

# Electronic signatures: a risky business

Stephen Mason sets out the types of electronic signature currently in use and some of the risks when relying on them

Between 2002 and June 2003, three pilot schemes for sending prescriptions electronically were run by three consortia: Flexiscript, Pharmacy2U and TransScript. The Government now proposes to amend the Prescription Only Medicines (Human Use) Order 1997, and to permit prescriptions to be transmitted electronically. It is intended to use so-called "secure" advanced electronic signatures under the provisions of the proposed amendments to the order. Those doctors and pharmacists who intend to take advantage of sending and receiving prescriptions electronically, might like to become more fully aware of what constitutes an electronic signature and the effect that an electronic signature can have.

## Forms of electronic signature

An electronic signature can take several forms. These are described below.

**Clicking the "I accept" icon** When buying goods or services on-line or when installing software on a computer for the first time, the buyer is, invariably, required to click on the "I accept" icon. The action of clicking on this icon has the effect of satisfying the function of a signature. This analysis is also in keeping with the decisions made by judges over the past 200 years regarding the form that a signature may take. In English law, the validity of the signature depends on the function it performs, not necessarily the form it takes. Even if the act of clicking on an icon to order goods or services is less secure than providing a handwritten signature, it is still valid as a signature.

### Typing a name into an electronic document

When a person types his name on to a file in electronic format, such as an e-mail, the text added is an electronic signature. This form of electronic signature was discussed and challenged in *Hall v Cognos Limited*. Mr Hall was employed as a sales executive and his expenses were reimbursed in accordance with a policy which stated that all expenses over six-months old would not be paid. Mr Hall failed to submit a claim covering the period December 1995 to June 1996. By January 1997 he wanted paying. A series of e-mails were subsequently exchanged between Mr Hall, Keith Schroeder (his line manager) and Sarah McGoun from personnel, in respect of the late payment. Mr Hall asked if the late submission was "OK with you?" and his line manager replied, "Yes, it is OK." The e-mails were signed "Sarah" and "Keith" respectively. The claim was inflated, and Mr Hall was

dismissed without payment. By clause 19 of Mr Hall's contract of employment, amendments or variations had to be in writing and signed by the parties to be effective. At issue was whether or not the exchange of e-mails between Mr Hall and his line manager varied the contract of employment. It was determined in this case that the printed version of the e-mail was in writing and signed. It constituted a variation of the contract of employment, although the printed version was merely a copy of the original version in electronic format. This decision demonstrates that a signature typed into an electronic document is acceptable as a form of electronic signature. The line manager intended Mr Hall to act upon the exchange of e-mails, and Mr Hall relied upon the assurance made by the line manager. The inclusion of the personnel department in the negotiations served to reinforce the authority of the line manager to vary the contract.

### Biodynamic version of a manuscript signature

There are products available that permit a person to produce a digital version of their handwritten signature. The person writes their signature by using a special pen and pad. The signature is reproduced on the computer screen, and a series of measurements record the speed, rhythm, pattern, habit, stroke sequence and dynamics that are unique to the individual. The subsequent file can then be attached to any document in electronic format to provide a signature.

### A handwritten signature that has been scanned

A handwritten signature can be scanned from paper and transformed into a digital format. The signature can then be attached to a document. This version of a signature is used widely in commerce, especially when marketing materials are sent through the postal system and addressed to hundreds of thousands of addresses.

**The digital signature** In simple terms, 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. When an electronic message is signed with a digital signature, the private key is used to associate a value with the message using an algorithm. The computer undertakes this task. The value, the message and a certificate, linking the key to the named person or entity, is then sent to the recipient. The recipient uses the public key to check the value is correct by "unlocking" the value created by the algorithm. A computer undertakes the entire operation. The only action required of the human being (in theory) is to cause the computer to associate the digital signature to the message.



Jane Smith

## What the Government is proposing

The Government proposes to require prescriptions to be signed using an advanced electronic signature, because, it is asserted, that this form of electronic signature is more secure. The definition provided in the covering letter (MLX 310) that sets out the proposals is taken from The Electronic Signatures Regulations 2002, which in turn is taken from the EU Directive on electronic signatures. The Electronics Communications Act 2000 (which recognises electronic signatures in law) has not altered the underlying flexibility of the meaning of a signature in English law. An electronic signature does not have to be in the form of digital signature for it to be accepted as a signature. The rules that apply to electronic signatures will apply equally to the concept of an advanced electronic signature, which is an invention of the EU Directive.

According to the Directive, the elements of an advanced electronic signature are that it is:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created using means that the signatory can maintain under his sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

However, an analysis of the definition shows that advanced electronic signatures are not special, nor any more secure or advanced than any other form of electronic signature. First, no electronic signature can be uniquely linked to the signatory. For instance, a user relinquishes control over their scanned signature once it has been sent. A digital signature is not linked to the person creating it: the unique link is made with the private key, not the user. Moreover, nobody remembers their

**Stephen Mason** is a barrister and the author of *Electronic Signatures in Law* (LexisNexis Butterworths, 2003). He can be contacted at [cwm@stpaulschambers.com](mailto:cwm@stpaulschambers.com)

private key, because it is far too complicated. As a result, private keys tend to be retained on a computer, disk or smart card.

Second, any form of electronic signature is capable of identifying the purported person that signed it. Third, any form of electronic signature can be created under the sole control of the user, but when a private key is used, a recipient will not know whether it was the owner that actually used the private key. Finally, the only form of electronic signature that is capable of complying with the fourth element is the digital signature, but even a digital signature is not immune from attack from determined criminals.

The proposals put forward by the Government have not mentioned the additional requirements that must be met for a signature to be considered "advanced". An advanced electronic signature must be based on a qualified certificate, which must comply with a substantial list of requirements, as set out in Annex I of the EU Directive, and replicated in the Schedule to the Electronic Signatures Regulations. It is not appropriate to discuss the minutia of the requirements in this article, only to warn the reader that the infrastructure involving the use of advanced electronic signatures can involve a number of players, each of whom will attempt to limit their liability while requiring users to pay substantial set-up costs and annual payments. For instance, it seems the Government is going to use digital signatures that require a doctor and pharmacist to have a key pair that may be issued by one organisation, and an individual identity certificate, which may well be issued by another organisation. The individual identity certificate acts to bind the identity of the private key to the identity of the person whose key it is. Even where the same authority issues both, checking the identity of the person or organisation that applies for a digital signature may be undertaken by yet another organisation, a registration authority.

**Keeping private keys secure** The doctor or pharmacist has the duty of securing the private key, while the recipient will probably be required to confirm whether or not the key has been revoked by the sender (for instance, that the sender has become aware that it has been stolen or used without their authority) before relying upon it. Potential liability lies with the doctor or pharmacist for not securing their private key properly, and with the recipient if he fails to confirm it was the sender that sent the message. It will be interesting to see what procedures will be put in place to resolve these issues, and who will be liable if something goes wrong.

One form of keeping a private key relatively safe is by placing the key on a smart card. The key can be protected with a code, so the doctor or pharmacist that buys the key can only use the key when they type in the relevant code — much like a PIN code for a bank card. With smart cards, the number of parties that will bear a risk will vary, depend-

ing on how a key is added to the card. So, if the keys are added to the card during production, the producer could fail to ensure the copies of the keys are properly destroyed after being added to each individual card, have insufficient security in place to prevent keys being siphoned off before they are added to cards, or fail to destroy the keys held in its computer after the keys are added to the card. The possibilities for organised crime are, potentially, enormous.

**Other uncertainties** Bearing in mind the ease by which any number of computers across the world can be hacked into, it will be readily noted that whatever the form of electronic signature used, most disputes, when they occur, will centre upon whether or not a signature was affixed to the message by the purported sender — the recipient will never know who caused the electronic signature to be used. Even the use of an advanced electronic signature does not guarantee that the purported sender caused the computer to create it or that he used the smart card.

Consider the following problems in relation to each of the different forms of electronic signature. When you receive an e-mail:

- With a name typed on the bottom of the e-mail, how do you know the person who sent the e-mail is the person whose name is typed into the bottom of the e-mail?
- With a biodynamic or scanned version of a handwritten signature, how do you know if the person whose biodynamic or scanned signature it is, has attached the file to the e-mail? What if they have used the file containing the signature thousands of times, so thousands of people from across the world have the file with their biodynamic or scanned signature on their computers? What if a criminal has obtained the file containing the biodynamic or scanned signature?
- With an advanced electronic signature, how do you know the purported sender caused the key to be affixed to the message? What if their computer was hacked into and a hacker sent a message with their key?

The important issue is proving the sender was the one that affixed the signature to the message, not the type of signature that was used.

The technical community thinks it has a solution to the problem. Technical people use the term "non-repudiation", which has, in turn, become part of the vocabulary of digital signatures. When this term is used in an engineering sense, it can mean that there is a high (and specifiable) degree of probability that it can be proved that an e-mail, with a digital signature attached, was sent from your computer. The technical community, therefore, argue that if it can be shown that an e-mail was sent from your computer with a digital signature attached, then it was you who sent it. As any reader will readily notice, this logic

is flawed — anybody with access to your computer could send a message. Perhaps your computer has a number of Trojan horses on it that you are not aware of, and one or more of these malicious items of software could enable a hacker to enter your computer without authority and to send e-mails at will, as well as affixing your digital signature to the message.

## Concluding remarks

The Government claims that transmitting prescriptions electronically is expected to provide significant benefits to patients and to those writing and dispensing prescriptions. No evidence has been adduced to set out what the benefits are or to indicate the costs of such an imposition. A range of questions immediately spring to mind, including:

- How much will the software cost?
- What upgrades will be required to computer systems?
- Will advanced electronic signatures be compatible across different types of computer?
- Will users be able to decide which form of advanced electronic signature they use?
- Who will pay for users to be registered with certificate authorities?
- Who will pay for the annual costs of maintenance and to replace the private keys each year?
- Who will be responsible for the additional security measures required to ensure a private key is not compromised on a computer?
- How will a user know when their private key is compromised, so that they must cancel it?
- Who will be liable if a private key is used to obtain drugs illegally?
- Who will be responsible for storing old private keys?
- How long will they need to be stored for?
- How will keys be managed?

The Law Society of Scotland abandoned a similar project (Lawseal), partly because too many questions remained unanswered, but also because of cost.

The present proposals demonstrate that the Government has failed to grasp that the technology it intends to use is flawed. Better and less expensive models exist that can be used. For instance, the Dutch bank, Postbank, has operated its Girotel system for a number of years. A user is given an identification number. The bank then issues a list of transaction codes on paper. Each time the user enters the system, they use the next transaction code. A new list of codes is issued as the old codes are used up.

While this system is not foolproof, at least the user knows when their paper has been stolen or used without authority — unlike an advanced electronic signature. This represents a good balance of technology and old world familiarity, using the best of both. Let us hope the Government grasps the error of its assumptions.

© Stephen Mason, 2004