

Digital signatures: Debate goes on

Reproduced from Global Perspectives — Risk e-Business by Deloitte Touche Tohmatsu*

The ability to capture an individual's signature digitally may be one of the most potent developments in e-business. But its acceptance into the business world necessitates resolving technological incompatibilities, revising legislation, and developing new business protocols.

Not only will the use of digital signatures shorten the time-consuming process of establishing new clients, it is also expected to reduce set-up costs by 50%. With new set-ups for financial services customers now costing approximately US\$180 per person in some brokerage operations, the potential savings are significant. However, many businesses will continue to feel more comfortable with a physical customer signature, in the event of disagreement, litigation, or to satisfy regulators.

Signing on the dotted line

This past June, the US Congress passed legislation paving the way for digital signatures, but only after extensive delays by a strong consumer lobby opposed to the legislation. Known as the Electronic Signatures in Global and National Commerce Act, it makes contracts signed online as legally binding as paper contracts. The Act, however, does not endorse a specific technology that must be used for digital signatures; instead, it leaves it up to the parties involved in the contract to agree on a method that they consider safe and reliable.

While the Act allows contracts to be signed electronically as of 1 October 2000, implementation of other parts of the law has been delayed. Companies may begin ending disclosure and other records electronically beginning 1 March 2001, but regulators may have an additional three months to finalise rules implementing that section of the law.

Consumer protection

The Act protects consumers by requiring financial services companies to acquire the

customer's consent and to provide the client with a 'clear and conspicuous' statement including the fees involved and the right of the customer to change his or her mind. Finally, they must execute a test to determine if the client has the software and hardware to properly open emails and attachments from the company. The firm may then make mortgage and other disclosures required by consumer-protection laws electronically instead of on paper.


Canada's Electronic Commerce Act — or Bill C-88 — ensures that electronic signatures will have the same legal status as written signatures in certain circumstances. The Bill was scheduled for passage in late 2000.

Meanwhile... in Europe

Enabling legislation for digital signatures is also in place in a majority of European countries. The Electronic Signature Directive went into effect in January 2000, although countries have until July 2001 to adopt the Directive into national legislation. This goes hand-in-hand with the E-Commerce Directive, which provides the infrastructure for enforcing electronic contracts and which was fast-tracked through the European Parliament this June.

Model legislation in the UK

The UK offers a case study in progressive legislation. It has made significant progress in implementing digital signatures with the passage of the Electronic Communications Act. While electronic signatures are already commonplace in the business-to-business world within secure networks, the Act now formally and legally recognises them. In addition, the requirement that certain types of contracts must be in writing has been eliminated. Finally, the Act allows electronically stored documents to be used as evidence in disputes. In support of the Electronic Communications Act, the UK's FSA is working to incorporate the new



technology into its rules. The FSA has addressed digital signatures in its draft Conduct of Business Sourcebook.

Built-in safety features

Digital signatures open the door to a whole new range of relationships between firms and their customers. It is essential that the underlying trust implicit between both parties be supported by technical checks and balances.

The enabler in this case is an infrastructure of public and private keys which, in combination, create excellent security. Public key infrastructure (PKI) use a comprehensive structure similar to that used in the credit card world.

PKIs currently support secure web access and online payments, a number of types of external access to systems and virtual private networks, as well as authentication for downloading software.

The potential benefits of this technology are extraordinary. In their simplest form, PKI offers a robust means of verifying a user's identity in an online environment. It is envisioned that this technology could expand to become the basis for a payment system over the Internet where the participant's identity is verified, creditworthiness affirmed, and the credit risk for selected transactions potentially transferred to a third party.

The Asia-Pacific perspective

Many governments in the Asia-Pacific region are leading the way in the adoption of PKI and digital signature technologies, with financial services organisations acting as 'fast followers'.

In countries as diverse as Australia, Hong Kong, Japan and Malaysia, governments have enacted digital signature legislation that recognise the validity of digitally signed financial transactions, and

have introduced PKI technologies for taxation and other applications. Additionally, banks have begun pilot PKI projects for Internet-based consumer banking, inter-bank funds transfer over the Internet, and similar applications.

In contrast to other Asia-Pacific nations, New Zealand's government does not have a centralised or coordinated approach to PKI, although some government agencies are independently seeking ways to implement PKI. Private industry, however, is moving forward with both solutions and infrastructure for PKI technology.

Like many new concepts, PKIs are confusing to consumers and to business people alike.

The use of digital signatures with smart cards, PCs, and personal digital assistants will become commonplace as e-business becomes more sophisticated. But achieving the same level of security with third-generation mobile phones — or m-commerce — will present a technological challenge.

The existence of various communications protocols and standards further increases the complexity. These issues need to be resolved as soon as possible, as m-commerce could be the winning application that will enable businesses to overcome national boundaries.

The penetration of mobile phones in Europe, particularly Scandinavia, is high. According to recent research from the International Telecommunications Union, Finland and Sweden lead the pack with 67% and 58% of the population subscribing to mobile phone services,

respectively. The U K has achieved a 41% penetration and the US, 31%.

Penetration in Japan has been estimated at about 40%.

PKIs and TTPs: Gateways or barriers to the electronic frontier?

Like many new concepts, PKIs are confusing to consumers and to business people alike. And the costs of developing the technology and putting the infrastructure in place are steep. Financial services firms must be certain they possess the products and services to justify the expense. Not surprisingly, businesses have been reluctant to adopt these systems.

Instead of PKIs, a number of major European players use password IDs and random number generators held by the customer to establish authenticity. Coupled with traditional written customer agreements, these allow them to avoid building the necessary PKIs in-house or relying on trusted third-party (TTP) providers. TTPs provide encryption services which enable the infrastructure for digital signatures.

Recognising the complexities of the situation, European legislators did not enforce a Europe-wide accreditation for TTPs. Nevertheless, a European committee of financial services organisations is currently working to establish uniform standards for TTP providers, with the goal of achieving technical interoperability of systems across Europe. Legal hurdles to establishing similar encryption standards still remain in some European jurisdictions.

There is also a requirement in the Electronic Signatures Directive that TTPs be supervised nationally.

For example, the UK has established a plan for accrediting TTP providers and for auditors of their services.

North America has adopted a voluntary approach to accreditation



based on best practice developed by a number of organisations. These include the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), and the American Bar Association (ABA). As a result, numerous providers vying to offer Internet-based services in North America are awaiting accreditation from these organisations.

Enter: Smart Cards

The introduction of smart cards may well be the key to securing the participation of major institutions in public key infrastructures as certificate service providers.

Smart cards record a user's identity and account value. Coupled with a personal identification number (PIN) to carry key information, they provide a more secure means of transacting than PC passwords (and one where user liabilities for loss and theft can be clearly set).

Both Sun and Microsoft have entered the smart card market — an indication of its tremendous business potential. Smart card reader devices, which work with the new American Express Blue Card, for example, will eventually become as commonplace as disk drives. Cardholders are sent a free smart card reader, along with software, to plug into their PC. This is used instead of a traditional credit

card to make online purchases.

Forward-looking companies may eventually use biometrics (fingerprints, iris scans, and voiceprints) instead of PINs to support smart cards and PC applications. The absence of a common platform, however, makes this technology prohibitively expensive at present.

The details have it

The overall concepts of PKI and digital signatures are very sound, but the challenges lie in working with reliable and trustworthy suppliers. In particular, the role of the certificate service provider (CSP) is crucial to the success of PKI and digital signatures. The CSP issues a digital certificate and earns revenue primarily from digital transactions.

However, CSPs also carry the liability from fraud and transaction risk. Under Europe's Electronic Signatures Directive, unless the CSP can prove that it has not been negligent, it is liable to any person or entity that has reasonably relied on the timing and contents of the digital certificate. The CSP is also responsible for ensuring that the data supporting both the origin and the verification of the digital signatures are in agreement.


Further, the CSP is obligated to revoke any invalid digital certificates. As a result, the role of the registrar that records the issuance and

revocation of digital certificates is also critical.

Seeking authenticity

The business-to-business environment is characterised by large-value transactions of highly sensitive information. In this environment, trust is even more important than in the business-to-consumer marketplace. Authentication of identity is key to the further development of global trade. There are initiatives to use PKI and digital certificate technology in this arena as well. Identrus, for example, is an international group of more than 40 financial institutions working together to provide certification of identity and credit status of counterparties through a PKI-style structure. Local industry groups, such as the Canadian Payment Association (CPA), are developing a similar cross-accreditation model linking local depository institutions.

It is in the interest of major financial institutions to assume the role of certificate issuer to their clients and thereby build acceptable levels of trust.

* For further information please contact David Thompson, National Director, Secure e-Business Group, Deloitte Touche Tohmatsu on (03) 9208 7810. 

Australia Day Honours

Congratulations to our members who were included in this year's Australia Day Honours!

Medal (OAM) in the General Division

- Mr Sidney Briggs, ACIS, for service to the community of Young, particularly through the administration of health and aged care facilities, to veterans and their families, and to the Young Shire Band.
- Mr John Waldegrave, FCIS, for service to the community, particularly through health administration in the Hornsby and Ku-ring-gai areas.

Ambulance Service Medal (ASM)

- Mr Ian Kay-Eddie, FCIS