The evidential issues relating to electronic signatures II

by Stephen Mason

Both the government and the industry are keenly promoting the use of electronic signatures. It is assumed that the widespread use of electronic signatures will encourage greater use of the internet as a means to buy goods and services. This two part article looks at the evidential issues relating to electronic signatures, and illustrates the weakness of the infrastructure, which in turn highlights the risks that both users and recipients encounter when using electronic signatures.

SHIFTING THE ONUS OF PROOF – ENGLAND AND WALES – COMMON LAW

On the face of the decision of Waller J in *Standard Bank London Limited v Bank of Tokyo Limited* [1995] CLC 496; [1996] 1 C.T.L.R. T-17, it appears that this presumption may have already been adopted in England and Wales. In this case, the Bank of Tokyo in Kuala Lumpur arranged for three tested telexes to be sent to Standard, containing a secret code confirming and authenticating the authorised signatory of three letters of credit with a total face value of US$19.8m, and confirming that the Bank of Tokyo accepted all responsibilities and liabilities under those letters of credit. Evidence was adduced to indicate that banks not only used this system with confidence, but used it to avoid arguments about authority. In this instance, the tested telexes were sent fraudulently.

The main thrust of the Bank of Tokyo's case was this: because they could establish that a fraudster must have been working in their tested telex department, Standard could only rely upon the apparent authority of the tested telexes. As a result, it argued that there was a lower test to establish the lack of apparent authority. Waller J disagreed with this argument, because the issue was not reliance on apparent authority, as set out at 502 C:

> *"Standard rely first on a general representation by BOT that if a telex comes by tested telex that telex will be duly authorised by BOT (that representation on any view is authorised);*
>
> *second they rely on the use of the tested telex mechanism itself as representing that the telex is authorised as the previous representation stated that it would be; and*
>
> *thirdly they rely on the statement in the telex as being the authorised statement of BOT."*

The Bank of Tokyo was found liable for negligent misrepresentation because the tested telexes could not have been sent without negligence on the bank's part. Whether Standard had a duty to inquire into the authenticity of the tested telexes depended, in Waller J's view at 501 H, on the circumstances of each and every case.

Tested telexes contain codes or tests which are secret between the sender and the recipient. This allows the recipient to accept without question that the telex was sent by and with the authority of the sender. The tested telexes in this instance were sent through other banks, because the Bank of Tokyo in Kuala Lumpur did not have a means of directly authenticating telexes between itself and Standard.

By sending tested telexes, banks intend the receiving bank to act on the content without further instructions. This means the receiving bank requires the sending bank to:

- confirm the person signing the document is an authorised signatory,
- verify the signatory is authorised to sign the particular document,
- provide sufficient evidence to satisfy the recipient that the sending bank authorised the sending of the telex.

Superficially, there is a similarity between the circumstances of this case and the world of public key infrastructure, where the authentication process has to go through so many channels. However, there is a distinction between a tested telex produced in a bank and the public key infrastructure. The authority of a telex is reliant upon internal systems within the bank. No third party is involved in identifying the sender of the telex or authenticating the codes or text sent. In addition, the tested telex is sent through other banks over secure lines of communication.

Conversely, the public key infrastructure operates over the internet, which was designed to be open and is, therefore, insecure. The link between the identity and authentication of a user of an electronic signature is not as cohesive as between such trusted parties as banks. There are significantly more links, which neither party has control over, in the chain between the user of an electronic signature and the party intending to rely on an electronic signature.

As a result, it can be argued that there is a distinction between what can be termed a "secure communication system" and an "open communications system". Clearly the burden of proving that an electronic signature was used without authority must be borne by either the user or the relying party. In this instance, Waller J took the view that the sender was in full control of the environment in which the tested telex was sent, and decided that the burden should fall on the sender.

Whether it is for the user, when using an electronic signature, to bear such a burden, is debatable. For instance, the type of technology used, both its purpose and methodology, may have a bearing on this issue. There are several factors that must be considered before reaching a conclusion in relation to this matter. First, if it is accepted that the relying party is required to establish whether they could rely on the certificate in all the circumstances, they will be required to provide any or all of the following evidence, depending on the nature of the challenge:

- the certifying certificate used to affix the electronic signature was used properly,
- the certifying certificate used to affix the electronic signature to the communication had not been revoked or compromised in some way, by providing the statement under the provisions of section 7(3) to prove the integrity and reliability of the relevant certifying certificate,
- that the communication could not have come from another source, or
- that the communication was intended to have legal effect, because extrinsic evidence can be produced to demonstrate the intention of the sender.

Providing the replying party has carried out all the relevant checks required, it can then be argued that it has discharged what can be described as a procedural and due diligence burden.

Once the relying party has satisfied a judge that it has discharged the procedural and due diligence burden, the user will need to address the issue of the security and integrity of their computer or system. This can be described as the burden of proof of security and integrity, which comprises both a persuasive burden (or burden of proof on the pleadings) and the evidential burden of adducing evidence.

In the event of a dispute, it follows that it is the holder of the certifying certificate who is in the best position to prove either that the security in place was inadequate, which implies it would be possible for an unauthorised third party (internal or external) to use the certifying certificate improperly, or that the security in place was such that the certifying certificate could not be used improperly. The user will be in control of the following (this list is not exhaustive):

- the hardware and the software of the computer or system upon which the private key sits,
- the security in place in relation to the computer or system, the use of the system by employees and the control of any tokens used to store the private key,
- the ability of the user to revoke their key promptly after finding out that their system or key was compromised.

If the user wishes to argue their security was so poor that an unauthorised third party could have gained access to the system to send an electronic communication with an electronic signature attached without authority, the user will undoubtedly be admitting breach of contract with the vendor from whom they obtained the certifying certificate. The user may also be admitting they were negligent.

Finally, once a communication leaves the user's computer or system, they relinquish control of the document. If the user can demonstrate the effectiveness of the security and integrity of their computer or system, the next link is the network over which the communication passes. In this instance, evidence may be required from a number of organisations in the chain (discussed in more detail below), including:

- the methods of management the trusted third party uses to control its infrastructure,
- whether the link between the issuing of the certificate and its use was to be trusted, and
- the effectiveness or otherwise of any third party supplier whose product or service is included in the chain.

If the relying party can demonstrate that they carried out due diligence, and the user can demonstrate the security and integrity of their computer or system, the question then becomes: which party to the proceedings has the

persuasive and evidential burden of demonstrating any weaknesses in the infrastructure. Whichever party bears this burden, it will be an expensive process, bearing in mind the number of organisations that make up the chain. In a dispute, the burden of proof will inevitably be on the party that asserts the problem lies with third parties in the chain. It seems that all the relying party needs to do is to demonstrate procedural and due diligence. Thereafter, it is for the sender to either demonstrate lack of security, or the fault occurred as the result of failure by third parties in the chain, unlike in the burden in proving a manuscript signature. This will inevitably mean that the sender will have to make this assertion in the pleadings, which will determine the persuasive burden (and invariably the evidential burden) will lie with the sending party.

SHIFTING THE ONUS OF PROOF – ENGLAND AND WALES – ELECTRONIC COMMUNICATIONS ACT 2000

By section 8(1) of the Act, Parliament has given the appropriate Minister the authority to modify the provisions of:

(a) any enactment or subordinate legislation, or

(b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation

in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).

Whilst the power to modify legislation may be considered to be helpful in changing the law relating to the use of electronic signatures, nevertheless it must be pointed out that the Act allows for the burden of proof to be shifted, if so desired by a minister. The relevant sections are section 8(4)(g), which reads as follows:

(4) Without prejudice to the generality of subsection (1), the power to make an order under this section shall include power to make an order containing any of the following provisions –

…

(g) provision, in relation to cases in which the use of electronic communications or electronic storage is so authorised, for the determination of any of the matters mentioned in subsection (5), or as to the manner in which they may be proved in legal proceedings;

and section 8(5)(d), which reads as follows:

(5) The matters referred to in subsection (4)(g) are –

…

(d) the person by whom such a thing was done

In combination, these section gives scope to a Minister to determine where the burden of proof will lie in any particular order issued under the Act.

As a result, persons deciding to use electronic signatures will need to ensure they guard the use of their certifying certificates very closely. In particular, they will need to ensure that their computer or the system upon which the electronic signature sits, is properly protected from the risks set out later in this article. People using electronic signatures will have to determine what steps are reasonable to protect their private keys. In all probability, companies and firms will have to consider abiding by DISC PD 5000:1999 Electronic documents and e-commerce transactions as legally admissible evidence. In this respect, it is only right that solicitors should be concerned about the proposals for conveyancing, because the risks are serious and certainly outweigh the benefits that some people claim.

EVIDENTIAL WEIGHT

It will evident from the above discussion that trusted third parties will need to guarantee that they can audit the evidential trail in relation to the use and control of the certifying certificates and key numbers they issue. In this respect, both the trusted third parties offering certifying certificates and individuals challenging the admissibility of communications associated with electronic signatures will need to be able to demonstrate the integrity of their respective systems (or lack of integrity), as the case may be. The evidential weight to be given to evidence relating to electronic signatures is predicated on the degree of control exercised over the controlled and secure environment of all the parties in the chain. It follows that it will be for a judge to decide what weight, if any, is to be placed on the integrity of the infrastructure in the event of a dispute.

THE TRUSTED THIRD PARTY

The use of a certifying certificate does not necessarily require the existence of a certification authority. Parties that wish to agree a procedure that ensures the authenticity of documents passing between them can make their own arrangements. They may choose to use a private key, where each party has the same key, and do not share it with any other entity. Alternatively, they may rely on a dual key, comprising a private key and a public key, issued by a certification authority or trusted third party.

When a certification authority issues a certificate, it bases the issuance of the certificate on its Certificate Practice Statement and terms of trade. A contractual relationship is formed between the certification authority and the customer who buys the certificate. Whilst the certificate purports to verify the identity of an individual person or legal entity, it is the merchant or person receiving the certificate that relies on the content of the certificate, known as the relying party. The logic is as follows:

- The individual provides the certification authority with sufficient evidence to demonstrate that they are who they say they are. Depending on the level of the certificate obtained, this information could be merely name, address and the number of a driving licence. For certificates that will support high value transactions, the person seeking a certificate may be required to provide more robust evidence, including physically appearing before a notary public.
- The certification authority provides the user with a certificate.
- The individual is then given a keyholder's name.
- The keyholder is the person that obtained the certificate.
- This all the recipient needs to know.

There are a number of flaws with this logic. For instance, John Smith of York may wish to enter a contract with a company who is not aware of his identity. The company cannot distinguish, when it looks at the certificate, how many John Smiths live in York and whether this particular John Smith is the person identified with the certificate. Unless the certificate provides the company with a unique identifier identifying this particular John Smith (which they may or may not provide), and the company wishes to confirm John Smith's identity, it must consider other ways of doing so. In conclusion, a certification authority provides a very narrow promise when issuing a certifying certificate. It does not appear that certification authorities seek first to establish the identity of a person and then go on to verify that identity. It is crucial to understand that verification is not the same as identification.

The point is, the certification authority generally does not share a secret with the person to whom they provide a certificate. Many certification authorities use the information collected by a credit bureau to identify the identity of the applicant. This means the identification process is based on the accuracy of the data collected by the credit bureau and the effectiveness of the credit bureau in keeping the information up-to-date. Another issue is whether the recipient of the electronic signature trusts the originator's certification authority.

THE ROLE OF THE TRUSTED THIRD PARTY

The certification authority is a trusted third party that purports to ascertain the identity of a person, and certifies that the public key of a private key pair used to create a certifying certificate actually belongs to a particular person or entity. The steps in the certification process will depend on what evidence the certification authority obtains from the person wishing to buy a certifying certificate, and the value attached to the certificate. The reader will be aware that Article 5 of the EU Directive 1999/93/EC on a Community framework for electronic signatures, OJ L13 19 January 2000 provides for both simple electronic signatures and certified advanced electronic signatures. It is debatable whether the UK government will have to amend the Act to provide for an advanced electronic signature, but the existence of an advanced electronic signature does not affect the technical problems that may arise where a person does not accept they used their electronic certificate to sign a communication.

For instance, an individual could generate their own public and private key pair, using software on their computer. The individual then provides the certification authority with evidence of their identity. The type of evidence and degree of proof will depend on the nature of the type of certifying certificate required. In outline, it has been suggested that a certification authority will undertake the following tasks:

- reliably identify the person or entity applying for a certifying certificate
- reliably verify their legal capacity
- confirm the attribution of a certifying certificate to an identified physical person or legal entity by means of a certifying certificate
- maintain online access to the public register
- take measures to ensure the confidentiality of the private key is guaranteed.

When the certification authority has verified the identity of the individual or entity to their satisfaction, they will issue a certificate. This is a computer record that affirms the connection of a public key to an identified person or corporate entity. The certificate can identify the following:

- the certification authority issuing the certificate
- the individual's public key, and
- other information including, but not limited to the serial number of the certificate, the user's name, place of birth, whether they are a natural person, their legal domicile, virtual domicile, an expiry date for the public key and, depending on the type of certificate issued, the value limit and any powers of agency.

THE INFRASTRUCTURE

To enable a user of a certifying certificate to trust a certification authority, a number of factors have to be taken into account, some of which will be determined by legislation, others which are internal to the certificate authority.

Internal management

The internal management of a certification authority, which the individual user will not be familiar with, can affect the trust to be placed in the certificates issued. For instance, the level and extent of the checks made on employees may be relevant together with whether the internal management of the certificate system is properly

carried out. The level and extent of any insurance cover may also have a bearing on the suitability of different types of certificate issued.

Public degree of trust

Factors that will affect the degree of trust in a certification authority that should be public knowledge, include the level of certificate issued and the limitation of liability for that particular certificate. The verification process is an important function that should be undertaken in public. The certification authority should be in a position to verify the integrity of the public key and validate the encoding techniques. Further, it should be possible for a person who wishes to rely on a public key issued by a certification authority to check that the certificate is valid by way of the certification revocation lists. Whether a certificate has been revoked is an important part of the trust placed in a certification authority.

An additional factor to be taken into account is the certification authorities often, it appears, sub-contract the work of issuing individual certifying certificates. Thus a user may receive a certificate from a certification authority which has been signed by the intermediate authority. The problem is compounded if the software of the relying party cannot check the intermediate certificate. If the relying party cannot check the full chain of certificates, the value to be attached to the individual certifying certificate is diminished significantly.

It should be noted that the United Kingdom government has provided relevant legislative provisions relating to certification authorities in the Act. The government intend that a voluntary scheme be introduced to regulate the industry, called the tScheme.

Revocation of certificate

Some certification authorities support certification revocation lists. This allows a person or business to check the revocation list to determine whether a certificate has been revoked or has expired. There may be many reasons for revoking a certificate, including:

- the private keys corresponding to the certificate have been lost or compromised,
- the certificate holder asks for the certificate to be revoked,
- the certification authority may revoke a certificate where the holder breaches a term of the agreement, or
- if the certificate was issued in error.

Where such a list exists, an important question is whether the certification authority keeps this list up-to-date and whether, therefore, it can be relied upon to provide a definitive answer that can be trusted. If a certification authority does not have a revocation list, the person seeking to determine whether to rely on a certificate needs to know how they can establish whether a key has been revoked or compromised.

Expiry of keys

Certification authorities provide for the expiry of keys. One technical question relates to how the life of the key is computed. Ellison and Schneier contend that the key has a "theft lifetime" as a function of the vulnerability of the sub-system that stores the key. Other factors that also should be taken into account include the threat of physical and network exposure to attacks and how attractive the key is to an attacker.

Root hierarchy

One of the models used to establish the validity of a certification authority is to have a hierarchy of authorities, each authority certifying the technologies and practices of the subordinate authorities. Thus there could be a top level authority, followed by one or more subordinate authorities, each verifying the certificates of the authority below it in the hierarchy.

FAILURE OF SECURITY

The extent of the security measures in place, either on the computer or the system upon which the certifying certificate is located, is an important factor in evaluating the possibility that a system can be compromised. Clearly there is a balance to be struck between the cost of a certificate and the liability accepted by the issuing authority, although this matter is not discussed in this paper. Below are some of the potential areas for concern:

Hacking into the system that supports the certifying certificate

A hacker can obtain access to the user's system and use the private key of the user. If a hacker is successful, the user may either not have taken sufficient steps to ensure they had adequate security in place to prevent such an attack, or they may have failed to properly implement the security measures that were in place to prevent such an attack. Examples of simple security measures that can be easily attacked include the use of a password to enter the computer (the password may be easy to guess) or, if the key number is stored on a smart card, how resistant the card is to attack.

Side-channel attacks

A hacker can, by carefully measuring the amount of time it takes the system to perform the operations of a private key, obtain the fixed Diffie-Hellman exponents, factor RSA keys and break other cryptographic systems. Such an attack is possible because other variables relating to the performance of the hardware and software can be monitored by the hacker to exploit measurements in timing to find the entire key. Such an attack is

computationally inexpensive against a vulnerable system. A hacker can also exploit the variation in voltage consumed in order to derive information about the private key number. For instance, some computational processes run so slowly that it is possible to see the mathematical functions performed by the software. Smart cards are also vulnerable to this type of attack. The card is plugged into a reader or encoder and the information contained on the memory is protected by secondary protection. Where the reader or encoder is powered by a battery which is running low in power, it is possible to obtain access to the memory by by-passing the security mechanism on the card.

Breaking into the user's computer: forgery and identity theft

A hacker can break into a user's computer and take over the system. By undertaking this activity, the hacker can use the private key of the holder. This is an example of forgery or identity theft: a legitimate certifying certificate is used that purports to come from the user, but which is actually not authorised by the legitimate user.

Misuse of computer power

It is also possible for a computer to be controlled to a degree that the holder is, unwittingly, contributing computer power as part of a collective effort to crack keys.

The fraudulent substitution of a public key for that of a genuine user

This is where an impostor substitutes their own public key for that of the genuine user. There is no attempt to recreate the certifying certificate of the genuine user. The attacker can sign a document with a false public key that identifies the genuine user incorrectly.

Theft of keys

Employees or directors may use their position of power and influence in collusion with others to steal keys or encryption secrets.

FAILURE OF THE VERIFICATION SYSTEM

Subverting the "root" key

Certification authorities use root public keys. Thus, if an attacker can add their own public key to the root key list, the attacker can issue its own certificates. These certificates will be treated exactly like legitimate certificates.

Obtaining access to the certification authorities private key

Where an attacker discovers the certification authorities private key, they can produce an unlimited number of ostensibly valid, but forged certificates.

Certification authority erroneously issuing certificates to somebody claiming to be other than they are

For the public key infrastructure to be trusted, a certification authority must ensure that the architecture and systems that support and issue certificates cannot be abused by somebody obtaining a certificate in the name of another person or entity. Unfortunately for VeriSign, a company that issues certifying certificates, this actually occurred in January 2001. VeriSign issued two Class 3 code-signing certificates incorrectly to a person falsely claiming to represent Microsoft. The certificates were issued to "Microsoft Corporation". During a routine audit in mid-March, the error was discovered and VeriSign notified Microsoft of the error, posted a public notice and revoked the certificates on its certificate revocation list.

This matter did not end with the posting of the public notice on the certificate revocation list, however, as pointed out by Gregory L Guerin in his article "Microsoft, VeriSign, and Certification Revocation", at http://amug.org/~glguerin/opinion/revocation.html. The person wishing to obtain access to the certificate revocation list must have the correct uniform resource locator (URL). The URL is the address from which the certificate revocation list can be downloaded. There are two technical issues that affect the ability to download a suitably-recent certificate revocation list:

- how the certification authority tells you where to obtain the relevant certificate revocation list, and
- whether your computer carries out the functions you require.

Guerin points out that there are many different ways to obtain a certificate revocation list, and because there is no standard within the industry, no one method is mandatory. Regardless of the method used, the key evidential issues for anybody relying on a certifying certificate are as follows:

- The certificate revocation list should be digitally signed by the certificate authority using its root certificate to prevent a certificate revocation list from being forged.
- The certificate revocation list is dated by the certification authority, which means that every certificate revocation list expires.
- Every certificate revocation list has a higher sequence than the one issued previously, to prevent forgery.
- The person wishing to check a particular certifying certificate must know where to find a suitably-recent certificate revocation list.
- The certificate revocation list must actually be obtained.
- The contents of the certificate revocation list must be authenticated.
- The person relying on a certifying certificate must actually use the certificate revocation list.

In the VeriSign case, the certificate revocation list was available from a URL that was well known to developers of security products, and the certificate revocation list can be downloaded with any browser. In this instance, as Guerin points out, VeriSign put the responsibility on the developer of the software to either ensure the software could retrieve the certificate revocation list, or provide a means to the user of the software to install the VeriSign certificate revocation list after it had been manually downloaded by the user of the computer.

According to Guerin, Microsoft designed the software to take a user to the address where the certificate revocation list existed only if the address was provided by VeriSign with the certifying certificate. Apparently, VeriSign does not issue Class 3 code-signing certificates with an address for the certificate revocation list. This appears to mean that the user of the relevant Microsoft software cannot retrieve the certificate revocation list of a given certifying certificate issued by VeriSign. At the time of this incident, Guerin reached the conclusion that Microsoft did not have software that had a working revocation infrastructure.

If it is the case that a vendor of software such as Microsoft did not have a working revocation infrastructure in place in the past, then it could be argued that past certifying certificates can hardly be said to be reliable. As a result, the evidential weight to be given to a certifying certificate must be considered against these practical problems, otherwise the evidence may be so poor as to make the concept of a certifying certificate irrelevant.

THIRD PARTY SUPPLIERS IN THE CHAIN

As the example above illustrates, there may be a number of weaknesses in the security chain that will affect the reliability of the certifying certificate, including the hardware, software, internet connectivity and time stamping functions – all of which are not within the control of the user or of trusted third parties. In addition, the concept of authentication vendors, or cyber notaries, all adds to the complexity of the infrastructure.

TECHNICAL ISSUES

The technical issues relating to certifying certificates are complex. The Internet Law and Policy Forum have identified a number of problems that will affect cross-border use of certifying certificates. They include the lack of detailed technical standards, whether certification authorities should be accredited, certified or registered, the legal effects of such certificates, whether to have supervisory bodies and whether the standards adopted by various countries are international in nature. The conclusion is that the various initiatives implemented to date will not allow certifying certificate technologies to be standardised. The reader will readily note that the evidential weight to be attached to an electronic signature will be affected by these issues.

CONCLUDING REMARKS

Over the past few years politicians have rushed into passing laws that attempt to place electronic signatures on par with manuscript signatures. In putting legislation on to the statute book, individual states have:

- failed to agree an international meaning of what is meant by an "electronic signature",
- taken different views in relation to the types of electronic signature to be made available (ordinary signatures and qualified signatures),
- ignored the issues relating to compatibility of software and hardware, and
- failed to agree whether trusted third parties should be licensed or unlicensed, public or private.

The *Electronic Communications Act 2000* provides for the statutory basis of the admissibility of electronic signatures. The admissibility of the public key as a component of an electronic signature may appear to be straightforward. However, in the event of a dispute where one party relies on the electronic signature of another and the owning party denies affixing their electronic signature to the communication in question (which also implies they deny they sent the content of the communication as well), then it will be for a judge to examine the evidence to determine whether it can be shown that the electronic signature in question was actually used by the owning party.

In such circumstances, the question of what, if any, legal presumptions operate, will need to be addressed in relation to the technical issues set out above. Contrary to the presumption that machines (i.e. the computer or system upon which the electronic signature sits) may be presumed to be in working order, it is suggested that there can be no single presumption, because an electronic signature is not reliant upon a single machine. Various factors must be taken into account, such as:

- the nature of the hardware and the software of the actual computer or system upon which the private key sat,
- the security in place on that computer or system,
- the methods of management used by the trusted third party and the holder of the electronic signature, and
- whether the link between the issuing of the certificate and its use was to be trusted.

Other issues will need to be canvassed, including the effectiveness of any third party supplier whose product or service is included in the chain. Further issues have also been identified by the American Bar Association:

- whether the holder of the certifying certificate carried out their contractual duty of care to avoid the private key being compromised
- whether the replying party could rely on the certificate in all the circumstances

- if the holder of the certifying certificate revoked their key promptly upon finding out their system or key was compromised
- which of the two innocent parties (relying party and holder) was in the better position to protect themselves from damage at the hands of an impostor.

Whether electronic signatures will ever be used widely is a matter that only the passing of time will determine. The main issue surrounding electronic signatures relates to the ease by which a signature can be misused. This article seeks to show that there are many ways in which the use of an electronic signature can be challenged, although it is doubtful that there will be large numbers of disputes which focus on the sole issue of whether an electronic communication was signed by an unauthorised electronic signature.

Stephen Mason is a barrister and Chairman of Pario Communications Limited. He specialises in e-risks, e-business, data protection and interception of communications.

stephenmason@pariocommunications.co.uk

This paper was written to accompany a lecture given to a joint meeting of the Society for Advanced Legal Studies and British Computer Society Internet Specialist Group on 15 November 2001 in Senate Room, Senate House, University of London, chaired by David Spinks, Director Information Assurance, EDS.

This paper was first published in two parts in *The Computer Law and Security Report*, **Part I** May/June 2002, Volume 18, Issue 3, 175 – 180, **Part II** July/August, Volume 18, Issue 4, 241 – 248.

Readers may download a copy of this paper from the web site, which contains the full references.

The law as Janus: children, crime and care

by Peter Harris

My inspiration for the choice of the subject of this article is the Michael Sieff Foundation conference which took place in September 2001 on "The Needs of Offending Children". The focus of that conference was the forensic dichotomy that is represented by the Civil and Criminal Justice Systems when the State intervenes in the lives of children in respect of events which require a judicial decision. This lead naturally to the title I have given to this article since the Roman god Janus is always depicted as a head with two faces looking in opposite directions.

The media treat children generally as either young villains or victims, and as if young offenders fall exclusively into the former category. However those who deal with them professionally know that children with unmet welfare needs and children who commit crime are not disparate populations. The two categories certainly overlap, and the latter category is pretty much a sub-set of the former, which is defined by section 17 (10) of the Children Act 1989 in respect of a child who:

> *" .... is unlikely to achieve or maintain, or have the opportunity of achieving or maintaining, a reasonable standard of health or development without the provision ... of services by a local authority ... his health and development is likely to be significantly impaired without the provision of such services ... [or] .... he is disabled, .."*.

Disability includes being blind, deaf, dumb or suffering from mental disorder of any kind. Development includes physical, intellectual, emotional, social or behavioural development, and health means physical or mental health. (The relevance of these definitions I shall refer to in greater detail in due course).

My starting point, however, is a quotation from the Roman poet Juvenal which was used by Lord Hewart, the Lord Chief Justice in 1931 when delivering the second Clarke Hall lecture on young offenders – or as he called