USA

An introduction to digital signatures

by Edward Cheng

With its wealth of electronic information, the Global Information Infrastructure (GII) has the potential to improve services, create new markets and increase overall efficiency. Using the GII, doctors can share opinions and information with medical professionals across the country, enhancing the care that they provide. Some government agencies now accept applications and contract bids in electronic form, reducing needless mountains of paperwork (as an example, the application for the US National Science Foundation scholarship is almost completely on-line). Industry even speculates about widespread electronic commerce in which the public will make transactional purchases on-line. However, all of these promising developments will require the electronic equivalent of a signature that performs two primary functions (in addition to confidentiality, requiring cryptographic solutions).

- *Authenticating the identity of the message sender.* Like conventional signatures, electronic ones must prove identity. For example, doctors in New York receiving advice from specialists in London need to verify that their colleagues (and not some hacker) sent the message.
- *Ensuring the integrity of the message.* Paper documents are somewhat difficult to alter because of their physical embodiment. In contrast, digital information can be changed without evidence of tampering, making integrity verification critical. For example, stockbrokers need to ensure that transaction orders are neither altered not damaged in transit, since $1,000 can easily become $10,000.

BACKGROUND READING

For background information on the operation of digital signatures, reader should consult the works of Daniel Greenwood, Wyrough, Bradford Biddle, A Michael Froomkin or any basic cryptography primer.

ESTABLISHING A LEGAL FRAMEWORK

Fortunately, digital signatures using public-key cryptography techniques can achieve the two requirements above. From a technical standpoint, digital signatures can prevent a person from falsely claiming that they never sent the message or that the message was altered, a quality called non-repudiation (Charles Merrill, 'An Attorney's Roadmap to the Digital Signature Guidelines' *Electronic Banking and Law Report,* September 1996, p. 13). However, technical non-repudiation does not automatically translate into legal non-repudiation. If a person uses a digital signature to sign an electronic agreement, it is not necessarily legally binding or enforceable. The law must first recognise the validity of digital signatures, and then it must provide a framework defining the relationships among the various parties (signer, recipient, third parties, etc.). A legal framework will allow judicial systems to uniformly and appropriately attribute liability and accountability.

LEGISLATE EXPEDIENTLY BUT CAUTIOUSLY

Industry and the public will be reluctant to develop electronic commerce under a cloud of legal certainty. Without a proper legal framework, parties will be exposed to unknown and potentially undesirable risks, discouraging their participation. For example, if a hacker forges a person's digital signature, to that extent they are liable (A Michael Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce', *Oregon Law Review* 49, 1996). Governments should act swiftly to create the policies and laws required by digital signatures. Case law should play a role, but its development is typically inconsistent, expensive and slow, providing little solace to parties wishing to assess their risk and liability. As a minimum, legislators should develop basic principles to direct and channel the judiciary, who will then flesh out the specifics.

However, as expressed by the UK's Department of Trade and Industry:

'These are complex issues and cannot be rushed. Such changes [in law] will help to underpin secure electronic commerce for a long time to come. We cannot afford to get it wrong.' (Ian Taylor, *Licensing of Trusted Third Parties for the Provision of Encryption Services,* http://www.steptoe.com/ukpub.htm).

Digital signatures are still an emerging technology and have not yet found widespread use. Thus, governments still have time to form task forces, issue draft legislation, hear testimony and carefully deliberate policy. However, ultimately, they should solidify the digital signature law through legislation, reassuring industry and promoting electronic commerce.

RECENT INITIATIVES

A number of US states, including Utah, California, Florida, Georgia and Massachusetts, have passed or are currently considering digital signature legislation 'to facilitate commerce by means of reliable electronic messages' (The Utah Digital Signature Act, cited by C Bradford Biddle, 'Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key infrastructure', *San Diego Law Review* 33, November 1966). However in cyberspace these nuances are unacceptable. Policymakers cannot reasonably expect consumers to track their relevant jurisdiction on the Web and then determine the applicable laws. Even if GII users tried jurisdiction in cyberspace is often ambiguous and undefined. Consequently, businesses and their customers will grow frustrated worrying about potential but unknown laws, obligations and liabilities.

CO-ORDINATED EFFORTS

Whether through the UN, World Trade Organization (WTO) or some other international body, governments should attempt to adopt uniform digital signature laws uniformly, as required by electronic commerce. This organization should review two avenues for co-ordinating digital signature legislation:

(i) endorsing an existing national, US state or model law and

promoting its enactment throughout the world.

(ii) write a new model law through compromise and negotiations. This new law should be acceptable to and enacted by most, if not all, nations.

TECHNOLOGY NEUTRAL v TECHNOLOGY SPECIFIC

A substantive question for any new law is its breadth. Broad laws tend to be vague, lacking emphasis and impact. Specific laws, particularly regarding technology, can quickly become obsolete, thereby hindering innovation, rather than promoting it. Accordingly, recent initiatives on digital signatures fall into two schools of thought: technology neutral and technology specific. Technology neutral legislation is broader and does not specify any particular method, technology, or level of security. It focuses on legally recognizing a broad class of 'electronic signatures', which encompass:

'... any symbol or method executed or adopted by a party with present intention to be bound by or to authenticate record, accomplished by electronic means.' (Daniel Greenwood, *Electronic Signatures and Records: Legal, Policy and Technical Considerations,* 9 January 1997, http://www.magnet.state.ma.us/ltd/legal/e-sig.htm).

Under this definition, even a name typed at the end of an e-mail qualifies as an electronic signature; only the intent of authentication is important. For example, the California law references:

'... an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature. This definition does not include encryption.' (William E Wyrough Jr and Ron Klein, 'The Electronic Signature Act of 1996: Breaking Down Barriers to Widespread Electronic Commerce in Florida, *Florida State University Law Review,* 1977, s. IVD3b)

Unfortunately, while broad 'electronic signature' legislation leaves flexibility for future innovation, it typically lacks any meaningful depth. Without a specific technology to reference, legislators experience great difficulty attributing any significant legal properties beyond simple recognition.

In contrast, technology specific laws exclusively promote digital signatures, the small subset of electronic signatures that utilizes cryptography to authenticate and verify messages. For example, Utah not only recognises their validity, but also develops a legal and regulatory framework specifically for public-key cryptography. However, with technology specific legislation, policymakers run the risk of prematurely supporting a technology before the market has declared a winner (American Bar Association, *Legislative and Regulatory Law and Policy Issues,* http://www.magnet.state.ma.us/ltd/legal/policy.htm). Some electronic signature solutions do not require public-key cryptography. For instance, the PenOp system transforms a handwritten signature into a secure electronic signature through handwriting analysis and mathematical functions (Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures,* http://www.efga.org/digsig/penop03.txt). The handwriting analysis algorithm in PenOp is proprietary and secret, which may lead to questions of its security if it was fully implemented. Unlike technology neutral laws, technology specific legislation will discourage use of these promising technologies.

Nevertheless, technology specific legislation is less vague and can actively promote electronic commerce by establishing needed infrastructure. It comforts industry and the public by removing uncertainty and defining potential liabilities. Furthermore, digital signatures are rapidly gaining acceptance, and no other signature system appears poised to challenge it. A few private 'certification authorities,' integral parts of a digital signature system, have already begun operation, suggesting an immediate need for a legislative and legal framework.

GENERAL LEGALITY FOR ELECTRONIC SIGNATURES

At present, digital signatures are the most developed and promising of the available signature technologies. Therefore, governments should not fear the implementation of technology specific legislation that develops digital signature-related infrastructures, including certification authorities (discussed below). However, legislation should not explicitly lock out other potential technologies. Policymakers should solidify general legal recognition for other forms of electronic signature, so the market can continue to assess their promise. This compromise will hopefully achieve the necessary balance to maintain flexibility (technology neutral) while facilitating the promising technology of digital signatures (technology specific).

CERTIFICATION AUTHORITIES

A digital signature cryptographically binds a private/public-key pair to an electronic document. With a signature, the recipient or relying party (Bob) can verify that the message was not altered and that a specific key pair was used to create it. However, by himself, Bob cannot authenticate; he cannot take the next step and link the key pair to the sender or subscriber (Alice). The verification process 'does not yet say anything about who actually signed the message' (Charles Merrill, *Roadmap*, p. 14) let alone who is legally bound by the message. For example, the whole package could have originated from a hacker (Oscar). Additionally, since Alice is not yet *legally* bound to the key pair, she may have no legal accountability,

Certification Authorities (CAs) solve this problem by checking a person's identity, registering the public key, and issuing a validation certificate. A CA binds the key to Alice who is then accountable for her subsequent signatures. Thus, after receiving a signed message, Bob can use a CA's service to authenticate it. Obviously, CAs perform a very critical role in the digital signature regime; if Alice's key is ever compromised, she needs the CA to revoke her key, invalidating all signatures after that date. Otherwise, Oscar can masquerade as Alice, enter into agreements, and perform unauthorized transactions. Similarly, Bob relies on the CA to keep an up-to-date listing of valid and revoked public keys. If a valid key is not listed, Bob may wrongfully refuse to sell goods to Alice, losing business and annoying his customer. If a compromised key remains valid, Oscar can defraud Bob and many other people.

With so many parties relying on CAs for accurate information, governments might want to regulate and license them in the public's interest. The Utah Digital Signature Act provides an illustrative example of a voluntary licensing framework, which defines certain minimal qualifications for CAs. These requirements include:

- verifying a number of minimum conditions regarding the key and keyholder (Alice) before issuing an authentication certificate;

- operating a 'trustworthy' computer system that is 'reasonably secure from intrusion and misuse; [and] provide[s] a reasonable level of availability, reliability, and correct operation' (Biddle, above, at p. 15);
- posting a financial guaranty consistent with the 'financial responsibility it provides to persons who rely on certificates,' (Utah Digital Signature Act, cited in Biddle, above at p. 14) covering any liability claims against the CA;
- having employees with appropriate training, and maintaining specified record-keeping and auditing procedures.

This licensing framework adds legitimacy to CAs and facilitates widespread use of digital signatures. First, maintaining minimal operation standards inspire greater public confidence and willingness to use digital signatures, Without licensing, the public has no measure of a CA's trustworthiness, and can only rely on reputation. The guarantee is equally important. It ensures that CAs have the financial resources to compensate victims of negligence; CAs cannot simply declare bankruptcy and disappear. Second, licensing forces the CAs to develop reasonable levels of security, including 'secure means for controlling usage of its private key' (Utah Code s. 46–3–201(1), cited in Biddle, above at p. 15). The CA uses its own private key to certify the keys of others. Thus, its compromise can lead to rampant fraud and mischief. Furthermore:

'... because the rewards from successfully obtaining a CA's private key could be great, criminals will likely expend considerable resources trying to obtain the private keys of CAs.' (Biddle, above at p. 59).

Although liability legislation (see below) will also encourage CAs to be extremely cautious with their keys, the minimum licensing standards are a step in the right direction.

VOLUNTARY CA LICENSING?

Unfortunately, the licensing of CAs has one inherent drawback: further regulation and interference with business. Conceivably, governmental involvement is unnecessary. The competitive market may demand that reputable CAs hold a guarantee, utilize high levels of security, and abide by certain identity verification principles and operating practices. Worse yet, regulation may hamper better service practices due to a 'regression to the mean'. Licensing standards represent minimal or, at best, mediocre requirements. CAs have little incentive to go beyond these quality control standards since the public tends to treat all licensed parties equally. Consequently security levels will stagnate. In contrast, a non-licensed, competitive environment may encourage CAs to constantly strive for high standards in the attempt to gain credibility and customers.

Even though it creates more regulation and government costs, CA licensing serves worthy public interest goals by bolstering initial consumer confidence, ensuring basic security, and facilitating a digital signature infrastructure. A well-accepted CA licensing framework will promote electronic commerce, thereby improving productivity and the economy. Besides, the boom may create additional tax revenue that will offset operating costs, and any residual costs can he recovered through fees for licensing, inspection, and maintenance.

However, licensing should remain strictly voluntary. While CAs will naturally gravitate toward government licensing requirements (to bolster confidence), other industry standards may emerge. In the spirit of a free enterprise system, the government should allow the public to decide which standard or licensing scheme to follow. A note of caution to policymakers: the licensing framework may create liability problems for the government. By approving a CA, the government implicitly guarantees a level of soundness and quality, If the licensed CA goes bankrupt as a result of a liability suit (see below), the courts may hold the CA regulatory agency partially liable for unrecoverable damages. Legislation should address this problem, and establish a government bail-out/insurance fund for CAs, similar to the bank depositors' insurance, if necessary.

CAs AND CONSUMERS

CAs will give digital signatures legal enforceability. Bob will have confidence in the legal non-repudiation of Alice's signature, and will accept it for electronic transactions. Under normal circumstances, both parties will agree to the transaction and everyone is happy. But what happens if Alice's (or worse yet, a CAs) private key is compromised, and hackers commit fraud before the CA can revoke the key? Money is lost and damage is done. Who will the law hold liable? This section looks at liability with respect to CAs and consumers in a digital signature regime.

CA LIABILITY

A CA potentially acquires heavy liability risks because it guarantees the authenticity of the signatures. For example, a CA faces the following problems.

(i) If a CA fails to verify identity properly, the law might not legally bind Alice to signatures made with her key. Even worse, some criminal might fraudulently link his key to Alice's name. Depending on the situation, parties will sue the CA for the resulting damages.

(ii) A CA may fail to promptly revoke Alice's compromised key, allowing a hacker to again make fraudulent transactions. Since Alice has already reported the compromise, most of the liability now falls on the CA.

(iii) Disaster scenario: hackers compromise the CA's own private key, and commit widespread fraud, In addition, new certificates must be reissued to all subscribers, and the public may lose confidence in the digital signature system.

These prospects of nearly unlimited legal liability present a serious 'barrier to entry' for new CAs. The ambiguity of the law furthers the problem: what exactly is a reasonable measure for verifying identity? Even one mistake regarding a subscriber's key can result in lawsuits from multiple parties.

In the absence of definitive legislation, newly formed CAs protect themselves through disclaimers and limited liability agreements. For example, Verisign, an US-based CA, defines three classes of authentication with increasing levels of confidence, as shown below.

Class level	Liability cap	Principal method of verifying identity*
1	$100	e-mail address
2	$5,000	as above plus: driver's licence, postal residence check
3	$100,000	as above plus: notarized

*Verisign requires other information, including name, address, phone numbers, public key, etc.

By creating the above classes, Verisign allows users to choose a desired security (authentication) level and liability limit. A

general disclaimer protects the CA further in the Verisign Certification Practice Statement (see 'internet' box below):

'Except as expressly provided in the foregoing (CPS s. 11.1), issuing authorities and Verisign disclaim all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and ***any warranty of the accuracy of information provided, and further disclaim any and all liability for negligence and lack of reasonable care****.'* [emphasis added]

The courts have not yet upheld the legality of this disclaimer, but it immediately illustrates a major problem. As long as the law fails to peg a CAs liability, CAs will attempt to reduce it to a minimum (A Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, *Oregon Law Review* 49, 1996, at p. 27). Under the above conditions, the CA accepts no liability for the accuracy of its certificates, leaving the certificates without solid backing (Froomkin, at p. 27). Consequently, the only comfort to relying parties is the CAs operational reputation, and an unsuspecting public is left liable for the negligent acts of the CA (since it has no liability). Policy must encourage or force CAs to take greater responsibility,

The Utah licensing framework attempts to inspire responsible behaviour by offering 'safe harbour' to licensed and regulation-abiding CAs. Under the Utah Act, if a CA complies with well-delineated and stringent requirements regarding accuracy, identity verification, etc., then it has limited liability for forged or false signatures (Biddle, above, p. 21, 45). Even if a CA fails to properly validate a person's identity, the liability is limited to the amount specified on the certificate, *but only if the CA is licensed* (Biddle, above, p. 21, 45). Thus, CAs wishing to eliminate or limit their liability, will seek licensing and acquiesce to all the rigorous verification requirements.

However, in the long run, Utah's 'safe harbors' method is detrimental to digital signatures, if the government caps the liability of CAs and holds them unaccountable beyond certain requirements, CAs will lack incentive to research and develop improved security technologies. Only a persistent threat of lawsuits will goad them into promptly making improvements. For example, if the courts severely penalize CAs for negligent identification methods, they will surely find new ways to guarantee that their validation methods are near perfect. The argument applies similarly to the protection of CA private keys. In addition, the Utah scheme contradicts the goals of consumer protection. If the law ascribes no liability to the CA, then the two transactional parties (Alice and Bob) must absorb and compensate for the damage and fraud caused by criminals. Consumers or small businesses will bear the brunt of the liability. This arrangement is unfair, because in many instances the CA is just as culpable (or innocent) as the other parties.

CONSUMER LIABILITY

Just as a CA can lose control of its private key Alice can also unknowingly compromise her private key. Oscar then creates havoc by impersonating Alice, signing phoney contracts, defrauding Bob, and conducting unauthorized transactions (e.g. draining Alice's bank account). However, since Alice did not actually enter into these agreements, is she really liable?

The Utah Digital Signature Act answers 'yes.' Contradicting traditional signature law, which places the burden of proving a valid signature on the claimant (Bob), Utah introduces a new presumption clause:

'Utah Act s.46–3–401 provides that a document signed with a digital signature is normally presumed to be signed by the person owning the relevant private key (so long as their public key is certified by a licensed CA).' (Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures,* http://www.efga.org/digsig/penop03.txt, at p. 4)

Essentially, beyond checking the CAs repository, Bob no longer worries about the validity or authenticity of a digital signature. The law automatically presumes that Alice created it. If a dispute ever goes to litigation, the onus is on Alice to prove that she did not sign the document. The advantage of this particular scheme is that Alice has a strong incentive to protect and track her private key. She will keep it secure and immediately report compromises, because the law is likely to hold her liable for all unauthorized agreements and charges. The statute arguably encourages consumer responsibility and reduces fraud.

However, this 'incentive' also strongly discourages Alice from using digital signatures at all. The general public is already uncomfortable with computers because of errors, glitches, and system crashes. Now, if consumers lose or compromise their private keys, they have unlimited liability. Worse still, the compromise in most cases will be difficult to detect and not due to their own fault or negligence. Focusing on the keys, criminals will trick people into revealing them, develop viruses to steal them, and crack the underlying software or cryptography. Since digital signatures today are not yet fundamental to business, consumers still have a choice. Under Utah's nearly unlimited liability regime, most people will simply refuse to participate, hindering the growth of electronic commerce.

The Utah law also destroys Bob's incentive to verify Alice's signature. Traditionally, when the onus was on Bob, he would use phone calls, the postal service, and other methods to further authenticate Alice's statement or contract. These additional checks protected both Bob and Alice from the risk of an impostor. Unfortunately, since Bob only needs to check the repository to assure a legal signature, the Utah law removes this incentive to doubly verify (Wright, above at p. 4).

THE ELECTRONIC FUNDS TRANSFER ACT 1995

An alternative liability regime is found in the familiar realm of credit cards (thanks to Biddle for drawing parallels between digital signatures and credit cards). The US Electronic Funds Transfer Act of 1995 (EFTA) limits consumer liability for unauthorised activities to $50. It is the essence of consumer protection attributing almost all liability to the credit card company, This scheme has worked well because credit card companies can absorb the costs of fraud and then redistribute them among all users. Thus an unlucky victim is not bankrupted by a stolen credit card. Unfortunately, however, EFTA's main drawback is moral hazard. Since their liability is limited to only $50, credit card users lack incentive to protect

on the internet

http://www.verisign.dot.com/repository/CPS/intro.html

Further details can be found within the Verisign Certification Practice Statement of 22 August 1996.

and secure their cards, resulting in rampant credit card fraud (Charles Merrill, McCarter & English, meeting with Edward Cheng, 9 May 1997).

In many ways, digital signatures are analogous to credit cards. Alice and Bob are similar to the customer and vendor. Alice's private key is like a credit card number, representing Alice's agreement to a contract or purchase. Furthermore, a CA is similar to a credit card company, which is centrally positioned to redistribute the costs and consequences of fraud among all its customers. However, before developing a liability framework for digital signatures based on credit cards, governments should consider a few discrepancies.

Unlike credit card companies, CAs are not monetary middlemen. They do not receive a percentage commission for each sale, and do not profit from high credit card interest rates. In addition, signatures are often used for non-commercial messages, such as letters, agreements, etc.

A credit card company's liability for each transaction is limited to the stated price of the merchandise or service. The liability incurred by a CA from a digitally signed contract is difficult to assess, unpredictable, and may involve incidental and indirect damages.

A credit card transaction is inherently insecure because customers must transfer their numbers to a store clerk or operator, In contrast, digital signatures can be kept completely private and should never be revealed.

REPLACE THE UTAH LIABILITY LAWS?

The Utah legislation places too heavy a burden on the consumer/subscriber while effectively removing liability from the CAs. Consumers do not have to use digital signatures; if ascribed too much liability, they will not. The Utah legislation also destroys incentives for the CAs to increase security and contradicts accepted consumer protection ideals. Thus, while Utah represents an admirable attempt to attribute liability for digital signatures, new model legislation should consider a framework based on the Electronic Funds Transfer Act instead. This liability framework is roughly delineated below.

- *Legislation should cap subscriber or consumer liability for fraudulent signatures at a high, but not unreasonable value (e.g., $500).*

  Lacking consumer protection, unlimited liability frameworks only heighten public fears about computers and drive consumers away from electronic commerce. Legislation should therefore cap consumer liability. However, in the case of digital signatures, the cap should be placed at a higher level (e.g. $500, or somehow related to the liability guaranty of the signature). The higher cap will encourage consumers to protect their private keys and diminish fraud that plagues the credit card industry. This expectation is justified because, unlike credit card numbers, digital signatures never need to be revealed to others. However, the consumer cap should remain low enough so that CAs, who have secondary liability (see below), will still have an incentive to actively monitor and prevent fraud.

- *All digital signature certificates must have a maximum liability value. If a CA exercises reasonable care in issuing its certificates, it is only liable up to this maximum value (minus the amount liable from the consumer detailed above).*

  Like Verisign, governments should require licensed CAs to limit a certificate's maximum liability. If a CA abides by the security and identity verification requirements consistent with the liability level, then the CA's liability is capped for the case of fraudulent or false signatures. However, the cap exists only if the CA responsibly fulfils its duty. If a court finds the CA to be negligent the cap is not applicable.

  The security requirements for each liability level should be determined loosely by a regulatory body and more specifically by the courts. The legislature should not micromanage such details that must constantly change with technology. This recommendation is notably different from the Utah statute. Utah ascribes no liability if a licensed CA fulfils its requirements and caps penalties due to negligence. This proposed policy give CAs limited liability if it fulfils requirements, but no 'safe harbor' for negligent CAs.

- *For each digital signature verified at its repository, a CA should charge a commission consistent with the liability level.*

  Although legislation will not explicitly state this recommendation, the above liability framework implies its development. Since the law will hold a CA liable for fraudulent acts committed with its certificates, CAs must ultimately charge their customers a premium for the insurance service they provide. Each time a signature is verified at a repository, the CA should charge the relying party an appropriate fee related to the liability coverage offered by the certificate. Naturally, the relying party can pass the fee on to the subscriber/consumer by incorporating it into a product's price.

ELECTRONIC FUNDS TRANSFER ACT

Interestingly, Biddle suggests (at p. 34) that the EFTA, as a federal law, may override and pre-empt the Utah legislation with respect to credit cards and money transfers. However, this paper will use the EFTA as a model for a digital signature liability regime and will not concern itself with the possible jurisidictional implications of the Utah Act.

Certificates used for every day communications may have no liability coverage. In that case, the CA may offer its verification services for free. However, certificates guaranteed to $10,000 may have a verification fee of a few dollars (fractions of a percent). Essentially, the CA becomes an insurance company against digital signature fraud. It plays the law of averages and matches fees with the probability of fraud. These premiums will allow a licensed CA to compensate for the damage caused by hackers who compromise the keys of subscribers or who otherwise trick the CA.

CONCLUSION

Digital signatures are a promising technology that can facilitate the growth of electronic commerce on the GII. However, before they can have commercial significance, national governments must establish a unified, suitable legal framework. Only then will digital signatures have the legal enforceability and non-repudiation necessary to make them effective and widely used. Several initiatives have been taken by international organizations, US states, and the ABA to develop model laws or guidelines for digital signatures, In examining these initiatives, particularly the Utah Digital Signature Act, which has become a well-respected model law for other states, this paper makes four principal recommendations.

(i) Governments, through some international body, should expediently co-ordinate legislative efforts to ensure uniformity.

(ii) Although legislation should specifically address digital signatures, it should also recognize general forms of electronic signature.

(iii) Governments should establish voluntary Certification Authority licensing.

(iv) Policymakers should attempt to establish a digital signature framework similar to the US Electronic Funds Transfer Act of 1995.

With time and the prudent implementation of a legal framework, the use of digital signatures will expand, increasing efficiency, ensuring integrity, and reducing paperwork. Ultimately, they will attain their position as the backbone of electronic commerce, the future of the world economy.

Edward K Cheng
MSc Candidate, Fulbright Scholar
Department of Information Systems, London School of Economics

Hong Kong

After the change of sovereignty

by Peter Willoughby

Peter Willoughby

On 1 July 1997 the People's Republic of China (PRC) resumed sovereignty over Hong Kong. From this date, Hong Kong became known as the Hong Kong Special Administrative Region (HKSAR) of the People's Republic of China.

THE BASIC LAW

The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China (the 'Basic Law') was adopted by the National People's Congress of the People's Republic of China on 4 April 1990. It took effect on 1 July 1997. The Government of the HKSAR is required to administer the HKSAR in accordance with the provisions of the Basic Law. In this way, the Basic Law has become Hong Kong's constitution.

The Basic Law provides that only the National People's Congress of the People's Republic of China has power to amend the Basic Law. Further, only the Standing Committee of the National People's Congress of the People's Republic of China has power to interpret it.

Six items of PRC legislation (in addition to the Basic Law) also apply in Hong Kong. This legislation covers the PRC's national capital, calendar, national anthem, national emblem, national flag, national day, nationality law, territorial sea and diplomatic privileges and immunities.

SOCIALISM/CAPITALISM

The Basic Law embodies the principle of 'one country, two systems'. This principle has been closely linked to Deng Xiaoping, the late paramount leader of the PRC. This expression means that the socialist system and policies of the PRC will not be practised in Hong Kong. Instead the capitalist system is to continue. Under the Basic Law, Hong Kong is to 'exercise a high degree of autonomy' and, subject to certain limitations, be self-governing for a period of 50 years following the hand-over. The Basic Law also specifically provides that Hong Kong's capitalist system and way of life will remain unchanged for 50 years (i.e. until 30 June, 2047).

JOINT DECLARATION

On 19 December 1984, the PRC and British Governments signed the Joint Declaration on the Question of Hong Kong, in which the two Governments agreed that the PRC Government would resume sovereignty over Hong Kong on 1 July 1997. At the same time, the PRC Government agreed to the principle of 'one country two systems', in relation to its administration of the HKSAR for the first 50 years of its existence.

CENTRAL PEOPLE'S GOVERNMENT

Hong Kong law continues to be made and administered by the HKSAR. However, under the Basic Law, the Central People's Government (the CPG) will be responsible for the HKSAR's foreign affairs and defence. The CPG's approval is therefore required for access to Hong Kong by foreign warships and foreign state aircraft; some foreign warships have visited the HKSAR since the hand-over. PRC military forces are be stationed in Hong Kong. Nevertheless, responsibility for the day-to-day maintenance of law and order in the HKSAR will continue to lie with the Hong Kong police force.

PROTECTION AFFORDED BY THE BASIC LAW

The Basic Law includes the following protections applicable following the hand-over.

- Hong Kong will continue to enact its own laws relating to taxes and tax rates and the PRC will have no right to tax Hong Kong citizens.
- The policy of no foreign exchange controls in Hong Kong will continue and the Hong Kong dollar will continue to be freely convertible.
- The ownership of enterprises and investment from outside Hong Kong will be protected by law.
- Hong Kong will continue to have an Independent Commission against Corruption accountable directly to the Chief Executive of the HKSAR.
- The free movement of goods and capital into and out of Hong Kong will continue.
- Hong Kong will continue to pursue a free trade policy.
- Hong Kong's revenues will be used exclusively for the purposes of the HKSAR and will not be handed over to the CPG.