United Nations A/CN.9/630/Add.1

General Assembly

Distr.: General
25 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 of a sample chapter (part one, chap. I, sects. B and C) of a comprehensive reference document dealing with legal issues related to the international use of electronic authentication and signature methods.

* Submission of this document by the secretariat of the United Nations Commission on International Trade Law was delayed owing to shortage of staff.

V.07-82780 (E) 240507 250507

Annex

Contents

Part One

Electronic signature and authentication methods

[…]

I. Definition and methods of electronic authentication and signature

[…]

B. Main methods of electronic signature and authentication

1. For the purposes of this discussion, four main signature and authentication methods will be discussed: digital signatures; biometric methods; passwords and hybrid methods; and scanned or typed signatures.

1. Digital signatures relying on public key cryptography

2. "Digital signature" is a name for technological applications using asymmetric cryptography, also referred to as public key encryption systems, to ensure the authenticity of electronic messages and guarantee the integrity of the contents of these messages. The digital signature has many different appearances, such as fail-stop digital signatures, blind signatures and undeniable digital signatures.

(a) Technical notions and terminology

(i) Cryptography

3. Digital signatures are created and verified by using cryptography, the branch of applied mathematics that is concerned with transforming messages into a seemingly unintelligible form and then back into their original form. Digital signatures use what is known as public key cryptography, which is often based on the use of algorithmic functions to generate two different but mathematically related "keys" (i.e. large numbers produced using a series of mathematical formulae applied to prime numbers).[1] One such key is used for creating a digital signature or transforming data into a seemingly unintelligible form, and the other key is used for verifying a digital signature or returning the message to its original form.[2]

---

[1] It should be noted, however, that the concept of public key cryptography, as discussed here, does not necessarily imply the use of algorithms based on prime numbers. Other mathematical techniques are currently used or under development, such as cryptosystems relying on elliptic curves, which are often described as offering a high degree of security through the use of significantly reduced key-lengths.

[2] While the use of cryptography is one of the main features of digital signatures, the mere fact that a digital signature is used to authenticate a message containing information in digital form should not be confused with a more general use of cryptography for purposes of confidentiality. Confidentiality encryption is a method used for encoding an electronic communication so that only the originator and the addressee of the message will be able to read it. In a number of countries, the use of cryptography for confidentiality purposes is limited by law for reasons of

Computer equipment and software utilizing two such keys are often collectively referred to as "cryptosystems" or, more specifically, "asymmetric cryptosystems" where they rely on the use of asymmetric algorithms.

(ii) Public and private keys

4. A complementary key used for digital signatures is named the "private key", which is used only by the signatory to create the digital signature and should be kept secret, while the "public key" is ordinarily more widely known and is used by a relying party to verify the digital signature. The private key is likely to be kept on a smart card or to be accessible through a personal identification number (PIN) or a biometric identification device, such as thumbprint recognition. If many people need to verify the signatory's digital signature, the public key must be available or distributed to all of them, for example by attaching the certificates to the signature or by other means that ensure that the relying parties, and only those who have to verify the signatures, can obtain the related certificates. Although the keys of the pair are mathematically related, if an asymmetric cryptosystem has been designed and implemented securely it is virtually impossible to derive the private key from knowledge of the public key. The most common algorithms for encryption through the use of public and private keys are based on an important feature of large prime numbers: once they are multiplied together to produce a new number, it is particularly difficult and time-consuming to determine which two prime numbers created that new, larger number.[3] Thus, although many people may know the public key of a given signatory and use it to verify that signatory's signature, they cannot discover that signatory's private key and use it to forge digital signatures.

(iii) Hash function

5. In addition to the generation of key pairs, another fundamental process, generally referred to as a "hash function", is used in both creating and verifying a digital signature. A hash function is a mathematical process, based on an algorithm that creates a digital representation or compressed form of the message (often referred to as a "message digest" or "fingerprint" of the message), in the form of a "hash value" or "hash result" of a standard length that is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used. In

---

public policy that may involve considerations of national defense. However, the use of cryptography for authentication purposes by producing a digital signature does not necessarily imply the use of cryptography to make any information confidential in the communication process, since the encrypted digital signature may be merely appended to a non-encrypted message.

[3] Certain existing standards refer to the notion of "computational unfeasibility" to describe the expected irreversibility of the process, that is, the hope that it will be impossible to derive a user's secret private key from that user's public key. "'Computationally unfeasible' is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance." (American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, American Bar Association, 1 August 1996), p. 9, note 23, available at http://www.abanet.org/scitech/ec/isc/dsgfree.html, accessed on 5 April 2007).

the case of a secure hash function, sometimes called a "one-way hash function", it is virtually impossible to derive the original message from knowledge of its hash value. Another basic feature of hash functions is that it is also virtually impossible to find another binary object (i.e. different from the one from which the digest was originally derived) producing the same digest. Hash functions therefore enable the software for creating digital signatures to operate on smaller and more predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

(iv) Digital signature

6. To sign a document or any other item of information, the signatory first delimits precisely the borders of what is to be signed. Then a hash function in the signatory's software computes a hash result unique (for all practical purposes) to the information to be signed. The signatory's software then transforms the hash result into a digital signature using the signatory's private key. The resulting digital signature is thus unique to both the information being signed and the private key used to create the digital signature. Typically, a digital signature (the encryption with the signer's private key of the hash result of the message) is attached to the message and stored or transmitted with that message. However, it may also be sent or stored as a separate data element, as long as it maintains a reliable association with the corresponding message. Since a digital signature is unique to its message, it is inoperable if permanently disassociated from the message.

(v) Verification of digital signature

7. Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key. Verification of a digital signature is accomplished by computing a new hash result for the original message, by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks whether the digital signature was created using the corresponding private key and whether the newly computed hash result matches the original hash result that was transformed into the digital signature during the signing process.

8. The verification software will confirm the digital signature as "verified" from a cryptographic viewpoint if (a) the signatory's private key was used to sign digitally the message, which is known to be the case if the signatory's public key was used to verify the signature because the signatory's public key will verify only a digital signature created with the signatory's private key; and (b) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

(vi) Other uses of digital signature technology

9. As indicated above, digital signature technology has a much broader use than merely to "sign" electronic communications in the same manner that handwritten signatures are used to sign documents (see paragraph […]). Indeed, digitally signed

certificates are often used, for instance, to "authenticate" servers or websites, for example in order to guarantee to their users that the server or website is the one it purports to be, or is genuinely attached to the company that claims to run the server or website. Digital signature technology can also be used to "authenticate" computer software, for example in order to guarantee the authenticity of a software downloaded from a website; or in order to guarantee that a particular server uses a technology that is widely recognized as providing a certain level of connection security, or in order to "authenticate" any other data that is distributed or stored digitally.

(b) Public key infrastructure and certification services providers

10. To verify a digital signature, the verifier must have access to the signatory's public key and have assurance that it corresponds to the signatory's private key. However, a public-key and private-key pair has no intrinsic association with any person; it is simply a pair of numbers. An additional mechanism is necessary to associate reliably a particular person or entity to the key pair. This is particularly important, as there may be no pre-existing relationship of trust between the signatory and the recipients of digitally signed communications. To that effect, the parties involved must have a degree of confidence in the public and private keys being issued.

11. The required level of confidence may exist between parties who trust each other, who have dealt with each other over a period of time, who communicate on closed systems, who operate within a closed group or who are able to govern their dealings contractually, for example in a trading partner agreement. In a transaction involving only two parties, each party can simply communicate (by a relatively secure channel such as by courier or telephone) the public key of the key pair each party will use. However, the same level of confidence may not be present when the parties deal infrequently with each other, communicate over open systems (e.g. the World Wide Web on the Internet), are not in a closed group, or do not have trading partner agreements or other laws governing their relationships. Moreover, it should be taken into account that, if disputes need be settled in court or by arbitration, it might be difficult to demonstrate that a certain public key had or had not actually been given to the recipient by its actual owner.

12. A prospective signatory might issue a public statement indicating that signatures verifiable by a given public key should be treated as originating from that signatory. The law of the enacting State would govern the form and the legal effectiveness of such a statement. For example, a presumption of attribution of electronic signatures to a particular signatory could be established through publication of the statement in an official bulletin or in a document recognized as "authentic" by public authorities. However, other parties might be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of inadvertently trusting an impostor or of having to disprove a false denial of a digital signature (an issue often referred to in the context of "non-repudiation" of digital signatures) if a transaction should turn out to prove disadvantageous for the purported signatory.

13. One solution to some of these problems is the use of one or more third parties to associate an identified signatory or the signatory's name with a specific public key. That third party is generally referred to as a "certification authority", "certification services provider" or "supplier of certification services" in most technical standards and guidelines (in the UNCITRAL Model Law on Electronic Signatures,[4] the term "certification service provider" has been chosen). In a number of countries, such certification authorities are being organized hierarchically into what is often referred to as a "public key infrastructure" (PKI). Certification authorities within a PKI can be established in a hierarchical structure, where some certification authorities only certify other certification authorities, which provide services directly to users. In such a structure, some certification authorities are subordinate to other certification authorities. In other conceivable structures, all certification authorities may operate on an equal footing. In any large PKI, there would likely be both subordinate and superior certification authorities. Other solutions may include, for example, certificates issued by relying parties.

(i) Public key infrastructure

14. Setting up a PKI is a way to provide confidence that (a) a user's public key has not been changed and in fact corresponds to that user's private key; and (b) the cryptographic techniques being used are sound. To provide the confidence described above, a PKI may offer a number of services, including the following: (a) managing cryptographic keys used for digital signatures; (b) certifying that a public key corresponds to a private key; (c) providing keys to end users; (d) publishing revocation information of public keys or certificates; (e) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (f) checking the identification of end users and providing them with services; (g) providing time-stamping services; and (h) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized.

15. A PKI may be based on various hierarchical levels of authority. For example, models considered in certain countries for the establishment of possible PKIs include references to the following levels: (a) a unique "root authority", which would certify the technology and practices of all parties authorized to issue cryptographic key pairs or certificates in connection with the use of such key pairs and would register subordinate certification authorities;[5] (b) various certification authorities, placed below the "root" authority, which would certify that a user's public key actually corresponds to that user's private key (i.e. has not been tampered with); and (c) various local registration authorities, placed below the certification authorities, which would receive requests from users for cryptographic key pairs or for certificates in connection with the use of such key pairs, requiring proof of identification and checking identities of potential users. In certain countries, it is envisaged that notaries public might act as, or support, local registration authorities.

---

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

[5] The question as to whether a Government should have the technical ability to retain or recreate private confidentiality keys may be dealt with at the level of the root authority.

16. PKIs organized in a hierarchical structure are scalable in the sense that they may incorporate entire new PKI "communities" simply by having the "root authority" establish a trust relationship with the new community's "root".[6] The root authority of the new community may be incorporated directly under the "root" of the receiving PKI, thus becoming a subordinate certification services provider within that PKI. The root authority of the new community may also become a subordinate certification services provider to one of the subordinate certification services providers within the existing PKI. Another attractive feature of hierarchical PKIs is that it makes it easy to develop certification paths because they run in one direction only, from a user's certificate back to the trust point. Furthermore, certification paths within a hierarchical PKI are relatively short and the users of a hierarchy know implicitly which applications a certificate may be used for, based on the position of the certification services provider within the hierarchy. However, hierarchical PKIs have drawbacks as well, mainly as a consequence of reliance on a single trust point. If the root authority is compromised, the entire PKI is compromised. Furthermore, some countries have found it difficult to select one single entity as a root authority and to impose such a hierarchy on all other certification services providers.[7]

17. The so-called "mesh" PKI is an alternative to a hierarchical PKI. Under this model, certification services providers are connected in a peer-to-peer relationship. All certification services providers in such a model can be trust points. Generally, users will trust the certification services providers that issued their certificate. Certification services providers will issue certificates to each other; the pair of certificates describes their reciprocal trust relationship. The lack of hierarchy in such a system means that certification services providers cannot impose conditions governing the types of certificate issued by other certification services providers. If a certification services provider wishes to limit the trust extended to other certification services providers, it must specify these limitations in the certificates issued to its peers.[8] Harmonizing conditions and limitations of mutual recognition may however be an extremely complex objective.

18. A third alternative structure is built around the so-called "bridge" certification services provider. This structure may be particularly useful to allow various pre-existing PKI communities to trust each other's certificates. Unlike a certification services provider in a "mesh" PKI, a "bridge" certification services provider does not issue certificates directly to users. Neither is a "bridge" certification services provider intended to be used as a trust point by the users of the PKI, as would be the case with a "root" certification services provider. Instead, the "bridge" certification services provider establishes peer-to-peer trust relationships with the different user communities, thus allowing the users to keep their natural trust points within their respective PKIs. If a user community implements a trust domain in the form of a hierarchical PKI, the "bridge" certification services provider will establish a

---

[6] William T. Polk and Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (September 2000), available at http://csrc.nist.gov/pki/documents/B2B-article.pdf, accessed on 30 March 2007.

[7] Polk and Hastings (see note [6]) note that in the United States of America, it was very difficult to single out one agency of the Federal Government to assume the overall authority over the federal PKI.

[8] Polk and Hastings, *Bridge Certification Authorities* … (see note [5]).

relationship with the root authority of that PKI. However, if the user community implements a trust domain by creating a mesh PKI, the "bridge" certification services provider will only need to establish a relationship with one of the PKI's certification services providers, which then becomes the "principal" certification services provider within that PKI for the purpose of establishing the "bridge of trust" to the other PKI. The "bridge of trust" that joins two or more PKIs through their mutual relationship with a "bridge" certification services provider enables users from the different user communities to interact with each other through the "bridge" certification services provider with a specified level of trust.[9]

(ii) Certification services provider

19. To associate a key pair with a prospective signatory, a certification services provider (or certification authority) issues a certificate, which is an electronic record that lists a public key together with the name of the certificate subscriber as the "subject" of the certificate, and which may confirm that the prospective signatory identified in the certificate holds the corresponding private key. The principal function of a certificate is to bind a public key with a particular signatory. A "recipient" of the certificate desiring to rely upon a digital signature created by the signatory named in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, a level of assurance is provided technically that the signatory created the digital signature and that the portion of the message used in the hash function (and, consequently, the corresponding data message) has not been modified since it was digitally signed.

20. To assure the authenticity of the certificate with respect to both its contents and its source, the certification services provider digitally signs it. The issuing certification services provider's digital signature on the certificate can be verified by using the public key of the certification service provider listed in another certificate by another certification services provider (which may, but need not, be on a higher level in a hierarchy), and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. Recording the digital signature in a certificate issued by the certification services provider (sometimes referred to as a "root certificate") is another possible way of verifying a digital signature.[10]

21. In each case, the issuing certification services provider may digitally sign its own certificate during the operational period of the other certificate used to verify the certification services provider's digital signature. Under the laws of some States, one way of building trust in the digital signature of the certification services provider might be to publish the public key of the certification services provider or certain data pertaining to the root certificate (such as a "digital fingerprint") in an official bulletin.

---

[9] The "bridge" certification services provider was the structure eventually chosen to set up the PKI system for the United States Federal Government (Polk and Hastings, see note [6]). This was also the model followed to develop the PKI system of the Government of Japan.

[10] *Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 17* and corrigendum (A/56/17 and Corr.3), para. 279.

22. A digital signature corresponding to a message, whether created by the signatory to authenticate a message or by a certification services provider to authenticate its certificate, should generally be reliably time stamped to allow the verifier to determine whether the digital signature was created during the "operational period" stated in the certificate, and in any case whether the certificate was valid (e.g. was not mentioned in a revocation list) at the relevant time, which is a condition of the verifiability of a digital signature.

23. To make a public key and its correspondence to a specific signatory readily available for verification, the certificate may be published in a repository, or made available by other means. Typically, repositories are online databases of certificates and other information available for retrieval and use in verifying digital signatures.

24. Once issued, a certificate may prove to be unreliable, for example in situations where the signatory misrepresents its identity to the certification services provider. In other circumstances, a certificate may be reliable enough when issued, but may become unreliable sometime afterwards. If the private key is "compromised", for example through loss of control of the private key by the signatory, the certificate may lose its trustworthiness or become unreliable, and the certification services provider (at the signatory's request or even without the signatory's consent, depending on the circumstances) may suspend (temporarily interrupt the operational period) or revoke (permanently invalidate) the certificate. In a timely fashion upon suspending or revoking a certificate, the certification services provider may be expected to publish a notice of the revocation or suspension, or to notify persons who enquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate. Similarly, where applicable, the certification services provider's own certificate should also be reviewed for possible revocation, as should the certificate issued for the verification of the signature of the time-stamping authority on the time-stamp tokens and the certificate of the certification services provider that issued the certificate of the time-stamping authority.

25. Certification authorities could be operated by private sector service providers or Government authorities. In a few countries, it is envisaged that, for public policy reasons, only Government entities should be authorized to operate as certification authorities. In most countries, however, certification services are either entirely left for the private sector or State-run certification services providers coexist with private sector providers. There are also closed certification systems, where small groups set up their own certification services provider. In some countries, State-owned certification services providers issue certificates only in support of digital signatures used by the public administration. Irrespective of whether certification authorities are operated by public entities or by private sector service providers, and of whether certification authorities would need to obtain a licence to operate, there is typically more than one certification services provider operating within the PKI. Of particular concern is the relationship between the various certification authorities (see paras. [15]-[18] above).

26. It may be incumbent upon the certification services provider or the root authority to ensure that its policy requirements are met on an ongoing basis. While the selection of certification authorities may be based on a number of factors, including the strength of the public key being used and the identity of the user, the trustworthiness of any certification services provider may also depend on its enforcement of standards for issuance of certificates and the reliability of its

evaluation of data received from users who request certificates. Of particular importance is the liability regime applying to any certification services provider with respect to its compliance with the policy and security requirements of the root authority or superior certification services provider, or with any other applicable requirement, on an ongoing basis. Of equal importance is the obligation of the certification services provider to act in accordance with the representations made by it with respect to its policies and practices, as envisaged in article 9, paragraph 1 (a), of the Model Law on Electronic Signatures.

(c) Practical problems in public key infrastructure implementation

27. Despite the considerable knowledge of digital signature technologies and the way they function, the implementation of public key infrastructures and digital signature schemes has, in practice, faced some problems that have kept the level of use of digital signatures below expectations.

28. Digital signatures work well as a means to verify signatures that are created during the period of validity of a certificate. However, once the certificate expires or is revoked, the corresponding public key loses its validity, even if the key pair was not compromised. Accordingly, a PKI scheme would require a digital signature management system to ensure the availability of the signature over time. The main difficulty results from the risk that the "original" electronic records (that is, the binary digits, or "bits" that make up the computer file on which the information is recorded), including the digital signature, may become unreadable or unreliable over time, mainly because of the obsolescence of the software, the equipment or both. In fact, the digital signature may become insecure, as a consequence of scientific advances in cryptanalysis, the signature verification software may not be available over long periods of time or the document may lose its integrity.[11] This makes the long-term retention of electronic signatures generally problematic. Even though digital signatures were for some time believed to be essential for archival purposes, experience has shown that they are not immune to long-term risks. Since every alteration to the record after the time when the signature was created will cause the verification of the signature to fail, reformatting operations intended to keep a record legible for the future (such as "migration", or "conversion") may affect the durability of the signature.[12] In fact, digital signatures were conceived

---

[11] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey", available at http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf, accessed on 5 April 2007 (paper published in a supplemental volume of the 2004 International Conference on Dependable Systems and Networks (DSN 2004), Florence, Italy, 28 June-1 July 2004), pp. 228-232.

[12] "In the end, all we can preserve in an electronic context are bits. However, it has been clear for a long time that it is very difficult to keep a set of bits indefinitely. With the lapse of time, the set of bits becomes illegible (to the computer and thus to humans) as a result of the technological obsolescence of the application program and/or of the hardware (e.g. the reader). The problem of the durability of PKI-based digital signatures has been poorly studied so far because of its complexity. … Although the authentication tools that were used in the past, such as handwritten signatures, seals, stamps, fingerprints etc. are also subject to reformatting (e.g. microfilming) because of the obsolescence of the paper carrier, they never become completely useless after reformatting. There is always at least a copy available that can be compared with other original authentication tools." (Jos Dumortier and Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, p. 5, available at http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where, accessed on 5 April 2007.

more for providing security for the communication of information than for the preservation of information over time.[13] Initiatives to overcome this problem have not yet resulted in a durable solution.[14]

---

[13] In 1999, archivists from various countries launched the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) project with the aim of "developing the theoretical and methodological knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form" (see http://www.interpares.org, accessed on 5 April 2007). The draft report of the Authenticity Task Force, which was part of the first phase of the project (InterPARES 1, concluded in 2001), indicated that "digital signatures and public key infrastructures (PKI) are examples of technologies that have been developed and implemented as a means of authentication for electronic records that are transmitted **across space**. Although record-keepers and information technology personnel place their trust in authentication technologies to ensure the authenticity of records, these technologies were never intended to be, and are not currently viable as, a means of ensuring the authenticity of electronic records **over time**" (emphasis added), available at http://www.interpares.org/documents/atf_draft_final_report.pdf, accessed on 5 April 2007. The final report of InterPARES 1 is available at http://www.interpares.org/book/index.htm. The continuation of the project (InterPARES 2), aims to develop and articulate the concepts, principles, criteria and methods that can ensure the creation and maintenance of accurate and reliable records and the long-term preservation of authentic records in the context of artistic, scientific and Government activities developed from 1999 and 2001.

[14] The European Electronic Signature Standardization Initiative (EESSI), for example, was created in 1999 by the Information and Communications Technology Standards Board, a collaborative group of organizations concerned with standardization and related activities in information and communications technologies established to coordinate the standardization activity in support to the implementation of European Union Directive on electronic signatures (see note […] [Official Journal of the European Communities, L 13/12]). The EESSI consortium (a standardization effort which seeks to translate the requirements of the European directive on electronic signatures into European standards) has sought to address the need for ensuring the long-term preservation of cryptographically signed documents through its standard on Electronic Signature Formats (Electronic Signature Formats ES 201 733, ETSI, 2000). The format distinguishes between signature validation moments: the initial validation and a later validation. The format for late validation encapsulates all of the information that can eventually be used in the validation process, such as revocation information, time stamps, signature policies, etc. This information is gathered at the stage of initial validation. The designers of these electronic signature formats were concerned with the security threat to the validity of the signature that results from decay in cryptographic strength. To guard against this threat of decay, EESSI signatures are regularly time stamped afresh, with signing algorithms and key sizes appropriate to state-of-the-art cryptanalytic methods. The problem of software longevity has been addressed in a 2000 report by EESSI, which introduced "trusted archival services", a new type of commercial service that would be offered by yet to be specified competent bodies and professions, in order to guarantee the long-term preservation of cryptographically signed documents. The report lists a number of technical requirements such archival services should provide, among them, "backward compatibility" with computer hardware and software, through either preservation of equipment and/or emulation (see Blanchette, "Defining electronic authenticity…" (see note [12])). A follow-up study on the EESSI recommendation on trusted archival services by the Interdisciplinary Centre for Law and Information Technology of the Katholieke Universiteit Leuven (Catholic University of Leuven), Belgium, entitled *European Electronic Signature Standardization Initiative: Trusted Archival Services* (Phase 3, final report, 28 August 2000) is available at http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, accessed on 12 April 2007). EESSI was closed in October 2004. Systems to implement these recommendations do not seem to be currently in operation (see Dumortier and Van den Eynde, *Electronic Signatures and Trusted Archival Services* (see note [13]).

29. Another area where digital signatures and PKI schemes may give rise to practical problems concerns data security and privacy protection. Certification services providers must keep safe the keys used to sign certificates issued to their customers and may be exposed to attempts by outsiders to gain unauthorized access to the keys (see also part two, paras. […]-[…] below). Furthermore, certification services providers need to obtain a series of personal data and business information from persons applying for certificates. This information needs to be stored by the certification services provider for future reference. Certification services providers must take the necessary measures to ensure that access to such information is in accordance with applicable data protection laws.[15] However, unauthorized access remains a real threat.

2. Biometrics

30. A biometric is a measurement used to identify an individual through its intrinsic physical or behavioural traits. Traits that may be used for recognition in biometrics include DNA, fingerprint, iris, retina, hand or facial geometry, facial thermogram, ear shape, voice, body odour, blood vessel pattern, handwriting, gait and typing patterns.

31. The use of biometric devices typically involves capturing a biometric sample of a biological feature of an individual. This sample is in the digital form. Then, biometric data is extracted from that sample to create a reference template. Eventually, the biometric data stored in the reference template is compared with the one extracted from the end user for the purpose of verification, so that it is possible to indicate whether or not an identification or verification of identity has been achieved.[16]

32. The nature of biometric devices entails unique features that need to be taken into due consideration. The existence of those features, which may to some extent differ with the trait chosen as a reference, has a major impact on the suitability of the technology for the intended application.

33. A number of risks relate to the storage of biometrical data since biometric patterns are typically not revocable. When biometric systems have been compromised, the legitimate user has no recourse but to revoke the identification

---

[15] See Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980) available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, accessed on 7 February 2007; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, *European Treaty Series*, No. 108), available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, accessed on 7 February 2007; Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95), available at http://193.194.138.190/html/menu3/b/71.htm, accessed on 7 February 2007; and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*Official Journal of the European Communities*, L 281, 23 November 1995), available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett, accessed on 7 February 2007.

[16] International Association for Biometrics (iAfB) and International Computer Security Association (ICSA), *1999 Glossary of Biometric Terms*, available at http://www.afb.org.uk/docs/glossary.htm, accessed on 7 February 2007.

data and switch to another set of uncompromised identification data. Therefore, special rules are needed to prevent the abuse of biometrics databases.

34. The accuracy of biometric techniques cannot be absolute since biological features tend to be inherently variable and any measurement may involve deviation. In this respect, biometrics are not considered unique identifiers but rather semi-unique identifiers. To accommodate those variations, the accuracy of biometrics may be manipulated by setting the threshold for matching the reference template with the extracted sample. However, a low threshold may bias the test towards false acceptance while a high threshold may tend towards false rejections. Nevertheless, the accuracy of authentication provided by biometrics may be adequate in the majority of commercial applications.

35. Moreover, data protection and human rights issues arise in relation to the storage and disclosure of biometrical data. Data protection laws,[17] although they may not refer expressly to biometrics, aim at protecting personal data relating to natural persons, whose processing, both in their raw form and as templates, is at the core of biometrics technology.[18] Moreover, measures may be required to protect consumers against risks generated by the private use of biometric data, as well as in case of identity theft. Other legal domains, including labour and health law, may also come into play.[19]

36. Technical solutions might assist in addressing some concerns. For instance, storage of biometrical data on smart cards or tokens may protect from unauthorized access, which could occur if the data is stored on a centralized computer system. Moreover, best practices have been developed to reduce risks in different areas such as scope and capabilities; data protection; user control of personal data; and disclosure, auditing, accountability and oversight.[20]

37. Biometric devices are generally considered as offering a high level of security. While they are compatible with a range of uses, their current main scope is on Government applications, particularly law enforcement applications such as immigration clearance and access controls.

38. Commercial applications have also been developed, where often biometrics are used in the context of a two-factor authentication process requiring provision of an element in possession of the individual (biometrics) and an element in the knowledge of the individual (typically, a password or a PIN). Moreover, applications were developed to store and compare the characteristics of a person's handwritten signature. Digital-based pen tablets record the pen pressure and

---

[17] See note [15].

[18] Paul de Hert, *Biometrics: Legal Issues and Implications*, background paper for the Institute for Prospective Technological Studies of the European Commission (European Communities, Directorate General Joint Research Centre, 2005), p. 13, available at http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

[19] For instance, in Canada, the use of biometrics was discussed with respect to the application of the Personal Information Protection and Electronic Documents Act (2000, c. 5) in the workplace (see *Turner v. TELUS Communications Inc*., 2005 FC 1601, 29 November 2005 (Federal Court of Canada)).

[20] See, for an example of best practices, the International Biometric Group BioPrivacy Initiative, "Best practices for privacy-sympathetic biometric deployment", available at http://www.bioprivacy.org.

duration of the signing process. The data are then stored as an algorithm to be used for comparison against future signatures. However, in light of the inherent features of biometrics, caution is also expressed on the dangers of a gradual, uncontrolled increase relating to their use in routine commercial transactions.

39. If biometric signatures are used as a substitute for handwritten signatures, a problem of evidence may arise. As mentioned before, the reliability of biometric evidence varies between the technologies used and the chosen false acceptance rate. Besides, there is the possibility to tamper with or falsify the biometric data stored in digital form.

40. The general reliability tests under the UNCITRAL Model Law on Electronic Signatures[21] and Model Law on Electronic Commerce,[22] as well as under the more recent United Nations Convention on the Use of Electronic Communications in International Contracts,[23] can be applied to the use of biometric signatures. To ensure uniformity, it might also be useful to develop international guidelines on the use and management of biometric methods.[24] Whether such standards would be premature, given the current state of development of biometric technologies, and might risk hampering the continued development of biometric technologies, needs to be carefully considered.

3. Passwords and hybrid methods

41. Passwords and codes are used both for controlling access to information or services and for "signing" electronic communications. In practice, the latter use is less frequent than the former, because of the risk of compromising the code if it is transmitted in non-encrypted messages. Passwords and codes are however the most widely used method for "authentication" for purposes of access control and identity verification in a broad range of transactions, including most Internet banking, cash withdrawals at automatic teller machines and consumer credit card transactions.

42. It should be recognized that multiple technologies can be used to "authenticate" an electronic transaction. Several technologies or several uses of a single technology can be utilized for a single transaction. For example, signature dynamics for authentication can be combined with cryptography for message integrity. Alternatively, passwords can be passed over the Internet, using cryptography (e.g. SSL in browsers) to protect them, in conjunction with the use of biometrics to trigger a digital signature (asymmetric cryptography), which, on receipt, generates a Kerberos ticket (symmetric cryptography). In developing legal and policy frameworks to deal with these technologies, consideration should be given to the role of multiple technologies. Legal and policy frameworks for electronic authentication will need to be flexible enough to cover hybrid technology

---

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

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

[23] The United Nations Convention on the Use of Electronic Communications in International Contracts was finalized by UNCITRAL at its thirty-eighth session (Vienna, 4-15 July 2005) and officially adopted by the General Assembly on 23 November 2005 (General Assembly resolution 60/21, annex), available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

[24] These could be compared with the criteria for reliability presented in the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (see note […]) [United Nations publication, Sales No. E.02.V.8], paragraph 75.

approaches, as those that focus on specific technologies could impede the use of multiple technologies.[25] Technology neutral provisions would facilitate the acceptance of such hybrid technology approaches.

4. Scanned signatures and typed names

43. The main reason for legislative interest in electronic commerce in the private law area has been concern about how new technologies may affect the application of rules of law that were conceived for other media. This attention to technology has often led, deliberately or not, to a focus on sophisticated technologies that offer a higher level of security for electronic authentication and signature methods. It is often neglected, in that context, that a very large number, if not the majority, of business communications exchanged throughout the world do not make use of any particular authentication or signature technology.

44. In day-to-day practice, companies around the world are often satisfied, for instance, with exchanging e-mails without the use of any form of authentication or signature other than the typed name, title and address of parties at the bottom of their communications. Sometimes a more formal appearance is given by the use of facsimile or scanned images of handwritten signatures, which of course constitute only a copy in digitalized form of a handwritten original. Neither typed names on unencrypted e-mails nor scanned signatures offer a high level of security or can definitely prove the identity of the originator of the electronic communication in which they appear. Nevertheless, business entities freely choose to use these forms of "authentication" in the interest of ease, expediency and cost-effectiveness of communications. It is important for legislators and policymakers to bear in mind these widespread business practices when considering regulating electronic authentication and signature. Stringent requirements for electronic authentication and signature, in particular the imposition of a particular method or technology, may inadvertently cast doubt as to the validity and enforceability of a significant number of transactions that are entered into every day without the use of any particular kind of authentication or signature. That, in turn, may stimulate parties acting in bad faith to avoid the consequences of obligations they freely assumed by questioning the authenticity of their own electronic communications. It is unrealistic to expect that imposing a certain high level of authentication and signature requirements would eventually lead all parties to actually use them on a daily basis. Recent experience with sophisticated methods, such as digital signatures, has shown that concerns about cost and complexity often limit the practical use of authentication and signature techniques.

C. Electronic identity management*

45. In the electronic world, natural or legal persons may access the services of a number of providers. Every time a person registers with a service provider to access

---

* This section would be further developed in a final version of the comprehensive reference document.

[25] Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 October 1998, which provides a compilation of responses made during consultations on the European Union draft directive on electronic signatures, prepared at the request of the European Commission, available at www.fipr.org/publications/sigdirecon.html, accessed on 12 April 2007.

those services, an electronic "identity" is created. Moreover, a single identity may be linked to a number of accounts for each application or platform. The multiplication of identities and of their accounts may hinder their management both for the user and for the service provider. These difficulties could be avoided by having a single electronic identity for each person.

46. The registration with a service provider and the creation of an electronic identity entails the establishment of a mutually trusted relationship between the person and the provider. The creation of a single electronic identity requires gathering together those bilateral relationships into a broader framework where they could be managed jointly, in what is referred to as identity management. Benefits of identity management on the provider side may include security improvements, easier regulatory compliance and greater business agility; on the user side, they may include facilitated access to information.

47. Identity management may be described in the context of two approaches: the traditional user access (log-on) paradigm, based on a smart card and its associated data that a customer uses to log on to a service; and the more innovative service paradigm, based on a system that delivers personalized services to users and their devices.

48. The user access approach to identity management focuses on the administration of user authentication, access rights, access restrictions, account profiles, passwords and other attributes in one or more applications or systems. It aims at facilitating and controlling access to applications and resources while protecting confidential personal and business information from unauthorized users.

49. Under the service paradigm approach, the scope of identity management becomes broader and includes all the resources of the company that are used to deliver online services, such as network equipment, servers, portals, content, applications and products, as well as a user's credentials, address books, preferences and entitlements. In practice, it could include, for instance, information relating to parental control settings and participation in loyalty programmes.

50. Efforts are under way to expand identity management both at the business and at the Governmental level. However, it should be noted that policy choices in the two scenarios may differ considerably. In fact, the Government approach may be more oriented towards better serving citizens' needs and therefore may be slanted towards interaction with physical persons. On the other hand, commercial applications need to take into account the increasing use of automated machines in business transactions and therefore may adopt features meant to accommodate the specific needs of those machines.

51. Difficulties identified in relation to identity management systems include privacy concerns due to the risks associated with the misuse of unique identifiers. Moreover, issues may arise also with respect to differences in applicable legal regulations, especially in relation to the possibility to delegate authority to act for another. Solutions based on voluntary business cooperation based on a so-called circle of trust, where participants are required to rely on the correctness and accuracy of the information provided to them by other members of the circle, have been suggested. However, this approach may not be fully sufficient to regulate all

related matters and might still require the adoption of a legal framework.[26] Guidelines have also been developed to provide legal requirements for the compliance of a circle of trusted infrastructures.[27]

52. With respect to technical interoperability, the International Telecommunication Union has established a Focus Group on Identity Management "to facilitate and advance the development of a generic [identity management] framework and means of discovery of autonomous distributed identities and identity federations and implementations".[28]

53. Identity management solutions are being provided also in the context of e-government. For instance, in the context of the European Union "i2010: a European Information Society for growth and employment" initiative, a study on identity management in e-government was initiated to facilitate progress towards a coherent approach in electronic identity management in e-government in the European Union based on existing expertise and initiatives in the European Union member States.[29]

54. The distribution of electronic signature devices, often in the form of smart cards, in the context of e-government initiatives is becoming increasingly common. Nationwide exercises of distribution of smart cards have been launched, among other places, in Belgium[30] and in Estonia. As a consequence of those initiatives, a very large number of citizens are receiving devices with, inter alia, secure electronic signature capabilities at low cost. While the primary goal of those initiatives may not be commercial, such devices may equally be used in the commercial world. The convergence of the two domains of application is increasingly acknowledged.[31]

---

[26] See *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (European Commission, Directorate General Information Society and Media, June 2006), pp. 9-12, available at https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf.

[27] The Liberty Alliance Project (see www.projectliberty.org) is an alliance of more than 150 companies, non-profit and Government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, Governments, employees and consumers a more convenient and secure way to control identity information in today's digital economy and is a key component in driving the use of e-commerce and personalized data services, as well as web-based services. Membership is open to all commercial and non-commercial organizations.

[28] See http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

[29] See https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

[30] See http://eid.belgium.be/en/navigation/12000/index.html.

[31] See, for instance, *2006 Korea Internet White Paper* (Seoul, National Internet Development Agency of Korea, 2006), p. 81, with reference to the dual use in e-government and e-commerce applications of the Electronic Signature Act of the Republic of Korea, available at http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1.