

A comparison of the risks between the use of manuscript and electronic signatures

by Stephen Mason

A signature serves a number of purposes, the primary function being to provide admissible and reliable evidence that the signatory approves and adopts the content of the document. In so doing, the signatory agrees that the content of the document shall be binding upon them and shall have legal effect, and further, the signatory is reminded of the significance of the act and the need to act within the provisions of the document.

THE MANIFESTATION OF A MANUSCRIPT SIGNATURE

We are familiar with the act of affixing a manuscript signature to a carrier, usually made of paper. Such a signature is usually manifest as being in a particular format, placed upon a document (such as a passport, will, lease, contract) and affixed for a purpose. However, rarely is anything simple when human beings are involved with any action, and it can be of no surprise that the format of a manuscript signature has been the subject of judicial decision-making over the past 250 years. As a result, the following alternative forms of manuscript signature have all been accepted in English courts:

- the use of words other than a name;
- the use of a pseudonym and identifying phrases;
- the impression of a mark, such as a manuscript cross; and
- the use of a seal imprint, rubber stamp, facsimile transmission and telex.

The case law illustrates the pragmatic approach of succeeding judges, whose overriding consideration has been to determine the function of the signature, and for the legal consequences to flow from the function, rather than permit the form a signature takes to affect its validity at law.

THE RISKS ASSOCIATED WITH MANUSCRIPT SIGNATURES

There are invariably a number of risks associated with the use of manuscript signatures, because manuscript signatures are not necessarily reliable. Examples include the variability of the signature, caused by factors such as the onset of arthritis or old age; psychological causes, such as

stress; or the deliberate variation of a signature by a writer to disguise their signature. Alternatively, a signature may be obtained as a result of unconscionable conduct, fraud instigated by a third party or undue influence by a third party. A signature may also be forged.

The criminal courts deal with matters relating to forged manuscript signatures on a regular basis. Quantifying how often a manuscript signature is forged is more difficult, although a recent study by the Cabinet Office in July 2002 (*Identity fraud: a study*) illustrated that the detection of fraudulent applications in the public sector were quite low in the year 2000–01. For instance, there were 1,484 fraudulent passport applications detected, representing 0.03 per cent of the total number of applications. In the same period, there were 564 cases of identity fraud identified by the Benefits Agency Security Investigation Services, and it was estimated that between one and two per cent of transaction value is lost through fraud in the private sector.

THE ELECTRONIC SIGNATURE

An electronic signature can be manifest in different forms, such as the biodynamic version of a manuscript signature; a manuscript signature that has been scanned; the typing of a name on an electronic document; by clicking the “I accept” button placed on a web site; and the use of cryptography to affix a digital signature. The fundamental difference between an electronic signature and a manuscript signature relates to the control of the signature by the user. A manuscript signature is under the total physical control of the individual, whereas an electronic signature will, in all probability, never be subject to the same degree of control (with, perhaps, the exception of mechanisms used by the military and government agencies).

The number of people involved in the chain of an electronic signature indicates the weaknesses of control. For instance, a digital signature can comprise three elements – a key pair (a private key and a public key) and a certificate, which is usually issued by a third party such as a certification authority. A specialist key-generating company may generate the private and public keys; a registration authority may check the identity of the individual or legal entity when an application is made for a certificate, and the certification authority will issue a certificate that acts as a link between the private key and the user of the private key.

The security of the entire structure is, in essence, predicated on ensuring the private key is kept secure, usually by way of a password, or a mixture of password and some other form of authentication, such as a smart card. Either a manuscript signature is signed by the person whose name the signature purports it to be, or it is forged. By comparison, an electronic signature may theoretically be used by any number of individuals for purposes other than legitimate reasons.

SOME RISKS ASSOCIATED WITH ELECTRONIC SIGNATURES

In outline, the range of problems that might cause an electronic signature (in particular, a digital signature) to be the subject of unauthorized use include some of the following noted below.

The properties of the computer system

There are hundreds of thousands of lines of computer code, programmes have thousands of components, and different types of software constantly interact with each other. Unfortunately, systems have emergent properties and do things that are not anticipated by users and designers, and systems also have bugs that cause misbehaviour and result in malfunctions that may not be able to be replicated. The problem is, that the security of a system is based on theory, whilst the real world is far more complicated. An ideal secure system cannot be built, hence there are compromises, such as design trade-offs, unseen variables and imperfect implementation.

Electronic security relies wholly on prevention, generally not the detection, response or auditing of a system. As a result, the prevention strategy only works if prevention mechanisms are perfect, otherwise somebody will manage to circumvent the security.

Storage of the signature or private key

Where a private key is used to create a digital signature, it first must be delivered to the user, then must be retained safely by the user during its useful life. Thereafter, it must be used, stored for as long as is necessary and then destroyed at an appropriate time. If a scanned manuscript signature is used, then the user must ensure the same

considerations apply to the electronic version of the scanned signature – and consideration also needs to be given to how to prevent the recipient from using or misusing the scanned signature when in their possession. Private keys and scanned signatures can be subject to attack, either from within the organization or by a malicious third party. Examples include an eavesdropper that intercepts communications; the breaking of passwords; the theft of a biometric measurement; the theft or copying of tokens such as smart cards; and the inclusion of a Trojan horse on a system that permits a third party to gain access to a system to use a signature at a time of their choosing. Sometimes a hacker will simply crack the security system and replace crucial pieces of software with code in the browser or signing tools to enable them to use a certificate, if a certificate is used with a private key.

Using an electronic signature

Many problems relating to poor security arise from a lack of understanding or training of end users. For instance, where a user has set their security setting to “High” they will have to enter their password every time they wish to enter their private key to affix a digital signature to a message. However, where their security setting is set to the default, “Low”, the messages will be automatically signed without any further intervention by the user. This illustrates that any person with access to a computer containing an electronic signature in a powered-up state will be able to send messages with an electronic signature affixed.

Another alternative is for the user to retain their private key in memory during the login session, depending on how many times a user intends signing messages during the day. If a user keeps the private key in memory, it exposes the key to being stolen. An example includes leaving the computer unattended, thus permitting a third party to take sufficient action to steal the key.

ASSESSING THE RISKS

In discussing the risks between manuscript and electronic signatures, it is obvious that in both cases a person can either sign a document with a manuscript signature or with an electronic signature, and then maintain that they did not cause the signature to be affixed to the document. In theory, this will then leave the party relying on the signature to prove the signature was affixed by the signing party. However, governments across the world have altered this burden in relation to electronic signatures, and it is possible that the signing party may be considered to have signed the electronic document where an electronic signature has been used, although this issue is not considered in this paper.

The overall risks between the two types of signature can be simplified, as discussed below.

Using a signature without authority

Both a manuscript signature and an electronic signature can be used without authority. Once a fraudster has obtained a specimen of a manuscript signature, they can try to replicate the signature. The person whose signature is forged will not necessarily know their signature is being used until after the event, although if a cheque book or credit card has been stolen, the owner will be aware that attempts might be made to forge their signature.

There is a vague possibility that a forged signature may be noticed at the point of use, but is it unlikely. As for an electronic signature, one such a signature has been taken, the user may not be aware until well after the event. There may be no physical evidence of loss, because digital copies are so easily obtained. In the case of a scanned manuscript signature, it is merely a matter of replicating the relevant file. With a digital signature, access must be gained to the private key, but this is not impossible, especially if retained on a smart card. Whilst a digital signature, if accompanied by a certificate, has an expiry date, nevertheless an unauthorized party will not lose any time in using the device for their own purposes well before the certificate expires.

Who is responsible

The forgery of a manuscript signature does not expose the person whose signature has been forged to any liability. However, the law is far from certain in relation to the use of electronic signatures, because it appears that a reversal of the burden of proof, and the provision of presumptions in legislation, may mean the person with an electronic signature may find themselves liable, depending on the facts. If this is the case, the party utilizing an electronic signature may well have to consider the risks attendant upon the use of such a device. This will be particularly important in relation to electronic conveyancing.

Assessing the risk


In assessing the nature of the risk, several factors can be taken into account. First, who bears the risk? Banks, if they are not required by legislation to shoulder risk, will allocate the risk to other parties. Thus the risk with credit cards tends to be with the merchant. Until recently, credit card providers required the user to authenticate the debit of their account with a manuscript signature. However, since the introduction of cards with a personal identification number (PIN) in France and other European countries, the United Kingdom and USA are reluctantly following this example.

Whilst the use of a PIN number is not a signature (it is merely a shared secret between the card issuer and the recipient), nevertheless the use of a PIN can reduce the risk associated with the card. The economics relating to

credit cards and debit cards using a manuscript signature and those using a PIN are of interest. Retailers in the USA took legal action against the credit card issuers in an attempt to stop them from charging high rates for processing cards using manuscript signatures to authorise a transaction. Apparently, merchants paid issuers of Visa and Mastercard US\$4.67bn for transactions that were processed with manuscript signatures, compared to US\$715.3m paid to banks that issued PIN based cards. The difference in charges is so significant that it is understandable the retailers decided to take action to rectify this position.

Another issue to consider is the degree of risk. With low value transactions, it can make sense to rely on a shared secret such as a PIN, between the card issuer and the customer. However, where a high value transaction is being negotiated, it may be wise to rely on manuscript signatures to sign a contract, rather than electronic signatures. The cost of the security to ensure that the electronic signature is not compromised will be far greater than the cost of printing a document in duplicate and requiring both parties to sign and countersign the relevant agreement using a writing instrument.

The risks will depend on the consequences faced by the parties and how the relationship between the two is governed in law. At present, it can be argued that the move towards electronic signatures is rapidly altering the burden of proof in relation to the signature. The British government has already passed a number of statutory instruments that have, effectively, reversed the burden of proof in relation to the use of electronic signatures.

There is no question that the government, which is in a far better position to pay for and institute a proper means of authentication, is placing a very onerous burden on subjects, should the subject decide to interact with government online. It will be mandatory for all organizations to submit their tax affairs to the Inland Revenue by 2010, yet many thousands of organizations will have no concept of the risks they face when submitting to such a regime, and will not be in a position to afford the costs of providing for proper security of their electronic signatures. One thing is certain: we can expect to see many problems over this issue in the future. 

Stephen Mason

Barrister, St Pauls Chambers, Leeds

This article is based upon the lecture given by Stephen Mason entitled "A comparison of the risks between the use of manuscript and electronic signatures" for the Society for Advanced Legal Studies on 8 May 2003. The author's book, *Electronic Signatures in Law* is to be published by Butterworths in the autumn of 2003. Details on the Butterworths web site.

© Stephen Mason 2003