



---

联合国国际贸易法委员会

第四十届会议

2007年6月25日至7月12日，维也纳

今后可能在电子商务领域开展的工作

关于建立有利于电子商务的法律框架所需的各项要素的综合性  
参考文件：关于国际上使用电子认证和签名方法的样章

秘书处的说明

增编

本文件附件载有一个样章的最后一部分（第二部分，第二章，B.2节），该章述及与国际上使用电子认证和签名方法有关的法律问题。



## 附件

### 目录

	段次	页次
第二部分 电子签名和认证方法的跨国界使用 (续)		
二. 确立法律等同性的办法和标准.....	1-22	3
B. 行为标准和赔偿责任制度的等同性.....	1-22	3
2. 公共钥匙基础设施框架中赔偿责任的特别实例.....	1-22	3
结论.....	23-28	9

## 第二部分

### 电子签名和认证方法的跨国界使用 (续)

[...]

#### 二. 确立法律等同性的办法和标准

##### B. 行为标准和赔偿责任制度的等同性

###### 2. 公共钥匙基础设施框架中赔偿责任的特别实例

1. 关于电子签名和认证方法的使用方面的赔偿责任的讨论主要着重于认证服务提供者赔偿责任的基础和特征。据普遍承认，认证服务提供者的基本义务是，使用可靠的系统、程序和人力资源，并按其所作出的关于其政策和做法的表述行事。<sup>1</sup>此外，认证服务提供者还应当采取合理的谨慎措施，确保其作出的关于证书的所有实质性表述均准确无误和完整无缺。上述所有活动都可能会使认证服务提供者面临不同程度的赔偿责任，视可适用的法律而定。以下段落指出了认证服务提供者面临较大的赔偿责任风险的情况，并概述了各国内法律处理这类赔偿责任的方法。

###### (a) 不签发或迟延签发证书

2. 认证服务提供者通常在签名申请人提出申请时签发证书。如果申请符合认证服务提供者的标准，认证服务提供者便可签发证书。申请人符合标准却仍被拒绝或延误的情况是有可能发生的，有的是因为认证服务提供者确实出了差错，有的是因为认证服务提供者故意不开放或因意外无法开放申请设施，还有的是因为认证服务提供者出于不可告人的动机，希望延迟或拒绝向申请人签发证书。在上述情况下，被拒绝或延误的申请人可以向认证服务提供者提出索赔。<sup>2</sup>

3. 在有一个竞争性认证服务市场的情况下，一个认证服务提供者因意外或故意拒绝签发证书，可能不会对申请人造成实际的损害。但是，在缺乏有意义的竞争的情况下，如果被拒绝的申请人没有证书就无法开展某种特定的业务，那么认证服务提供者拒绝或迟延签发证书就可能造成严重的损害。即使有与之竞争的其他认证服务提供者，但假设申请人为某一特定交易申请证书，由于延误或被拒绝而无法为想要进行的交易及时取得证书，从而不得不放弃有重大价值的交易，则可以想象特定的交易因这种情况而遭受的损失。<sup>3</sup>

<sup>1</sup> 《贸易法委员会电子签名示范法》（见注[...]），第9条，第1款(a)项和(b)项。

<sup>2</sup> Smedinghof, “认证当局：赔偿责任问题”（见注[...]）3.2.1节。

<sup>3</sup> 同上。

4. 上述情形在国际环境中不太可能发生，因为大多数签名人更有可能找位于本国的认证服务提供者提供服务。

(b) 签发证书时出现疏忽

5. 证书的主要功能是将签名人的身份同公共钥匙联系起来。因此，认证服务提供者的主要任务是，按照其表述的做法，证实申请人即为署名的签名人，且掌握着与证书中所列的公共钥匙相对应的私人钥匙。认证服务提供者若未这样做就可能面临对签名人或依赖证书的第三方承担赔偿责任。

6. 例如，如果错误地向盗用身份的冒名顶替者签发证书，就可能对签名人造成损害。认证服务提供者自己的雇员或合同人可能会串通起来，利用认证服务提供者预防冒名顶替者的不当申请的签名钥匙签发错误的证书。这些人还可能因疏忽而错发证书，原因是在审查冒名顶替者的申请时未正确履行认证服务提供者所表述的核实程序，或者使用认证服务提供者的签名钥匙制作了未经核准的证书。最后，犯罪分子可能会使用貌似真实的伪造身份文件冒充签名人，认证服务提供者尽管谨慎而一丝不苟地遵守了其公开阐明的政策，仍然不免上当，向冒名顶替者签发证书。<sup>4</sup>

7. 错误地向冒名顶替者签发证书有可能造成严重的后果。在网上与冒名顶替者进行交易的依赖方可能会依赖错误签发的证书上不正确的数据，从而运送货物、划拨资金、发放信贷或进行其他交易，以为与之做交易的是被冒名顶替的一方。等骗局被识破时，依赖方可能已经遭受重大损失。在这种情况下，受到损害的有两方：一方是因错误签发的证书而受骗的依赖方，另一方是在错误签发的证书中身份被假冒的人。这两方都会向认证服务提供者提出索赔。还有一种情形可能是因疏忽而向一个虚构的人签发证书，在这种情况下，遭受损害的只有依赖方。<sup>5</sup>

8. 《贸易法委员会电子签名示范法》第 9 条除其他外规定，认证服务提供者应当“采取合理的谨慎措施，确保其作出的关于证书整个有效期的或需要列入证书内容的所有实质性表述均准确无误和完整无缺。”执行《示范法》的若干国家的国内法已经原封不动地列入了这项一般性义务，<sup>6</sup>但某些国家似乎将“合理的谨慎”这一标准提高到了保证的标准。<sup>7</sup>

9. 《欧洲联盟电子签名指令》所建立的制度要求欧洲联盟各成员国“最低限度地”确保，认证服务提供者应在面向公众签发合格的证书或为该证书向公众

<sup>4</sup> 同上。

<sup>5</sup> 同上。

<sup>6</sup> 例如，泰国《电子交易法》（2001 年）第 28 节第 2 款；以及开曼群岛（联合王国的海外领土）《电子交易法》，2000 年，第 28(b) 节。

<sup>7</sup> 例如，中国，《电子签名法》第 22 条“电子认证服务提供者**应当保证**电子签名认证证书内容在有效期内完整、准确，并保证电子签名依赖方能够证实或者了解电子签名认证证书所载内容及其他有关事项”，标出了强调部分。

提供保证时，在以下几个方面对合理地依赖该证书的任何实体、法人或自然人承担损害赔偿责任：**(a)**合格证书在签发时所载的所有信息的准确性以及该证书实际载有合格证书按规定应载有的所有详细信息；**(b)**保证在证书签发时，合格证书上指明的签名人持有与证书中所提供或指明的签名核实数据相应的签名制作数据；**(c)**保证在认证服务提供人生成签名制作数据和签名核实数据的情况下，这两种数据可互补使用；但认证服务提供人证明自己没有疏忽行事除外。<sup>8</sup>

10. 其他国内法一般不约而同地规定认证服务提供人有义务核实签发证书所依据的信息的准确性。在一些国家中，一般认定认证服务提供人自经正式认可的证书签发之日起，应在该证书所含全部信息的准确性方面，对合理依赖证书的任何人均负有赔偿责任，<sup>9</sup>或为其准确性作出“保证”，<sup>10</sup>不过在其中一些国家认证服务提供人可以通过在证书中列入一条适当的声明来限定这一保证。<sup>11</sup>但一些法律明确规定，认证服务提供人只要根据验证惯例声明进行了核实，对签名人提供的不准确信息便不承担赔偿责任，条件是认证服务提供人能够证明其采取了一切合理措施对信息进行了核实。<sup>12</sup>

11. 还有一些国家不是通过法定保证，而是通过规定认证服务提供人一般有义务在签发证书之前核实签名人所提供的信息，<sup>13</sup>或有义务建立核实此类信息的系统，<sup>14</sup>来达到与上文相同的结果。在一些情况下，若发现所签发的证书所依据的信息是不准确或虚假的，有义务立即撤销证书。<sup>15</sup>但在少数情况下，法律对证书的签发不作规定，仅要求认证服务提供人遵守其验证惯例声明<sup>16</sup>或按照与签名人的约定来签发证书。<sup>17</sup>这并不表示法律没有考虑到认证服务提供人的任何赔偿责任。相反，一些法律明确设想了认证服务提供人的赔偿责任，其中要求认证服

<sup>8</sup> 《欧洲联盟电子签名指令》（见注[...]）第6章第1款。

<sup>9</sup> 巴巴多斯《电子交易法》（1998年）第308B章第20节第1(a)款；百慕大《电子交易法》，1999年，第23节；香港（中国特别行政区），《电子交易条例》第39节；印度《信息技术法》，2000年，第36(e)节；毛里求斯《电子交易法》，2000年，第27节第2(d)款；新加坡《电子交易法》第29节第(2)(a)和(c)小节和第30节第(1)小节。

<sup>10</sup> 突尼斯，《贸易和电子商务相关法》，第18条；越南《电子交易法》第31(d)条。

<sup>11</sup> 例如巴巴多斯、百慕大、中国香港特别行政区、毛里求斯和新加坡。

<sup>12</sup> 阿根廷，《数字签名法》（2001年），第39(c)条。

<sup>13</sup> 同上，第21(o)条；智利，《电子单证、电子签名和电子签名认证服务法》，第12(e)条；墨西哥《商务法典：电子签名法令》；第104(I)条；和委内瑞拉波利瓦尔共和国《数据电文和电子签名法》，第35条。

<sup>14</sup> 厄瓜多尔，《店子商务、电子签名和数据电文法》，第30(d)条。

<sup>15</sup> 阿根廷，《数字签名法》（2001年），第19(e)(2)条。

<sup>16</sup> 秘鲁《关于电子签名和电子证书法的条例》，第29(a)条。

<sup>17</sup> 哥伦比亚，《关于电子商务的第527号法律》，第32(a)条；多米尼加共和国，《电子商务、电子单证和电子签名法》（2002年），第40(a)条；巴拿马，《电子签名法》（2001年），第49条第7款。

务提供者购买第三方赔偿责任保险，该保险应足以涵盖在合同内外对签名人和第三方所造成的损害。<sup>18</sup>

12. 认证服务提供者核实所提供信息的准确性的义务是以签名人的下述义务为补充的：“采取合理的谨慎措施，确保签名人作出的关于证书整个有效期的或需要列入证书内的所有实质性表述均准确无误和完整无缺。”<sup>19</sup>因此可以认定，签名人若在申请证书时向认证服务提供者提供了虚假或不准确的信息，须对认证服务提供者或依赖方承担赔偿责任。这有时表述为一种向认证服务提供者提供准确信息的一般性义务，<sup>20</sup>或采取合理的谨慎措施确保信息准确的一般性义务；<sup>21</sup>有时明确说明签名人未遵守这一特定要求须对因此而造成的损害承担赔偿责任。<sup>22</sup>

**(c) 擅自使用签名或破坏验证惯例声明**

13. 擅自使用签名制作办法和证书有两个方面，一方面，签名制作装置可能没有得到适当的保管或因其他原因而失密，如被签名人的代理人盗用。另一方面，认证服务提供者的签名实际层级系统可能失密，例如，认证服务提供者自己的签名钥匙或根钥匙丢失，或被透露给未经授权的人或被未经授权的人使用，或因其他原因而失密。

14. 签名层级系统失密的方式可能多种多样。认证服务提供者、其雇员或合同人可能意外破坏钥匙或失去对钥匙的掌控，持有私人钥匙的数据中心可能意外受到破坏，或者认证服务提供者的钥匙可能被某人为了非法目的（如黑客）而故意毁坏或泄密。签名层级系统失密的后果可能会十分严重。例如，如果私人签名钥匙或根钥匙落入罪犯手中，他会伪造证书并使用这些证书假冒真正的或虚构的签名人，给依赖方造成损失。此外，认证服务提供者一旦发现有损坏，必须撤销所签发的所有证书，这可能导致签名人因失去使用权而集体大规模提出索赔。

15. 这一事项在《贸易法委员会电子签名示范法》中没有详细述及。可以说，《示范法》所规定的认证服务提供者“使用可信赖的系统、程序和人力资源提供其服务”<sup>23</sup>的义务可以解释为规定认证服务提供者有义务采取一切必要措施预

<sup>18</sup> 委内瑞拉波利瓦尔共和国《数据电文和电子签名法》，第 32 条。

<sup>19</sup> 《贸易法委员会电子签名示范法》（见注[...]），第 8 条第 1(c)款。

<sup>20</sup> 阿根廷，《数字签名法》（2001 年），第 25 条；智利，《电子单证、电子签名和电子签名认证服务法》，（2002 年），第 24 条；墨西哥，《商务法典：电子签名法令》（2003 年），第 99(III)条。

<sup>21</sup> 开曼群岛，《2000 年电子交易法》，第 31(c)节。

<sup>22</sup> 哥伦比亚，《关于电子商务的第 527 号法律》，第 40 条；多米尼加共和国，《电子商务、电子单证和电子签名法》（2002 年），第 55 条；墨西哥，《商务法典：电子签名法令》（2003 年），第 99(III)条；巴拿马，《电子签名法》（2001 年），第 39 条。

<sup>23</sup> 《贸易法委员会电子签名示范法》（见注[...]），第 9 条第 1 款(f)项。

防其自身的钥匙（进而预防其整个签名层级系统）失密。一些国内法明确规定了这种义务，通常将其与认证服务供应商使用可信赖的系统的义务结合在一起。<sup>24</sup>有时规定了采取措施避免伪造证书这一具体义务。<sup>25</sup>认证服务提供人有义务避免制作或接触签名人的签名制作数据，还可能因其雇员故意这样做而承担赔偿责任。<sup>26</sup>认证服务提供人往往有义务在其签名制作数据失密的情况下要求撤销自身的证书。<sup>27</sup>

16. 还要求签名人采取一切适当的谨慎措施。例如，《贸易法委员会电子签名示范法》要求签名人“采取合理的谨慎措施，避免他人擅自使用其签字制作数据”。<sup>28</sup>多数国内法规定了类似的义务，但有一些不同之处。在某些情况下，法律严格规定签名人有义务确保单独控制签名制作办法并预防其被擅自使用，<sup>29</sup>或使签名人完全负责保护签名制作装置的安全。<sup>30</sup>但这项义务往往被界定为保持充分控制签名制作装置或采取充分措施保持控制签名制作装置的义务，<sup>31</sup>或努力避免擅自使用，<sup>32</sup>或采取合理的谨慎措施避免其签名装置被擅自使用。<sup>33</sup>

#### (d) 未终止或撤销证书

17. 认证服务提供人还可能因未终止或撤销已经失效的证书而承担赔偿责任。为使数字签名基础设施正常发挥职能并得到信任，关键是有到位的机制，

<sup>24</sup> 阿根廷，《数字签名法》（2001年），第21(c)和(d)条；哥伦比亚，《关于电子商务的第527号法律》，第32(b)条；毛里求斯《2000年电子交易法》第24条；巴拿马，《数字签名法》（2001年），第49条第5款；泰国，《电子交易法》（2000年），第28节，第6款；突尼斯，《贸易和电子商务相关法》，第13条。

<sup>25</sup> 委内瑞拉波利瓦尔共和国，《数据电文和电子签名法》，第35条。

<sup>26</sup> 阿根廷，《数字签名法》（2001年），第21(b)条。

<sup>27</sup> 同上，第21(p)条。

<sup>28</sup> 《贸易法委员会电子签名示范法》（见注[...]），第8条，第1(a)项。

<sup>29</sup> 阿根廷，《电子签名法》（2001年），第25(a)条；哥伦比亚，《关于电子商务的第527号法律》，第39条第3，按；多米尼加共和国，《电子商务、电子单证和电子签名法》，（2002年），第53(d)条；巴拿马，《数字签名法》（2001年），第37条第4款；俄罗斯联邦，《联邦电子数字签名法》（2002年），第12条第1款；土耳其，《关于执行电子签名法的程序和原则条例》（2005年），第15(e)条。

<sup>30</sup> 突尼斯，《贸易和电子商务相关法》第21条。

<sup>31</sup> 智利，《电子单证、电子签名和电子签名认证服务法》（2002年），第24条；越南《电子交易法》，第25条第2(a)款。

<sup>32</sup> 委内瑞拉波利瓦尔共和国，《数据电文和电子签名法》第19条。

<sup>33</sup> 开曼群岛，《电子交易法》，2000年，第39(a)节；厄瓜多尔《电子商务、电子签名和数据电文法》，第17(b)条；印度，《信息技术法》，2000年，第42节第1款；毛里求斯，《2000年电子交易法》，第35节第1(a)和(b)款；墨西哥，《商务法典：电子签名法令》（2003年），第99(c)条；新加坡，《电子交易法》（第88章），第39节；泰国，《电子交易法》（2001年），第27节，第1款。

实时判断某一证书是否有效，或该证书是否已被终止或撤销。例如，每当私人钥匙失密时，冒名顶替者可能已经获得了私人钥匙的拷贝，因此，撤销证书是签名人避免冒名顶替者进行欺诈交易的首要机制。

18. 因此，认证服务提供人在接到签名人请求后撤销或终止签名人证书的速度是至关重要的。从签名人请求撤销证书到实际撤销证书并发布撤销通知这段时间内，冒名顶替者就有可能进行欺诈交易。因此，如果认证服务提供人无故延迟，不把已撤销的证书及时放到撤销清单上，或没有这样做，签名人和受骗的依赖方可能会因依赖了所谓的有效证书而遭受重大损失。此外，作为其认证服务的一部分，认证服务提供人可主动维持网上储存库和证书撤销清单供依赖方查阅。维持这一数据库有两个基本风险：数据储存库或证书撤销清单可能不准确，因而会提供错误信息，而信息接受人可能会因依赖错误信息而遭受损失；还有一个风险是，数据储存库或证书撤销清单可能无法查阅（如由于系统故障），从而妨碍签名人和依赖方完成交易。

19. 如前文所述，《贸易法委员会电子签名示范法》假定认证服务提供人可签发各种等级的、可靠程度和安全程度不一的证书。因此，《示范法》不要求认证服务提供人始终保持撤销系统可供查阅，因为对某些类型的“低价值证书”来说，这在商业上可能是不合理的。《示范法》仅要求认证服务提供人提供“合理可及的手段”，使依赖方得以从证书中主要证实以下两点：“是否存在签名人发出通知的途径”，通知签名制作数据已经失密，以及“是否开设及时的撤销服务”。<sup>34</sup>如果开设了及时的撤销服务，认证服务提供人有义务确保其可供使用。<sup>35</sup>

20. 《欧洲联盟电子签名指令》所确立的制度要求欧洲联盟各成员国“最低限度”确保向公众签发了合格证书的认证服务提供人，若未对撤销证书的情况进行登记，便应当对合理地依赖证书的任何实体、法人或自然人因此而遭受的损失承担赔偿责任，除非该认证服务提供人证明其并未疏忽行事。<sup>36</sup>一些国内法规规定认证服务提供人有义务采取措施防止伪造证书的行为<sup>37</sup>，或在发现签发的证书所依据的是不准确或虚假的信息时立即撤销证书。<sup>38</sup>

21. 签名人和其他有授权的人也可能有类似的义务。例如，《贸易法委员会电子签名示范法》要求签名人在“知悉签名制作数据已经失密”或“知悉签名制作数据很有可能已经失密的情况”时，“毫无任何不应有的迟延”，“使用认证服务提供人所提供的手段”或“作出其他合理的努力，向按签字人合理预计可能依赖电子签名或提供支持电子签名服务的任何人员发出通知”。<sup>39</sup>

<sup>34</sup> 《贸易法委员会电子签名法》（见注[...]），第9条第1(d)(v)和(vi)项。

<sup>35</sup> 同上，第9条，第1(e)项。

<sup>36</sup> 《欧洲联盟电子签名指令》（见注[...]），第6条第2款；另见该指令附件二(b)段。

<sup>37</sup> 巴拿马，《数字签名法》（2001年），第49条，第6款。

<sup>38</sup> 阿根廷，《数字签名法》（2001年），第19(e)(2)条。

<sup>39</sup> 《贸易法委员会电子签名法》（见注[...]），第8条第1(b)(i)和(ii)项。

22. 国内法律常常认定签名人有义务在签名制作数据可能已经失密的任何情况下请求撤销证书，<sup>40</sup>但在某些情况下，法律仅要求签名人有义务将该项事实告知认证服务提供者。<sup>41</sup>一些国家的法律已经采用了《贸易法委员会电子签名示范法》的表达方式，规定签名人有义务进一步通知按签名装置持有人合理预计可能依赖电子签名或提供支持电子签名服务的任何人员。<sup>42</sup>一些法律制度可能暗示了违反该义务的后果，但某些国家的法律明确说明签名人若未通报对私人钥匙失去控制一事或未请求撤销证书，应承担赔偿责任。<sup>43</sup>

## 结论

23. 电子认证和签名办法的广泛应用可能是在国际交易中减少贸易文件和降低相关费用的重要一步。虽然在很大程度上来说，该领域的发展速度主要取决于技术解决办法的质量和安全性，但法律可以为便利电子认证和签名办法的使用作出重要的贡献。

24. 许多国家已经朝这个方向采取了国内措施，通过了承认电子通信法律价值的立法，并为其与纸质通信的等同性制定了标准。规范电子认证和签名办法的条款常常是这类法律的一个重要组成部分。《贸易法委员会电子商务示范法》<sup>44</sup>已成为该领域立法的唯一最具影响力的标准，其广泛执行已经为促进国际上高度的统一协调发挥了作用。随着对《联合国国际合同中电子通信公约》<sup>45</sup>的广泛批准，将有一套特别的国际交易规则，带来更大的协调统一。

25. 国际上对电子认证和签名办法的使用也可能因上述贸易法委员会标准的通过而受益。特别是，《联合国国际合同使用电子通信公约》中所载的电子签名和纸面签名功能等同的灵活标准可以提供一个国际共同框架，使电子认证和签名办法得以满足国外形式的签名要求。但是，某些问题可能会继续存在，特别

<sup>40</sup> 阿根廷，《数字签名法》（2001年），第25(c)条；哥伦比亚《关于电子商务的第527号法律》，第39条第4款；多米尼加共和国，《电子商务、电子单证和电子签名法》（2002年），第49条和第53(e)条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第17(f)条；毛里求斯，《2000年电子交易法》，第36条；巴拿马，《数字签名法》（2001年）第37条第5款；新加坡，《电子交易法》（第88章），第40节；俄罗斯联邦，《联邦电子数字签名法》（2002年）第12条第1款。

<sup>41</sup> 印度，《信息技术法》（2000年），第42节，第2款；和土耳其，《关于执行电子签名法的程序和原则的条例》（2005年），第15(f)和(i)条。

<sup>42</sup> 开曼群岛，《电子交易法》，2000年，第31(b)节；中国，《电子签名法》，第15条；泰国，《电子交易法》（2001年）第27节，第2款；越南，《电子交易法》第25条，第2(b)款。

<sup>43</sup> 中国，《电子签名法》，第27条；多米尼加共和国，《电子商务、电子单证和电子签名法》（2002年），第55条；厄瓜多尔，《电子商务、电子签名和数据电文法》，第17(e)条；巴拿马《电子签名》（2001年），第39条；俄罗斯联邦，《联邦电子数字签名法》（2002年），第12条，第2款；委内瑞拉波利瓦尔共和国，《数据电文和电子签名法》第40条。

<sup>44</sup> 见注[...]联合国出版物，出售品编号E99.V.4]。

<sup>45</sup> 见注[...]大会第60/21号决议，附件]。

是在电子认证和签名办法的国际使用方面，它要求在认证或签名过程中有值得信赖的第三方参与。

26. 这一特定领域中出现的各种问题在很大程度上是因为技术标准不一致或设备软件不兼容，因而缺乏国际互操作性。统一标准并改善技术兼容性的努力可能会为目前存在的难题找到一种解决办法。但是，还有一些与电子认证和签名办法有关的法律难题，特别是在一些国内法律方面。这些国内法律规定或主张电子签名使用某种特定技术，通常是数字签名技术。

27. 规定了数字签名法律价值的法律通常也赋予外国证书所支持的签字同样的法律价值，但以这些外国证书被认为等同于国内证书为限。在本次研究中所做的审查表明，对法律等同性的适当评估要求不仅对某一特定签名技术所附带的技术和安全标准进行比较，还要对管辖各有关当事人的赔偿责任的规则进行比较。《贸易法委员会电子签名示范法》提供了一套基本的通用规则，管辖认证和签名程序所涉及的各方当事人的某些可能对其各自的赔偿责任有影响的义务。另外还有区域性的文书，如《欧洲联盟电子签名指令》，为在该区域运营的认证服务提供人的赔偿责任提供了类似的立法框架。但是，这些文本都没有涵盖因国际上使用某些电子认证和签名办法而出现的所有赔偿责任问题。

28. 立法者和决策者必须理解各种国内赔偿责任制度之间的区别和共同要素，以便为承认外国证书所支持的签名拟定适当的办法和程序。各个国家的国内法律因为具有共同的法律传统或属于一个区域性统一框架等原因，可能已经对本参考文件中讨论的各种问题做出了大体上等同的回答。这些国家可能认为拟定共同的赔偿责任标准或甚至统一其国内规则是有益的，这样可有利于跨国界使用电子认证和签名办法。

---