Authentication & Digital Signatures in E- Law and Security

A Guide for Legislators and Managers

December 2004

This document was prepared for the Procurement Harmonization Project of The Asian Development Bank, The Inter-American Development Bank and The World Bank by Dr Paul Schapper of Curtin University of Technology of Australia and Dra Mercedes Rivolta of the Attorney General's Department Government of Argentina.

Disclaimer

The views expressed in this document are purely those of the writers and may not, in any circumstances, be interpreted as stating an official position of The Asian Development Bank (ADB), The Inter-American Development Bank (IADB) or The World Bank.

The ADB, the IADB and the World Bank do not guarantee the accuracy of the information included in this study, nor do they accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the ADB, the IADB or the World Bank.

Contents

Authentication

The art of discovering whether appearances are true or false

1. Introduction

The concept of authentication has been around for a long time in many forms. For example 'due diligence' in commerce has traditionally been formalised to determine whether the data presented in commercial propositions are accurate and comprehensive.

With the emergence of e-commerce the concept of authentication has encompassed new realities that are a feature of the relatively narrow avenues for information and potentially high risks inherent in an online environment. The problem of authentication in the online world goes to the heart of trust and therefore confidence-building for e-commerce and all of the benefits that this entails.

This paper seeks to provide an understanding about the different ways of assuring authentication. These authentication rules and tools – including for example Public Key Infrastructure (PKI) - are sometimes meant to set a legal and technological framework for trustworthy electronic transactions, promoting e-procurement, e-commerce, e-business and e-government.

Many countries have already enacted legislation giving effect to *legal validity* of electronic documents and electronic or digital signatures, and are in process of designing and implementing electronic government procurement models.

Electronic commerce transactions for business and other applications may also seek confidentiality, integrity and security from digital signature technology. This means that, for example, the receiver of an electronic commerce message may seek assurance about *business risk* - that the message came from the purported sender, that no part of the message has been altered during transmission, and that the contents of the transaction have been kept confidential.

These two considerations of *business risk* and *legal validity* are both intrinsic to the concept of authentication and define the structure of this report. This report explores the issues and solutions affecting the concept of authentication in terms of legislation, management and technology. This report finds that for online authentication things are not always what they may seem and that legislation and technology alone cannot build a trust environment and, if misunderstood, may produce a high risk illusion. It is crucial that the limitations and fallibility of the technology be explicit in its commercial applications and that business risks be managed accordingly. It is vital also to understand this conclusion if legislative and technological efforts are to be focussed effectively and management protocols engineered accordingly.

2. Trust in Business

To understand the challenge of online authentication it is necessary to appreciate the sources of trust that underlies the established commercial environment.

People don't do business with people they don't trust. But this commercial trust is not a matter of faith, regulation or technology; it is the outcome of relationship management.

The development of commercial relationships derives from traditional business interactions involving a range of diverse sources and types of complementary information about the other party, including:

- Correspondence
- Faxes
- Emails
- Telephone calls and video
- Meetings
- Networks
- Recognized behaviors
- Credit checks
- Document exchange
- Familiar business rules and legislation
- Assignment of liability / accountability
- Transparency, bank guarantees
- Etc

These multiple channels of information and processes are mutually reinforcing and build trust such that, if carefully managed, the *process* risks for businesses represent limited liability and free up commerce to manage the potentially unlimited liabilities and risks around the deal itself.

A familiar part of this trust environment is the signature. The idea of a signature need not be specifically defined. For the purposes both of business risk and legal application the role of a signature can be similar. For the management of risk it is important to authenticate the origin, destination and integrity of documentation – the requirement is to link a document exclusively with and entity, site, individual, authority, etc. These requirements demand information security both in traditional commerce and in e-commerce.

To address statutory requirements a signature needs to link a document with the intent of an entity. The crucial element is the specific intent of the signer to do a legally significant act in relation to a specific document. This intent may be demonstrated through any manner of means including an ink signature, a voice recording, chop marks, initialisation, a mouse click, a private key, etc. Creating a valid signature does not require a specific technology. Proof of signing relates to the intent rather than the technology. Proof of that fact needs to be made under other applicable law. E-commerce legislation needs simply to confirm that signatures may also be accomplished

through electronic means, and the term 'signature' has been used to connote that functional equivalence.

An important aspect of this legal interpretation lies in the necessity that a signature be logically associated with the record such as an ink signature at the end of a contract or a mouse click on a web page. This too implies security management.

Ink Signatures

Traditional ink signatures demonstrate the physical presence and the intent of an individual as well as the time and date of a transaction. The ink signature has been a cornerstone of traditional trust relationships. The ink signature, as well as being surrounded by a history of case-law:

- Associates signer with the document
- Proves involvement in signing and content
- Provides endorsement of contents
- Proves time and place association
- Addresses statutory obligations
- Evidences user awareness of importance
- Represents user control and user consent.

The ink signature, while not bionic, has a forensic quality which is relatively difficult to misuse by third parties often because this also implies physical access to hard copy documentation which in turn resides in obscure places such as filing cabinets, safes, etc. These physical stores of documentation will usually be accessible by only a handful of people.

3. E-Business

Much of this traditional risk and trust environment has no ready-made equivalent in the online world.

Any analysis of business in the online environment needs firstly to distinguish between B2C (or retail) and B2B (business-to-business or business-to-government). In most cases B2C transactions are less problematic using established processes involving very limited liabilities between contracted parties (such as credit card holders, merchants, credit card vendors and banks). A large transaction in this environment would usually be of the order of a few thousand dollars. The liabilities are measurable and limited which allows the processes to be insured (generally paid for through credit card fees). This 'traditional' e-commerce continues to carry the great bulk of e-transactions and is characterised by closed contractual relationships between each party. The success of these traditional closed systems is measurable by their ubiquity and risk controls. For example credit cards are everywhere but require no identity check to use them. The costs, risks and convenience of credit cards are reasonably transparent to each participant.

The B2B Environment

The same comforts do not apply to B2B or B2G commerce and the circumstances of these bear little relationship to the B2C environment. It is these applications that are the main focus of this report.

With the emergence of the internet as a part of the commercial environment demands have arisen for commerce and information exchange to occur through systems that do not support the familiar relationships of EDI. This new environment is missing many of the risk control points of traditional e-commerce, including standards, risk sharing and access controls.

Often regarded as basic to commercial undertakings in this context are the properties of

- Identity
- Authority
- Integrity
- Security & confidentiality
- Availability

- where 'Integrity' refers to the accuracy and completeness of documentation rather than the qualities of the parties. These properties are elaborated on below.

Electronic / Digitised Signatures

For the online environment the immediate analogue to the handwritten signature would seem to be the electronic or digitised signature which often means a person's handwritten signature, password or some other identifier scanned, recorded or by some other means converted into electronic form for association with an electronic record or message or for other purposes. However an electronic or digitised signature might not be specific to a particular document and might be vulnerable to be attached or transferred to anything, anywhere at any time and therefore might not provide strong evidence about the intent of the signatory or the origin of the document. The value of an electronic signature depends very much on the circumstances and context of its application and the understandings (contractual or otherwise) of the parties involved.

Nevertheless even seemingly insecure digitised signatures can have their place in authentication with the appropriate technology, management and trust systems and are overwhelmingly the dominant method in the digital world with widespread use in, for example, emails, faxes, banking devices, building security entries, biometric devices, etc.

Digital Signatures

Electronic signatures are sometimes defined as *exclusive* of digital signatures, especially by technologists. However, it seems more meaningful to define electronic signatures as *inclusive* of digital signatures. Most electronic signature legislation is inclusive in this way and conceives of electronic signatures as a broad generic concept which can come in many forms. At this generic level digital signatures logically form a special subset.

Thus while electronic signature legislation is inclusive of digital signatures, digital signature legislation is not inclusive of electronic signatures.

Accordingly for the purposes of this discussion and in the interest of economy of language, electronic signatures will refer to the broad generic legal meaning which is inclusive of digital signatures.

Digital signatures are not recognizable as ordinary traditional signatures. A digital signature is a technique for associating with a digital document a code that demonstrates that the document could reasonably only have come from someone or something accessing the signatory's secret or private key. A digital signature is intended to provide the legal equivalence of an individual's handwritten signature insofar as it is designed to be uniquely, irrefutably and unambiguously associated with a particular document and also authenticate that it could have been affixed only by that individual. (The individual could also be an organisation or some other entity but the meaning is the same). To what degree digital signatures succeed in delivering these attributes, at what cost and what practicality are crucial business considerations to be addressed below.

4. Some Basic e-Concepts

The central objective of Information Security is to preserve the confidentiality, integrity and availability of an organisation's information. Also for e-commerce the parties to a transaction must be confident that the transaction is secure, verifiable, authorised and legally recognised. It is only with this assurance that enterprises can engage in commercial activities. The loss of one or more of these attributes may cause significant damage to the organisation or individuals. However rarely are all of these properties required by a specific transaction. The following concepts all have their obvious counterparts in the non-digital environment but face new and often more stringent demands in the online world.

Security

Security means the quality or state being protected from uncontrolled losses or effects. Absolute security may in practice be impossible to reach; thus the security "quality" can be relative. Within state-models of security systems, security is a specific "state", which is to be preserved under various operations. This introduces the concept of a Security level - that is, the combination of hierarchical classifications and non-hierarchical categories that represents the sensitivity of information.

Confidentiality

Confidentiality means that information is shared only amongst authorised persons or organisations. Breaches of confidentiality can occur when data is not handled in an adequate manner to safeguard the information concerned. Such disclosure can take place by word of mouth, printing, copying, e-mailing, etc. The classification of the information should determine its confidentiality and hence the appropriate security.

Integrity

Information integrity means that the information is authentic and complete and can be relied upon to be sufficiently accurate for its purpose. The term Integrity is frequently used when considering Information Security as it represents one of the primary indicators of security (or lack of).

Availability

Availability means that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Record-keeping

Commercial information must be auditable, regardless of whether it is based on paper or electronic records. This capacity to be audited does not change; the rules are the same even though the technical supports will differ. This means that the information must be secure and available to a standard of integrity that ensures that it continues to have a high level of evidentiary value for long periods of time.

Non-Repudiation

A further property often defined as essential for e-business is non-repudiation which is simply an outcome of authentication combined with integrity and is intended to represent enforceable commitment.

Authentication

Authentication refers to the verification of the authenticity of identifiers claimed for or by either an entity such as a person or organisation, or data such as a message or other claimed properties.

An authentication[1] process is the second of two steps comprising:

- presenting an identifier to the security system and
- presenting or generating information that corroborates the binding between the entity and the identifier.

Authentication of a signature may often have legal consequences while authentication of originating site, destination as well as identity may have security objectives.

Presumption of Authentication

To protect and ensure a level of digital trust, the parties to e-commerce may employ digital signatures, which are intended not only to validate the sender, but can also 'time stamp' the transaction, so it cannot readily be claimed subsequently that the transaction

[1] The Electronic Authentication Guideline defines Authentication as 'the process of establishing confidence in user identities': NIST September 2004. A broader definition includes entities and artefacts in addition to identities.

was not authorised or not valid. But rather than digital signatures the parties may also use legal engineering based on electronic signatures, passwords or other methods like biometrics. The only differences are the presumptions associated with the transaction. If a digital signature is used, almost all laws assign an authorship and integrity presumption to the transaction. If the authentication is based on electronic signatures, it is necessary for there to be a previous agreement between both parties in order to establish the method. That agreement will replace the legal presumptions of the authorship and integrity of the document.

By *presumption*, in a legal context, an evidentiary rule eases the burden of proof as to a particular fact, usually so that the proponent of the fact is relieved of the burden of coming forward with evidence in support of such fact.

Presumptions are usually *rebuttable*, so that the presumption may be overcome by introduction of sufficient contrary evidence of the fact by the opposing party. For example, the Argentine Digital Signature Law Nº 25.506 sets forth a presumption that a digital signature verified by a certificate issued by a licensed CA is attributed to the subscriber named as subject in the certificate. One method of rebutting this presumption might be to introduce evidence that the applicant for the certificate was an impostor who fraudulently convinced the CA to issue the certificate to the impostor in the name of the subscriber.

The idea of non repudiation is strong and substantial evidence of the identity of the signer of an electronic document and of its integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents. In a legal context, this means sufficient evidence to persuade the ultimate authority (judge, jury or arbiter) as to such origin, submission, delivery, and integrity, despite an attempted denial by the purported sender.

Digital and Electronic Documents

Some laws define a 'digital document' as the information encoded in digital form over a logical or physical support, in which electronic, photolithographic, optical, or similar methods are used which become the legally relevant representation of acts, facts, or data.

Other laws use the concept of 'electronic record'. For example, the E-Sign Federal Law of the USA, defines an electronic record as 'a contract or other record created, generated, sent, communicated, received, or stored by electronic means'.

The Uncitral Model laws on e-commerce and e-signatures recognize the legal validity of data messages, defined as:

- information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; also

- "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information.

The notion of "data message" in the Uncitral Model Law on Electronic Commerce is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of "message" includes that of "record".

Other definitions of an Electronic Document may be as an electronic statement, recorded on magnetic, optical or other carrier that allows it to be reproduced.

Authorship

Like a paper based document, authorship may be assigned to an electronic document. In the paper culture, that link between a document and a person is satisfied by a handwritten signature. The signature assures authorship, authority or endorsement and consent. For e-commerce the challenge is to find the functional equivalent of the traditional ink signature.

Initially, one of the principal obstacles to e-commerce that traditional civil laws presented was the requirement of a 'signature'. Many countries have addressed this problem with new e-commerce regulations or e-signatures laws.

Article 7 of the UNCITRAL Model Law on Electronic Commerce recognises the functions of a signature in a paper-based environment to include the following:

- they identify a person;
- provide certainty as to the personal involvement of that person in the act of signing;
- associate that person with the content of a document.

It was noted that, in addition, a signature could perform a variety of other functions, depending on the nature of the document that was signed.

For e-commerce there are various e-signature techniques currently being used or still under development. The common purpose of those techniques is to provide functional equivalents to handwritten signatures and other kinds of authentication mechanisms used in a paper-based environment (e.g. seals or stamps). The same electronic techniques may also perform additional functions that do not have a strict equivalent in a paper-based environment.

The authorship presumption that a digital signature implies, is based on the basic principle that the signatory should apply reasonable care with respect to the use of its signature including avoidance of unauthorised use. A digital signature in itself does not guarantee that the person who has in fact signed is the signatory. At best, a digital signature provides assurance that it is attributable, with various levels of certainty, to the signatory. In the digital environment the distinction between an original and a copy has no useful meaning. This means that where the forensic quality of an ink signature provided substantial assurance of authentication in traditional commerce there is no real equivalence in the digital environment, where the signature application procedure itself must be secure. Thus *security* in the digital environment substitutes for the *forensic qualities* of the paper-based environment.

Where the signatory knows or should have known that its e-signature has been compromised, the signatory should give notice without undue delay to any person who may reasonably be expected to rely on, or to provide services in support of, the e-signature. This represents a non trivial management challenge with uncertain liabilities.

5. Statutory versus Risk Requirements

Within the foregoing discussion are two important thematic components. E-commerce, like paper-based commerce, has requirements firstly in terms of its legal status and secondly its capacity to convey business trust or security. These two components are often not distinguished and become the source of much confusion of the issues. The separation of the statutory from the security requirements of e-commerce is illustrated in Figure 1 where elements of the preceding discussion are evident. Part of this confusion of these requirements has arisen because both security and statutory requirements use the same technology, or more accurately the same technology has been applied to both requirements.

Figure 1
Authentication for E-Commerce

However the requirements of legal validity in e-commerce are quite different from those for business security, and the confusion between the two has sometimes led to inappropriate applications of the technology, poor business models and even a lack of legislative interoperability. So while it is common to use digital signature technology to assure confidentiality, for example for sending encrypted messages, this use has no

relationship with the legal concept of digital signatures. Thus from a business risk perspective, where an entity can experience major losses in a matter of seconds, the fact that a digital signature carries a rebuttable legal presumption may be of no relevance whatsoever. This dichotomy will be returned to in following sections.

6. Cryptography

The transmission of information through the internet is inherently an insecure process. It is appropriate to assume that all information can be accessed by unintended parties who might be, for example, commercial competitors.

Technical responses to these requirements of authentication, security and integrity have arisen from the application of cryptography in combination with some off-line processes. It is important to understand these elements if the role and limitations of legislation and risk management are also to be understood.

Cryptography, Greek for "hidden writing", is the art and science of transforming (encrypting) information (plaintext) into an unintelligible form (cipher-text) for securing information in storage or transit. Encryption and complex mathematical algorithms are available to render information unintelligible to anyone except the intended recipient.

These algorithms typically produce a pair of large numbers or *keys* – an encryption key and a decryption key.

Generally the cryptographic algorithm is not required to be secret and indeed is usually well known. The strength of the encryption depends on a range of factors such as the length of the key, whether the key itself is predictable or secure, the mathematical algorithm and the capacity of machines available to attack the code. Properly designed and applied encryption regimes represent a formidable defence against intrusion. However it would be a mistake to equate strong encryption with strong security, but more about this below. Also encryption that is regarded as strong today will be less so tomorrow as computing power increases and the encryption protecting sensitive material should be regarded as having a finite life, which cannot necessarily be extended through re-encryption with stronger applications.

Symmetric Encryption

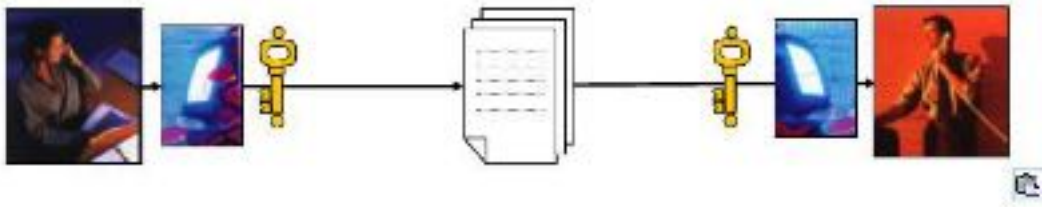
For symmetric key encryption the encryption key and the decryption key may be the same or easily calculated from each other. In most cases the keys are the same – Figure2.

Symmetric key encryption can be very fast and efficient in terms of computer use and it has a major role in, for example, ephemeral machine-generated machine-to-machine links for confidential transmissions.

However for many other uses it is less satisfactory. Symmetric key encryption has, in particular, two severe limitations. First symmetric key encryption means that both parties hold the secret key, meaning that authentication is not viable.

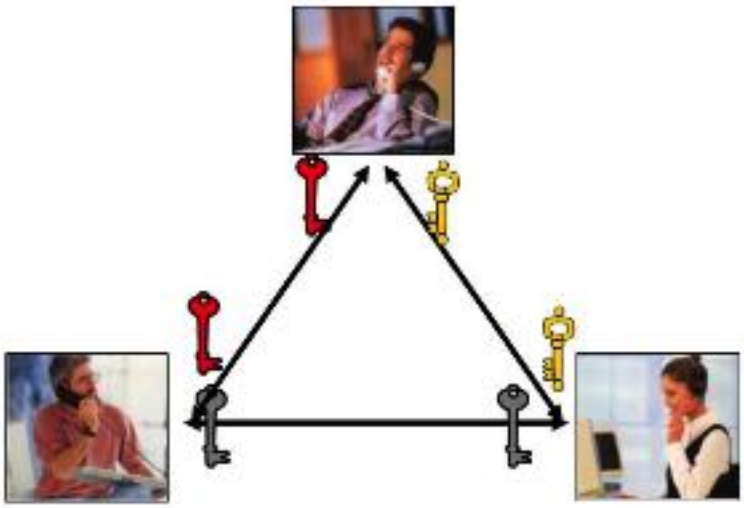
Misunderstandings or disputes may emerge as to who sent a message or, in the case of compromised key security, who was responsible.

Figure 2
Symmetric Encryption



Second there are problems in conveying the key from one party to another (transmission security), during which it might be captured by a third party, meaning that an intruder can not only read the confidential material but also create bogus messages or alter the original documentation. Also symmetric key technology is too cumbersome for many applications that will usually require a different secret key for each two parties, which for even a modest network of users rapidly become impractical – Figure 3.

Figure 3
Multiple Symmetric Keys



Some of these issues have been addressed by the 'Kerberos' system but this has other limitations such as the reliance on a central key management server which in itself becomes cumbersome when there is more than one.

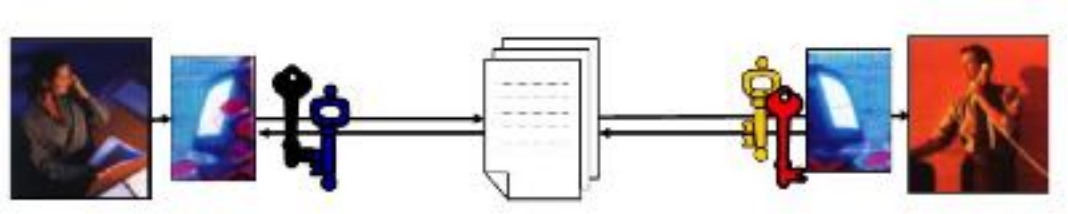
Public Key Encryption

Another kind of cryptography, known as "public key cryptography," addresses the limitations of symmetric key cryptography. Public key cryptography employs algorithms using two different but mathematically related keys, one for encrypting data, and another key for decrypting data. Because the two keys cannot be derived from each other, except with great difficulty (even if the algorithm that created the key pair is known), this is sometimes referred to as asymmetric encryption and has the property of 'irreversibility'.

The complementary keys of an asymmetric cryptosystem are arbitrarily termed the private key, which is known only to the holder, and the public key, which is more widely known (and can be made public knowledge) and hence the term Public Key Technology.

This means that the private key holder is the only party able to decrypt (or alternatively to encrypt) the transmission. This represents greater security than for symmetric encryption. Also it means that many parties can communicate confidentially with the private key holder without any of them having a secret key of any kind. Also the private key holder can encrypt a message and publish it for anyone with the public key to decipher – this providing confidence that the message was encrypted uniquely and only by the private key holder – a crucial step in authenticating the origins of the message.

Figure 4
Asymmetric Encryption



For two-way confidential communication each user requires a pair of unique keys, a public and a private key – Figure 4. However, unlike for symmetric key encryption, each party requires only one secret key regardless of how many other parties are being communicated with. If something is encrypted with the private key it can be decrypted only with the public key. Conversely something which is encrypted with the public key can be decrypted only with the private key.

Encrypted transmissions form the first step for security, but provide no assurance about the identity of the sender or its origins or whether the entire message has been received. These issues lead to the ideas of 'digital signatures' and 'integrity'.

Creating a Digital Signature

Public key encryption lays the foundation for digital signatures on the grounds that it makes it possible for information to be recognised as having originated from the holder of a private key and none other than the holder of that key. This would seem to be the answer to online authentication. Any document is encoded in such a way that anyone with the public key can read it but only the signatory could have created it because the private key of the asymmetric encryption is secret to the signatory.

However public key encryption alone does not provide a legally robust digital signature because, while it provides strong evidence that the message or document was signed by the holder of the private key, it provides no information about the link between the private key and any individual. Therefore a digital signature also needs a further attribute that provides it with an ownership by a real world entity.

From both a risk control and a legal point of view, a digital signature is required to be some electronic equivalent of an individual's signature which authenticates the message to which it is attached and validates the authenticity of the sender.

To validate the authenticity of the sender one solution has been to engage independent agents to certify that the digital signature belongs to a particular identity or entity. This means the use of digital certificates issued by a 'Certification Authority', who may / may not have been licensed by a public body. Logically digital signatures, just like all other forms of signatures, stand alone from the idea of 'certification' and the idea of the certification process is to enhance the value of the signature. This enhancement gives rise to the notion of an 'enhanced signature' which is afforded greater legal standing in some jurisdictions as discussed below.

It is to provide this last link of 'certifying' a link between a key and an identity that Public Key Infrastructure (PKI) has been developed.

A digital signature is of little value on its own. It gains value by being attached to something – a document for example. Relying parties therefore need to have confidence in two things – the validity of the signature, and the accuracy of the document to which it is attached. For commercial applications users will want assurance not only that the documentation is confidential but also that it has not been altered in some way during transmission, for example that part of it has not been cut off. Thus in verifying a digital signature the relying parties must also verify the *integrity* of the attachment.

To address this requirement the software creating and verifying digital signatures makes use of 'hash' functions (also known as message digest functions). A 'hash' function is a mathematical operation on a document that creates a unique number that is the digital equivalent of a fingerprint, or the document's 'DNA'. The hash function creates a fingerprint for the document. Even the smallest change to a document such as the conversion of a comma into a full-stop will produce a very different hash result. A hash, properly constructed, is essentially unique to a document. Thus a hash provides an essentially unique identifier of a document.

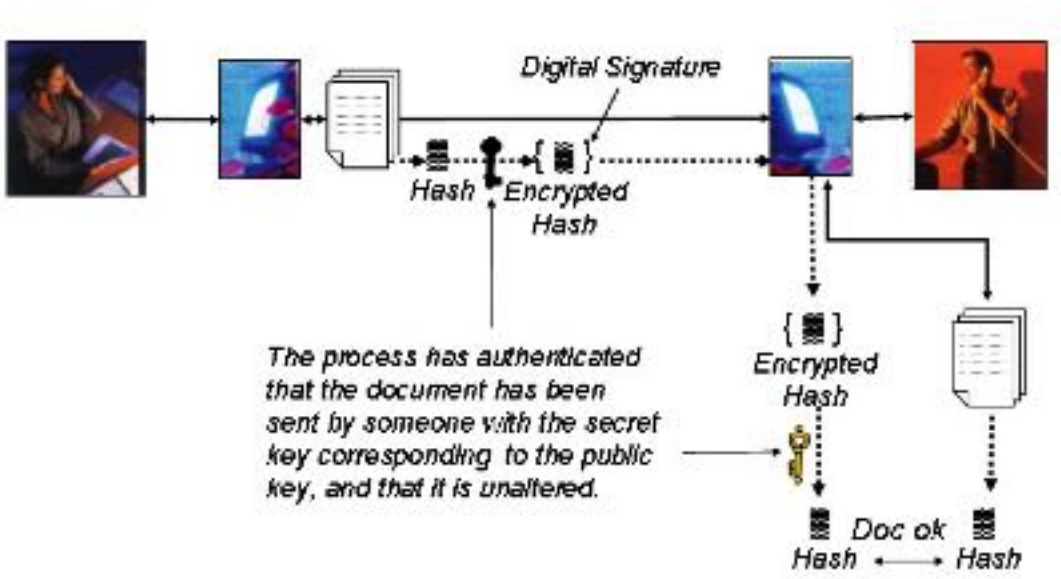
If the hash is computed and encrypted with a secret key by the secret key holder then this provides a strong association between the document and the secret key holder. This is what is defined as a digital signature – *the linking of the secret key (supposedly uniquely associated with an individual or organisation) with a hash (uniquely associated with a document).*

The recipient verifies the digital signature and the document by independently computing the same hash function from the received document as well as using the sender's public key to decrypt the digital signature and recover the hash that the signer computed. If the two hash results are the same then this provides strong evidence that the document was indeed the one 'signed' by the sender, and that it has not been altered.

Figure 5 shows how these components come together.

However there are problems that mean that this public key encryption still does not translate into authentication. One major problem is to find a way of conveying the correct public key to the intended recipients and be sure it has not been captured and substituted for another key by an attacker – a Key Management issue. The second major problem is linking the key ownership with the individual (who is the person associated with this key?).

Figure 5
Digital Signatures



Thus authentication is not provided because the private key holder is not identified. The unique attribute about the 'digital signature' is the private key. The essence of a digital signature is the private key and its link to a document is through its application in encrypting the hash or document fingerprint.

Key Management

Symmetric and asymmetric algorithms and their cryptographic keys all have different strengths, weaknesses, and properties that require good policies and practices to protect them.

Digital signatures differ from traditional ink signatures where much of the authentication is assured by the forensic quality of the signature itself. In the digital world the notion of an 'original record' is effectively meaningless and the authentication derived from a digital signature cannot derive from its 'quality' or attributes but instead derives from the *security* itself around the secret key.

The security both of symmetric and asymmetric cryptography relies upon the sophistication of the publicly known algorithms and the secrecy of the keys. Authentication derives from the degree to which management and technological capabilities are able to provide trust in the link between the secret key and a real-world entity – an individual or organisation.

The most difficult problem for online authentication and therefore for internet commerce is key management. The key management problem includes a range of issues including:

- The link between a public key and an identity or entity
- The association of a secret key with a public key
- The security of the secret key
- The publication or communication of the public key
- The currency or obsolescence of the key associations

And depending on the degree to which these issues are resolved:

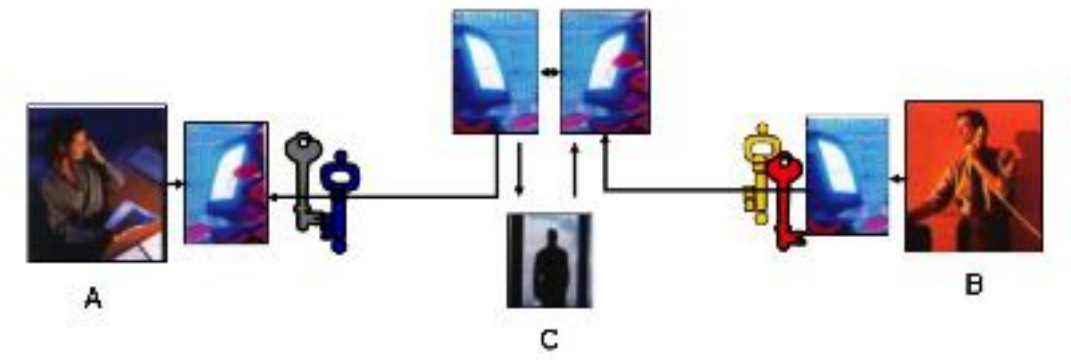
- Accountabilities and liabilities associated with key use
- Whether key use implies informed consent

For public key cryptography to be useful for authentication it is essential that each party has complete confidence that the public keys they are using to encrypt their messages are in fact the correct public keys of the corresponding parties without any security compromise. The prospects of encrypting highly valuable commercial information, such as for a government contract, with a key linking back to a commercial competitor could represent unlimited risk. Conveying this non-confidential information (the public key) to the other party is in reality a major security challenge.

The reason that this public information represents a security risk is shown in Figure 6:

By intercepting the public key transmission from A to B the man-in-the-middle substitutes a bogus key that B uses to encrypt confidential information to be sent back to A. This information is received by C who can decrypt the information and elect to re-encrypt using the genuine public key from A and neither A nor B will know that their communications are completely transparent to the third party C.

Figure 6
A Key Exchange Problem



To provide authentication of the associated identity requires that assurance is also provided that:

- Another user or device did not also have access to the private key
- The public key was the key corresponding to the presumed private key
- The signature generation process cannot be forged by another device.

Without this very specific assurance none of the pre-defined attributes of:

- Identity
- Authority
- Integrity
- Security

- can be assured and commercial trust cannot be conveyed by this method.

It is important to appreciate the degree to which existing technology can address these requirements and the risks that remain.

It is this problem that is the focus of Public Key Infrastructure (PKI).

7. PKI

Ink signatures have one attribute that effectively has no digital equivalent – the application of ink signatures cannot meaningfully be detached from the signer. In the digital world the digital signature is very definitely detached from the signer – it resides in a machine or device. To have the legal effect of a signature relying parties must trust the link between the signer and the signature – a link that in the ink and paper world could be taken for granted. In the digital world one response has been to develop an extensive infrastructure (PKI) to provide trust in this last link. Thus recognising that online technology effectively detaches the signature from the identity, the role of authentication techniques such as PKI, is to restore trust in the link between the two.

Public Key Infrastructure (PKI) is the sum total of the hardware, management software, processes, and policies that is used to deploy public key technology to facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair). PKI is intended to provide a high degree of assurance or trust that the message was digitally signed / originated from a device that had access to a particular private key and that the use of that key is attributable to an individual or authority.

To solve this problem the public key is certified by an independent and trusted authority as to who it actually belongs to. This certification comes in the form of a Digital Certificate which is attached to the public key. This certification process includes a digital signature by a recognised certification authority (CA) and is difficult to mimic. Under this regime a public key comes with an identity certificate (Digital Certificate) from which it is difficult to separate, so that with each use of a public key the identity can be verified by the digital signature from the trusted authority.

A public key infrastructure includes:

- A Certification Authority (CA) - issues and assures the authenticity of its Digital Certificates. A Digital Certificate includes the public key or other information about the public key.
- A Registration Authority (RA) - validates requests for Digital Certificates. The Registration Authority authorises the issuance of keys to the applicant by the Certificate Authority.
- A certificate management system - a software application provided by the PKI vendor.
- A directory where the certificates, together with their public keys are stored.
- A trusted third party clearing house for issuing Digital Certificates and Digital Signatures. Digital certificates include your entity's name and public key, the digital signature of the certificate-issuing authority, a serial number as well as an expiry date.
- Subscribers – individuals or entities named or identified in digital certificates holding the private keys that correspond to the public keys listed in the certificates.
- Users - those who can validate the integrity and authenticity of a digital document or data message, based on a digital certificate of the signer.

A digital certificate, or public key certificate, is therefore the electronic version of an ID card that establishes an entity's credentials and authenticates its connection.

The digital certificate contains the Digital Signature of the Certification Authority to allow any recipient to confirm the authenticity of the digital certificate. This digital signature of the CA will itself require verification and this is done through a hierarchy between the CAs where the CA at the highest level (a root CA) has only a self signed certificate. This certificate is delivered off-line or otherwise built into commercial browsers.

Where there are multiples of CAs operating the idea of cross-certification arises. Before a user can verify a digital signature generated by a subscriber of an alternative CA

he/she must obtain the verification public key of the generating CA. To avoid various masquerade attacks this public key must be provided to the user in a way that will assure its integrity. This is accomplished by having the user's CA and the signer's CA cross-certify each other whereby each CA provides the other with a verification certificate – called a cross-certificate – containing the other CA's public verification key. The user is then able to verify the cross-certificate generated by its own CA for the other and, with the public key it contains, verify the integrity of the signer's certificate.

There may be various "business models" or ways in which a PKI is organized, the purpose of the PKI, who is permitted to participate in the PKI, who performs the various functions of the PKI participants, and what relationships the parties have with each other. For instance, a PKI may have a "business model" of company owned certification authorities that outsource front-end functions to registration authorities and that have the right to outsource back-end functions to certificate manufacturing authorities, where the CAs issue certificates to employees of the companies for the purpose of facilitating business-to-business transactions among the companies who contracted to create the PKI.

An important type of PKI business model presented is the "open" PKI model. The open model typically involves one or more certification authorities issuing certificates that can be used by anyone in the general public. In other words, anyone can be a relying party. In addition, this model assumes that the CA is a third party with respect to the relationship between the subscriber and relying party. That is, the CA is not directly involved in contractual or other relationships between the subscriber and relying party.

Because of this detached relationship, the open PKI model often involves one or more certification authorities that issue certificates to subscribers who may use the certificates for general purposes. For example, a region may have several CAs, all of whom issue certificates to individuals for use in secure e-mail and electronic commerce. The CA provides a general service of confirming the identity or other attributes of subscribers, and anyone in the public can benefit from the assurances provided by the CA. Legislation that assumes the open PKI model is directed generally towards assuring the quality of these third party CAs to protect the subscriber and relying party communities from CAs falling below minimum quality standards. Examples of such legislation include the digital signature laws of Utah, Washington, and the Federal Republic of Germany.

In some instances however, the notion of "open PKI" is defined in an even more extensive sense. In this more extensive notion of "open PKI," there is not only no direct CA involvement in the relationship between the subscriber and relying party, there is also no contractual relationship at all between the CA and the relying party. This view of "open PKI" also assumes that the act of reliance itself does not create a contract with the CA.

Therefore, the relying party in this model is never bound by contract to the CA, and any legal implications of the relationship between the CA and the relying party arise from tort law, rather than contract law. This extended model of "open PKI," however, is largely theoretical and, in hindsight, an outdated perspective; no major CAs avoid or disclaim privity with relying parties, or even admit the lack of privity. To the contrary, the major CAs that are the most "open" within the marketplace purport to have a

contractual relationship with relying parties. To be more accurate, therefore, even the most "open" significant PKIs in existence are technically "contractual" PKIs as described below.

Another kind of PKI is the "closed" PKI model. In the closed model, the CA is itself the relying party (or the employer of the relying party). In one alternative, the relying party may outsource PKI services to a CA that will issue certificates to subscribers on behalf of the relying party.

Examples of a closed PKI model include a bank operating a CA and issuing certificates to its customers. This model may or may not involve a separate PKI-related contract between a company acting as CA and its customers. This model is frequently used by "enterprise" deployments of PKI to establish PKI services and issue certificates to the employees and possibly customers, suppliers, or other extranet members of an enterprise.

The liabilities and obligations contained in the closed model are usually a function of the business relationship (including bargaining position) between the parties. This may be the employer-employee relationship or a contractual relationship with a customer or supplier.

An additional PKI business model is the "contractual" model. In the contractual model, the provider of PKI service is bound by contract with its subscribers and relying parties. No party outside the contractual relationship is permitted to participate in the PKI. The contracts may create a contractual relationship between the subscriber and the CA or among many parties, including other subscribers. The advantage of this model is that risk, responsibility, and recourse can be clearly defined and managed. Thus, there is less reliance on tort law. Depending upon the implementation, the execution of a contract (and thus, creation of privity) between the parties may happen at anytime including immediately prior to reliance on a certificate.

There are also different formats for certificates available for use, with the X509 standard the most prevalent. Various types of certificates are possible, such as attesting to the authenticity of an authority, but most of those in use are identity certificates.

This discussion, however, is not intended to be an exhaustive listing of possible business models, and new models or variations on existing models are inevitable. Moreover, a PKI may contain elements from more than one business model, or imperfectly implemented ones.

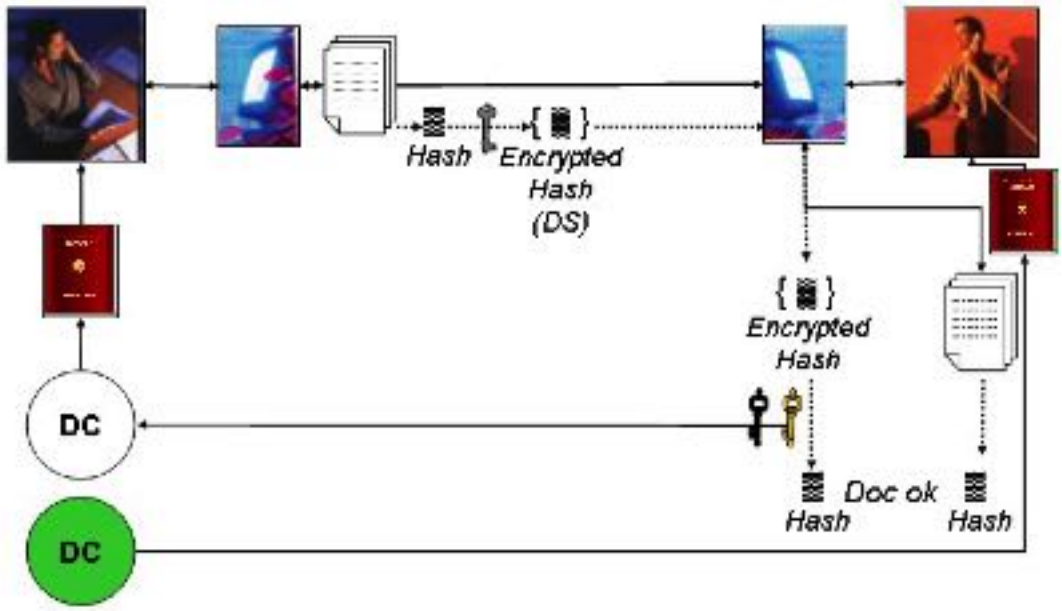
This solution effectively transfers the problem of key / identity association to the 'trusted authority'. Issues then arise as to how satisfactory are the processes of the authority, what is the integrity of the authority, how can there be assurance that the authority has, knowingly or unknowingly associated a public key to a false ID.

These issues become public policy and risk management problems as to the authenticity of the ID attached to the public key by the CA and the accreditation of the CA itself.

In addition there are the issues surrounding the security about the secret key itself, as well as its currency / obsolescence.

The role of the CAs (of which there are many) are illustrated in Figure 7.

Figure 7
PKI



In addition to issuing digital certificates CAs provide other services including managing certificate repositories and time stamping.

For this system to be commercially practical requires that its risks be known, measurable and manageable. The characteristics of commerciality include:

- Scope – identity, entity, organizational, human , attribute, value, agent
- Robustness – revocation, key compromise, key security, reliability, etc
- Cost and Efficiency – data demands, maintenance, contextual risks
- Transparency – ease of understanding, clear onus of responsibility, onus of proof, etc
- Limited liability, risk sharing and accountability of operation.

It is not possible to claim without qualification that PKI currently satisfies these requirements, nor is it possible to say that the risks are measurable and manageable. For the risks to be measurable and manageable requires that the applications are specified.

CA Technical Rules and Documents

The main documents governing CAs are:

- Certification Practice Statements (CPS)
- Certification Policies (CP)
- Agreements

A CPS is a statement of the practices including the systems, policies and procedures that a certification authority employs in issuing certificates.

The Certificate Policy (CP) indicates the applicability of a certificate to a particular class of application with common security requirements.

CPs, CPSs, subscriber agreements, and relying party agreements are the core documents within a PKI. From a legal perspective, the subscriber agreements and relying party agreements are the fundamental building blocks within the PKI. In a legal sense, PKI is all the technical, policy and management framework plus the accreditation of public bodies that accredit the Certification Authorities and the Registry Authorities to give greater legal value to a digital signature (creating an 'advanced' electronic signature or a 'reliable' electronic signature).

However, the PKI may engage other agreements as well.

Examples may include:

- Interoperability agreements
- Vendor agreements, ASP agreements.
- Marketing and certificate distribution, RAs
- Internal agreements related to the proper operations of a PKI, non-disclosure.

Other Authorities

An Accreditation Authority is the public body responsible, within the legal jurisdiction, for:

- issuing licenses, setting minimum CP requirements and giving formal recognition to standards,
- authorization, regulations or other government or legal recognition to community CAs as managed by the respective CA Policy Authorities and Operational Authorities.

Accreditation is the procedure by which an authoritative body declares that an assessor has satisfied the designated criteria for assessing a PKI component.

The Accreditation Authority is a PKI management entity with the authority to permit a subordinate PKI entity (such as a CA) to operate within a particular domain.

An Assessor Accrediting Body is a recognized entity that accredits an assessor or evaluator as being qualified to perform assessments of CAs or other PKI components, applying designated criteria (such as standards derived from the certificate policies adopted by the policy-adopting body).

An Assessor may be an independent agent, member of an accounting body, or other qualified professional recognized by the PKI Accreditation Body. A PKI Accreditation Body is responsible for evaluating the CA Operational Authority's compliance and management in relation to stated policies, practice statements, standards and criteria, and providing an audit opinion.

8. PKI Limitations

The idea of PKI is simple enough and was developed more than twenty years ago. Today, it is applied with many standards and protocols (such as SSL/TLS, IPSEC, etc.). Everyday, people visit websites for shopping or banking and PKI is part of the connection security.

However it is evident that PKI management and legal dimensions are complex, even without the developments required to extend the legal validity of the digital certificates between different countries and different accreditation systems.

For business risk and security management this complexity also means many points of potential weakness. Thus although PKI can be used to help authenticate people, secure commercial transactions and protect the privacy of emails and telephone conversations, a number technical and management vulnerabilities and barriers, including lack of applications, high costs, poor understanding of PKI, and interoperability problems have restricted the use of PKI. Some experts on PKI caution that, in fact, PKI has limited scope.

To help identify some of the most important obstacles to PKI deployment and usage, a survey has been conducted by the PKI Forum ("PKI Action Plan", OASIS Public Key Infrastructure (PKI) Technical Committee (TC), February 22, 2004).

This survey attracted a large number of highly qualified respondents, who identified certain specific issues. The top five obstacles to PKI deployment and usage identified by the survey were:

- Software applications don't support it
- Costs too high
- PKI poorly understood
- Too much focus on technology, not enough on need
- Poor interoperability

The survey respondents indicated that their most important applications for PKI were Document Signing, Secure Email, Electronic Commerce, and Single Sign On. Document Signing was further broken down into Signing Forms, Signing Contracts, and Signing Documents before Dissemination, with roughly equal interest in each of these subcategories.

Survey respondents were asked to describe in their own words the causes of the obstacles:

- "Support for PKI is inconsistent. Often, it's missing from applications and operating systems. When present, it differs widely in what's supported. This increases cost and complexity substantially and makes interoperability a nightmare.

- Current PKI standards are inadequate. In some cases (as with certificate management), there are too many standards. In others (as with smart cards), there are too few. When present, the standards are too flexible and too complex. Because the standards are so flexible and complex, implementations from different vendors rarely interoperate."

Common PKI System Weaknesses

PKI potential weaknesses can be identified in many of its parts, the significance of which cannot be assessed independently of the individual applications. A list of potential weaknesses with both security and legal significance includes:

- Lack of clarity about pre-authentication procedures
- CA based trust
- Lack of warranties
- Certificate revocation issues
- Privacy
- Public key deployment
- Insecurity of storage
- Insecurity of timing issues

PKI provides strong assurance that a message originated from a device that had access to the corresponding private key. An associated digital certificate provides assurance that the Certificate Authority had grounds in the past for believing that the private key had some association with the identity (together with some rights and capabilities of use)

However PKI does not provide assurances:

- That the private key was not also available to other identities
- That the private key application was by the appropriate identity with informed consent

Also:

- Same signature may apply for any application and any risk
- Single channel (sometimes two or three channels - compare with determinants of Trust in business discussed above)
- No way to measure risk
- No way to assign accountability
- Therefore no way to handle liability
- Potentially unlimited risk liability → uninsurable

Certification 'Authorities' are a central element of PKI that also is not entirely satisfactory. There are multiple CAs and yet a user does not want to have to deal with them all so there needs to be some sort of exchange together with the function of the Registration Authorities. Neither is it necessarily clear what or whose the 'authority' actually is or what responsibility, accountability or liability is associated with this.

Certificate Revocation

Certificate revocation is another problem for which PKI has not been able to provide a satisfactory answer. If a certificate is compromised and revoked all documents that have previously been signed now become impossible to read. Alternatively the certificate can be kept for decryption purposes but this will require that the dates of new documents cannot be forged. Also it is difficult if not impossible to ensure certificate revocation in real time appropriate for some commercial realities and retrospective revocation is incompatible with non-repudiation.

Emerging Protocols

In recognition of some of these weaknesses new technical and management protocols and standards are being developed. For example NIST has developed a four level authentication standard that engages one, two and three factor authentication with the use of tokens in association with CAs[2]. This approach provides much greater protection of the critical secret key. Other vulnerabilities such as the reliance on CAs remain. The NIST framework, like the EU, endeavors to set standards on CA processes as well. Progress is slow and take-up even slower, while the sophistication of malicious attacks appears to evolve rapidly.

9. E-Legislation

Within this context many countries now have or are planning e-legislation and regulation which seeks to build and consolidate confidence in the online environment and facilitate e-commerce both at the B2B and B2C levels including:

- B2C low value
- B2B
- B2G
- E-service delivery
- E-publishing

Critical issues may include:

- Requirements for e-transactions
- Privacy protection
- Consumer protection
- Public liability, standards
- Information integrity

[2] The Electronic Authentication Guideline (NIST, September 2004), provides technical guidance to Federal Agencies implementing electronic authentication. The recommendations cover remote authentication of users over open networks. The four levels are:
Level 1: no identity proofing requirement.
Level 2: provides single factor remote network authentication
Level 3: provides multi-factor remote network authentication
Level 4: provides the highest practical remote network authentication assurance.

- Powers of investigation, compliance, monitoring and audit
- Computer crime

These areas are all active areas of development of technical systems, public policy, management protocols and legislation on a worldwide basis often with international cooperation recognizing the cross-border realities of e-commerce and e-services generally.

Of central significance to e-commerce are the requirements for e-transactions and information integrity. Legal developments in these areas have been concerned to ensure that legal uncertainty does not hinder the application of new technology to national and international commerce. In particular the requirements and status of electronic and digital records and documents, signatures, and services such as notarization are fundamental.

In many cases, existing traditional legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written", "signed" or "original" documents.

The purpose here is to emphasize the importance of two legal concepts:

- Digital documents (also known as electronic documents or electronic records)
- Electronic signatures

These concepts form the legal backbone for e-commerce and e-GP development, because they are complementary to traditional laws.

Evolution of E-Commerce Legal Framework

The main objective of Electronic/Digital Signature Legislation has been the removal of obstacles to the use of already enacted legislation to new applications based on electronic transactions.

For that purpose countries have developed specific legislation providing new alternatives to written signatures, based either on the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures, the European Union Directive on Electronic Signatures or the USA E-Sign, or a combination of these.

The purpose of the UNCITRAL Model Laws is to offer national legislators a set of internationally acceptable rules on how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for e-commerce. The principles expressed in the Model Laws are also intended to be of benefit to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce. The Uncitral Model Law on Electronic Commerce may also help to address problems that arise from the fact that inadequate legislation at the national level may create obstacles to international trade, much of which is linked to the use of modern technology. Disparities among, and uncertainty about, national legal regimes governing the use of such communications may contribute to limiting the extent to which businesses may access international markets.

These points are related to the concept of interoperability. The development of e-commerce in a global environment requires interoperability between the parties, between the systems and between the legal frameworks. Harmonization is needed in order to assure an effective e-commerce environment.

Most countries have developed specific legislation on electronic commerce or electronic signatures. The approaches adopted are based on the particular legal system of each country. In those regimes based on common law[3], where regulation is more open, it has often been necessary only to recognize the non-repudiation of an electronic document (also known as electronic record) or an electronic signature (like the USA E-Sign). In other countries with civil law regimes[4], prescriptive types of legislation on electronic signatures or electronic commerce have been established, with emphasis on technical and operational rules and on the formalities of acts, specifically based on digital signatures.

A new legal concept has also been born, the legal recognition of the "CLICKWRAP CONSENT"[5]. Although recently enacted electronic signatures laws have not yet been extensively interpreted by the courts, the validity of such electronic contracts has been firmly established under basic contract law principles. Many courts in the United States have confirmed the "click-wrap agreements" legal validity.[6]

In these cases, the person accepting the goods or services is required to access the terms or conditions before clicking on an acceptance icon. This kind of "legal engineering" is based upon the legal recognition of electronic records (or electronic documents) and of the notion of electronic signatures (when the person uses a password to log on the system, or some other authentication method).

Furthermore, several courts have enforced contracts where email exchanges provide evidence that the parties have reached an agreement to which they intended to be bound.

Various jurisdictions have developed certain rules in order to recognize the legal validity of the electronic transactions, by enacting laws or statutes on electronic commerce, electronic signatures or digital signatures. These rules may be grouped into three categories:

- **Technology Specific laws**. The first laws and statutes were not technologically neutral; they specifically identified technologies, usually digital signatures, to be used in order to have a valid electronic signature. Utah was the first US state to pass such an electronic signature law. Other states subsequently adopted digital signature specific statutes or statutes like those containing presumptions about "secure electronic signatures," that require specific criteria to be met for the

[3] COMMON LAW REGIME The legal tradition of Anglo-American jurisdictions that accumulates legal principles primarily in reaction to actual cases that are used as precedent in future cases, supplemented by statutes.
[4] CIVIL LAW REGIME: The legal tradition of jurisdictions that base fundamental legal principles primarily upon statutory codes such as the Code Napoleon.
[5] In a legal context, the technique of giving approval or consent to an agreement presented online with opportunity to review it, by a mouse-click on a button stating "I Agree" or words to that effect.
[6] For example, electronic software licenses accepted by clicking an "I Accept" button)

signature to be deemed valid. Thus far, only Digital Signatures or signatures using Signature Dynamics technology have been identified as acceptable under such statutes. In Europe, the first Germany law was like this as in Argentina with the Decree for the Federal Public administration.

- **Technology Preferred laws**: Some jurisdictions have adopted laws that appear to be technology neutral, but provide an evidentiary presumption in favour of validity if the parties use specific technologies. Although a specific technology may not always be expressly identified, in order to be eligible for the presumption, the "secure electronic signatures" must meet specified criteria, which only certain technology (typically, digital signatures) may satisfy. The principal example is the Directive 99/93 from the European Union on Electronic Signatures. Also, Latin American laws contemplate legal recognition of the digital documents, electronic signatures and digital signatures, in this last case with a strong presumption associated.[7]

- **Technology Neutral Laws**: A majority of American states with electronic records and signature laws allow any form of electronic signature to be binding so long as the parties have agreed to the use and type of signature and the signing party intended to be bound by the signature. In those states no specific signature technology is given prominence over other technologies. This is the scheme of the American E-SIGN Act that recognizes the legal validity of the electronic record and the electronic signature, without a specific association with any kind of technological tool.

Generally there is a trend towards technology neutral laws as technology continues to evolve rapidly, but almost all the enacted legislation is based in the UNCITRAL Model laws on Electronic Commerce and Electronic Signatures.[8]

---

[7] See the Argentine Law on Digital Signatures Nro. 25.506, the Dominican Law on Electronic Commerce, Electronic Documents and Digital Signatures Nro. 126-02, the Peruvian Law on Digital Signatures Nro. 27269, the Brasilian Provisory Rule Nro. 2200-2, the Chilean Law on Electronic Signatures Nro. 19.979, the Colombian Law on Electronic Commerce and Digital Signatures Nro. 527-1999, the Ecuatorian Law on Electronic Commerce, Electronic Signatures and Data Messages, the Venezuelan Law on Message Data and Electronic Signatures.

[8] The Model Law on Electronic Commerce, adopted in 1996, is intended to facilitate the use of modern means of communications and storage of information, such as electronic data interchange (EDI), electronic mail and telecopy, with or without the use of such support as the Internet. It is based on the establishment of a functional equivalent for paper-based concepts such as "writing", "signature" and "original". By providing standards by which the legal value of electronic messages can be assessed, the Model Law should play a significant role in enhancing the use of paperless communication. In addition to general norms, the Model Law also contains rules for electronic commerce in specific areas, such as carriage of goods. The Model Law on Electronic Signatures, adopted in 2001, is intended to bring additional legal certainty regarding the use of electronic signatures. Building on the flexible principle contained in article 7 of the UNCITRAL Model Law on Electronic Commerce, it establishes a presumption that, where they meet certain criteria of technical reliability, electronic signatures shall be treated as equivalent to hand-written signatures. In establishing that presumption, the Model Law follows a technology-neutral approach and avoids favouring the use of any-specific technical product. In addition, the Model Law establishes basic rules of conduct that may serve as guidelines for assessing possible responsibilities and liabilities that might bind upon the various parties involved in the electronic signature process: the signatory, the relying party and trusted third parties that might intervene in the signature process.

The "Functional-Equivalent" Approach

Efforts to enact laws related to electronic transactions are based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern communication. This problem in national laws can be addressed by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, such as article 7 of the UNCITRAL Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods.

New regulations on electronic commerce and electronic signatures should permit jurisdictions to adapt their existing legislation to developments in communications technology without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, the electronic fulfilment of writing requirements might in some cases necessitate the development of new rules.

The Uncitral Model Law thus relies on a new approach, sometimes referred to as the ”functional equivalent” approach, which is based on an analysis of the purposes and functions of traditional paper-based requirements with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. For example, among the functions served by a paper document are the following:

- to provide that a document would be legible to all;
- to provide that a document would remain unaltered over time;
- to allow for the reproduction of a document so that each party would hold a copy of the same data;
- to allow for the authentication of data by means of a signature; and
- to provide that a document would be in a form acceptable to public authorities and courts.

In general, in respect of all of the above functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and related costs) than in a paper-based environment.

Similarly, and related, are the requirements of a written signature. Article 7 of the UNCITRAL Model Law on Electronic Commerce reads as follows:

> “(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> “(a) a method is used to identify that person and to indicate that person’s approval of the information contained in the data message; and

"(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

"(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

"(3) The provisions of this article do not apply to the following: [...]."

This article 7 is based on the recognition of the functions of a signature in a paper-based environment.

With a view to ensuring that a message that was required to be authenticated should not be denied legal value for the sole reason that it was not authenticated in a manner peculiar to paper documents, article 7 adopts a comprehensive approach. It establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements that may currently present barriers to electronic commerce. Article 7 focuses on the two basic functions of a signature, namely, to identify the author of a document and to confirm that the author approved the content of that document.

Paragraph 1 (a) establishes the principle that, in an electronic environment, the basic legal functions of a signature are performed by way of a method that identifies the originator of a data message and confirms that the originator approved the content of that data message.

Paragraph 1 (b) establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph 1 (a). The method used under paragraph 1 (a) should be as reliable as is appropriate for the purpose for which the data message is generated or communicated, in the light of all the circumstances, including any agreement between the originator and the addressee of the data message.

In determining whether the method used under paragraph 1 is appropriate, legal, technical and commercial factors that may be taken into account include the following:

- the sophistication of the equipment used by each of the parties;
- the nature of their trade activity;
- the frequency at which commercial transactions take place between the parties;
- the kind and size of the transaction;
- the function of signature requirements in a given statutory and regulatory environment;
- the capability of communication systems;
- compliance with authentication procedures set forth by intermediaries;
- the range of authentication procedures made available by any intermediary;
- compliance with trade customs and practice;
- the existence of insurance coverage mechanisms against unauthorized messages;
- the importance and the value of the information contained in the data message;
- the availability of alternative methods of identification and the cost of implementation;

- the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
- any other relevant factor.

The UNCITRAL Model Law on Electronic Signatures, looking forward to the increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures, has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures") Moreover, by establishing with appropriate flexibility a set of basic rules of conduct for the various parties that may become involved in the use of electronic signatures (i.e. signatories, relying parties and third-party certification service providers) the Model Law may assist in shaping more harmonious commercial practices in cyberspace.

The new Model Law on Electronic Signatures equally reflects the principle that no discrimination should be made among the various techniques that may be used to communicate or store information electronically, a principle that is often referred to as "technology neutrality".

The Model Law on Electronic Signatures adds substantially to the UNCITRAL Model Law on Electronic Commerce by adopting an approach under which the legal effectiveness of a given electronic signature technique may be predetermined (or assessed prior to being actually used). The Model Law offers practical standards against which the technical reliability of electronic signatures may be measured. In addition, the Model Law provides a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Model Law is thus intended to foster the understanding of electronic signatures and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions.

The Electronic signature Model Law defines electronic signature as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message. It also defines "certificate", "data message", "signatory", "certification service provider" and "relying party"[9].

This Model Law is thus based on a PKI scheme and is technology-specific despite intentions to the contrary. One of the points that is not solved is the recognition of digital certificates issued by certification authorities from other countries. Most laws

[9] "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;
"Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents;
"Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
"Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;
"Relying party" means a person that may act on the basis of a certificate or an electronic signature.

have some rules on this, but the legal recognition depends on national recognition, thus representing a problem for the e-commerce development between different countries[10].

This Model Law, expressly foresees systems of voluntary accreditation of the providers of certification services before specific regulatory bodies, differentiating the legal effects of digital certificates issued by authorized certifiers and identified with the full legal value of handwritten signature, with respect to the certificates issued by unauthorized certifiers, which do not enjoy the same legal value which the norms assign to the digital signature, but which do not lack all value, because they are considered as an electronic signature.

In such cases, one assigns the same legal effect which is granted to the handwritten signature to the digital signature, also called advanced electronic signature, which is a reliable electronic signature, only when said signatures are generated from digital certificates issued by certification entities authorized by the corresponding regulatory body, foreseen for each norm in particular in comparative law.

Electronic Signatures in Global and National Commerce Act – E-Sign

The E-SIGN objective is to promote the acceptance and use, on an international basis, of electronic signatures, in accordance with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.

The principles that inspire the E-SIGN are the following:

- Removal of paper-based obstacles to electronic transactions by adopting relevant principles from the Model Law on Electronic Commerce adopted in 1996 by the United Nations Commission on International Trade Law.
- Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.

---

[10] Article 12. Recognition of foreign certificates and electronic signatures
1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
(a) To the geographic location where the certificate is issued or the electronic signature created or used; or
(b) To the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.
4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.
5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

- Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.
- Take a non discriminatory approach to electronic signatures and authentication methods from other jurisdictions.

The definitions of "electronic record" and "electronic signature" are very important, because they recognize the legal validity of the electronic transactions. In another sense, these legally admitted concepts establish the requirements for electronic transaction enforceability.

E-SIGN's definition of "electronic record" covers almost any form of electronic communication. Contracts, records and related communications that are transmitted or stored in e-mail, the Internet, diskette, compact disk, or other similar form all fall within the ambit of E-SIGN.

The E-SIGN definition of "electronic signature[11]" is important because it establishes the requirements for making an electronic record enforceable. For the purposes of contract enforcement, the two essential requirements are that an electronic sound, symbol, or process must firstly be "associated with" a contract or other record, and secondly adopted by the signatory with the intent to sign the record. These requirements can be difficult to prove in the transitory world of electronic commerce. It is significant, however, that under E-SIGN any symbol or process can qualify as an electronic signature, as long as it is properly connected with the document and shown to have been made (or later adopted) by a person having the intent to sign.

In this way, E-SIGN adopts an age-old approach from the common law of contracts that any symbol that the sender intends to serve as a signature will suffice, irrespective of the technology used.

A variety of processes can be used to indicate whether the signing party has in fact assented to the electronic message received. Electronic signature processes can range in sophistication from the sending of a simple e-mail to the engagement of encryption technology. The development of the more sophisticated signature processes has been driven by the need to ensure compliance with the two elements of the contracting processes addressed in the E-SIGN electronic signature definition mentioned above
.
The E-SIGN establishes a general rule of validity[12] for electronic transactions, based on the recognition of the legal effect of the signature, contract, or other record made in electronic form.

---

[11] The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

[12] E-SIGN TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE
SEC. 101. GENERAL RULE OF VALIDITY.
(a) IN GENERAL.—Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce—
(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation

European Union Digital Signature Directive 99/93

The purpose of this Directive, enacted on December 13 1999, is to facilitate the use of electronic signatures[13] and to contribute to their legal recognition within the community. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards to their form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

A regulatory framework is not needed for electronic signatures exclusively used within systems which are based on voluntary agreements under private law between specified numbers of participants. The freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law. The legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised.

The European Directive distinguishes between electronic signatures and "advanced electronic signatures", by giving a stronger legal recognition to the latter.

The definition of an advanced electronic signature is an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control; and
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The European Directive gives legal effects of both electronic signatures, by the following rules:

- Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature-creation device:
    - satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
    - are admissible as evidence in legal proceedings.

[13] Definition of Electronic Signature: Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

- Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

    - in electronic form, or
    - not based upon a qualified certificate, or
    - not based upon a qualified certificate issued by an accredited certification-service-provider, or
    - not created by a secure signature-creation device.

The European Directive is, in part, based on a PKI scheme.

Almost all the electronic commerce rules and electronic signature laws admit that:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- If a law requires a record to be in writing, an electronic record or digital document satisfies the law.
- If a law requires a signature, an electronic signature satisfies the law.

The requirement of digital signatures may be appropriate or adequate for those electronic transactions that require special forms, like notarisation.

For others that in a paper based scheme do not require special forms, an electronic signature may be enough to prove the intention of that person to sign the contract.

If a DC is required for all the electronic transactions, this greatly extends the complexity in terms of key management, the digital certificates management (issue, revocation, suspension, CLR administration, time stamping, identification procedures) and most important, represents user un-friendly authentication. These issues are compounded by a lack of mature international standards and a corresponding lack of interoperability. A range of other issues also exist including timing rules- sent vs received, venue and errors in transmission.

10. Notarization

Notarial services are undertaken by notaries. There are two different major types of notaries: common law notaries and Latin notaries. Common law notaries are found mostly in the English speaking world; eg America and the UK. Latin notaries are predominately found in the rest of the world. These definitions and the differences between the two each provides a different service to the requestor. Latin notaries are responsible for the correctness of the notarised data; they may also act as an archivist of the document. Common law notaries authenticate the execution of the document but do not authenticate the accuracy of the data in the notarised document.

The E-SIGN rules about notarisation and acknowledgement contemplate where a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce is to be notarised, acknowledged, verified, or made under oath. It recognises the requirement as satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

This permits a notary public and other authorized officers to act electronically, effectively removing the stamp/seal requirements. However, this does not eliminate any of the other requirements of notarial laws, but simply allows the signing and information to be accomplished in an electronic medium.

For example, a Buyer wishes to send a notarised Real Estate Purchase Agreement to Seller via e-mail. The notary must appear in the room with the Buyer, satisfy him/herself as to the identity of the Buyer, and swear to that identification. All that activity must be reflected as part of the electronic Purchase Agreement and the notary's electronic signature must appear as a part of the electronic real estate purchase contract.

11. E-Government Procurement

With public sector procurement accounting for up to 20% of a national economy the take-up of e-commerce techniques by this activity can be a powerful driver of e-commerce throughout the economy. For public sector procurement to be e-enabled requires not only that it become legally recognised but that it be robust in terms of its business case and risks within the context of multimillion dollar transactions.

Government E-Procurement Regulation

To extend the legal concepts and developments into government and the private sector it is appropriate that the regulations governing public e-commerce seek to:

- facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures;
- eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements;
- simplify, clarify and modernize the rules governing commerce and governmental transactions through the use of electronic means;
- permit the continued expansion of commercial and governmental electronic practices through custom, usage and agreement of the parties;
- promote harmonization of the law among the different states of each country and worldwide relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions;
- promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions; and
- promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.

In relation to facilitating the use of public e-commerce and e- procurement systems, serious consideration should be given to the idea of exploiting existing legal tools: the legal force of the electronic records and electronic signatures. These already have legal force, and only require adequate legal engineering to use them.

Vulnerabilities

The security risks for public sector commerce represent a special case of the foregoing discussion. The management of government business is usually dichotomized in terms of high-value low-volume versus low-value high-volume acquisitions which are managed through quite separate management systems. These two approaches are usually referred to as tendering and purchasing. In the online environment these translate unsurprisingly as e-tendering and e-purchasing.

Typically governments will commence their transition of government commerce into the online environment with e-tendering. This provides a simple, phased approach starting with the advertising of tender opportunities online, through to the downloading of documentation and the uploading of tender submissions.

From the previous discussions the vulnerabilities of e-tendering appear to be:

- Distribution of tender documents
- Distribution of updates & modifications
- Uploading of tender submission
- Government site reliability
- Online tender box security
- Tender withdrawal during 'open time'
- Integrity of record keeping
- Government site security
- Supplier site security and processes

Authentication of the relevant government site is required by bidders who will want strong assurance that there is no likelihood of their bid falling into the hands of a competitor. There appears to be no real imperative for the authentication of bidders which seems to be of more concern to regulators

The highest risk component of this facility would seem to be the uploading of tender submissions for large contracts where the incentive to discover the details of a competitor's bid can be worth many millions of dollars. It is important to appreciate the reality of this – the online lodgment of tenders worth millions of dollars is equivalent to undertaking multimillion dollar transactions across the internet even though there has been no financial transfer. Governments need to recognize that simply having comprehensive e-legislation in place with digital certificates attached to the online tender box may provide little comfort to corporations involved in major bids into which they have invested substantial intellectual property. Further, knowledgeable auditors in many jurisdictions may even qualify a corporation for engaging in this way. There are a number of points of potential manipulation of this facility. There are also a variety of potential motivations for manipulation:

- A security breakdown whereby a competitor discovers another's bid details undetected and before bids close
- A competitor blocks delivery of another's bid with or without a false receipt acknowledgement. Even without a receipt a bidder might not be alarmed because most bids are submitted near the allowed closing time, and delays might mean that a late receipt would seem unexceptional in some jurisdictions. Bidder would need to disprove a negative – denial of service attack
- Bidder submits and blocks delivery of own bid to claim malpractice and gain time
- Bidder submits bids in competitor's name to discredit opposition and force competition into disproving authentication
- Bidder submits multiple bids and disputes authentication
- Bids are received and discovered in insecure system in government.
- Competitor bids are corrupted such that their integrity is rejected at bid opening.

Another constraint relates to the digital certificates distributed to suppliers. With a single e-GP platform in a country it is plausible to exploit the advantages of digital certificates issues by a unique CA. But, then consider where there are several e-GP implementations as well as suppliers from international trading partners, then add other e-government services such as the tax system, digital notification, e-banking, that perhaps also use DCs – integration issues and key administration problems become more complex.

If each system for which authentication is based on PKI would accept any DC issued by any publicly accredited CA this would be an advance. But this does not happen. Usually, those few systems that use PKI for user authentication work only with a single DC, because of software, commercial and management reasons. There are other aspects as well - DCs are expensive methods for authentication.

Government sites and their business rules need to be designed in recognition of all of these issues. It seems that there cannot be simply a carrying over to the internet of business rules used by governments in the paper world but that a re-engineering of parts of the processes of government procurement is necessary.

The use of DCs is an important tool for authentication of the e-GP site or even the system. Suppliers need to be sure that those web sites they connect to belong to the actual contracting authorities. This DC use is available but should not need a PKI scheme for suppliers. In the same way, an e-GP system may admit encrypted tenders facilitated by a DC. The electronic tender box may encrypt the tenders and decrypt at the moment of opening by using a DC. The supplier sends the tender encrypted with the public key of the e-GP system, and the e-GP system officers responsible for opening the tenders decrypts it by using its private key - this use doesn't need a supplier PKI scheme. Similar considerations apply to many other parts of e-government that require e-transactions. For example government taxation departments deal online everyday with taxpayers without requiring taxpayers to have certified digital signatures. Similarly for online banking. This seems incongruous with the expectations of some public sector departments that the online lodgements of tenders should be accompanied by a certified digital signature.

A lesson has been that, in the light of the potential and actual difficulties related to PKI schemes, insistence on the use of DCs in many circumstances may often become an obstacle for the electronic commerce development.

By analysing e-GP applications it is apparent that many of the requirements can be satisfied through other mechanisms of authentication that are not based on PKI - through the concept of a *trustworthy system*.

E-GP implementation can develop around the concept of 'trustworthy system', that means hardware, software, and procedures that:

- . are secure from intrusion and misuse;
- . provide a reasonable level of availability, reliability, and correct operation;
- . are reasonably suited to performing their intended functions; and
- . adhere to generally accepted security principles.

This approach contains the necessary technical qualities to implement an e-GP framework and should be accepted within the legal framework that recognizes the legal validity of electronic documents and electronic signatures. Conversely it is significant that in the absence of a trustworthy system of the above characteristics the veracity of PKI is substantially eroded anyway, while if the above requirements are satisfies then the concept of PKI may often be redundant.

12. Discussion

With the emergence of new means of communication and information transfer, business methods have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies.

These developments have occurred in the face of existing barriers to the legal efficacy of records and documents which exist solely in electronic media. Whether the legal requirement that information or an agreement or contract must be contained or set forth in a pen and paper writing derives from a statute of frauds affecting the enforceability of an agreement, or from a record retention statute that calls for keeping the paper record of a transaction, such legal requirements raise real barriers to the effective use of electronic media.

Countries have developed electronic legal frameworks to assure that electronic records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.

The new rules on electronic commerce try to avoid the old rule obstacles, especially where these require "handwritten signatures", the "written form" and the "original". The principal goal of these new rules is to facilitate electronic commerce, rather than to replace the old civil and commercial laws. These new electronic commerce frameworks are complementary with the traditional laws.

The main features of the new legal electronic frameworks are the removal of such obstacles, and allow the application of civil and commercial laws. In this scenario, the main concepts are the following:

- the legal recognition of electronic records / digital documents
- the legal recognition of electronic signatures

Both are the essential backbone of the electronic legal framework. The validity of electronic records, or digital documents, allows the legal engineering that is needed in the systems applications. It refers to the concept of an "original" document, and the recognition of the "written form". Almost all the electronic laws recognize that an electronic record or digital document is as valid as a paper document, and that it satisfies the requirement of written form, also that an electronic record or a digital document may be considered as originals, in fact, that their copies are originals too.

The time required to approve a new law is long, the processes are difficult, and so it is preferable that rules are technologically neutral, to accommodate the pace of change of technology.

E-commerce rules establish, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. Therefore the term "signature" has been used to connote and convey that equivalency. The purpose is to overcome unwarranted biases against electronic methods of signing and authenticating records.

There is a wide range of alternatives signatures, between a simple email, the use of PGP technology, the use of passwords based on symmetric cryptography, up to the use of public key technology, with digital certificates issued by a non licensed certification authority. A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere inclusion of one's name as a part of an e-mail message - so long as in each case the signer executed or adopted the symbol with the intent to sign.

These issues and responses in the legal environment are complemented by the issues around business risk and security and together define the requirements of authentication as was shown in Figure 1. From a risk perspective there has in some sense been underlying anthropic assumptions about technological capabilities in the e-commerce environment. Thus in defining the security requirements of B2B commerce there has been a presumption that they, and therefore trust, can be delivered technologically. If it were assumed instead that these attributes of trust can not be delivered in this way then it is likely that these would not have been defined as essential requirements. Instead other processes would be developed to make good the implied deficiencies. To ensure that other solutions are able to emerge it is important therefore that e-legislation does not lock in just one option that may have only limited application and that has vulnerabilities of its own.

Much of the discussion around authentication has been lead by technologists or lawyers and the lawyers have begun to converge on a robust and meaningful legal approach to this matter. However the understanding of risk has yet to mature and is unlikely to do so until management itself becomes conversant with this issue given that much of any

risk equation of authentication is off-line and has little to do with either the law or technology.

E-commerce represents a fundamental departure from the traditional trust environment in that firstly parties are now expected to trust the process itself and secondly they are expected to derive this trust from a single channel of information where previously there were multiple channels. This reality delivers only a weak capacity to develop commercial trust and magnifies potential risk.

Internet open systems have differed from the closed EDI establishment in that the former have substantially lacked a well defined structure of accountability. The lack of accountability equates to a lack of acceptable risk management, without which confidence will be difficult to build. Much work has been undertaken in an attempt to build technical systems in lieu of this accountability. The focus of authentication has followed this paradigm shift.

No authentication process is both practical and foolproof. Accordingly no transaction should, from a risk perspective, either require or presume that it be so, nor can non-repudiation be completely achieved and accountability assured via this technical arrangement.

Risks cannot be managed, even in principle, in the absence of information about the nature of the transaction and therefore accountabilities cannot be assigned and confidence cannot be built. There is therefore unlikely to be a generic solution applicable to e-commerce generally. Solutions need to be developed for specific applications, such as low value retail sales, versus confidential document transmission through to high value contractual commitments. Part of this landscape is public procurement or B2G.

It is often presumed that in order for parties to have confidence in an online transaction they may need assurances about the identity of the other party (an individual or organization), the authority of the other party to undertake the transaction and possibly some sort of accreditation of the reliability and standing of the other party, as well as assurances about the integrity and security of the processes conveying this information. These encompass formal, casual and transactional relationships. Authentication is the process of providing assurance about these relationships and associated claims, for which there is no single solution and flexibility and customization are key.

13. Short Bibliography

Burr-Donna, W. E., Dodson, E., Polk, W. T.. "**Electronic Authentication Guideline"**. Recommendations of the National Institute of Standards and Technology. September 2004.

Clarke, R. **Authentication: A Sufficiently Rich Model to Enable E-Business**. http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html

Clarke, R. **The Reinvention of Public Key Infrastructure** http://www.anu.edu.au/people/Roger.Clarke/EC/PKIReinv.html

Committee on Government Reform, House of Representatives. **"Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology",** Report to the Chairman, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, February 2001.

Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy, **"Summary of responses to the survey of legal and policy frameworks for electronic authentication services and e-signatures in OECD member countries"**, July 2004. www.oecd.org/sti/security-privacy

Dumortier, Jos et al, **"The Legal and Market Aspects on Electronic Signatures",** Study for the European Commission, DG Information Society, Interdisciplinary Centre for Law and Information Technology, October 2003.

Graff, J.C. **Cryptography and E-Commerce**. Wiley, 2001.

Gutmann, P "**How to build an X.509 PKI that works",** University of Auckland, June 2004.

Gutmann, P. "**Secure Internet-based Electronic Commerce: The View from Outside the US",** Department of Computer Science, University of Auckland, 1998

Information Security Committee Electronic Commerce Division, Section of Science & Technology Law, American Bar Association, **"PKI Assessment Guidelines",** Guidelines to help assess and facilitate interoperable trustworthy public key infrastructures, PAG v0.30 Public Draft for Comment, June 2001.

June Leung., Amir Jafri**. "PKI Deployment – Business Issues",** FundServ Inc., Febrero 2003

Mitnick, K.D. **The Art of Deception: Controlling the Human Element of Security**. Wiley 2003.

Netscape **Introduction to Public Key Cryptography** http://developer.netscape.com/docs/manuals/security/pkin/contents.htm

NIST Computer Security Division http://csrc.ncsl.nist.gov/

OASIS **"PKI Action Plan",** Prepared and Published by the OASIS Public Key Infrastructure (PKI) Technical Committee (TC), February 22, 2004 Version: 1.0

OMB **"Guidance on Implementing the Electronic Signatures in Global and National Commerce Act (E-Sign)",** developed with assistance from the Departments of Commerce, Justice, and Treasury. September 2000.

Rivolta, M "**Electronic Government Procurement – Lessons Learned"** Proceedings of the Electronic Government Procurement Conference, Manila, Asian Development Bank, Inter-American Development Bank, World Bank., Oct 2004

Rivolta, M. Rivolta, M and Prandini, P, "**Argentine Public Key Infrastructure Development – a comparative study of PKI experiences in Latin America",** April 2002, Internet Society.

Rivolta, M and Prandini, P, Jorge Marta, Walter, **"Comercio Electrónico y Firmas Digitales - Análisis de la Legislación actual y Mejores Prácticas Internacionales",** Diciembre 06, 2002, INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)

Samelson, A. and Bedwell-Coll, A. "**Electronic Signature Statutes "E-Signature Trends for 2003 - Legal Trends"",** subsection contributed by for conference paper titled, "Hey! Where did the good ole `dotted line' go?" Prepared for the National E-Commerce Coordinating Council conference, December 2002.

Schapper, P. R. "**Authentication: The Art of Discovering Whether Appearances are True or False"** Proceedings of the Electronic Government Procurement Conference, Manila, Asian Development Bank, Inter-American Development Bank, World Bank., Oct 2004

Schneier, B. **Applied Cryptography**. Wiley, 1996.

Smedinghoff, T. J. "**The Legal requirements for Creating Secure and Enforceable Electronic Signatures**" smedinghoff@bakernet.com 2002.

United States General Accounting Office. **"Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology"**. February 2001.