United Nations A/CN.9/630/Add.5

General Assembly

Distr.: General
16 April 2007

Original: English

United Nations Commission on International Trade Law
Fortieth session
Vienna, 25 June-12 July 2007

Possible future work on electronic commerce

Comprehensive reference document on elements required to establish a favourable legal framework for electronic commerce: sample chapter on international use of electronic authentication and signature methods

Note by the Secretariat

Addendum

The annex to the present note contains the final part of a sample chapter (part two, chap. II, sect. B.2) dealing with legal issues related to the international use of electronic authentication and signature methods.

V.07-82296 (E) 110507 140507

Annex

Contents

Part Two

Cross-border use of electronic signature and authentication methods (*continued*)

[…]

II. Methods and criteria for establishing legal equivalence

B. Equivalence of standards of conduct and liability regimes

2. Particular instances of liability in a public key infrastructure framework

1. The main focus of discussions concerning liability in connection with the use of electronic signature and authentication methods has been the basis and characteristics of the liability of certification services providers. It is generally accepted that the basic duty of a certification services provider is to utilize trustworthy systems, procedures and human resources and to act in accordance with representations that the certification services provider makes with respect to its policies and practices.[1] In addition, the certification services provider is expected to exercise reasonable care to ensure the accuracy and completeness of all material representations it makes in connection with a certificate. All these activities may expose a certification services provider to a varying degree of liability, depending on the applicable law. The following paragraphs identify the instances that carry a greater risk for a certification services provider of being exposed to liability and summarize the way in which domestic laws deal with such liability.

(a) Failure to issue or delay in issuing a certificate

2. A certification services provider typically issues certificates upon application by candidate signatories. If an application meets the certification services provider's criteria, the certification services provider may issue a certificate. It is conceivable that an applicant might meet the criteria but nevertheless be rejected or delayed, either because the certification services provider simply makes a mistake, or because the certification services provider's application facilities are unavailable by design or accident, or because the certification services provider, for ulterior motives, wishes to delay or deny issuance of a certificate to the applicant. Applicants rejected or delayed under these circumstances may have claims against the certification services provider.[2]

3. If there is a competitive market for certification services, there might be no real harm to an applicant if a certification services provider were to refuse to issue a certificate, either by accident or on purpose. However, in the absence of meaningful competition, a certification services provider's refusal to issue a certificate or delay in issuing a certificate could cause serious harm where the rejected applicant is

---

[1] UNCITRAL Model Law on Electronic Signatures (see note […]), article 9, subparagraphs 1 (a) and 1 (b).

[2] Smedinghoff, "Certification authority: liability issues" (see note […]), section 3.2.1.

unable to engage in a particular business without the certificate. Even if competitive alternatives were available, one could envision transaction-specific losses arising from circumstances where a certificate was requested in connection with a particular transaction and, as a result of delay or denial, the certificate was not available in time for the intended transaction, forcing the applicant to forego the valuable transaction.[3]

4. This kind of scenario is unlikely to arise in an international context, since most signatories would be more likely to seek the services of certification services providers located in their own countries.

(b) Negligence when issuing a certificate

5. The principal function of a certificate is to bind an identity of the signatory to a public key. Accordingly, the principal task of a certification services provider is to verify, in conformance with its stated practices, that an applicant is the purported signatory and is in control of the private key corresponding to the public key listed in the certificate. Failure to do so may expose the certification services provider to potential liability to the signatory, or to a third party that relies on the certificate.

6. Damage to the signatory might be caused, for example, by the erroneous issuance of a certificate to an impostor using a misappropriated identity. The certification services provider's own employees or contractors might conspire to issue erroneous certificates using the certification services provider's signing key against improper applications by the impostor. Those persons might negligently issue an erroneous certificate, either by failing to perform properly the certification services provider's stated validation procedures in reviewing the impostor's application, or by using the certification services provider's signing key to create a certificate that has not been approved. Lastly, a malefactor might impersonate a signatory using forged, but seemingly authentic, identification documents, and convince the certification services provider, despite careful and non-negligent adherence to its published policies, to issue a certificate to the impostor.[4]

7. Erroneous issuance to an impostor could have very serious consequences. Relying parties who conduct online transactions with the impostor may rely on the incorrect data in the erroneously issued certificate and, as a result of that reliance, ship goods, transfer funds, extend credit, or undertake other transactions with the expectation that they are dealing with the impersonated party. When the fraud is discovered, the relying parties may have suffered substantial loss. In this situation, there are two injured parties: the relying party who was defrauded by the erroneously issued certificate, and the person whose identity was impersonated in the erroneously issued certificate. Both will have claims against the certification services provider. Another scenario might be the negligent issuance of a certificate to a fictitious person, in which case only the relying party would suffer damage.[5]

8. Article 9 of the UNCITRAL Model Law on Electronic Signatures provides, inter alia, that a certification services provider shall "exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that

---

[3] Ibid.
[4] Ibid.
[5] Ibid.

are relevant to the certificate throughout its life cycle or that are included in the certificate". This general duty has been literally transposed into the domestic legislation of several countries implementing the Model Law,[6] although in some countries the standard seems to have been raised from "reasonable care" to a higher warranty standard.[7]

9. The regime established by the European Union Directive on electronic signatures obliges European Union member States, as "a minimum", to ensure that by issuing a certificate as a qualified certificate to the public, or by guaranteeing such a certificate to the public, a certification services provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate: (a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate; (b) for assurance that, at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate; (c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification services provider generates them both; unless the certification services provider proves that he has not acted negligently.[8]

10. Other domestic laws generally coincide in imposing on certification services providers the obligation to verify the accuracy of the information on the basis of which a certificate is issued. In some countries, a certification services provider is generally held liable to any person who reasonably relied on the certificate for the accuracy of all information in the accredited certificate as from the date on which it was issued,[9] or guarantees its accuracy,[10] although in some of those countries the certification services provider may qualify this warranty by an appropriate statement in the certificate.[11] Some laws, however, expressly exempt the certification services provider from liability for inaccurate signatory-provided information, subject to verification according to the certificate practice statement, provided that the

---

[6] For example, Thailand, Electronic Transactions Act (2001), section 28, paragraph 2; and Cayman Islands (overseas territory of the United Kingdom), Electronic Transactions Law, 2000, section 28 (b).

[7] For example, China, Electronic Signatures Law, article 22: "Electronic certification service providers **shall ensure** that the contents of electronic signature certificates are complete and accurate during their valid term, and shall ensure that parties relying on electronic signatures can verify or comprehend all of the recorded contents of electronic signature certificates and other relevant matters", emphasis added.

[8] European Union Directive on electronic signatures (see note […]), article 6, paragraph 1.

[9] Barbados, chapter 308B, Electronic Transactions Act (1998), section 20, paragraph 1 (a); Bermuda, Electronic Transactions Act, 1999, section 23; Hong Kong (Special Administrative Region (SAR) of China), Electronic Transactions Ordinance, section 39; India, Information Technology Act, 2000, section 36 (e); Mauritius, Electronic Transactions Act 2000, section 27, paragraph 2 (d); and Singapore, Electronic Transactions Act, sections 29, subsection (2)(a) and (c), and 30, subsection (1).

[10] Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 18; and Viet Nam, Law on Electronic Transactions, article 31 (d).

[11] For example, Barbados, Bermuda, Hong Kong SAR, Mauritius and Singapore.

certification services provider can prove that it took all reasonable measures to verify the information.[12]

11. In other countries the same result is achieved not by a statutory warranty, but by imposing on certification services providers a general duty to verify the information supplied by the signatory before issuing a certificate,[13] or to establish systems for verifying such information.[14] In some cases, there is an obligation to revoke a certificate immediately upon finding out that information on which the certificate was issued was inaccurate or false.[15] In a few cases, however, the law is silent about the issuance of certificates, merely requiring the certification services provider to comply with its certification practice statement[16] or to issue the certificate as agreed with the signatory.[17] This does not mean that the law does not contemplate any liability for certification services providers. On the contrary, some laws clearly contemplate certification services provider liability, by requiring the certification services provider to purchase adequate third-party liability insurance covering all contractual and extra-contractual damage caused to signatories and third parties.[18]

12. The certification services provider's duty to verify the accuracy of the information that is provided is supplemented by a duty of the signatory to "exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate."[19] The signatory could therefore be held liable, either to the certification services provider or to the relying party, for providing false or inaccurate information to the certification services provider when applying for a certificate. Sometimes this is formulated as a general duty to provide accurate information to the certification services provider,[20] or to exercise reasonable care to ensure the correctness of the information;[21] sometimes the signatory is expressly declared liable for damages resulting from its failure to comply with this particular requirement.[22]

---

[12] Argentina, *Ley de firma digital (2001)*, article 39 (c).

[13] Ibid., article 21 (o); Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, article 12 (e); Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (I); and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[14] Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 30 (d).

[15] Argentina, *Ley de firma digital (2001)*, article 19 (e)(2).

[16] Peru, *Decreto reglamentario de la ley de firmas y certificados digitales*, article 29 (a).

[17] Colombia, *Ley 527 sobre comercio electrónico*, article 32 (a); Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 40 (a); and Panama, *Ley firma digital (2001)*, article 49, paragraph 7.

[18] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 32.

[19] UNCITRAL Model Law on Electronic Signatures (see note [...]), article 8, subparagraph 1 (c).

[20] Argentina, *Ley de firma digital (2001)*, article 25; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; and Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III).

[21] Cayman Islands, Electronic Transactions Law 2000, section 31 (c).

[22] Colombia, *Ley 527 sobre comercio electrónico*, article 40; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III); and Panama, *Ley de firma digital (2001)*, article 39.

(c) Unauthorized use of signature or compromised certificate practice statement

13. There are two aspects of unauthorized use of signature creation devices and certificates. On the one hand, a signature creation device might not be properly kept or be otherwise compromised, for instance by misappropriation by an agent of the signatory. On the other hand, the actual signing hierarchy of the certification services provider might be compromised, for instance if either the certification services provider's own signing key or the root key are lost, or disclosed to or used by unauthorized persons, or otherwise compromised.

14. The signing hierarchy might be compromised in various ways. The certification services provider or one of its employees or contractors might accidentally destroy or lose control of the key, the data centre that held the private key might be damaged by an accident, or the certification services provider's key might be destroyed intentionally or compromised by someone for unlawful purposes (e.g. a hacker). The consequences of a compromise of the signing hierarchy could be very serious. For instance, if either the private signing key or the root keys were to fall into the hands of a malefactor, that person could generate false certificates and use them to impersonate real or fictitious signatories, to the detriment of relying parties. Furthermore, once the damage was discovered, all certificates issued by the certification services provider would need to be revoked, resulting in a potentially massive claim by the entire signatory community for loss of use.

15. This matter is not dealt with in detail in the UNCITRAL Model law on Electronic Signatures. Arguably, the general obligation of the certification services provider under the Model Law to "use trustworthy systems, procedures and human resources"[23] could be construed as imposing a duty on a certification services provider to take all necessary measures to prevent its own key (and thereby its entire signing hierarchy) from being compromised. Several domestic laws explicitly provide for such an obligation, often combined with the certification services provider's obligation to utilize trustworthy systems.[24] Sometimes there is a specific duty to take measures to avoid forgery of certificates.[25] A certification services provider is under a duty to refrain from creating or accessing the signature creation data of the signatories, and may be liable for acts of its employees that deliberately do so.[26] A certification services provider would be placed under a duty to request the revocation of its own certificate, if its signature creation data is compromised.[27]

16. The signatory is also required to exercise all due care. The UNCITRAL Model Law on Electronic Signatures, for example, requires the signatory to "exercise reasonable care to avoid unauthorized use of its signature creation data".[28] A similar duty exists under most domestic laws, although with some variations. In some cases, the law subjects the signatory to a strict obligation to ensure exclusive control over

---

[23] UNCITRAL Model Law on Electronic Signatures (see note [...]), article 9, subparagraph 1 (f).

[24] Argentina, *Ley de firma digital (2001)*, article 21 (c) and (d); Colombia, *Ley 527 sobre comercio electrónico*, article 32 (b); Mauritius, Electronic Transactions Act 2000, article 24; Panama, *Ley de firma digital (2001)*, article 49, paragraph 5; Thailand, Electronic Transactions Act (2001), section 28, paragraph 6; and Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 13.

[25] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[26] Argentina, *Ley de firma digital (2001)*, article 21 (b).

[27] Ibid., article 21 (p).

[28] UNCITRAL Model Law on Electronic Signatures (see note [...]), article 8, subparagraph 1 (a).

the signature creation device and prevent its unauthorized use,[29] or makes the signatory solely responsible for safekeeping the signature creation device.[30] Often, however, this obligation is qualified as a duty to keep adequate control over the signature creation device or to take adequate measures to keep control over it,[31] to act diligently to avoid unauthorized use,[32] or to exercise reasonable care to avoid unauthorized use of its signature device.[33]

(d) Failure to suspend or revoke a certificate

17. The certification services provider could also incur liability for failing to suspend or revoke a compromised certificate. For a digital signature infrastructure to function properly and enjoy trust, it is critical that a mechanism be in place to determine in real time whether a particular certificate is valid, or whether it has been suspended or revoked. Whenever a private key is compromised, for example, revocation of the certificate is the primary mechanism by which a signatory can protect itself from fraudulent transactions initiated by impostors who may have obtained a copy of their private key.

18. As a consequence, the speed with which the certification services provider revokes or suspends a signatory's certificate following a request from the signatory is critical. The lapse of time between a signatory's request to revoke a certificate, the actual revocation and the publication of the notice of revocation, could allow an impostor to enter into fraudulent transactions. Consequently, if the certification services provider unreasonably delays posting a revocation to a certificate revocation list, or fails to do so, both the signatory and the defrauded relying party could suffer significant damages in reliance upon an allegedly valid certificate. Furthermore, as part of their certification services, certification services providers may offer to maintain online depositories and certificate revocation lists that will be accessible by relying parties. Maintaining this database involves two basic risks: that the repository or certificate revocation list might be inaccurate, thereby providing erroneous information upon which the recipient will rely to its detriment; and the risk that the repository or certificate revocation list will be unavailable (e.g. because of system failure), thereby interfering with the ability of signatories and relying parties to complete transactions.

---

[29] Argentina, *Ley de firma digital (2001)*, article 25 (a); Colombia, *Ley 527 sobre comercio electrónico*, article 39, paragraph 3; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 53 (d); Panama, *Ley de firma digital (2001)*, article 37, paragraph 4; Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 1; and Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15 (e).

[30] Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 21.

[31] Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; and Viet Nam, Law on Electronic Transactions, article 25, paragraph 2 (a).

[32] Bolivarian Republic of Venezuela, *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

[33] Cayman Islands, Electronic Transactions Law, 2000, section 39 (a); Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (b); India, Information Technology Act, 2000, section 42, paragraph 1; Mauritius, Electronic Transactions Act 2000, section 35, paragraph 1 (a) and (b); Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (II); Singapore, Electronic Transactions Act (chapter 88), section 39; and Thailand, Electronic Transactions Act (2001), section 27, paragraph 1.

19. As indicated earlier, the UNCITRAL Model Law on Electronic Signatures assumes that the certification services provider may issue various levels of certificates with varying degrees of reliability and security. Accordingly, the Model Law does not require a certification services provider to always make available a revocation system, which may not be commercially reasonable for certain types of low-value certificate. Instead, the Model Law only requires the certification services provider to provide "reasonably accessible means" that enable a relying party to ascertain from the certificate, inter alia, "whether means exist for the signatory to give notice" that the signature creation data have been compromised and "whether a timely revocation service is offered".[34] Where a timely revocation service is offered, the certification services provider is obliged to ensure its availability.[35]

20. The regime established by the European Union Directive on electronic signatures obliges European Union member States, as "a minimum", to ensure that a certification services provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate, unless the certification services provider proves that it has not acted negligently.[36] Some domestic laws oblige the certification services provider to take measures to prevent certificate forgery[37] or to revoke a certificate immediately upon finding out that information on which the certificate was issued was inaccurate or false.[38]

21. A similar duty may also exist for the signatory and other authorized persons. The UNCITRAL Model Law on Electronic Signatures, for example, requires the signatory "without undue delay", to "utilize means made available by the certification service provider", or "otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature" if the signatory "knows that the signature creation data have been compromised" or if "circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised".[39]

22. Domestic laws often affirm the duty of the signatory to request revocation of the certificate in any circumstance where the secrecy of the signature creation data might have been compromised,[40] although in some cases the law only obliges the

---

[34] UNCITRAL Model Law on Electronic Signatures (see note […]), article 9, subparagraph 1 (d), (v) and (vi).

[35] Ibid., article 9, subparagraph 1 (e).

[36] European Union Directive on electronic signatures (see note […]), article 6, paragraph 2; see also paragraph (b) of annex II to the Directive.

[37] Panama, *Ley de firma digital (2001)*, article 49, paragraph 6.

[38] Argentina, *Ley de firma digital (2001)*, article 19 (e)(2).

[39] UNCITRAL Model Law on Electronic Signatures (see note […]), article 8, subparagraph 1 (b), (i) and (ii).

[40] Argentina, *Ley de firma digital (2001)*, article 25 (c); Colombia, *Ley 527 sobre comercio electrónico*, article 39, paragraph 4; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, articles 49 and 53 (e); Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (f); Mauritius, Electronic Transactions Act 2000, article 36; Panama, *Ley de firma digital (2001)*, article 37, paragraph 5; Singapore, Electronic Transactions Act (chapter 88), section 40; and Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 1.

signatory to communicate that fact to the certification services provider.[41] The laws of several countries have adopted the formulation in the UNCITRAL Model Law on Electronic Signatures, which places the signatory under an obligation to further notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature.[42] Although the consequences of breach of this duty may be implied in a number of legal systems, in some countries the law expressly declares the signatory liable for failure to communicate the loss of control over the private key or failure to request the revocation of the certificate.[43]

Conclusion

23. Wide use of electronic authentication and signature methods may be a significant step to reduce trade documentation and the related costs in international transactions. While to a very large extent the pace of developments in this area is mainly determined by the quality and security of technological solutions, the law may offer a significant contribution towards facilitating the use of electronic authentication and signature methods.

24. A large number of countries have already taken domestic measures in that direction by adopting legislation that affirms the legal value of electronic communications and sets the criteria for their equivalence to paper-based ones. Provisions regulating electronic authentication and signature methods are often an important component of such laws. The UNCITRAL Model Law on Electronic Commerce[44] has become the single most influential standard for legislation in this area and its wide implantation has helped to promote an important degree of international harmonization. Wide ratification of the United Nations Convention on the Use of Electronic Communications in International Contracts[45] would provide even greater harmonization, by offering a particular set of rules for international transactions.

25. International use of electronic authentication and signature methods may also benefit from the adoption of those UNCITRAL standards. In particular, the flexible criteria for functional equivalence between electronic and paper-based signatures contained in the United Nations Convention on the Use of Electronic Communications in International Contracts may provide an international common

---

[41] India, Information Technology Act, 2000, section 42, paragraph 2; and Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15 (f) and (i).

[42] Cayman Islands, Electronic Transactions Law, 2000, section 31 (b); China, Electronic Signatures Law, article 15; Thailand, Electronic Transactions Act (2001), section 27, paragraph 2; and Viet Nam, Law on Electronic Transactions, article 25, paragraph 2 (b).

[43] China, Electronic Signatures Law, article 27; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17 (e); Panama, *Ley de firma digital (2001)*, article 39; Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12, paragraph 2; and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 40.

[44] See note […] [United Nations publication, Sales No. E.99.V.4].

[45] See note […] [General Assembly resolution 60/21, annex].

framework for allowing electronic authentication and signature methods to meet foreign form signature requirements. Nevertheless, some problems may persist, in particular in connection with international use of electronic authentication and signature methods that require the involvement of a trusted third party in the authentication or signature process.

26. The problems that arise in this particular area derive to a very large extent from inconsistency of technical standards or incompatibility of equipment or software, resulting in lack of international interoperability. Efforts to harmonize standards and improve technical compatibility may lead to a solution to the difficulties that exist at present. However, there are also legal difficulties related to use of electronic authentication and signature methods, in particular in connection with domestic laws that either prescribe or favour the use of a particular technology for electronic signatures, typically digital signature technology.

27. Laws that provide for the legal value of digital signatures typically attribute the same legal value to signatures supported by foreign certificates only to the extent that they are regarded as equivalent to domestic certificates. The review done in this study indicates that proper assessment of legal equivalence requires a comparison not only of the technical and security standards attached to a particular signature technology, but also of the rules that would govern the liability of the various parties involved. The UNCITRAL Model Law on Electronic Signatures provides a set of basic common rules governing certain duties of the parties involved in the authentication and signature process that may have an impact on their individual liability. There are also regional texts, such as the European Union Directive on electronic signatures, that offer a similar legislative framework for the liability of certification services providers operating in the region. However, neither of those texts addresses all liability issues arising out of the international use of certain electronic authentication and signature methods.

28. It is important for legislators and policymakers to understand the differences between domestic liability regimes and the elements common to them, so as to devise appropriate methods and procedures for recognition of signatures supported by foreign certificates. The domestic laws of various countries may already provide substantially equivalent answers to the various questions discussed in the present reference document, for instance because they share a common legal tradition or belong to a regional integration framework. Such countries may find it useful to devise common liability standards or even harmonize their domestic rules, so as to facilitate cross-border use of electronic authentication and signature methods.