The evidential issues relating to electronic signatures I

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.

WHY ELECTRONIC SIGNATURES ARE USED

It is argued that consumers do not use the internet widely to purchase goods and services because of the perceived threat to security of personal data, in particular of the possible misuse of credit card details. In addition, it is also assumed that businesses selling goods and services over the Internet are concerned about the integrity, confidentiality, authenticity and non-repudiability of messages sent electronically. The author is not convinced of these assumptions, and has previously suggested in this Journal that the reason people do not buy from business with a presence on the internet in the volumes predicted are related to more fundamental issues, rather than a lack (perceived or not) of security on the internet. This is a view shared by the eminent cryptographer Ross Anderson, amongst others, who argues that the overwhelming majority of cryptographic support systems will be concerned with protecting intellectual property rights.

Regardless of the volumes of certifying certificates issued and used, the reasons for using an individual certifying certificate are as follows:

- To ensure the *authenticity* of the information. When sending or receiving information or placing an order, both parties need to know the sender of the message is the person they claim to be. There is a need to authenticate the identity of the sender.
- To demonstrate the *integrity* and *accuracy* of the message, because it is important to know if the content of the message has not been tampered with.
- To prevent the person making the statement from denying that they made the statement. This is called *non-repudiation* in the security industry.

In the normal course of events, many thousands of transactions take place over the Internet each day without recourse to the use of cryptographic devices. Not only are goods and services bought and sold, but also individuals and businesses in ever increasing volumes conduct correspondence by way of e-mail. People using the Internet do not tend to use electronic signatures to conduct business. In the same way that a consumer will enter a contract to purchase an item from a business at a distance after viewing an illustration of a product in a catalogue or newspaper, for instance, so people use their intuition to gauge the risk they may be taking when entering a contract over the Internet. Even where strangers enter contracts with each other, people tend to rely on the information they glean from conversations over the telephone, face-to-face meetings, advertising, brand images and references from friends.

Whilst individual certifying certificates can help to confirm the identity of a consumer, the use of such a certificate does not necessarily help the consumer determine

(a) whether the business they purport to be entering a contract with exists, or

(b) if the business exists, whether and when it will supply the goods or services ordered as promised or

(c) if the web site they have viewed is a ghost site, purely intent on capturing their identity or credit card details or both, with a view to using such information fraudulently.

Conversely, it is perfectly possible for certifying certificates to provide authentication in relation to the points raised above. For instance, where the visitor has logged on to a web site with a secure connection, they can click on to the secure icon to follow the trail to look at and check the certificate sitting behind the web site. The practical point about human behaviour, which is not the subject of this article, indicates that certifying certificates may never be used widely. However, even if human behaviour was such that certifying certificates were widely used, the potential user faces serious practical problems before they can use a an electronic signature. Individual certifying certificates are difficult to buy, install on a computer and use properly. It is probably for these latter reasons that consumers will not use such certificates widely.

HOW THIS PAPER IS ARRANGED

The aim of this paper is to introduce the reader to the range of issues that need to be considered when seeking to adduce an electronic signature into evidence. It may be that the relying party wishes to show that the party affixing the electronic signature to a document intended to be legally bound to the terms of the document. Alternatively, the party whose electronic signature was used may challenge the assertion that they affixed or authorised the fixing of their electronic signature to the document in question. As a result, it is felt appropriate to set out the legal framework before considering the infrastructure relating to electronic signatures. The problems relating to the way electronic signatures are created and used will highlight the types of evidential issues that may arise in the future.

First, the terms used in this paper are considered. There follows a short discussion of manuscript signatures and the nature of an electronic signature. Consideration is then given to the admissibility and legal presumptions of electronic signatures. Thereafter, 'non-repudiation' is discussed before considering the reliability of the certifying certificate and the issues that must be considered in assessing the evidential weight to be given to the evidence. Finally, a brief outline of the technical structure is given before setting out the weaknesses, which will have a bearing on the evidential weight of an electronic signature.

TERMS

The terms 'electronic signature' and 'digital signature' are used interchangeably. An electronic document can be sent with the following attributes:

- An electronic document can be sent in its plain text.
- Alternatively, an electronic document can be sent in plain text with an electronic signature attached to it in accordance with the provisions of s.7(1) of the *Electronic Communications Act* 2000 (the Act), ss 7, 11 and 12 which came into force on July 25, 2000 in accordance with the provisions of the *Electronic Communications Act* 2000 (*Commencement No 1*) Order 2000 (SI 2000 No 1798), which provides as follows:

> *7(1) In any legal proceedings-*
>
> *an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and*
>
> *the certification by any person of such a signature,*
>
> *shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data?*

- Further, an electronic document can be sent in encrypted text with an electronic signature attached to it.

In this paper, the following definitions have been adopted:

The term 'electronic signature' is the incorporation of an electronic or digital method (comprising a numerical value using a known mathematical procedure associated with the private cryptographic key of the sender) to an electronic communication, which is:

- unique to the person using it, and
- which is capable of being verified, and
- is linked to the communication in such a way that if the content of the communication is changed, the electronic signature is invalidated.

For the purposes of this paper, 'electronic signature' has the specific meaning attributed to it in s.7(2) of the Act, as follows:

> *(2) For the purposes of this section an electronic signature is so much of anything in electronic form as-*
>
> *(a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and*
>
> *(b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.*

An 'individual certifying certificate' means the individual certificate issued by a trusted third party (such as a certification authority), which identifies a natural or legal person and indicates that a public key and a private key has been issued to the natural or legal person.

The meaning of a digital signature as adopted by ISO/IEC 7498-2: OSI *Basic Reference Model - Security Architecture* will be used in this paper. This is data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit. The digital signature mechanism defines two processes: that of

(a) the signing of a data unit by the person initiating the signature, which is a private action, and

(b) verifying a signed data unit by using the procedures and information publicly available, the process of which is discussed later in this paper.

If there is a difference between an electronic signature and a digital signature, it is the fine distinction between:

- the incorporation of data that *purports* to be incorporated or associated to help establish the authenticity or integrity of the communication, and
- the ability to *prove* the source and integrity of the data unit.

It can be argued that the digital signature can provide a higher degree of certainty for the relying party, subject to the verification process and the possibility that a digital signature can be removed from a document in electronic format without trace.

MANUSCRIPT SIGNATURE

The electronic signature is often compared to the manuscript signature. Whilst there is a similarity in purpose between the two, an electronic signature comprises more attributes than a manuscript signature. A manuscript signature, which can be a full name, initials, a nickname or a seal, can serve a number of functions:

- To provide evidence of the identity of the person creating the document, thereby associating that person with the document they have signed, such as a will.
- It can demonstrate that the signatory approves the content of a document.
- Is a declaration of the signatory's intention that the document is to have legal effect and acts as proof of the event of signature.
- By signing a document, the signatory is reminded of the significance of the act and the need to act within the provisions of the document.

As a corollary, the party receiving the document containing a manuscript signature recognises that the other party affirms the content of the document, they are assured of the identity of the signatory and they are in receipt of the proof of the source and contents of the document.

However, it is well known that manuscript signatures are forged. To prevent this problem, and to test both the validity and the effectiveness of a manuscript signature, some documents require the signature to be affixed in the present of a witness or an authorised official. There is a distinction between the form and function of a manuscript signature, and Professor Chris Reed notes in his article 'what is a Signature?' 2000 (3) *Journal of Information, Law and Technology* (JILT), http://elj.warwick.ac.uk/jilt/00-3/reed.html that the modern approach to the validity of a manuscript signature emphasises function over form in the test for validity.

THE NATURE OF THE ELECTRONIC SIGNATURE

An electronic signature, in accordance with the provisions of s.7(1) of the Act, can be admissible in evidence in relation to the authenticity of the communication or data and the integrity of the communication or data. In addition, an electronic signature serves other information-security purposes that manuscript signatures cannot:

- the recipient can determine whether the communication was altered after it was digitally signed
- as a result, a certifying certificate can provide assurance about the source and integrity of the document.

Electronic signatures can be produced in different formats, including a manuscript signature that is scanned into a document, an electronic representation of a hand written signature or a digital representation of a biometric, such as a retina scan or fingerprint.

THE ADMISSIBILITY OF THE ELECTRONIC SIGNATURE

The Act permits an electronic signature to perform a similar role to that of a manuscript signature. The Act provides, in s.7(3) for any person to certify that the electronic signature is a valid means of establishing the authenticity and integrity of the communication or data or both:

> (3) *For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that person (whether before or after the making of the communication) has made a statement confirming that-*
>
> (a) the signature,
>
> (b) a means of producing, communicating or verifying the signature, or
>
> (c) a procedure applied to the signature,
>
> *is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.*

It appears, therefore, that the person or organisation certifying the electronic signature may need to certify *before or after* or *both before and after* sending the communication, that the signature is authentic and the integrity of the data or communication is therefore not to be questioned. From a practical point of view, the certification process will probably occur before the sending of the communication, although there may be circumstances where the certification process can occur after the communication is sent. The actual certification will probably be an assertion by the person or organisation certifying the signature that there is an association linking the public key with the private key. It is the provision of this extrinsic evidence that is necessary to provide evidence of the user's identity.

THE LEGAL PRESUMPTION OF AN ELECTRONIC SIGNATURE

It should be noted that the electronic signature is admissible in evidence in relation to the authenticity or integrity of the communication, and that the communication is deemed to have a legal effect (s.2(a)(iii) of the Act is authority on this latter point). Section 7(1) of the Act provides for a two-stage process to ensure an electronic signature can be admissible in evidence for the purposes of the Act:

- First, by s.7(1)(a) the electronic signature must be incorporated into or logically associated with a particular electronic communication or data, and
- Second, by s.7(1)(b) there must be a certification process where a statement is produced which links the key with the person, including, but not limited to, the undertaking of checks on the identify of the individual or corporate entity.

The second stage of the process infers that it is the duty of the trusted third party to certify that a key linked to a person or legal entity is admissible. It seems, therefore, that if a recipient receives an electronic communication which is (a) signed with an electronic signature, and (b) the certifying certificate relating to the electronic signature can be verified by a trusted third party, the communication in question is admissible in evidence, subject to the provisions of s.15(2) of the Act.

THE MEANING OF NON-REPUDIATION

In legal terms, the meaning of 'non-repudiation' is different to that used in the technical cryptographic sense. A manuscript signature can be repudiated for a number of reasons, including:

- the signature is a forgery
- whilst not a forgery, the signature was obtained as a result of unconscionable conduct by a party to a transaction fraud instigated by a third party undue influence exerted by a third party.

Legal meaning

In civil proceedings, the Judicial Studies Board indicate that a certifying certificate may be hearsay evidence as to the identity of the public key, and if a party relies on such a certificate, they must meet the requirements relating to notice of this evidence in accordance with section 2 of the *Civil Evidence Act* 1995 and the provisions of Part 33 of the *Civil Procedure Rules*. Once the party relying on the public key provides the relevant notice and particulars, it will be for the other party to raise an objection as to the authenticity or otherwise of the certifying certificate. A party to civil litigation is taken to admit, in accordance with Part 31 of the *Civil Procedure Rules*, the authenticity of a document disclosed to them under Part 32, Rule 19(1) of the Rules unless they serve notice that they wish the document to be proved at trial.

As far as criminal proceedings are concerned, a judge will be required to consider whether a certificate is admissible under the terms of s.24 of the *Criminal Justice Act* 1988 and s.68 of the *Police and Criminal Evidence Act* 1984.

Technical cryptographic meaning

The term "non-repudiation" in the cryptographic sense for technical purposes is a property, attained through cryptographic methods, which prevents the person sending the message from denying they sent the message, as well as denying the origin, submission, delivery and integrity of the content. This technical meaning of the term has begun to be used in a legal sense by vendors of public key infrastructure, which in turn has had tended to confuse legislators. It has been suggested that the technical response by the International Organisation for Standardisation is either to deny the right of the individual to repudiate an electronic signature or shifts the burden of proof from the recipient to the alleged user.

Repudiating electronic signatures

A key issue with respect to electronic signatures is the connection between the mental state of the person who may wish to be bound by the affixing of the electronic signature to a communication, and the act of affixing the electronic signature to the electronic message. The following issues are pertinent when establishing a nexus between the electronic communication and the electronic signature:

- whether the genuine user intended to be bound by the contents of the electronic document
- if another person used the electronic signature without authorisation, how they obtained access to the certifying certificate
- who should bear responsibility for the unauthorised use.

CHALLENGING AN ELECTRONIC SIGNATURE

An electronic signature can be challenged for a number of reasons:

- where the person whose certifying certificate is used, claim they did not authorise the affixing of the key number to the document (this could be because an unauthorised person gained access to and used the certifying certificate, such as a member of the family, fellow employee or a hacker),
- the communication was sent with the electronic signature affixed, but the sender did not intend the communication to have any legal effect,
- the communication was sent with the electronic signature affixed, but the sender was coerced into sending the communication with the electronic signature affixed against their will,
- the communication was sent with the electronic signature affixed, but the sender revoked the certifying certificate,
- a certifying certificate may have been issued to an impostor.

The party challenging the admissibility of the electronic signature may be making either one or all of the following claims:

- the security used by the sender was not sufficient to prevent a third party from gaining access to their computer or system and making improper use of their key number,
- the procedures and technical abilities (such as the means of producing, communicating or verifying the signature) of the trusted third party were at fault,
- another organisation in the chain that links the sending of the electronic key and its receipt by the relying party, other than the trusted third party, was at fault.

Where the electronic signature is used to authenticate the document or to establish its authenticity, a number of questions (some of which are set out above) must be considered, in accordance with s.15(2) of the Act, which provides as follows:

> *In this Act-*
>
> *(a)references to the authenticity of any communication or data are references to any one or more of the following-*
>
> *whether the communication or data comes from a particular person or other source;*
>
> *whether it is accurately timed and dated;*
>
> *whether it is intended to have legal effect;*
>
> *and*
>
> *(b) references to the integrity of any communication or data are references to whether there has been any tampering with or other modification of the communication or data.*

Whichever party has the burden of proof will be required to submit evidence in response to the provisions of s.15(2), together with any other extrinsic evidence that may be necessary to support the evidential burden.

The technology can, to a high degree of probability, prove that an electronic signature was affixed to a communication, but it cannot prove who used the signature. It is to be inferred that the holder of the certifying certificate affixed the electronic signature to the communication. The inference is weaker where there is little or no security in place on the computer or system upon which the certifying certificate sits.

RELIABILITY OF CERTIFYING CERTIFICATES AND BURDEN OF PROOF

Regardless of the technical meaning of the term 'non-repudiation', there are a number of problems that affect the reliability of certifying certificates, which are used to affix electronic signatures to an electronic communication:

- The confusing design on the screen, which can lead a user to activate the non-repudiation function without knowing the significance others attach to the certifying certificate.
- The software application may be set to send a receipt, but the recipient may not know the original sender sent the receipt. This also raises the question as to whether the receipt is authentic.
- Flaws in the design of the security system that permits one person to activate the non-repudiation bit in the electronic certificate of another user without permission.
- A design flaw in the public key infrastructure.
- The open nature of the Internet, which means hackers, could infect computers with a virus or Trojan horse that can be designed to steal private keys. The risks of hackers gaining entry to computers and networks increased with Digital Subscriber Link (DSL) and cable modem technologies. Without a DSL connection, the computer is assigned a dynamic address each time a person connects to the Internet. Whilst connected on a DSL line, a computer may have either a permanent Internet Protocol (IP) address or a dynamic IP address, depending on the Internet service provider (ISP), although a customer can request a static address. Where a computer has a persistent connection to the Internet, the risk to attack and penetration by a third party is greater. A user is more vulnerable to attack by a hacker by having a permanent IP address.

The general rule with respect to signed documents is this: where a party relies on a signed document and wishes to enforce the document against the signing party, the relying party must prove the signature is that of the signing party, or the document was authorised by the signing party. This is so where the signing party claims they did not sign the document, or if they did sign the document, they did so under duress. It is not for the signing party to prove that they did not authorise the document or sign it.

SHIFTING THE ONUS OF PROOF – *UNCITRAL*

It has been suggested by Adrian McCullagh and William Caelli in their article 'Non-Repudiation in the Digital Environment', http://firtsmonday.org/issues/issue5_8/mccullagh/index.html, that the technical meaning of 'non-repudiation' has the effect of either shifting the onus of proof from the recipient of the alleged electronic signature, or denying the right of the user of the certifying certificate to repudiate the certificate. Whilst it is clear that 'non-repudiation' has different meanings in the legal sense and the technical cryptographic sense, there is a further difference between the two, as pointed out by the same authors. That is the technical meaning relates to events that have taken place after the signature has taken place, and has no relation to the actual mechanism of the affixing of the digital certificate.

McCullagh and Caelli argue that Art.13 of the UNCITRAL Model Law on Electronic Commerce puts the onus of proof on the signatory to prove that the certifying certificate is a forgery. Article 13 reads as follows:

> *Article 13. Attribution of data messages*
>
> *(1) A data message is that of the originator if it was sent by the originator itself.*
>
> *(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:*
>
> *(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or*
>
> *(b) by an information system programmed by, or on behalf of, the originator to operate automatically.*
>
> *(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:*
>
> *(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or*
>
> *(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.*
>
> *(4) Paragraph (3) does not apply:*
>
> *(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or*
>
> *(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.*
>
> *(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.*
>
> *(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.*

The following points are pertinent in relation to the provisions of Art.13:

- The guidance note 83 indicates that Art.13 originates in Art.5 of the UNCITRAL Model Law on International Credit Transfers. This defines the obligations of the sender of a payment order. Bearing in mind such a transfer would normally be subject to a contractual agreement between the parties, setting out the technical procedures agreed between each party (and any other parties in the chain) for such a transfer, it seems improbable that such a provision should affect a public key infrastructure which uses the open network of the internet.
- Guidance note 83 further states that it is not the purpose of Art.13 to assign responsibility between the parties.
- Guidance note 84 reinforces the point of Art.13(1), which is simply that the person originating the message is liable if they sent it.
- Earlier drafts of Art.13 included, according to guidance note 92, an additional paragraph inferring that national law would be used to determine attribution of the authorship of the message.

Whilst the Article as presently drafted does not expressly make this point, nevertheless it seems clear from the provisions of Art.13(1), that the onus of proof has indeed been reversed. The logic can be described as follows:

- If a user chooses to have a certifying certificate, it is assumed that the user will be the only person to use it.
- Where a recipient wishes to rely upon the electronic signature, provided they carry out adequate procedures to demonstrate the authenticity of the certifying certificate under Art.13(5) (i.e. undertake the verifying procedures set out for a digital signature), the recipient

is permitted to assume the electronic signature is that of the sender. In this instance, the recipient is under a duty to carry out such procedures.

- Should the sender dispute they sent the electronic message with the electronic signature attached, it will be for the sender to demonstrate that they did not send the message.

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, and University of London, chaired by David Spinks, Director Information Assurance, and 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.

Stephen Mason

Barrister and Chairman of Pario Communications Limited. He specialises in e-risks, e-business, data protection and interception of communications.

stephenmason@pariocommunications.co.uk

The author wishes to thank Professor Tapper, Peter Howes COO of rchive-it.com, Charles Hollander QC, John Theobald of Ikan plc, Nicholas Bohm consultant to Fox Williams and Alec Muffett Principle Engineer Security at Sun Microsystems Limited, for reading the first draft of this paper and for their valuable comments. All errors and omissions remain with the author.

The Canadian experience with class actions: access to justice or just a new moneymaking product line for lawyers?

by Professor Garry D Watson QC

BACKGROUND

The most significant development in litigation in Canada in the past decade is the emergence of class actions. To understand the introduction of class actions into Canada, and their rapid growth, one needs to appreciate a basic fact – the high cost of litigation and its negative impact on access to justice. As in England, the cost of litigation in Canada is very high, and its impact is much exacerbated by the risks resulting from the loser pay rule (which is not ameliorated in Canada by "before the event" or "after the event" insurance). With the virtual disappearance of civil legal aid (except in family law) the result is that for the average, risk averse citizen, litigation is more or less out of the question unless the individual's damages are very large, liability is reasonably clear, and a lawyer is willing to underwrite the cost of the litigation (on a no win, no pay basis).

Also, in Canada motor vehicle and industrial accident litigation do not play the central role that they do in the English litigation system. As far as industrial accidents are concerned, no fault workers' compensation schemes have replaced common law actions across Canada since the 1930s. Since the 1980s, motor vehicle injury cases have been dealt with by no fault schemes in almost two thirds of the country (Ontario and Quebec) unless a claimants' injuries are "serious and permanent". The relevance of all this is that it makes litigation lawyers hungry for product lines. Before the introduction of class actions, we had little or no mass tort