—38、50—57 和 58—60 段;

A/CN.9/437, 第 29—50 和 90—113 段 (A、B 和 C 条草案) ; 和

A/CN.9/WG.IV/WP.71, 第 52—60 段。

说明

“电子签字”的定义

22. 根据工作组第三十四届会议的决定(A/CN.9/457, 第 23—32 段) 对电子签字的定义作了修订。列入方括号中的文字“[与数据电文有关的任何方法]”是为了使统一规则中定义的文字与《示范法》第 7 条的文字一致。

“强化电子签字”的定义

23. 根据工作组第三十四届会议的决定(A/CN.9/457, 第 23—32 段)对“强化电子签字”的定义作了修订,以便在(b)(三)项中列入置于方括号内的文字,作为数据电文的强化签字与该数据电文所含信息之间的必要联系,具有完整性的功能。工作组似宜考虑是否应当将完整性作为强化电子签字定义的一部分加以列入,还是作为一种概念,如《示范法》第 8 条和统一规则第 7 条草案那样,它与原件的意思更加有关。这次修订中略去了第(二)项中原先包含的文字“可用于客观地鉴别与数据电文有关的签字持有人”,这是因为它是(a)项“电子签字”定义的一部分。

24. 在(b)项的起始句中,使用了“方法”一词作为对使用“安全程序”的替代,以便使该用语与《示范法》的用语更加接近。

25. (b)(三)项中将“不是由任何其他他人而是”文字置于方括号内,这是因为插入这些文字会引起一系列问题。首先,在强化电子签字的定义中插入这些文字会意味着任何不是由签字持有人制造并附于数据电文中的签字(因而可能是未经授权的)不是一个强化电子签字。这种解释可能会具有将这种签字排除出统一规则某些条文例如第 8、9 和 10 条草案的范围之外的效果。特别是,第 9 条草案中关于签字装置失密的责任问题的那些部分是否适用可能不能确定。

26. 其次,插入这些文字将要求,为了使某一种安全程序或方法成为强化电子签字,它必须能够表明该签字确实是由签字持有人制造和附于电文的。由于对某些技术来说这也许不可能,列入这样一项要求可能意味着在使用签字装置的同时还需要使用身份鉴别器,例如使用生物测定法或其他一些此类技术。

27. 在(b)(三)项中工作组适宜考虑的再一个问题是“单独掌握”的要求与规定共同掌握的第 9 条草案第 2 款之间的关系。在下文“签字持有人”的定义中也有这个问题。

28. (b)(三)项中“合理的保证”一语改成了“可靠的保证”以便于《示范法》第 8 条的用语一致。

“证书”的定义

29. 为了完整起见,在统一规则中列入了关于“证书”的定义。这项定义的基础是 A/CN.9/WG.IV/WP.79 中关于“身份证书”定义,虽然在统一规则中不再将其称为“身份证书”。工作组似宜考虑是否可以出于以下要求将方括号内的文字“或其他重要特征”删除。身份这个概念可能不仅仅是签字持有人的姓名,还可能指其他重要特征,例如职位或权力,它可以与姓名一起使用也可以不提及姓名。据此,将没有必要区分身份和其他重要特征,也没有必要将统一规则限于仅使用指明签字持有人姓名的身份证书这些情形。关于对“身份”含义的其他看法,参

见 1999 年 6 月 2 日至 4 日在加利福尼亚举办的经合组织—私营部门电子认证联合讲习班“关于电子认证技术手段和问题的背景文件”，第 6 至 9 页。

30. 工作组似宜考虑“确认身份”是否妥当，因为证书实际上可能并不确认签字持有人的身份，而是通过某些程序来确定签字持有人并证明其身份是与证书中所列的签字装置或共用钥匙相连接的。为了确保统一规则不偏重于任何技术手段，工作组还似宜考虑使用“签字装置”之类的不偏重某一技术手段的措辞以替代“一对特定钥匙”，因为“一对特定钥匙”专指数字签字。当证书仅在数字签字环境中使用时，相对于“证书”的定义使用“一对钥匙”一语可能是妥当的。

“数据电文”的定义

31. 为了完整起见，在统一规则草案中列入了关于“数据电文”的定义。工作组似宜考虑鉴于统一规则与《示范法》的关系，是否需要列入这项定义。

“签字持有人”的定义

32. 工作组在其第三十四届会议上没有结束它对“签字持有人”定义的讨论(A/CN.9/457,第 47 段)。现在的修订定义在方括号内包括了工作组认为可能比“签字持有人”更恰当的一些用语。如第 27 段所述，这项定义可能需要结合上文(b)(二)项关于“强化电子签字”的定义和第 9(2)条草案加以审查。

“信息验证人”的定义

33. 工作组上一届会议上没有审议这项定义，因此未作任何改动加以保留。然而，鉴于早先的讨论(A/CN.9/457,第 109 段)，工作组似宜考虑“信息验证人”定义中的“在其业务范围内”，是应当解释为意指与验证有关的活动应当是信息验证人的专属业务活动，还是为了将信用卡公司签发证书这类情况包括在内，也应当将签发证书仅是一实体业务的附带组成部分这类情形也包括在内。

国家立法和其他文书参考资料

美国律师协会指导原则

第 1 部分：定义

1.5 证书

一份电文，它至少

- (1) 确定签发该电文的验证局，
- (2) 列出其订户的姓名或身份，
- (3) 含有该订户的公共钥匙，
- (4) 确定使用期限，和
- (5) 有签发该电文的验证局的数字签字。

1.6 验证局

签发一证书者。

1.27 依赖方

收到一证书和电子签字、能借助该证书中所列公共钥匙对该证书和电子签字加以核查而且能够依赖该证书和电子签字者。

1.30 签字人

为一电文制造一电子签字者。

1.31 订户

某人

- (1) 其姓名或身份在向其签发的证书中被确定，和
- (2) 持有与该证书所列公用钥匙相配的私人钥匙者。

欧委会指令草案

第2条

定义

为了本指令的目的：

1. “电子签字”系指附于或逻辑上与其他电子数据有关的并将用作一种认证方法的电子形式的数据。
 - 1a. “高级电子签字”系指满足以下要求的电子签字：
 - (a) 它与签署人有独特的连接；
 - (b) 它能够确定签署人；
 - (c) 它是利用签署人能对其进行单独控制的手段制造的；和
 - (d) 它与有关数据的连接方式能查出随后对该数据所作的任何改动。
 2. “签署人”系指持有签字制造装置且代表自己或者代表其所代表的人或实体行事者。
 3. “签字制造数据”系指代码或私人密码钥匙等独特的数据，供签署人在制造电子签字时使用。
 - 3a. “签字制造装置”系指经过配置的、用来执行签字制造数据的软件或硬件装置。
 - 3b. “安全签字制造装置”是符合附件三各项要求的签字制造装置。
 4. “签字核查数据”系指在核查电子签字时使用的代码或公共加密钥匙等数据。
 - 4a. “签字核查装置”系指经过配置的、用来执行签字核查数据的软件或硬件装置。
 - 4b. “证书”系指将某一签字核查数据与某人连接起来并确认该人的身份的电子证明。
 5. [……]
 6. “验证服务提供者”系指签发证书或提供与电子签字有关的其他服务者。

德国

§2 定义

- (1) 本法所指的数字签字是用私人签字钥匙制造的数字数据上的印记，借助该印记，通过使用附有§3中所述验证人或验证局签字钥匙证书的相关公共钥匙，能够确定该签字钥匙的所有人和数据是否已被篡改。
- (2) 本法所指的验证人是一个自然人或法人，他证明公共签字钥匙归属某自然人并持有§4中所述的许可证；
- (3) 本法所指的证书是关于某一公共签字钥匙归属某一自然人并附有一电子签字的电子证明(签字钥匙证书)，或者明白无误地提及签字钥匙证明并载有其他信息的特别数字证明(属性证书)。

数字式受保通用法

六. 术语

2. 证书

由某人担保的电文，该电文证明对另一人行为的法律效力有重大影响的事实的准确性。

4. 验证人

签发证书并为此证明对另一人行为的法律效力有重大影响的事实的准确性者。

12. 公共钥匙证书

为其订户确定一把与该订户所持私人钥匙相配的公共钥匙的证书。

14. 订户

作为证书的主体者。

伊利诺伊

第 5 条. 电子记录和签字总则

第 5—105 节. 定义

“证书”系指一份记录，它起码：**(a)**确定签发该证书的验证局，**(b)**确定其订户的姓名或身份或者由该订户控制的某一装置或电子工具；**(c)**含有与该订户控制的某一私人钥匙相配的公共钥匙；**(d)**具体规定其使用期限；和**(e)**有签发该证书的验证局的数字签字。

“验证局”系指授权和促使签发证书者。

“电子签字”系指附于某一电子记录或与其有逻辑关联的电子形式的签字。

“签字装置”为制造归属于某一特定个人的电子签字而单独或与其他信息或装置一起需要的独特信息，例如代码、算法、字母、数字、私人钥匙或个人识别号码(PINS)或者一具配置独特的实体装置。

新加坡

第 1 部分.第 2 节. 解释

“证书”系指为了佐证数字签字而签发的、拟用来确认某一特定配对钥匙持有者的身份或其他重大特点的记录；

“验证局”系指签发证书的人或组织；

“电子签字”系指附于某一电子记录或与其有逻辑关联的任何字母、字、数字或其他数字形式的符号，拟在认证或核准该电子记录时执行或采用；

“配对钥匙”在非对称密码系统中系指一把私人钥匙和与其有数学相关性的公共钥匙，具有的性能是该公共钥匙能核查由该私人钥匙制造的数字签字；

“私人钥匙”系指一配对钥匙中用来制造数字签字的钥匙；

“公共钥匙”系指一配对钥匙中用来核查数字签字的钥匙；

“订户”系指在向其签发的证书中确定了其姓名或身份并持有一把与该证书中所列某一公共钥匙相配的私人钥匙者。

第 3 条. [不歧视][不偏重任何技术]

[不得适用本规则中的任何规定][不得适用本规则中的各项规定]来排斥、限制或剥夺符合[《贸易法委员会电子商业示范法》第 7 条]要求的任何[签字]方法的法律效力。

贸易法委员会文件参考资料

A/CN.9/457, 第 53—64 段

说明

34. 第 2 条草案最初是在工作组第三十四届会议上作为关于当事方自主权条款的第 3 款提出的(E 条草案，

A/CN.9/457, 第 55、60 段)。由于第(3)款涉及的是歧视和不偏重任何技术的问题,而不是涉及当事方的自主权,本草案在“不歧视”和“不偏重任何技术”这两个备选标题下将其单独列为一条。“排除、限制或剥夺法律效力”字样取带了原来的“排斥、限制或歧视”,以便更直接地描述本项规定的宗旨和目的。提及《电子商业示范法》第 7 条即是提及在国家法律中颁布的该《示范法》。

第 4 条. 解释

- (1) 对本规则作出解释时,应考虑到其国际渊源以及在电子商务中促进其统一适用和遵守诚信的必要性。
- (2) 对于由本规则管辖的事项而在本规则内并未明文规定解决办法的问题,应按本规则所依据的一般原则解决。

说明

35. 第 3 条草案重复了《电子商业示范法》第 3 条,但增加了“在电子商务中”,列入这条是出于完整的考虑。工作组似宜考虑这样一个问题,即现在编拟的统一规则案文是否不应当成为《示范法》的组成部分,虽然它与《示范法》保留着明显的联系。如果工作组如此决定,第 3 条可以为法院和其他国家和地方当局解释统一规则提供指导。第 3 条的预期效果将是,在这一统一案文一旦被纳入地方立法之后,通过提及它的国际性质和渊源而不是通过仅仅提及地方法律的概念来促进对统一案文的解释。

第 5 条. 经由协议的改动

变式 A

[当事方可通过明示或默式的协议自行偏离或变更本规则的任何方面,][可通过明示或默示的协议偏离或变更本规则的任何方面,]但这种偏离或变更将会对第三方的权利产生有害影响的除外。

变式 B

- (1) 本规则概不影响可能存在的、以协议方式对第 6 和第 7 条所述任何法律规则作出修改的权利。
- (2) 可通过明示或默示的协议偏离和变更本规则第 9 至 12 条的任何方面,但这种偏离或变更将对第三方的权利产生有害影响的除外。

贸易法委员会文件参考资料

A/CN.9/457, 第 53—64 段

说明

36. 第 5 条草案变式 A 反映了工作组第三十四届会议上作出的这样一项决定,即列入一项规定,确保当事方可自行商定仅对作出如此商定的当事方之间的交易能够偏离或变更本规则的规定,以供今后讨论。但是,这种协议不得影响不参与该协议的当事方,即第三方的权利。这项自主权规定仅涉及本规则,它无意影响公共秩序或适用于合同的强制法,例如关于不公平合同的规定。

37. 变式 B 承认,以《示范法》第 7 和 8 条为基础的统一规则第 6 和 7 条草案的规定包括提及法律的要求,它可能是国家法律的强制性要求,不受经由协议的改动的约束。第(1)款允许经由协议的改动,如果国家法律

的这种强制性要求可以作如此改动的话。为此，它重复了《示范法》第4(2)条的措辞，因为它涉及的是同一问题。

38. 变式 B 第(2)款维持了当事方对第 9 至 12 条草案的完全自主权。拟订这条规定的依据是，第 9 至 12 条草案将是实质性的法律规则，在缔约当事方之间没有协议规定可以偏离或变更这些规定的适用时将适用。当事方将自行修改或选择不适用这些规定。第(2)款意在确保任何这种协议应用时不应损害第三方的利益，但不是要具有使当事方之间的协议任何部分均告无效的效力。

39. 除非有专门规定，处理跨境承认的规定将不受制于经有协议的改动。

40. 工作组似宜考虑第 5 条草案的措辞以及它在满足第 6 和 7 条草案中可能是法律强制性要求方面提出的问题。工作组还似宜考虑当事方自主权原则应如何适用于第 9 至 12 条草案。例如，这项规定可以确立缔约当事方之间没有相反协议时适用的缺省规则（“选出”）或可以确立当事方可以商定适用的规则（“选入”）。

关于第 6—8 条草案的总的说明

41. 工作组第三十四届会议在讨论统一规则的范围时(A/CN.9/457, 第 48—52 段)，决定将重点放在商务交易中目前正在使用的那些技术手段的规则，例如公用钥匙基础设施范围内的数字技术。因此，会议商定工作组应当在公用钥匙基础设施的范围内着重讨论 F 至 H 条草案（在本草案中为第 9 至 12 条）。对 A 至 D 条草案（在本草案中为 2、6、7 和 8 条）的讨论将推迟到 F 至 H 条审查完了之后。据指出，特别是 B 条草案（在本修订本中为第 6 条—符合签字要求）可在界定 F 至 H 条的适用范围方面起重要作用。另据认为，关于当事方自主权原则的 E 条（在本草案中为第 5 条—经由协议的改动），对于审议 F 至 H 条中当事各方的义务来说非常重要。

第 6 条. [符合签字要求][签字的推定]

变式 A

(1) 如对于一数据电文使用了强化电子签字，则推定该数据电文已经签字。

(2) 在法律规定需要某人的签字时，如果使用的电子签字根据各种情况，包括根据任何有关协议，既适合生成或传送数据电文所要达到的目的，而且也同样可靠，则对该数据电文而言，即满足了该项签字要求。

[(3) 在法律规定需要某人的签字时，如果使用了强化电子签字，则对该数据电文而言，即满足了该项签字要求。]

(4) 无论第(2)和第(3)款中提及的要求是否作为一项义务，或法律是否只规定了没有签字的后果，第(2)和第(3)款均适用。

(5) 本条规则不适用于下述情况：[···]。

变式 B

(1) 如对于一数据电文使用了[一种方法][一种电子签字]，而这种[方法][电子签字]能满足以下要求，则推定该数据电文已经签字：

(a) [为了它的使用目的][在它的使用]范围内，对签字持有人而言是独一无二的；

[(b) 可用于客观地鉴别与数据电文有关的签字持有人；和]

(c) [非有任何其他人而是]由签字持有人或使用完全处于签字持有人控制下的方法制造并附于数据

电文中；

- (2) 在法律规定需要某人的签字时，如果使用的电子签字根据各种情况，包括根据任何有关协议，既适合生成和传送数据电文所要达到的目的，而且也同样可靠，则对该数据电文而言，即满足了该项签字要求。
- (3) 无论第(2)款中提及的要求是否作为一项义务，或法律是否只规定了没有签字的后果，第(2)款均适用。
- (4) 本条规定不适用于下述情况：[···]。

贸易法委员会文件参考资料

A/CN.9.457，第 48—52 段

A/CN.9/WG.IV/WP.80，第 11—12 段

说明

变式 A

42. 变式 A 规定，如对于一数据电文使用了强化电子签字，可以推定该数据电文已经签字。第(2)款重述了《示范法》第 7 条中的原则，即电子签字如果能满足某些可靠性条件就满足了法律对签字的要求。工作组可以回忆，《示范法颁布指南》第 58 段列出了一些在确立适当的可靠性程度方面可以加以考虑的因素。第(3)款规定强化电子签字满足这些条件并为满足《示范法》第 7 条的要求建立了一条捷径，现加上方括号列入本草案。工作组适宜考虑鉴于已经有了第(1)款，本条规定是否仍然必要。

变式 B

43. 变式 B 的目的是要确定在只有一个电子签字类别情况下如何推定签字和满足法律对签字的要求。因此，它不提及“强化电子签字”。变式 B 第(1)款确定，如对一个数据电文使用了一种方法且该方法满足了某些要求，可以推定该数据电文已经签字。该方法需要满足第 2(b)条草案中“强化电子签字”定义中所列的各项条件，但(b) (三)项中提及的完整性的例外。第(1)(b)款加上了方括号，因为只有当第(1)款起始句中提及“一种方法”而不是“一种电子签字”时才需要这些字样。

44. 工作组适宜考虑这些规则的适用范围是否应仅限于有法定形式要求的情况，或限于法律对无某些条件（例如书面凭证或签字）规定了后果这类情形。应该回顾到，形式要求的含义已在编写《示范法》时作过讨论。《示范法颁布指南》第 68 段指出，《示范法》中使用的“法律”一词应理解为不仅包括成文法或规范法，而且还包括司法形成的法律和其他程序法。因此，“法律”一词还涵盖证据规则。在法律未规定要求某项条件但对缺少该条件（例如书面凭证或签字）规定了其后果的情况下，这也应包括在《示范法》使用的“法律”概念范围内。

国家立法和其他文书参考资料

新加坡

第五部分. 安全电子记录和签字安全电子签字

17. 如果通过使用某一具体规定的安全程序或有关当事方商定的某一商业上合理的安全程序，能够核实某一电子签字在制造时——

- (a) 为使用者所独有；
- (b) 能够确定该人；
- (c) 制造的方式或手段由其使用者单独掌握；和
- (d) 与有关电子记录的连接方式能使该电子签字在该记录被改动时失效，

则这种签字应视为安全电子签字。

有关安全电子记录和签字的推定

18. [...]

(2) 在涉及安全电子签字的任何诉讼中，除非能提出反证，否则应推定——

- (a) 该安全电子签字是与之相关联者的签字；和
- (b) 该安全电子签字是由该人为了签署或核准该电子记录所附加的。

第 7 条. [原件的推定]

(1) 如对于一数据电文[使用了强化电子签字][使用了一种电子签字[一种方法]，它能提供可靠的手段确保自最初生成信息的最后形式，作为一项数据电文或其他用途之时起始终保持该信息的完整无损]，则推定该数据电文为原件。

(2) 本条规定不适用于下述情况：[...]。

贸易法委员会文件参考资料

A/CN.9.457, 第 48—52 段

A/CN.9/WG.IV/WP.80, 第 13—14 段

说明

45. 第 7 条草案的目的是确认与《示范法》第 8 条和完整性要求的联系。第(1)款列出了两种备选做法。第一种做法规定，使用第 2(b)条草案中界定的强化电子签字将使数据电文为原件这一推定成立。第二种做法是当使用某一电子签字或某一方法而它又能对完整性提供可靠的保证时，可以推定该数据电文为原件。虽然原件形式不总是要求签字，但可以使用某种电子签字形式（无论强化与否）来核查数据电文或记录的完整性。

第 8 条. [强化]电子签字的确定

(1) [颁布国规定的主管机关或机构]可确定[某一电子签字是一种强化电子签字][哪种[方法][电子签字]满足第 6 和第 7 条的要求。]

(2) 依照第(1)款作出的任何决定应与公认的国际标准相一致。

贸易法委员会文件参考资料

A/CN.9.457, 第 48—52 段

A/CN.9/WG.IV/WP.80, 第 15 段

说明

46. 第 8 条草案的目的是要明确规定，颁布国可指定一个机关或机构，它有权确定哪种具体的技术符合强化电子签字的条件。第(1)款中的备选文字是为了使第 8 条草案与修订后的第 6 和第 7 条中提供的备选文字相一致。第(2)款的目的是鼓励各国确保根据第(1)款所作的决定符合适用的国际标准，从而有助于在强化电子签字以及签字的跨境使用和承认方面促成做法上的协调统一。

第 9 条. 签字持有人的[责任][义务]

(1) 签字持有人[有责任][应当]：

- (a) 尽职行事以确保该签字持有人关于签发、中止或废止证书的所有重大表述或者证书中所列的所有重大表述是准确无误和完整的；
- (b) 在[它知道其签字已经失密][其签字已经或可能已经失密]时，并无过分迟疑地通知有关的人；
- (c) 从签字持有人单独掌握签字装置时起适当注意保持对其签字的控制并防止他人擅自使用其签字。

(2) 如果[有共同持有人][有一人以上掌握]该[钥匙][签字装置]，则各人共同承担第(1)款所规定的[义务][责任]。

(3) 签字持有人应当对未[履行第(1)款中的义务责任][满足第(1)款的要求][负责][负赔偿责任]。

(4) [签字持有人的赔偿责任不得超过在其未履行义务时依照其当时所知或理应知道的事实和情况，对其未[履行第(1)款中的义务[责任]][满足第(1)款的要求]的可能后果预料或理应预料到的损失。]

贸易法委员会文件参考资料

A/CN.9.457，第 65—98 段

A/CN.9/WG.IV/WP.80，第 18-19 段

关于第 9 和第 10 条草案的总的说明

47. 工作组似宜考虑实际中第 9 条与第 10 条草案之间的关系。可以对第 9 条草案中的责任以及第 10 条草案中未能履行这些责任的后果作一些组合。其中有两种组合可以用来说明拟考虑的某些问题。

48. 首先一种情形是签字持有人并未违反第 9(1)(c)条草案中规定的适当注意这一责任，但尽管如此签字还是失密了。签字持有人不知道失密一事，所以没有通知信息验证人，但他不可能违反第 9(1)(b)条草案中的责任。根据第 10 条草案，依赖方不能够通过核查由信息验证人提供的信息来发现签字失密，因而可以依赖签字。这一情形提出了一些问题：在这种情形下依赖方依赖签字是否合理？依赖方是否要承担依赖的风险？这种依赖对于签字持有人的后果是什么？签字持有人是否要受使用已经失密的签字所签的任何东西的约束？

49. 第二种情形是签字持有人的确违反了第 9(1)(c)条草案中关于适当注意的责任，而且签字失密了。签字持有人知道已经失密并通知了信息验证人。根据第 10 条草案，依赖方可以通过核对由信息验证人提供的信息发现签字失密，因而不能依赖签字。这样，根据第 9(3)条草案，签字持有人要对未履行第(2)款中的责任负责，并根据第(4)款对损失负赔偿责任。在这种情形下，其结果要比第 48 段所述的情形明确得多。

说明

第9条，第1款

50. 根据工作组第三十四届会议上的决定(A/CN.9/457, 第 73—92 段), 对第 9 条草案第(1)款作了修订。工作组曾关切地表示, (a)项中的责任应限于验证过程(A/CN.9/457, 第 92 段), 因为不然的话有可能对责任作广义解释, 甚至包括签字持有人对某一依赖当事方所作的表述和陈述。由于在这一关系方面所作的表述或陈述应当受制于基本合同的法律, 故缩小了(a)项的范围, 将责任限制于签发、中止或废止证书的过程。

51. 对(b)项作了修订, 以便将工作组商定的两种备选案文(A/CN.9/457, 第 83 段)包括在内。“或本应知道”字样没有列入本修订案文, 因为要签字持有人满足一项通知责任将是困难的, 如果这项通知责任依据的是他本应知道但实际上不知道的某件事情。

52. (c)项不仅提到防止签字被擅自使用的义务, 而且还提到保持对钥匙的控制的义务。修订后的规定还提到适当注意这一责任开始产生的时间。这反映了工作组的普遍看法, 即虽然钥匙持有人保护钥匙的责任仅应当相对于受证书有效保护的那些成对钥匙而言, 但钥匙持有人保护经过验证的钥匙以免被误用的责任应当追溯到签字持有人开始单独掌握该配对钥匙之时(A/CN.9/457, 第 67 段)。

第(2)款

53. 将第(2)款加入到第 9 条草案是为了澄清在有一人以上掌握同一把钥匙的情形下适当注意的义务问题。工作组似宜审议本项规定及其与第 2 条中单独掌握的要求的关系。

第(3)款

54. 根据工作组第三十四届会议的决定(A/CN.9/457, 第 93—98 段)对本款作了修订。删除了“[签字持有人]未能履行第(1)款规定的义务而产生的后果”, 以便(一)避免考虑受到违反的义务是否是合同义务, 和(二)避免因使用“后果”一词而可能产生的任何不确定性, 因为“后果”一词可能意指所有各种可能的后果都在考虑之中, 而不传递关于这些可能的后果与未履行义务不相关联的程度的任何概念。

第(4)款

55. 本款是以《联合国国际货物销售合同公约》第 74 条为基础, 现列入供工作组进一步审议。它确立了一条以损害可预见性标准为基础的规则, 但仅限于违反第(1)款中签字持有人各项义务这类情形。工作组第三十四届会议上表示了某些关切(A/CN.9/457, 第 93—98 段), 即在货物销售合同情况下可能出现的赔偿责任不同于使用签字后可能产生的赔偿责任, 而且不可能等量齐观。另据指出, 可预料性标准虽然在签字持有人与某一依赖方之间的关系方面可能是适宜的, 但在签字持有人与信息验证人之间的合同关系方面可能不适宜。工作组似宜在进一步审议本条草案时考虑这些问题以及第 9 条草案与第 10 条草案的关系。

国家立法和其他文本参考资料

第(1)(a)款—重大表述

美国律师协会指导原则

4.2 订户的义务

订户向验证局所作的所有重大表述，包括为该订户所知并在该证书中所表述的所有信息，不管这种表述是否经验证局的确认，必须达到该订户所知和所信的最准确程度。

数字式受保通用法

七. 对电文的担保

7. 对验证人的表述

订户必须准确地向验证人表述对该证书来说意义重大的所有事实。

伊利诺伊

第 20 条. 订户的责任

第 20—101 节获得证书

一人为了获得一份证书指定本人为订户而向验证局知情地所作的所有重大表述都必须达到该人所知和所信的最准确和最完全的程度。

第 20—105 节接受证书

[…]

(b) 证书所列订户接受证书，即向在该证书使用期内合理并真诚依赖该证书所载信息的任何人表述：

- (1) 该订户正当地持有与该证书所列公共钥匙相配的私人钥匙；
- (2) 该订户向验证局所作的并与该证书上所列信息关系重大的所有表述都是真实的；和
- (3) 该证书中该订户所知范围内的所有信息都是真实的。

新加坡

第九部分. 订户的责任

获得证书

37. 订户为了获得证书而向验证局所作的所有重大表述，包括为该订户所知并在该证书中所表述的所有信息，无论这种表述是否经验证局的确认，都应当达到该订户所知和所信的最准确和最完全的程度。

第(1)(b)款—通知

美国律师协会指导原则

4.4 提出中止或废止

已经接受一证书的订户，在与该证书所列公共钥匙相配的私人钥匙失密时，必须请签发证书的验证局中止或废止该证书。

伊利诺伊

第 20 条. 订户的责任

第 20—110 节证书的废止

除非另一适用法规另有规定，如果在证书的使用期内与该有效证书上所列公用钥匙相配的私人钥匙遗失、被窃、能被擅自使用或在其他方面失密，得知失密的订户必须立即请签发证书的验证局废止该证书并在该订户原曾授权公布该证书的所有存放处公布废止通知或以其他方式提供合理的废止通知。

第 10—125 节 签字装置的制造和控制

除非另一适用法规另有规定，凡通过[···]所述某一合格的安全程序制造的电子签字的制造、有效性或可靠性取决于对该签字人签字装置的保密或控制的，：

(1) 生成或制造该签字装置者必须可信地行事；

(2) 签字人和能正当使用这种签字装置的所有其他人必须适当注意维持对该签字装置的控制和保密，以防在依赖由该装置制造的签字为合理的时期内被擅自进入、泄露或使用；

(3) 万一该签字或能正当使用这种签字装置的任何其他人知道或有理由知道任何这种签字装置已经失密或失去控制，该人必须作出合理的努力，立即通知就其所知预计可能会因这种失密而受损害的所有人，或者在有某一适当的公布机制时[···]，公布失密通知和拒绝接受此后制造的任何签字。

新加坡

提出中止或废止

40. 已经接受某一证书的订户在与该证书所列公共钥匙相配的私人钥匙失密时应尽快要求签发证书的验证局中止或废止该证书。

第(1)(c)款—擅自使用

美国律师协会指导原则

4.3 保护私人钥匙

在一有效证书的使用期内，订户应当不使与该证书所列某一公共钥匙相配的私人钥匙失密，而且还必须在任何中止期内防止失密。

数字式受保通用法

七. 对电文的担保

6. 保护担保装置

如某人借助一装置担保电文，该人必须起码适当注意防止该装置被擅自使用。

伊利诺伊

第 10—125 节 签字装置的制造和控制

除非另一适用法规另有规定，凡通过[···]所述某一合格的安全程序制造的电子签字的制造、有效或可靠性取决于对该签字人签字装置的保密和控制的，：

(1) 生成或制造该签字装置者必须可信地行事；

(2) 签字人和能正当使用这种签字装置的所有其他人必须适当注意维持对该签字装置的控制和保密，以防在依赖由该装置制造的签字为合理的时期内被擅自进入、泄露或使用；

(3) 万一该签字或能正当使用这种签字装置的任何其他人知道或有理由知道任何这种签字装置已经失密或失去控制，该人必须作出合理的努力，立即通知就其所知预计可能会因这种失密而受损害的所有人，或者在有某一适当的公布机制时[...], 公布失密通知和拒绝接受此后制造的任何签字。

第(3)和(4)款—赔偿责任

明尼苏达

325K.12 接受证书时的表述和责任

第4小节 订户的赔偿

订户一经接受证书，即承诺向签发证书的验证局赔偿因其依赖以下内容而签发或公布证书所遭受的损失或损害：

- (1) 订户对事实作重大的虚假表述；
- (2) 订户没有透露某一重大事实，如果表述或没有透露是要有意欺骗验证局或某一依赖该证书者或者属于严重失职。本节规定的赔偿不得否认或由合同限制其范围。然而，合同可以为赔偿规定与此相符的追加条件。

新加坡

第九部分. 订户的责任

对私人钥匙的控制

39. (1) 一旦接受由某一验证局签发的证书，该证书中确定的订户即承担责任，适当注意保持对与该证书所列公共钥匙相配的私人钥匙的控制，并防止泄漏给他人擅自制造该订户的数字签字。
- (2) 这种责任在证书的使用期内和证书的任何中止期内一直存在。

第 10 条. 对强化电子签字的依赖

- (1) 任何人均[有][无]权在依赖[是][并不]合理的情况下依赖一强化电子签字。
- (2) 确定依赖是否合理时，应酌情考虑：
 - (a) 签字拟予佐证的基础交易的性质；
 - (b) 依赖方是否已采取适当步骤来确定签字的可靠性；
 - (c) 依赖方是否知道或本应知道签字已失密或废止；
 - (d) 依赖方与订户的任何协议或交易做法，或者可能适用的任何商业惯例；
 - (e) 任何其他有关因素。

第 11 条. 对证书的依赖

- (1) 任何人均[有][无]权在依赖[是][并不]合理的情况下依赖一项证书。
- (2) 在确定依赖是否合理时，应酌情考虑：
 - (a) 证书所受到的任何限制；

- (b) 依赖方是否已采取适当步骤来确定证书的可靠性，包括参阅有关的证书废止清单；
- (c) 依赖方同信息验证人或订户的任何协议或交易做法，或者可能适用的任何商业惯例；
- (d) [任何][所有]其他有关因素。

贸易法委员会文件参考资料

A/CN.9/457，第 99—107 段；

A/CN.9/WG.IV/WP.80，第 20—21 段。

说明

56. 第 10 和第 11 条草案分别处理了依赖强化电子签字和证书的合理性问题，它们是根据工作组第三十四届会议上对内容的普遍看法（A/CN.9/457，第 107 段）重新拟订的。虽然最初是作为一条条文提出的，既涉及对签字的依赖又涉及对有证书佐证的签字的依赖，但本草案将这两个概念区分开来，因为对各自情况适用不同的考虑。工作组似宜考虑已经有了一条关于对签字的依赖的规则之外是否还需要列入一条关于对证书的依赖的规则，以及在确定每一情况下的合理依赖时应当考虑哪些因素。

57. 工作组曾关切地表示，将第 10 和第 11 条草案拟成一种可依赖的权利可能会推定某些法律效力，而确定拟考虑哪些因素据以决定是否可以将依赖视为合理可避免涉及签字或证书可能具有什么法律效力的问题。一种反对意见认为，将这两条草案拟成一种依赖的权利增添了某种在《示范法》中并未提供的利益，但没有在签字的有效性方面确定法律效力。如工作组所商定的那样，修订条文草案包括了一正一反两种形式，并列出了在签字和证书两种情况下拟考虑的各项因素。

58. 还对第 10 和第 11 条草案与《示范法》第 13 条的关系以及第 9、10 和 11 条草案放在一起时是否将确立一条属性规则表示了某种关切。工作组似宜考虑第 10 和 11 条与第 9 条草案和与《示范法》第 13 条的关系。

国家立法和其他文本参考资料

美国律师协会指导原则

5.3 不可靠的数字签字

(1) […]

(2) 除非法律或合同另有规定，如果在某种情况下根据指导原则 5.4（依赖的合理性）所列的因素依赖数字签字并不合理，依赖方对该数字签字作为签字或认证所签署的电文无效承担风险。

5.4 依赖的合理性

在评价一收件人依赖某一证书和依赖参照该证书所列公共钥匙而能核查的数字签字是否合理时，除其他外，有下列重大因素：

- (1) 该依赖方知悉或被告知的事实，包括证书上所列或以提及方式纳入该证书的所有事实，
- (2) 经数字签字的电文的任何现知价值或重要性，
- (3) 该依赖方与订户之间的交易方式以及数字签字外现有的是否可靠的形迹，
- (4) 贸易惯例，特别是由可信的系统或其他以计算机为基础的手段进行的贸易惯例。

2.3 可预料的对证书的依赖

可以预料，依赖一数字签字者也将依赖载有能据以核查该数字签字的公共钥匙的有效证书。

数字式受保通用法

八. 证书

1. 有效证书的效力

凡未被告知验证人未满足受保电文惯例的某一项重大要求者，可依赖一有效证书，把它视为准确地表述了所载的事实。

新加坡

第六部分. 数字签字的效力

不可靠数字签字

22. 除非法律或合同另有规定，在某种情况下如果考虑到下列因素依赖数字签字为不合理，则依赖有该数字签字的电子记录者承担该数字签字作为签字或认证该签字的电子记录无效的风险：

- (a) 依赖该有数字签字的电子记录者知悉或被告知的事实，包括该证书所列或通过提及方式予以纳入的所有事实；
- (b) 有该数字签字的电子记录的任何现知价值或重要性；
- (c) 依赖有该数字签字的电子记录者与订户之间的交易方式以及除该数字签字外现有的是否可靠的形迹；和
- (d) 任何贸易惯例，特别是由可信的系统或其他电子手段进行的贸易惯例。

第 12 条. 信息验证人的[责任][义务]

(1) [信息验证人][有义务应当][特别]：

- (a) 按其所作出的有关其验证做法的表述行事；
- (b) 采取合理的步骤来确定信息验证人在证书中验证的任何事实或信息的准确性[包括签字持有人的身份]；
- (c) 提供比较易于使用的手段，使依赖方得以证实：
 - (一) 信息验证人的身份；
 - (二) 证书[所指的][所确定的]人[在有关时间]持有证书所述的[与公用钥匙相配的私人钥匙][签字装置]；
 - (三) 这两把钥匙是功能性的一对配套钥匙]；
 - (四) 用以鉴别签字持有人身份的方法；
 - (五) 对使用签字的目的或价值规定的任何限制；和
 - (六) 签字装置是否有效以及是否已失密；
- (d) 提供某种手段，使签字持有人得以发出强化电子签字已失密的通知并确保及时废止服务的运作；
- (e) 尽职行事以确保信息验证人关于签发、中止或废止证书的所有重大表述或者证书中所列的所有重大表述都是准确无误和完整的；
- (f) 使用可依赖的系统、程序和人力资源来履行其服务。

变式 X

- (2) 信息验证人应当对其未[履行第(1)款中的义务[责任]][满足第(1)款的要求][负责][负赔偿责任]。

(3) 信息验证人的赔偿责任不得超过在其未履行义务时依照其当时所知或理应知道的事实和情况，对其未[履行第(1)款中的义务[责任]][满足第(1)款的要求]的可能后果预料或理应预料到的损失。

变式 Y

(2) 不违反第(3)款的情况下，如果造成损害的原因是证书不正确或有缺陷，信息验证人应当对以下蒙受损害者负赔偿责任：

(a) 就提供证书事宜与验证人签订了合同的一当事方；或

(b) 凡合理依赖了信息验证人签发的证书的任何人。

(3) 在下述情况下，验证人不应承担第(2)款所述赔偿责任：

(a) 如果验证人在证书中列有一项限制其对任何人所负赔偿责任的范围或程度的陈述并以此为限；或

(b) 如果验证人证明其[并未玩忽职守][采取了一切合理的措施来防止造成损害]。

贸易法委员会文件参考资料

A/CN.9/457，第 108—119 段；

A/CN.9/WG.IV/WP.80，第 22—24 段

说明

59. 根据工作组第三十四届会议的决定（A/CN.9/457，第 108—119 段）对第 12 条草案作了修订。

第(1)款

60. 第(1)款起始句包括若干选择。第一个选择涉及到这项规定拟订时是应当使用“有义务”还是“应当”。第二个选择涉及的是使用“特别是”字样。如果使用了这几个词，第 12 条草案将开列一个不封底的说明性责任清单。虽然如此拟订对信息验证人来说可能显得累赘，但工作组认为它不会与许多法律制度中目前适用于信息验证人的普遍规则相冲突。如果删除“特别是”这几个字，第 12 条草案将开列一个详尽无遗的信息验证人的责任清单，让信息验证人赔偿责任的确切范围有待确定，并且避免因使用不同的行文而在也许不对信息验证人规定尽职行事这项一般责任的国家可能出现的困难。

61. 关于第(1)款所列的具体责任，这些责任有所扩大以反映工作组的观点（A/CN.9/457，第 112—114 段）。关于(c)项，通过“比较易于使用的手段”提供的信息包括依赖当事方可能有理由预见将在证书中载列的某些信息和可能只有通过查阅某些其他来源才能获得的其他信息，例如证书废止清单。工作组似宜考虑是否应当具体规定拟在证书中列出的某些信息以及在统一规则中是否应当增列一条规定证书最起码内容的规则。

62. 第(1)(c)(=)款既提及“配对钥匙”又提及“签字装置”。为了确保统一规则不偏重任何技术，工作组似宜考虑使用“签字装置”等不偏重某一技术的行文，以取代“配对钥匙”，因为“配对钥匙”专指数字签字。当证书仅用于数字签字环境时，相对于“证书”的定义使用“配对钥匙”才可能是妥当的。

63. 第(1)(c)(=)款是按上一届会议上的提议而列入的，但工作组似宜考虑这是否是一项合适的要求。如果证书中所指的公共钥匙与签字持有人持有的私人钥匙相配因而在这两把钥匙之间有数学相配性，则要求该配对钥匙应是“功能性的一对配套钥匙”将能实现其他什么功能并不明确。还不确定的是除了第(1)(c)(=)款要求的之外，

信息验证人还能提供什么信息来表示这一额外功能。

第(2)和(3)款

64. 变式 X 确立了一条规则，即信息验证人要对其未能履行第(1)款中的义务或责任负责，但它让国家法律来确定这种违约的后果可能是什么。在这条经修订的第 12 条草案中删除了“的后果”字样，其原因与在第 9 条草案第(3)款中删除这几个字的相同，即(一)避免考虑所违反的义务是否是合同性的，(二)避免因使用“后果”一词而可能产生的任何不确定性，因为“后果”可能意指所有各种可能的后果都在考虑之中，而没有传递这些可能的后果与未履行义务不相关联的程度的任何概念。

65. 在修订第(1)款以列入两种变式——一种是详尽无遗的义务清单，另一种是不封底的说明性的义务清单——后工作组似宜考虑当第(1)款的措辞按详尽无遗的清单而不是作为另一种不封底的清单拟订时变式 X 是否将更为恰当。

66. 变式 X 第(3)款以《联合国国际货物销售合同公约》第 74 条为基础确立了一条损害可预见性规则。运用这条规定可以限制因第(1)和第(2)款而可能产生的信息验证人任何赔偿责任的数量。

变式 Y

67. 工作组内普遍认为 (A/CN.9/457, 第 115 段)，似宜确立一条不仅限于提及适用法律的统一规则，而是确立一项关于玩忽职守的一般性赔偿责任规则，但不影响可能存在的合同免责规定（条件是这种限制将不是严重不公），也不影响信息验证人通过表明其已履行了第(1)款所规定的义务而免于承担赔偿责任。变式 Y 第(2)款处理了信息验证人可能对谁负赔偿责任的问题。第(3)款规定了一条规则，允许信息验证人依赖证书中所载的任何对赔偿责任的限制，或表明它并非玩忽职守或采取了合理的措施来防止损害发生。与变式 X 的情况一样，工作组似宜考虑当第(1)款中有一份详尽无遗的责任清单而不是不封底的义务清单时，变式 Y 中所提议的规定是否恰当。它还似宜考虑是否需要在变式 Y 第(2)款草案中明确规定信息验证人的赔偿责任仅限于其未履行第(1)款中的各项义务。

68. 与变式 X 的情况一样，工作组似宜考虑，变式 Y 所提议的这样一项规定，是否在第(1)款一份详尽无遗的责任清单情况下，而不是在义务不封底的情况下，较为恰当。它还似宜考虑是否需要在变式 Y 第(2)款草案中明确规定，信息验证人的赔偿责任以其未履行第(1)款中的义务为限。

国家立法和其他文书参考资料

第 12 条第(1)款——一般性责任

美国律师协会指导原则

3 验证局

3.1 验证局必须使用可信的系统

验证局进行业务时必须使用可信的系统。

3.2 透露

(1) 验证局必须透露任何重大的验证做法声明，并发出废止或中止某一验证局证书的通知。

- (2) 验证局必须作出合理的努力，通知任何已知将会或预料会受废止或中止其验证局证明的影响者。
- (3) [...]
- (4) 万一发生事情对验证局的可信系统或其验证局证书有重大的不利影响，该验证局必须作出合理努力，通知已知将会或预料会受该事件影响者，或者根据在其验证做法声明中具体规定的程序行事。

3.7 验证局在证书中的表述

验证局签发证书，即向任何合理依赖该证书或可由该证书所列公共钥匙核查的数字签字者表述，该验证局根据该依赖人被告知的任何适用的验证做法声明，确认

- (1) 验证局遵守了本指导原则对签发证书的所有适用要求，如果验证局公布了该证书或以其他方式将其提供给那种合理依赖人，验证局还确认证书中所列订户已经接受该证书，
- (2) 证书中所确定的订户持有与证书所列公共钥匙相配的私人钥匙，
- (3) [...]
- (4) 订户的公共钥匙和私人钥匙构成一对功能性的钥匙，和
- (5) 证书中所有信息都是准确的，除非验证局在证书中声明或在证书中以提及方式表示某项信息的准确性未获确认。

另外，验证局还表述在证书中没有遗漏根据本指导原则会对其表述的可靠性产生有害影响的任何现知重大事实。

3.9 应订户的请求中止证书

除非验证局与订户之间的合同另有规定，验证局必须在某人提出请求后尽快中止证书，如果该验证局有理由相信该人为：

- (1) 该证书所列的订户，
- (2) 经正当授权为该订户行事者，或者
- (3) 在该订户不在时代表该订户行事者。

3.10 应订户的请求废止证书

签发一证书的验证局必须应证书上所列的用户请求废止该证书，如果验证局确认

- (1) 请求废止者为拟废止的证书上所列的订户，或者
- (2) 当该请求者作为代理行事时，该请求者有充分的授权实行废止。

3.11 未经订户同意的废止或中止

无论一证书上所列订户是否同意，如果验证局确认下述情况，则其必须中止或废止该证书：

- (1) 证书上表述的某一项重大事实是假的，
- (2) 签发该证书的某一项重大前提没有满足，或者
- (3) 验证局的私人钥匙或可信系统失密，以致对证书的可靠性产生重大影响。

一旦实行这种中止或废止，验证局必须立即通知该中止或废止了的证书上所列的订户。

3.12 中止或废止的通知

一旦中止或废止某一证书，如果该证书曾予以公布，验证局必须公布中止或废止通知，并且在有一依赖方查询时必须以其他方式透露中止或废止这一事实。

欧委会指令草案

附件二 对签发合格证书的验证服务提供者的要求

验证服务提供者必须：

- (a) 明示提供验证服务所必须的可靠性；
- (b) 确保名册和废止服务能迅速和安全地运作；
- (ba) 确保在签发或废止一证书时能确定日期和时间；
- (c) 根据国家法律通过合适的手段核查为其签发合格证书者的身份和其他适用的特定属性；
- (d) 雇用这样的工作人员，他们具有为所提供验证服务所必须的专业知识、经验和资历，特别是管理一级的才能、电子签字技术方面的专门知识并熟悉正当的安全程序；他们还必须执行与公认的标准相符的充分的行政和管理程序；
- (e) 使用可信的系统和产品，以防改动并必须确保它们所支持的程序的技术安全和加密安全；
- (f) 采取措施防止伪造证书，并且在验证服务提供者生成签字制造数据时，保证生成该数据过程中的保密性；
- (g) 维持充分的资金以便遵照本指令规定的要求运行，特别是要通过获得适当的保险等为损害赔偿承担责任承担风险；
- (h) 在一定时间内记录有关某一合格证书的所有有关资料，特别是为法律诉讼提供验证证据。这种记录可以电子方式作成；
- (i) 不得储存或拷贝从验证服务提供者获得了钥匙管理服务的人的签字制造数据；
- (j) 在与设法从验证服务提供者获得证书以支持其电子签字者订立合同关系之前，必须通过可靠的通信手段将使用该证书的条件告诉该人，包括对使用证书的任何限制、是否有自愿委托和申诉与争端的解决程序。这种信息必须书面写成，但可以电子方式传输，文字必须明白易懂。该信息的有关部分在有依赖该证书的第三方提出请求时必须向其提供；
- (k) 使用可信的系统以一种可核查的方式储存证书以便
 - 只有经过授权者才能输入和修改，
 - 查对信息的真实性，
 - 只有在获得证书持有人同意后才公布证书供检索；和
 - 操作者将能发现损害这些安全要求的任何技术性变动。

德国

§5 证书的签发

- (1) 验证人应当可靠地确定申请证书者。他应当确认某一把公共钥匙归属于签字钥匙证书中确定的人，并应当经该签字钥匙所有人的同意，以可以核查的方式在可供公众使用的电信通道中，在任何时候使每个人都能查询该证书以及附属证书。
- (2) 经申请人要求，验证人应当在签字钥匙证书或附属证书中记录关于该申请人代表一第三方或其专业许可证或其他许可证的权力的资料，如果第三方关于记录这种代表权的许可证或同意能可靠地显示的话。
- (3) 经申请人请求，验证人应当在证书中记录一个假名以取代该申请人的姓名。
- (4) 验证人应当采取措施使证书的数据不能被不露痕迹地伪造或窜改。他还应当采取措施保证私人签字钥匙的保密性。私人签字钥匙不得由验证人储存。
- (5) 他应当使用可靠的工作人员来进行验证活动，并应当根据§14 使用技术部件以提供签字钥匙和制造证书。这也适用于用来根据第 1 款第 2 句对证书进行核查的技术部件。

§6 指示责任

验证人应当指示§5 第 1 款中的申请人采取必要措施为安全的数字签字及其可靠的核查作出贡献。他应当指示申请人哪些技术部件能满足§14 第 1 和第 2 款中的要求以及使用私人签字钥匙制造的数字签字的归属。他应当向申请人指出对带有数字签字的数据可能需要再次签字，以免现有签字的安全价值随着时间而减少。

§8 证书的冻结

- (1) 如果签字钥匙所有人或其代表提出要求，如果签发证书时所依据的§7 所列信息失实，如果验证人停止其活动且没有其他验证人予以继续，或者如果当局根据§13 第 5 款第 2 句下令冻结，验证人应当冻结证书。冻结时应当指明冻结开始适用的时间。不允许追溯性冻结。

数字式受保通用法

八. 验证

2. 证书中表述的准确性

验证人必须确认有效证书上所载所有事实的准确性，除非从证书本身可显而易见地看出某些信息未经核查。

3. 验证人的可信性

验证人必须：

- (a) 在签发证书以及中止或废止公共钥匙证书和保护其私人钥匙时，仅使用技术上可靠的信息系统和程序；
- (b) 没有任何利益冲突，致使该验证人在签发、中止或废止证书时不可信；
- (c) 不为订户违约提供方便；
- (d) 不作任何所为或不作为，以免对合理和可预料的依赖有效证书产生重大有害影响；
- (e) 对订户和依赖有效证书者以可信的方式行事。

4. 通知做法和问题

验证人必须作出合理的努力，将下列事项通知预料会受影响者：

- (a) 任何重大的验证做法声明，和
- (b) 对其所签发的证书的可靠性或其提供服务的能力关系重大的任何事实。

8. 应请求中止公共钥匙证书

如有人自称是一公共钥匙证书中列出姓名的订户，或者自称是有可能知道一订户的私人钥匙已失密者，例如代理、雇员、商业合伙人或该订户的直系亲属，并提出请示，签发该证书的验证人必须立即中止该证书。

9. 应请求废止公用钥匙证书

签发公用钥匙证书的验证人在：

- (a) 收到了该证书上指明的订户或该订户授权的代理提出的废止请求后，并
 - (b) 确认请求废止者确系该订户或该订户授权请求废止的代理后，
- 必须立即废止该证书。

10. 未经同意中止或废止公用钥匙证书

签发公用钥匙证书的验证人必须废止该证书，如果：

- (a) 验证人确认该证书上所表述的某一重大事实失实；
- (b) 验证人确认验证人的信息系统丧失了可信性，以致对证书的可靠性产生重大影响。

验证人可以在一段必要的时间内中止有理由令人怀疑的证书，以便进行充分的调查来确认根据本条予以废止的理由。

11. 通知废止或中止公共钥匙证书

验证人一旦中止或废止某一公共钥匙证书，必须立即发出有关的废止或中止通知。

伊利诺伊

第 15 条. 数字签字的效力

第 15—301 节. 可信的服务

除非在其验证做法声明中有明显规定，验证局和管理存放处者必须以可信的方式进行业务活动和提供服务。

第 15—305 节. 透露

(a) 对于验证局为了让第三方据以核查由订户制造的数字签字而签发的每一份证书，验证局必须向该订户和所有这种依赖方公布或以其他方式提供：

(1) 适用于该证书的任何验证做法声明；和

(2) 它的证书，其中确定该验证局为一订户并载有与该验证局用来对该证书进行数字签字的私人钥匙相配的公共钥匙（它的“验证局证书”）。

(b) 一旦发生事情对验证局的运作或系统、其验证局证书或其以可信的方式运作的能力的任何其他方面产生重大有害影响，验证局必须根据其验证做法声明中规定的关于发生这种事件的程序行事，如没有这种程序，验证局必须作出合理的努力，向验证局所知预计可能会因发生这种事情而受到损害的任何人发出通知。

第 15—310 节. 证书的签发

验证局只有在下述行动之后才可以向潜在的订户签发证书以允许第三方核查由该订户制造的数字签字：

(1) 验证局收到了该潜在订户提出的签发请求，和

(2) 验证局：

(a) 遵守了其适用的任何验证做法声明中所载的所有有关做法和程序；或者

(b) 如没有关于这些问题的验证做法声明，以可信的方式确认了：

(一) 该潜在订户是拟签发的证书上所列者；

(二) 拟签发的证书上的信息是准确的；和

(三) 该潜在订户正当持有一把能够制造数字签字的私人钥匙，而且证书上拟列出的公共钥匙能用来核查由该私人钥匙所附加的私人签字。

第 15—315 节. 签发证书时的表述

(a) 验证局签发一证书供第三方据以核查订户制造的数字签字，即在其使用期内真诚地向该订户和合理依赖该证书所载信息的任何人表述：

(1) 验证局已经根据证书上所作的或以提及方式予以纳入的或已通知该人的适用验证做法声明，或者根据本法令或辖区关于签发证书的法律，处理、核准和签发了证书并将据此管理和必要时废止该证书；

(2) 验证局已按证书上的陈述或其适用的验证做法声明核查了订户的身份，或者验证局以可信的方式核查了该订户的身份；

(3) 验证局已经查实申请证书者持有与该证书所列公共钥匙相配的私人钥匙；和

(4) 除非该证书或其适用的验证做法声明中有明显规定，就验证局在签发证书之日所知，证书中的所有其他信息是准确的，不会造成重大的误导。

(b) 如果验证局签发受制于另一辖区法律的证书，验证局还应根据关于签发该证书的法律作出任何在其他方面适用的所有保证和表述。

第 15—320 节. 证书的废止

(a) 在一证书使用期内，签发该证书的验证局必须尽快根据其适用的验证做法声明中规定的关于废止的政策和程序废止该证书，如没有这种政策和程序时，则必须在发生了下列事情之后尽快废止该证书：

(1) 收到了证书中指定的订户提出的废止请求并且确认请求废止者是该订户或是该订户授权请求的代理；

- (2) 收到了某一订户个人的死亡证书的经核准的副本，或者有其他可靠证据确认该订户已死亡；
 - (3) 收到文件宣告某一公司订户已解散或有其他证据确认该订户已解散或已停止存在；
 - (4) 收到主管辖区法院签发的要求废止的命令；或
 - (5) 验证局确认：
 - (A) 证书中表述的某一重大事实不实，
 - (B) 签发该证书的某一重大先决条件没有满足，
 - (C) 验证局的私人钥匙或系统运作失密以致对证书的可靠性造成重大影响，或
 - (D) 订户的私人钥匙失密。
- (b) 一旦实行这种废止，验证局必须根据其适用的验证做法声明中规定的关于通知废止的政策和程序通知订户和依赖方，如没有这种政策和程序，必须迅速通知订户，在验证局原曾公布该证书的所有存放处公布废止通知，并以其他方式应依赖方的查询透露废止事实。

新加坡

第八部分

验证局的责任

可信的系统

27. 验证局必须利用可信的系统进行业务活动。

透露

28. (1) 验证局应当透露——
- (a) 载有与该验证局用来对另一证书进行数字签字的私人钥匙相配的公共钥匙的证书（在本节中称为验证局证书）；
 - (b) 任何有关的验证做法声明；
 - (c) 废止或中止其验证局证书的通知；和
 - (d) 对该验证局已经签发的证书的可靠性或该验证局进行业务活动的的能力有重大有害影响的任何其他事实。
- (2) 一旦发生事情对验证局的可信的系统或其验证局证书产生重大有害影响，验证局应当——
- (a) 作出合理努力，通知任何已知会或预料将会受该事情影响者；或
 - (b) 根据在其验证方法声明中规定的关于发生这种事情的程序行事。

证书的签发

29. (1) 验证局只有在发生了下列情形之后才能向潜在的订户签发证书——
- (a) 该验证局收到了该潜在订户提出的签发请求；和
 - (b) 该验证局——
 - (i) 在有验证方法声明时，已经遵循了该验证方法声明中所载的所有做法和程序，包括关于确定潜在订户的程序；或
 - (ii) 在没有验证方法声明时，遵循了第(2)分节中的条件。
- (2) 如没有验证方法声明，验证局应当自己或通过一个授权的代理确认——
- (a) 该潜在订户是拟签发的证书中所列的人；
 - (b) 如潜在订户通过一个或多个代理行事，该订户已授权该代理保管该订户的私人钥匙并请求签发出相应公共钥匙的证书；
 - (c) 拟签发的证书中的信息是准确的；
 - (d) 该潜在订户正当持有与证书中将列出的公共钥匙相配的私人钥匙；
 - (e) 该潜在订户持有能够制造数字签字的私人钥匙；
 - (f) 证书中拟列出的公共钥匙可用来核查由该潜在订户持有的私人钥匙所附加的数字签字。

签发证书时的表述

30. (1) 验证局签发证书，即向合理依赖该证书或可由该证书所列公共钥匙核查的数字签字的任何人表述，该验证局已经根据在该证书中以及方法纳入的任何适用的验证方法声明或该依赖人被告知的任何适用的验证方法声明签发了该证书。
- (2) 如果没有这种验证方法声明，验证局则表述它已经确认——
- (a) 验证局在签发该证书时已经遵守了本法令所有适用的要求，而且如果该验证局已经公布了该证书或以其他方式向这种依赖人提供该证书，并确认证书所列订户已经接受；
- (b) 证书上所确定的订户持有与该证书所列公共钥匙相配的私人钥匙；
- (c) 该订户的公共钥匙和私人钥匙构成一对功能性的钥匙；
- (d) 证书上的所有信息是准确的，除非验证局在该证书上声明或以提及方式纳入一项声明，指出哪些特定信息的准确性未获确认；
- 和
- (e) 验证局不知悉未在证书中列入将会对(a)至(d)项中的表述的可靠性产生有害影响的任何重大事实。
- (3) 如果有适用的验证方法声明已经在证书中以及方式纳入或通知依赖人，第(2)分节应当在所作表述与验证方法声明不一致时适用。

证书的中止

31. 除非验证局和订户另有协议，签发一证书的验证局应当在收到了某人提出的请求后尽快中止该证书，如果验证局有理由相信该人为——
- (a) 该证书所列的订户；
- (b) 经正当授权为该订户行事者；或
- (c) 在该订户不在时代表该订户行事者。

证书的废止

32. 验证局应当在下列情况下废止它所签发的证书——
- (a) 收到了该证书指明的订户提出的废止请求；并确认请求废止者是该订户或者是该订户授权请求废止的代理；
- (b) 收到了该订户死亡证书的一份经核准的副本，或者有其他证据确认该订户已经死亡；或者
- (c) 收到表示对该订户实行解体的文件，或者有其他证据确认该订户已经解体或已停止存在。

未经订户同意的废止

33. (1) 无论证书上所列订户是否同意，验证局应当废止证书，如果该验证局确认——
- (a) 该证书上表述的某一项重大事实失实；
- (b) 签发该证书的某一项要求没有满足；
- (c) 验证局的私人钥匙或可信的系统失密，以致该证书的可靠性受到重大影响；
- (d) 订户个人已经死亡；或者
- (e) 订户已经解体、停业清理或者停止存在。
- (2) 一旦实行这种废止，除第(1)(d)或(e)分节情形外，验证局应当立即通知被废止的证书上所列的订户。

中止的通知

34. (1) 验证局中止一证书后，应立即在该证书所指定的存放处公布一份经过签署的中止通知以便公布中止通知。
- (2) 如果指定了一个或几个存放处，验证局应当在所有这些存放处公布经签署的中止通知。

废止的通知

35. (1) 验证局废止一证书后，应立即在该证书所指定的存放处公布一份经过签署的废止通知以便公布废止通知。
- (2) 如果指定了一个或几个存放处，验证局应当在所有这些存放处公布经签署的废止通知。

第 12 条第(2)和(3)款—赔偿责任

美国律师协会指导原则

3.14 守约验证局的赔偿责任

验证局凡遵守了本指导原则和任何适用的法律和合同的，不对下列任何损失负赔偿责任：

- (1) 验证局签发的证书的订户或任何其他其他人所受到的任何损失，或
- (2) 因依赖验证局签发的证书、依赖通过参考证书中所列的公共密钥可据以核查的数字签字或依赖这种证书或存放处表述的信息所造成的任何损失。

欧委会指令草案

第 6 条 赔偿责任

1. 成员国应当起码确保，验证服务提供者在向公众签发了证书作为合格的证书或者向公众保证某一份证书后，对任何合理依赖该证书者因以下原因受到的损害负赔偿责任：

- (a) 签发时该合格证书上所有信息的准确性；
- (b) [...]；
- (c) 保证在签发该证书时该合格证书上确定的人持有与该证书上给出的或确定的签字核查数据相配的签字制造数据；
- (d) 在验证服务提供者既生成签字制造数据又生成签字核查数据时，保证该签字制造数据和该签字核查数据可以相配使用；

但验证服务提供者能证明其并无玩忽职守者除外。

1a. 成员国应当起码确保，向公众签发证书作为合格的证书的验证服务提供者，因没有对证书的废止进行登记而对任何合理依赖该证书者造成的损害负赔偿责任，除非该验证服务提供者能证明其并无玩忽职守。

3. 成员国应当确保验证服务提供者可以在合格的证书上指出对某一证书用途的限制，这种限制必须是能为第三方所识别。验证服务提供者不应应对违反某一合格证书的用途限制而使用该证书所造成的损害负赔偿责任。

4. 成员国应当确保验证服务提供者可以在合格证书上指明可以使用该证书的交易价值限额。

密苏里

第 17.1 节

签发证书的验证局和接受证书的订户在证书中具体规定某一建议依赖限额，即建议人们只在风险总额不超过所建议的依赖限额时依赖该证书。

第 17.2 节

除非一持牌验证局放弃适用本分节，持牌验证局：

- (1) 不对依赖伪造或被篡改的订户的数字签字所造成的任何损失负赔偿责任，如果就该伪造或被篡改的数字签字而言，该验证局遵守了

本法令 1 至 27 节的所有重大要求：

- (2) 在下列任一情形中，不对超出证书中作为其建议依赖限额而确定的数额负赔偿责任：
 - (a) 因依赖证书对须由该持牌验证局加以确认的任何事实所作的错误表述而造成的损失；或
 - (b) 在签发证书时没有遵守本法令第 10 节；
- (3) 只对任何诉讼中补偿因依赖证书所造成的损失的直接、赔偿损害负赔偿责任，这种损害不包括：
 - (a) 惩罚性或象征性的损害；
 - (b) 丧失利润、节余或机会的损害；或
 - (c) 痛苦或折磨的损害。

新加坡

持牌验证局的赔偿责任限额

45. 除非一持牌验证局放弃适用本节，持牌验证局—
 - (a) 不应当对依赖伪造或经篡改的订户的数字签字所造成的任何损失负赔偿责任，如果就该伪造或被篡改的数字签字而言，该持牌验证局遵守了本法令的各项要求；
 - (b) 在下列任一情况中，不应当对超出证书中作为其建议依赖限额而确定的数额负赔偿责任—
 - (一) 因依赖证书对须由该持牌验证局加以确认的任何事实所作的错误表述而造成的损失；或
 - (二) 在签发证书时没有遵守第 29 和 30 节。

第 13 条. 对外国证书和签字的承认

(1) 在确定一证书[签字]是否具有法律效力或确定其在多大程度上具有法律效力时，不得考虑签发该证书[签字]的地点，也不得考虑签发人营业地所在国。

变式 A

- (2) 如果外国信息验证人的做法至少达到根据…[立法国法律]要求信息验证人所应达到的可靠性，就应承认该外国信息验证人签发的证书与根据…[立法国法律]运作的信息验证人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。]
- (3) 符合另一国有关数字或其他电子签字的法律的签字，被确认为与符合…[立法国法律]的签字具有同等法律效力。但该另一国的法律要求此种签字的可靠程度至少与符合…[立法国法律]的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。]
- (4) 尽管有上述条款，商务或其他交易当事方仍可规定在利用某一特定信息验证人、某一类特定信息验证人或证书时必须结合向其提交的电文或签字。

变式 B

- (2) 如果外国验证人的做法至少达到根据…[立法国法律]要求信息验证人所应达到的可靠性，就应承认该

外国验证人签发的证书与根据…[立法国法律]运作的信息验证人所签发的证书具有同等法律效力。

[(3) 可通过已公布的国家决定或与其他国家达成的双边和多边协定，来确认第(2)款所述及的同等效力。]

(4) 在确定同等效力时，应顾及如下因素：

- (a) 财政资源和人力资源，包括管辖区内的现有资产；
- (b) 硬件和软件系统的可信性；
- (c) 办理证书、申请证书和保留记录的程序；
- (d) 证书确认的[签字人][主体]和潜在的依赖方利用信息的情况；
- (e) 独立机构审计的经常性和程度；
- (f) 是否有国家、鉴定机构或验证局关于上述规则遵守情况或现状的声明；
- (g) 立法国法院管辖权是否易受影响；和
- (h) 适用于验证局责任的法律与立法国法律之间的差异程度。

贸易法委员会文件参考资料

A/CN.9/454，第 173 段；

A/CN.9/446，第 196—207 段（第 19 条草案）；

A/CN.9/WG.IV/WP.73，第 75 段；

A/CN.9/437，第 74—89 段（I 条草案）；和

A/CN.9/WG.IV/WP.74，第 73—75 段。

说明

69. 第 13 条草案处理的是在工作组第三十四届会议上被称为“跨境承认”的事项（见 A/CN.9/437，第 77—78 段）。第(1)款所依据的是工作组第三十四届会议上提出的一项提案（A/CN.9/457，第 102 段），即工作组似宜考虑订立一条规则，确定不得因证书的签发地点而对其加以歧视。

70. 变式 A 所依据的是将在工作组第三十二届会议上提出的若干款规定加以合并的建议（见 A/CN.9/446，第 197—204 段）。为此，它提出了为了承认由外国信息验证人签发的证书以及符合另一国法律的签字而可以在立法国适用的一些标准。第(4)款反应了工作组的普遍看法，即应当承认商务或其他交易的当事各方都有权利结合其所收到的电文或签字选择所希望使用的特定信息验证人、某一类信息验证人或某一类证书。提及商务和其他交易的当事方将包括以商务身份行事的政府机构。

71. 变式 B 提供了一份在评估外国证书的可靠性时拟加以考虑的说明性标准清单。

国家立法和其他文书参考资料

欧委会指令草案

第 7 条 国际方面

1. 成员国应确保由设立在第三国的验证服务提供者作为合格的证书向公众签发的证书应被承认为与在欧洲联盟内设立的验证服务提供者签发的证书具有同等效力：
 - (a) 如果该验证服务提供者满足了本指令所规定的各项要求并已根据欧洲共同体一成员国订立的自愿委托计划作了委托；或
 - (b) 如果在共同体内设立的且满足了本指令所规定的各项要求的一验证服务提供者保证该证书；或
 - (c) 如果该证书或该验证服务提供者根据共同体与第三国或国际组织间的双边和多边协定得到承认。
2. 为了简便与第三国的跨境验证服务和在法律上承认源自第三国的高级电子签字，欧委会将酌情提出建议，以便有效地实施适用验证服务的标准和国际协定。特别是它将在必要时向理事会提出提案，要求在与第三国和国际组织谈判双边和多边协定时有适当的授权。理事会应按特定的多数作出决定。

德国

§15 外国证书

- (1) 数字签字，凡可用由欧洲联盟任一成员国或欧洲经济区条约任一缔约国有关外国证书的公共签字钥匙加以核对者，只要它们表明有同等的安全等级，与符合本法律的数字签字同等。
- (2) 第 1 款也适用于其他国家，只要订立了有关承认证书的超国家或国际协定。

伊利诺伊

第 25 条 州机构使用电子签字和记录

第 25—115 节. 共同操作性

只要根据情况是合理的，由中央管理服务局或州某一机构通过的关于使用电子记录或电子签字的规则，拟订时应当鼓励和促进与其他州政府机构和联邦政府通过的类似要求的一致性和共同使用性。

新加坡

X 部分 验证局的管制

对外国验证局的承认

43. 本部可以通过条例规定审计员可以为了下述任一目的承认新加坡境外满足特定要求的验证局：
 - (a) 在由该验证局签发的证书中具体规定的任何建议依赖限度；
 - (b) 第 20(b)(c)节[在某些情况下将数字签字视为安全的电子签字]和 21 节[如果用户接受则推定证书正确]所述的推定。

注

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

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

³ 同上，《第五十三届会议，补编第 17 号》（A/53/17），第 208 段。