United Nations A/CN.9/630/Add.4

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 part (part two, chap. II, sects. A and B.1) of a sample chapter of a comprehensive reference document dealing with legal issues related to the international use of electronic authentication and signature methods.

V.07-82265 (E) 080507 090507

Annex

Contents

Part Two

Cross-border use of electronic signature and authentication methods

[…]

II. Methods and criteria for establishing legal equivalence

1. As indicated above, the survey undertaken by the Working Party on Information Security and Privacy (WPISP) of the Organization for Economic Cooperation and Development (OECD) (hereinafter OECD WPISP) found that most legislative frameworks were at least in principle non-discriminatory towards foreign electronic signatures and authentication, provided local requirements or their equivalent were met, in the sense that they did not deny legal effectiveness to signatures relating to services originating from countries, provided those signatures had been created under the same conditions as those recognized under domestic law.[1] However, OECD WPISP also noted that mechanisms for recognizing foreign authentication services were generally not well developed and identified this as an area where future work might be useful. Given that any work in this area would be closely related to the more general subject of interoperability, OECD WPISP suggested that the topics could be combined. OECD WPISP suggested that a set of best practices or guidelines might be developed.

2. The following sections discuss the legal arrangements and mechanisms for international interoperability and factors that determine the equivalence of liability regimes. They focus primarily on issues arising out of the international use of electronic signature and authentication methods supported by certificates issued by a trusted third-party certification services provider, in particular digital signatures under a public key infrastructure (PKI), since legal difficulties are more likely to arise in connection with the cross-border use of electronic signature and authentication methods that require the involvement of third parties in the signature or authentication process.

A. Types and mechanisms of cross recognition

3. The additional burden placed on foreign certification services providers by domestic technology-driven requirements has the potential to become a barrier to international trade.[2] For example, laws relating to the means by which national authorities grant recognition to foreign electronic signatures and certificates could discriminate against foreign businesses. So far, every legislature that has considered this issue has included in its laws some requirement relating to the standards

---

[1] See note […] [*The Use of Authentication across Borders in OECD Countries*].

[2] See Alliance for Global Business, "A discussion paper on trade-related aspects of electronic commerce in response to the WTO's e-commerce work programme", April 1999, http://www.biac.org/statements/iccp/AGBtoWTOApril1999.pdf, accessed on 5 February 2007, p. 29.

adhered to by the foreign certification services provider, so the issue is inextricably related to the broader question of conflicting national standards. At the same time, legislation may also impose other geographic or procedural limitations that prevent cross-border recognition of electronic signatures.

4. In the absence of an international PKI, a number of concerns could arise with respect to the recognition of certificates by certification authorities in foreign countries. The recognition of foreign certificates is often achieved by a method called "cross certification". In such a case, it is necessary that substantially equivalent certification authorities (or certification authorities willing to assume certain risks with regard to the certificates issued by other certification authorities) recognize the services provided by each other, so their respective users can communicate with each other more efficiently and with greater confidence in the trustworthiness of the certificates being issued. Legal issues may arise with regard to cross certifying or chaining of certificates when there are multiple security policies involved, such as determining whose misconduct caused a loss and upon whose representations the user relied.

1. Cross recognition

5. Cross recognition is an interoperability arrangement in which the relying party in the area of a PKI can use authority information in the area of another PKI to authenticate a subject in the area of the other PKI.[3] This is typically the result of a formal licensing or accreditation process in the area of the other PKI, or of a formal audit process performed on the representative certification services provider of the PKI area.[4] The onus of whether to trust a foreign PKI area lies with the relying party or the owner of the application or service, rather than with a certification services provider that the relying party directly trusts.

6. Cross recognition would typically occur at the PKI level rather than at the level of the individual certification services provider. Thus, where a PKI recognizes another PKI, it automatically recognizes any certification services providers accredited under that PKI scheme. Recognition would be based on assessment of the other PKI's accreditation process rather than assessing each individual certification services provider accredited by the other PKI. Where PKIs issue multiple classes of certificates, the cross-recognition process involves identifying a class of certificates acceptable for use in both areas and basing the assessment on that class of certificates.

7. Cross recognition entails issues of technical interoperability at the application level only, i.e. the application must be able to process the foreign certificate and access the directory system of the foreign PKI area to validate the status of the foreign certificate. It should be noted that, in practice, certification services providers issue certificates with various levels of reliability, according to the

---

[3] The concept of cross recognition was developed in 2000 by the then Asia-Pacific Economic Cooperation Telecommunications and Information Working Group, Electronic Authentication Task Group, see APEC publication No. 202-TC-01.2, *Electronic authentication: issues relating to its selection and use* (APEC, 2002), available at http://www.apec.org/apec/publications/all_publications/telecommunications.html, accessed on 7 February 2007.

[4] Definition based on the work of the APEC Telecommunications and Information Working Group, Electronic Authentication Task Group.

purposes for which the certificates are intended to be used by their customers. Depending on their respective level of reliability, certificates and electronic signatures may produce varying legal effects, both domestically and abroad. For example, in certain countries, even certificates that are sometimes referred to as "low-level" or "low-value" certificates might, under certain circumstances (e.g. where parties have agreed contractually to use such instruments), produce legal effect (see below, paras. [42-50]). Therefore, the equivalence to be established is between functionally comparable certificates.

8. As said above, in cross recognition the decision to trust a foreign certificate lies with the relying party, not with its certification services provider. It does not necessarily involve a contract or agreement between two PKI domains. Detailed mapping of certificate policies[5] and certificate practice statements[6] is also unnecessary, as the relying party decides whether to accept the foreign certificate based on whether the certificate has been issued by a trustworthy foreign certification services provider. The certification services provider is regarded as trustworthy if it has been licensed or accredited by a formal licensing or accreditation body, or has been audited by a trusted independent third party. The relying party makes an informed decision unilaterally based on the policies stipulated in the certificate policy or certificate practice statement in the foreign PKI domain.

2. Cross certification between public key infrastructures

9. Cross certification refers to the practice of recognizing another certification services provider's public key to an agreed level of confidence, normally by virtue of a contract. It essentially results in two PKI domains being merged (in whole or in part) into a larger domain. To the users of one certification services provider, the users of the other certification services provider are simply signatories within the extended PKI.

10. Cross certification involves technical interoperability and the harmonization of certificate policies and certificate practice statements. Policy harmonization, in the form of the harmonization of certificate policies and certificate practice statements, is necessary to ensure that PKI domains are compatible both in terms of their certificate management operations (i.e. certificate issuance, suspension and revocation) and in their adherence to similar operational and security requirements. The amount of liability coverage is also relevant. This step is highly complex, as these documents are typically voluminous and deal with a wide range of issues.

11. Cross certification is most suitable for relatively closed business models, e.g. if both PKI domains share a set of applications and services, such as e-mail or financial applications. Having technically compatible and operable systems, congruent policies and the same legal structures would greatly facilitate cross certification.

---

[5] A certificate policy is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

[6] A certificate practice statement is a statement of the practices that a certification services provider employs in issuing certificates.

12. Unilateral cross certification (whereby one PKI domain trusts another but not vice versa) is uncommon. The trusting PKI domain must ensure unilaterally that its policies are compatible with those of the trusted PKI domain. Its use seems to be limited to applications and services where the trust required for the transaction involved is unilateral, e.g. an application in which the merchant has to prove the identity to the customer before the latter submits confidential information.

B. Equivalence of standards of conduct and liability regimes

13. Whether international use of electronic signature and authentication methods is based on a cross-recognition or cross-certification scheme, a decision to recognize a whole PKI or one or more foreign certification services providers, or to establish equivalent levels between classes of certificates issued under different PKIs, presupposes an assessment of the equivalence between the domestic and the foreign certification practices and certificates.[7] From a legal point of view, this requires an assessment of the equivalence between three main elements: equivalence in legal value; equivalence in legal duties; and equivalence in liability.

14. Equivalence in legal value means attributing to a foreign certificate and signature the same legal effect of a domestic equivalent. The resulting domestic legal effect will be determined essentially on the basis of the value attributed by the domestic law to electronic signature and authentication methods, which has already been discussed (see above, paras. […]-[…]). Recognizing the equivalence in legal duties and liability regimes entails a finding that the duties imposed on the parties operating under a PKI regime correspond in substance to those existing under the domestic regime and that their liability for breaches of those duties is substantially the same.

15. Liability in the context of electronic signatures may give rise to different issues depending on the technology and the certification infrastructure used. Complex issues may arise especially in those cases where certification is provided by a dedicated third party, such as a certification services provider. In this case, there will essentially be three parties involved, namely the certification services provider, the signatory and the relying third party. To the extent that their acts or omissions cause harm to any of the others, or contravene their express or implied duties, each could become liable, or may lose the right to assert liability, against another party. Various legislative approaches have been adopted with respect to liability in connection with the use of digital signatures:

(a) **No specific provisions on standards of conduct or liability**. One option may be for the law to remain silent on this point. In the United States of America, the Electronic Signatures in Global and National Commerce Act 2000[8] does not provide for the liability of any of the parties involved in the certification service.

---

[7] The United States Federal Public Key Infrastructure Policy Authority, Certificate Policy Working Group, for example, has developed a methodology for providing a judgement as to the equivalence between elements of policy (based on the framework defined in RFC ("Request for Comments") 2527). This methodology may be used when mapping different PKIs or mapping a PKI against these guidelines (see http://www.cio.gov/fpkipa, accessed on 20 February 2007).

[8] See note […] [United States Code, title 15, chapter 96, section 7031 (Principles governing the use of electronic signatures in international transactions)].

Generally speaking, this approach has been adopted in most other jurisdictions taking a minimalist approach to electronic signatures, such as Australia;[9]

(b) **Standards of conduct and liability rules for certification services providers only**. Another approach is for the law to provide only for the liability of the certification services provider. This is the case under European Union Directive 1999/93/EC on a Community framework for electronic signatures,[10] in which recital 22 states that "Certification-service-providers providing certification-services to the public are subject to national rules regarding liability", as outlined in article 6 of the Directive. It is worth noting that article 6 applies only to "qualified signatures", which, for the time being, means PKI-based digital signatures only;[11]

(c) **Standards of conduct and liability rules for signatory and certification services providers**. In some jurisdictions, the law provides for the liability of the signatory and of the certification services provider, but does not establish a standard of care of the relying party. This is the case in China, under the Electronic Signatures Law of 2005. This is also the case in Singapore, under the Electronic Transactions Act, 1998;

(d) **Standards of conduct and liability rules for all parties**. Finally, the law may provide for standards of conduct and a basis for the liability of all parties involved. This approach is adopted in the UNCITRAL Model Law on Electronic Signatures,[12] which indicates the duties relating to the conduct of the signatory (art. 8), of the certification services provider (art. 9) and of the relying party (art. 11). The Model Law can be said to set out criteria against which to assess the conduct of those parties. However, it leaves to the domestic law to determine the consequences of the inability to fulfil the various duties and the basis for the liability that may affect the various parties involved in the operation of electronic signature systems.

16. Differences in domestic liability regimes may be an obstacle to the cross-border recognition of electronic signatures. There are two main reasons for this. Firstly, certification services providers may be reluctant to recognize foreign certificates or the keys issued by foreign certification services providers whose liability or standards of care may be lower than their own. Secondly, users of electronic signature and authentication methods, too, may fear that lower liability limits or standards of care of a foreign certification services provider may limit the remedies available to them in case, for instance, of forgery or false reliance. For the same reasons, where the use of electronic signature and authentication methods, or

---

[9] It was felt, for example, that private law mechanisms admitted by Australian law, such as contractual exclusions, waivers and disclaimers of liability, and the limits posed to their operation by the common law, were better suited for regulating liability than statutory provisions (see Mark Sneddon, Legal liability and e-transactions: a scoping study for the National Electronic Authentication Council (National Office for the Information Economy, Canberra, 2000), http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf, accessed on 7 February 2007, pp. 43-47).

[10] See note […] [*Official Journal of the European Communities*, L 13/12].

[11] Legislation adopted in the European Union follows this approach, for instance, the German law on electronic signature (SignaturGesetz – SigG) and the related ordinance (SigV), 2001, the Austrian Federal Electronic Signature Law (SigG) and the United Kingdom of Great Britain and Northern Ireland Electronic Signature Regulation 2002, section 4.

[12] See note […] [United Nations publication, Sales No. E.02.V.8].

the activities of certification services providers, is provided for by legislation, the law typically subjects recognition of foreign certificates or certification services providers to some assessment of substantive equivalence with the reliability offered by domestic certificates and certification services providers. The standards of care and levels of liability to which the various parties are subject constitute the main legal benchmark against which the equivalence is measured. Moreover, the ability of the certification services provider to limit or disclaim its liability will also have an impact on the level of equivalence afforded to its certificates.

1. Basis for liability in a public key infrastructure framework

17. Allocation of liability under a PKI framework is effected essentially in two ways: by means of contractual provisions, or by the law (precedent, statute or both). The relations between the certification services provider and the signatory are typically of a contractual nature and, therefore, liability will typically be based on a breach of either party's contractual obligations. The relations between the signatory and the third party will depend on the nature of their dealing in any concrete instance. They may or may not be based on contract. Lastly, the relations between the certification services provider and the relying third party would in most cases not be based on contract.[13] Under most legal systems the basis of liability (whether contract or tort) will have extensive and significant consequences for the liability regime, in particular as regards the following elements: (a) the degree of fault that is required to engage a party's liability (in other words, what is the "standard of care" owed by one party to the other); (b) the parties that may claim damages and the extent of damages recoverable by them; and (c) whether and to what extent a party at fault is able to limit or disclaim its liability.

18. It flows from the above not only that the standards of liability will vary from one country to the other, but also that within one country they will vary depending on the nature of the relationship between the party held liable and the injured party. Furthermore, various legal rules and theories may have an impact on one or the other aspect of liability under both a contractual or a common law or statutory liability regime, which sometimes lessens the differences between the two regimes. The present study cannot attempt to offer a complete detailed analysis of these general questions. It will instead focus on questions specifically raised in a PKI context and briefly discuss how domestic laws have approached them.

(a) Standard of care

19. Although different legal systems use different ranking systems and theories, for the purposes of this study it is assumed that the liability of the parties involved in a PKI framework would essentially be based on three possible standards: ordinary

---

[13] Steffen Hindelang, in "No remedy for disappointed trust: the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared", *Journal of Information, Law and Technology*, 2002, Issue No. 1, (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang, accessed on 6 February 2007), at 4.1.1, discussed in detail the possibility of creating a contractual relationship between the certification services provider and the third party under English law, coming to a negative conclusion. However, there are jurisdictions where a contractual relation might arise.

negligence or fault; presumed negligence (or fault with reversed burden of proof); and strict liability.[14]

(i) Ordinary negligence

20. Under this general standard, a person is legally required to compensate other people for the negative consequences of his or her actions, provided that the relationship to that other person is one that gives rise at law to a duty of care. Furthermore, the standard of care generally required is that of "reasonable care," which may be defined simply as the degree of care that a person of ordinary prudence, knowledge and foresight would exercise in the same or similar circumstances. In common law jurisdictions, this is often referred to as the "reasonable person" standard, whereas in several civil law jurisdictions this is often referred to as the "good family father" (*bonus pater familias*) standard. Viewed specifically from a business perspective, reasonable care refers to the degree of care that an ordinarily prudent and competent person engaged in the same line of business or endeavour would exercise under similar circumstances. Where liability is generally based on ordinary negligence, it is incumbent upon the injured party to demonstrate that the damage was caused by the other party's faulty breach of its obligations.

21. Reasonable care (or ordinary negligence) is the general standard of care contemplated in the UNCITRAL Model Law on Electronic Signatures. This standard of care applies to certification services providers in respect of issuance and revocation of certificates and disclosure of information.[15] A number of factors may be used in assessing compliance by the certification services provider with its general standard of care.[16] The same standard also applies to signatories in respect of preventing unauthorized use and safekeeping signature creation devices.[17] The

---

[14] For the discussion of the liability system in this context, see Balboni, "Liability of certification service providers …" (see note […]), pp. 232 ff.

[15] See note […] [United Nations publication, Sales No. E.02.V.8]. Article 9, paragraph 1, of the Model Law states: "Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall": (…) "(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate; (c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:" (…); "(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (…)".

[16] See note […] [*Model Law on Electronic Signatures with Guide to Enactment 2001*]. Paragraph 146 of the Guide to Enactment states "In assessing the liability of the certification service provider, the following factors should be taken into account, inter alia: (a) The cost of obtaining the certificate; (b) The nature of the information being certified; (c) The existence and extent of any limitation on the purpose for which the certificate may be used; (d) The existence of any statement limiting the scope or extent of the liability of the certification service provider; and (e) Any contributory conduct by the relying party. In the preparation of the Model Law, it was generally agreed that, in determining the recoverable loss in the enacting State, weight should be given to the rules governing limitation of liability in the State where the certification service provider was established or in any other State whose law would be applicable under the relevant conflict-of-laws rule."

[17] See note […] [United Nations publication, Sales No. E.02.V.8]. Article 8 of the Model Law states: "Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data; and (b) Without undue delay, utilize means made available by the certification

Model Law extends the same general standard of reasonable care to the relying party, which is expected to take reasonable steps to verify both the reliability of an electronic signature and the validity, suspension or revocation of the certificate and to observe any limitation with respect to the certificate.[18]

22. A few countries, typically enacting States of the UNCITRAL Model Law on Electronic Commerce,[19] have adopted the general standard of "reasonable care" for the conduct of the certification services provider.[20] In some countries, it appears that a certification services provider will "most likely be held to a general standard of reasonable care", although the fact that certification services providers, by their nature, will be parties with specialized skills in whom laypersons place trust beyond that extended to normal marketplace participants "may eventually give rise to professional status, or otherwise subject them to a higher duty of care to do what is reasonable given their specialized skills."[21] Indeed, as discussed below (see para. 29) this seems to be the situation in most countries.

23. As regards the signatory, some jurisdictions that have adopted the UNCITRAL Model Law on Electronic Signatures provide for a general standard of "reasonable care".[22] In various countries the law includes a more or less extensive list of positive obligations without describing the standard of care or indicating the consequences of failure to comply with those obligations.[23] In some countries, however, the law expressly complements the list of obligations with a general declaration of liability of the signatory for his or her breach,[24] which in one case is

---

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: (i) The signatory knows that the signature creation data have been compromised; or (ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised". Further, the signatory must "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".

[18] UNCITRAL Model Law on Electronic Signatures (see note […]), article 11, subparagraphs (a), (b)(i) and (b)(ii).

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

[20] For example, the Cayman Islands, Electronic Transactions Law, 2000, section 28; and Thailand, Electronic Transactions Act (2001), section 28.

[21] "Certification authority: liability issues", prepared for the American Bankers Association by Thomas J. Smedinghoff, February 1998 (http://www.bakernet.com/ecommerce/CA-Liability-Analysis.doc), accessed on 5 February 2007, section 1.1.

[22] For example, Thailand, Electronic Transactions Act (2001), section 27.

[23] For example, Argentina, *Ley de firma digital (2001)*, article 25; Cayman Islands, Electronic Transactions Law, 2000, section 31; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17; India, Information Technology Act, 2000, sections 40-42; Mauritius, Electronic Transactions Act 2000, articles 33-36; Peru, *Ley de firmas y certificados digitales*, article 17; Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 15; Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 21; and Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

[24] China, Electronic Signatures Law, promulgated 2004, article 27; Colombia, *Ley 527 sobre comercio electrónico*, article 40; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99; Dominican Republic, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, articles 53 and 55; Panama, *Ley de firma digital (2001)*, articles 37 and 39;

even of a criminal nature.[25] Arguably, there may not be a single standard of care, but a staggered system, with a general standard of reasonable care as a default rule for the signatory's obligations, which is however raised to a warranty standard in respect of some specific obligations, typically those that relate to accuracy and truthfulness of representations made.[26]

24. The situation of the relying party is a peculiar one, because it is unlikely that either the signatory or the certification services provider could be damaged by an act or omission of the relying party. In most circumstances, if the relying party fails to exercise the requisite degree of care, he or she would bear the consequences of his or her actions, but would not incur any liability towards the certification services provider. It is not surprising, therefore, that, when addressing the role of relying parties, domestic laws on electronic signatures seldom provide more than a general list of basic duties of the relying party. This is generally the case in jurisdictions that have adopted the UNCITRAL Model law on Electronic Signatures, which recommends a standard of "reasonable care" in relation to the conduct of the relying party.[27] In some cases, however, this requirement is not expressly stated.[28] It should be noted that the express or implied duties of the relying party are not irrelevant for the certification services provider. Indeed, a breach by the relying party of its duty of care may provide the certification services provider with a defence against liability claims by a relying party, for example, when the certification services provider can show that the damage sustained by the relying party could have been avoided or mitigated had the relying party taken reasonable measures to ascertain the validity of the certificate or the purposes for which it could be used.

(ii) Presumed negligence

25. The second possibility is a fault-based system with a reversed burden of proof. Under this system, a party's fault is presumed whenever damage has resulted from

---

Russian Federation, Federal Law on Electronic Digital Signature (2002), clause 12; Venezuela (Bolivarian Republic of), *Ley sobre mensajes de datos y firmas electrónicas*, article 19; and Viet Nam, Law on Electronic Transactions, article 25.

[25] Pakistan, Electronic Transactions Ordinance, 2002, section 34.

[26] For example, Singapore, Electronic Transactions Act (chapter 88). Section 37, paragraph 2, of the Act provides that by accepting a certificate the signatory "certifies to all who reasonably rely on the information contained in the certificate that (a) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate; (b) all representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and (c) all information in the certificate that is within the knowledge of the subscriber is true." Section 39, paragraph 1, in turn only contemplates "a duty to exercise reasonable care to retain control of the private key corresponding to the public key listed in such certificate and prevent its disclosure to a person not authorized to create the subscriber's digital signature." This seems also to be the case in the Bolivarian Republic of Venezuela, where article 19 of the *Ley sobre mensajes de datos y firmas electrónicas*, expressly qualifies the obligation to avoid unauthorized use of the signature creation device as one of "due diligence" (*"actuar con diligencia"*), whereas other obligations are expressed in categoric terms.

[27] Cayman Islands, Electronic Transactions Law, 2000, section 21; Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 107; and Thailand, Electronic Transactions Act (2001), section 30.

[28] Turkey, Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (2005), article 16; and Viet Nam, Law on Electronic Transactions, article 26.

an act attributable to it. The rationale for such a system is generally the assumption that, under certain circumstances, damage could in the normal course of events only have occurred because a party failed to comply with its obligations or abide by a standard of conduct expected from it.

26. In civil law, presumed fault may occur in connection with liability for breach of contract,[29] and also for various instances of tort liability. Examples include vicarious liability for the acts of employees, agents, infants or animals, liability arising in the course of some commercial or industrial activity (environmental damage, damage to adjacent property, transportation accidents). The theories justifying the reversal of the burden of proof and the particular instances in which it is admitted vary from country to country.

27. In practice, such a system leads to a result similar to the enhanced standard of care that is expected from professionals under common law. Professionals must have a minimum amount of special knowledge and skills necessary to act as a member of the profession and have a duty to act as a reasonable member of the profession would in a given circumstance.[30] This does not necessarily mean that the burden of proof is reversed, but the higher standard of care expected from the professional means in practice that professionals are deemed to be capable of avoiding doing harm to persons that hire their services or whose welfare is otherwise entrusted to them if they act according to those standards. Under certain circumstances, however, the so-called *res ipsa loquitur* doctrine allows courts to presume, absent proof to the contrary, that the occurrence of damage in the "ordinary course of things" is only possible due to a person's failure to exercise reasonable care.[31]

28. If this rule is applied to the activities of certification services providers, it would mean that whenever a relying party or a signatory sustains a damage as a

---

[29] Section 280, paragraph 1, of the Civil Code of Germany, for instance, declares the debtor liable for damage arising out of the breach of a contractual obligation unless the debtor is not responsible for the breach (*"Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat"*). Article 97, paragraph 1, of the Code of Obligations of Switzerland states this principle in even clearer terms: if the creditor does not obtain performance, the debtor is liable to compensate the resulting damage unless it can prove that the failure to perform was not attributable to its own fault (*"Lorsque le créancier ne peut obtenir l'exécution de l'obligation ou ne peut l'obtenir qu'imparfaitement, le débiteur est tenu de réparer le dommage en résultant, à moins qu'il ne prouve qu'aucune faute ne lui est imputable"*). A similar rule is contained in article 1218 of the Civil Code of Italy. Under French law, negligence is always presumed if the contract involved a promise of a certain result (*obligation de résultat*), but negligence must be established where the object of the contract was to offer a standard of performance (*obligation de moyen*), rather than a specific result (see Gérard Légier, "Responsabilité contractuelle", *Répertoire de droit civil Dalloz*, August 1989, No. 58-68).

[30] W. Page Keeton and others, *Prosser and Keeton on the Law of Torts*, 5th ed., (Saint Paul, Minnesota, West Publishing Co., 1984), section 32 at p. 187.

[31] "There must be reasonable evidence of negligence. But where the thing is shown to be under the management of the defendant or his servants, and the accident is such, as in the ordinary course of things, that it does not happen if those who have the management use proper care, it affords reasonable evidence, in the absence of explanation by the defendants, that the accident arose from want of care." (C. J. Erle in *Scott v. The London and St. Katherine's Docks Co.*, Ex. Ch., 3 H & C 596, 601, 159 Eng. Rep. 665, 667 (1865)).

result of using an electronic signature or certificate, and that damage can be attributed to a failure by the certification services provider to act in accordance with its contractual or statutory obligations, the certification services provider is presumed to have been negligent.

29. Presumed negligence seems to be the prevailing standard used under domestic laws. Under the European Union Directive on electronic signatures, for example, the certification services provider is liable for damages towards any entity that reasonably relies on the qualified certificate unless the certification services provider proves that it has not acted negligently.[32] In other words, the certification services provider liability is based on negligence with a reversal of the burden of proof: the certification services provider must prove that its actions were not negligent, since it is in the best position to do so, having the technical skills and access to the relevant information (both of which signatories and relying third parties might not possess).

30. This is also the case under various domestic laws outside the European Union that provide for an extensive list of duties to be observed by certification services providers, which generally subject them to liability for any loss caused by their failure to comply with their statutory obligations.[33] It is not altogether clear whether all of these laws actually reverse the burden of proof, but several do provide quite explicitly for such a reversal, either generally,[34] or in relation to specific obligations.[35]

---

[32] See note […] [*Official Journal of the European Communities*, L 13/12]. Article 6 of the Directive provides a minimum standard of liability. It would be possible for enacting States to strengthen the liability of the certification services provider, for instance by introducing a strict liability regime or extending liability also to non-qualified certificates. However, this has not happened so far and is unlikely to happen since it would place the certification services providers of one country in a disadvantaged position with respect to other European Union certification services providers (Balboni "Liability of certification service providers …" (see note […]), p. 222).

[33] Argentina, *Ley de firma digital (2001)*, article 38; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; Ecuador, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 31; Panama, *Ley de firma digital (2001)*, article 51; and Tunisia, *Loi relative aux échanges et au commerce électroniques*, article 22.

[34] China, Electronic Signatures Law, promulgated 2004, article 28: "If an electronic signatory or a person who relies on an electronic signature incurs a loss as a result of relying on the electronic signature certification service provided by an electronic certification service provider while engaging in civil activities, and if the electronic certification service provider fails to provide evidence that the provider was not at fault, then the electronic certification service provider shall bear liability for damages"; see also Turkey, Electronic Signature Law 2004, article 13: "Electronic Certificate Service Providers shall be liable for compensation for damages suffered by third parties as a result of infringing the provisions of this Law or the ordinances published in accordance with this Law. Liability of compensation shall not occur if the Electronic Certificate Service Provider proves the absence of negligence".

[35] Barbados, chapter 308B, Electronic Transactions Act (1998), section 20: "An authorized certification service provider is not liable for errors in the information in an accredited certificate where (a) the information was provided by or on behalf of the person identified in the accredited certificate; and (b) the certification service provider can demonstrate that he has taken all reasonably practical measures to verify that information."; see also Bermuda, Electronic Transactions Act, 1999, section 23, paragraph 2 (b).

31. The preference for a system of presumed fault is arguably the result of concerns that liability based on ordinary negligence would be not be fair to the relying party, which may lack the technological knowledge, as well as the access to relevant information, to satisfy the burden of showing the certification services provider's negligence.

(iii) Strict liability

32. Strict liability or "objective liability" (*responsabilité objective*) is a rule used in various legal systems to attach liability to a person (typically manufacturers or operators of potentially dangerous or harmful products or equipment) without a finding of fault or breach of a duty of care. The person is held to be liable simply for placing a defective product on the market or for the malfunctioning of a piece of equipment. Since liability is assumed from the mere fact that loss or damage has occurred, the individual legal elements required to establish an action such as negligence, breach of a warranty, or intentional conduct need not be established.

33. Strict liability is an exceptional rule under most legal systems and is ordinarily not presumed, absent clear statutory language. In the context of electronic signature and authentication methods, strict liability might impose an excessive burden on the certification services provider, which, in turn, might hinder the commercial viability of the industry at an early stage of its development. At present, no country appears to impose strict liability on either the certification services provider or any other parties involved in the electronic signature process. It is true that in countries that provide for a catalogue of positive obligations for certification services providers, the standard of care for certification services providers is typically very high, approaching in some cases a strict liability regime, but the certification services provider can still be released from liability if it can show that it acted with the required diligence.[36]

(b) Parties entitled to claim damages and extent of damages recoverable

34. One important issue in determining the extent of liability of certification services providers and signatories concerns the group of persons that might be entitled to claim compensation for damage caused by a breach by either party of their contractual or statutory obligations. Another related matter is the extent of the obligation to compensate and the types of damage that should be recompensed.

35. Contractual liability generally follows upon the breach of a contractual obligation. In a PKI context, a contract would usually exist between the signatory and the certification services provider. The consequences of breaches by one of its contractual obligations to another are determined by the words of the contract, as governed by applicable laws of contract. For electronic signatures and certificates, liability outside a clearly defined contractual relationship would typically arise in situations where a person has sustained damage in reasonable reliance on information provided either by the certification services provider or the signatory, which has turned out to be false or inaccurate. Normally, the relying third party does not enter into a contract with the certification services provider and probably does not interact with the certification services provider at all, except for relying on the

[36] For example, Chile, Ecuador and Panama.

certification. This may give rise to difficult questions not entirely answered in some jurisdictions.

36. Under most civil law systems, it could be assumed that a certification services provider would be liable for loss sustained by the relying party as a result of reliance on inaccurate or false information even without specific provisions to that effect in specific legislation dealing with electronic signatures. In several jurisdictions, this liability may follow from the general tort liability provision that has been introduced into most civil law codifications,[37] with few exceptions.[38] In some jurisdictions, an analogy could be drawn between the activities of a certification services provider and notaries public, who are generally held liable for damage caused by negligence in the performance of their duties.

37. In common law jurisdictions, however, the situation may not be so clear. Where a tort is committed in the performance of acts governed by a contract, common law jurisdictions have traditionally required some privity of contract between the tortfeasor and the injured party. Since the relying third party does not enter into a contract with the certification services provider and probably does not interact with the certification services provider at all, except for relying on the false certification, it may be difficult in some common law jurisdictions (absent an explicit statutory provision) for the relying party to establish a cause of action against the certification services provider.[39] If there is no privity of contract, a cause of action at tort under the common law would require a showing of a breach of a duty of care owed by the tortfeasor to the injured party. Whether or not for the certification services provider such a duty exists in respect of all possible relying parties is not entirely clear. Generally, the common law is reluctant to subject a person to "liability in an indeterminate amount, for an indeterminate time, to an indeterminate class"[40] for negligent misrepresentation unless the negligent words "are uttered directly, with knowledge or notice that they will be acted on, to one to whom the speaker is bound by some relation of duty, arising out of public calling, contract or otherwise, to act with care if he acts at all".[41]

---

[37] Article 1382 of the Civil Code of France provides that "whatever" human act that causes damage to someone else obliges the one by whose fault it occurred, to compensate it. This general liability rule has inspired similar provisions in various other countries, such as article 2043 of the Civil Code of Italy and article 483 of the Civil Code of Portugal.

[38] The Civil Code of Germany contains three general provisions (sections 823 I, 823 II and 826) and a few specific rules dealing with a number of rather narrowly defined tortuous situations. The main provision is section 823 I, which differs from the French Code to the extent that it expressly refers to injury to someone else's "life, body, health, freedom, property or another right".

[39] For instance, for English common law, an author concludes that "In the absence of legislation, [the certification services provider]'s liability to [the third party] is far from certain, yet [the third party] foreseeably suffers loss as a result of her negligence. Moreover, it is difficult to see how [the third party] can protect itself. If there is no liability, there is at least an arguable lacuna, and negligence on the part of the [certification services provider], in particular, creates a clear lacuna. The common law might fill lacunae, but the process is uncertain and unreliable" (Paul Todd, *E-Commerce Law* (Abingdon, Oxon, Cavendish Publishing Limited, 2005, pp. 149-150). Similar conclusions were reached for Australian law, see Sneddon, *Legal liability and e-transactions* … (see note [11]), p. 15.

[40] Words by Judge Cardozo in *Ultramares Corporation v. George A. Touche et al*, Court of Appeals of New York, 6 January 1931, 174 N.E. 441, p. 445.

[41] Ibid., p. 447.

38. In this case, the issue at stake is to determine what is the spectrum of persons to whom a certification services provider (or the signatory for that matter) would owe a duty of care. There are basically three standards that may be used to define the spectrum of persons who in such a situation may validly assert claims against the certification services provider:[42]

(a) **Foreseeability standard**. This is the broadest standard of liability. Under this standard, the signatory or the certification services provider will be liable to any person for whom reliance on the false representations was reasonably foreseeable;

(b) **Standard based on intent and knowledge**. This is a narrower standard that limits liability to loss suffered by a member of the group of the persons for whose benefit and guidance one intends to supply information or knows that the recipient intends to supply it;

(c) **Privity standard**. This is the most limited standard, creating a duty owed solely to the client, or one with whom the information provider had specific contact.

39. The UNCITRAL Model Law on Electronic Signatures does not attempt to circumscribe the universe of persons who may fall under the category of "relying parties", which could include "any person having or not a contractual relationship with the signatory or the certification services provider."[43] Similarly, under the European Union Directive on electronic signatures, the certification services provider is liable for damages towards "any entity or legal or natural person who reasonably relies" on the qualified certificate. The European Union Directive is clearly built around a PKI scheme, since it applies only in cases of digital signatures (qualified certificates). The notion of entity is usually interpreted as referring to third relying parties, and the Directive has been implemented by all but two States in that sense.[44]

40. Like the UNCITRAL Model Law on Electronic Signatures, the European Union Directive on electronic signatures does not narrow down the categories of persons that may qualify as relying parties. It has therefore been suggested that, even under common law, "in the provision of certification services it is self-evident that a certification service provider owes a duty of care towards anyone who may rely upon their certificate in deciding to accept a particular electronic signature in a particular transaction, since the very purpose for which the certificate was issued is to encourage such reliance."[45]

41. Another point of interest concerns the nature of loss recoverable from a signatory or certification services provider. For instance, in some common law jurisdictions, claims for purely economic losses for product defects are not recoverable in tort. However, cases of intentional fraud, or in some jurisdictions even negligent misrepresentation, are regarded as exceptions to the economic loss

---

[42] Smedinghoff, "Certification authority: liability issues" (see note [23]), section 4.3.1.

[43] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (see note […]), para. 150.

[44] The exceptions being Denmark and Hungary (Balboni, "Liability of certification service providers …" (see note […]), p. 220.

[45] Lorna Brazell, *Electronic Signatures: Law and Regulation* (London, Sweet and Maxwell, 2004), p. 187.

rule.[46] It is interesting to note, in that connection, that the United Kingdom Electronic Signatures Regulations 2002 did not reproduce the provisions on liability of the European Union Directive on electronic signatures. Therefore, standard rules on liability apply, which, in this case, relate to the test of the proximity of the damage.[47] The amount of damages recoverable is typically left for general contract or tort law. Some laws expressly require certification services providers to purchase liability insurance or otherwise make public to all potential signatories, among other information, the financial guaranties for its possible liability.[48]

(c) Ability to contractually limit or disclaim liability

42. Certification services providers are expected to seek routinely as much as possible to limit their contractual and tort liability towards the signatory and relying parties. As far as the signatory is concerned, limitation clauses will typically be contained in elements of the contract documentation, such as certification practice statements. Such statements may impose a cap to the liability per incident, per series of incidents, per period of time and exclude certain classes of damages. Another technique would be the inclusion in certificates of the maximum amount of the value of the transaction for which the certificate may be used, or restrict the use of the certificate to certain purposes only.[49]

43. While most legal systems generally recognize the right of contract parties to limit or exclude liability through contractual provisions, this right is usually subject to various limitations and conditions. In most civil law jurisdictions, for instance, a total exclusion of liability for a person's own fault is not admissible[50] or is subject to clear limitations.[51] Moreover, if the terms of the contract are not freely negotiated, but rather are imposed or pre-established by one of the parties ("adhesion contracts"), some types of limitation clauses may be found to be "abusive" and therefore invalid.

44. In common law jurisdictions a similar result may flow from various theories. In the United States, for instance, courts generally will not enforce contract provisions found to be "unconscionable". Although this concept usually depends on

---

[46] Smedinghoff, "Certification authority: liability issues" (see note [23]), section 4.5.

[47] Dumortier and others, "The legal and market aspects of electronic signatures" (see note [...]), p. 215.

[48] Turkey, Electronic Signature Law, 2004, article 13; and Argentina, *Ley de firma digital (2001)*, article 21 (a)(1); see also Mexico, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (III).

[49] See Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.5.4; and Hindelang, "No remedy for disappointed trust …" (see note [15]), section 4.1.1.

[50] In France, it is in principle possible to exclude liability arising out of a breach of contract. In practice, however, courts tend to invalidate such clauses whenever it is found that the clause would release the party from the consequences of a breach of a "fundamental" contractual obligation (see Légier, "Responsabilité contractuelle" (see note […]), nos. 262 and 263).

[51] In most civil law countries, the law prohibits the disclaimer of liability arising out of gross negligence or violation of duty imposed by a rule of public policy. Some countries have explicit rules to this effect, such as article 100 II of the Code of Obligations of Switzerland and article 1229 of the Civil Code of Italy. Other countries, such as Portugal, do not have a similar statutory rule, but achieve essentially the same result as Italy (see António Pinto Monteiro, *Cláusulas Limitativas e de Exclusão de Responsabilidade Civil* (Coimbra, Faculdade de Direito de Coimbra, 1985), p. 217).

a determination of the particular circumstances of the case, it generally refers to contract terms "which no man in his senses, not under delusion would make, on the one hand, and which no fair and honest man would accept on the other"[52] and that are characterized by "an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favourable to the other party."[53] Similarly to the civil law notion of "contract of adhesion", the doctrine has been applied to prevent instances of "commercial sharp practices" by parties with superior bargaining power.[54] Not every contract term that comes about this way is invalid. However, although courts generally enforce standard form or adhesion contracts where there is no ability to bargain regarding the terms, even in consumer contracts, sometimes a court will decline to enforce a clause in a standard contract if its insertion amounts to unfair surprise.[55]

45. Lastly, in both civil law and common law systems, consumer protection rules may significantly reduce the ability of a certification services provider to limit its liability vis-à-vis the signatory, in circumstances where the limitation of liability would effectively deprive the signatory of a right or remedy recognized by the applicable law.

46. The possibility for the certification services provider to limit its potential liability vis-à-vis the relying party would in most cases be subject to even greater restrictions. Apart from closed business models where a relying party would be required to adhere to contract terms,[56] quite often the relying party will not be bound by contract to the certification services provider or even the signatory. Thus, to the extent that the relying party might have a claim at tort against the certification services provider or the signatory, those parties might have no means of effectively limiting their liability, since under most legal systems this would require giving the relying party adequate notice of the limitation of liability. Lack of knowledge of the identity of the relying party prior to the occurrence of the damage may prevent the certification services provider (and arguably even more so, the signatory) from putting in place an effective system for limiting its liability. This problem is typical of open systems where strangers interact with no prior contact and leaves the signatory exposed to potentially devastating consequences.[57] This situation was felt by many, in particular representatives of the certification industry, to be a major impediment to wider use of electronic signature and authentication methods, given the difficulty for certification services providers to assess their exposure to liability.

---

[52] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), citing *Hume v. U.S.*, 132 U.S. 406, 410 (1975), cited in Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.5.4.

[53] Ibid., citing *Williams v. Walker-Thomas Furniture Co.,* 350 F.2d 315, 320 (D.C. 1965), cited in Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.5.4.

[54] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), cited in Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.5.4.

[55] Raymond T. Nimmer, *Information Law*, section 11.12[4][a], at 11-37, cited in Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.5.4.

[56] Such as envisaged for the E-Authentication Federation administered by the General Services Administration of the United States Government (see E-Authentication Federation, Interim Legal Document Suite, version 4.0.7, available at http://www.cio.gov/eauthentication/documents/LegalSuite.pdf, accessed on 8 February 2007).

[57] Sneddon, "*Legal liability and e-transactions* ..." (see note [11]), p. 18.

47. The desire to clarify the law on this aspect has led a number of countries to expressly recognize the right of certification services providers to limit their liability. The European Union Directive on electronic signatures, for example, obliges European Union member States to ensure that a certification services provider may indicate in a qualified certificate "limitations on the use of that certificate" as long the limitations "are recognizable to third parties".[58] These limitations may be typically of two categories: there may be limits on the types of transaction for which particular certificates or classes of certificates may be used; there may also be limits on the value of the transactions in connection with which the certificate or class of certificates may be used. Under either hypothesis, the certification services provider is expressly exempted from liability "for damage arising from use of a qualified certificate that exceeds the limitations placed on it."[59] Furthermore, the European Union Directive on electronic signatures mandates European Union member States to ensure that a certification services provider "may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognizable to third parties."[60] In such a case the certification services provider shall not be liable for damage resulting from this maximum limit being exceeded.[61]

48. The European Union Directive on electronic signatures does not establish a cap for the liability that the certification services provider may incur. However, the directive does allow a certification services provider to limit the maximum value per transaction for which certificates may be used, exempting the certification services provider from liability exceeding that value cap.[62] As a matter of business practice, certification services providers also often introduce an overall cap to their liability, on a contractual basis.

49. Several other domestic laws support those contractual practices by recognizing a limit on the liability of the certification services provider towards any potentially affected party. Typically, these laws allow limitations as specified in the certificate of practice statement of the certification services provider, and in some cases expressly exempt the certification services provider from liability where a certificate was used for a purpose different from the one for which it was issued.[63] Furthermore, some laws recognize the right of certification services providers to issue certificates of different classes and to establish different recommended levels

---

[58] European Union Directive on electronic signatures (see note […]), article 6, paragraph 2.

[59] Ibid.

[60] Ibid., article 6, paragraph 3.

[61] Ibid.

[62] Dumortier and others, "The legal and market aspects of electronic signatures" (see note […]), p. 55, and discussion in Hindelang, "No remedy for disappointed trust …" (see note [15]), section 4.1.1. Balboni, "Liability of certification service providers …" (see note […]), p. 230, goes further by stating that "… by article 6 (4), it is only possible to limit the value of the transaction (…), which has nothing to do with a limitation of the potential amount of damage that can arise from that transaction."

[63] Argentina, *Ley de firma digital (2001)*, article 39; Barbados, chapter 308B, Electronic Transactions Act (1998), section 20, paragraphs 3 and 4; Bermuda, Electronic Transactions Act, 1999, section 23, paragraphs 3 and 4; Chile, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; and Viet Nam, Law on Electronic Transactions, article 29, paragraphs 7 and 8 (the latter however without express exemption of liability).

of reliance,[64] which typically provide different levels of limitation (and of security) depending on the fee paid. However, some laws expressly prohibit any limitations of liability other than as a result of limitations on the use or value of certificates.[65]

50. Countries that have adopted a minimalist approach have, in turn, regarded legislative intervention as generally undesirable and have preferred to leave the matter for the parties to regulate by contract.[66]

---

[64] Singapore, Electronic Transactions Act (chapter 88) 1998, sections 44 and 45; and Mauritius, Electronic Transactions Act 2000, articles 38 and 39.

[65] Turkey, Electronic Signature Law, 2004, article 13.

[66] See, for Australia, Sneddon, *Legal liability and e-transactions* (see note [11]), pp. 44-47; and for the United States, Smedinghoff, "Certification authority: liability issues" (see note [23]), section 5.2.51.