Electronic signatures in practice

by Stephen Mason, Barrister, British Institute of International and Comparative Law, UK

The internet and e-mail are now considered to be the main conduits of communication for commercial enterprises as well as public organisations.

Thousands of contracts are entered over the internet every day, whether it is to buy something on a website or by way of an exchange of e-mails. Before the internet, we did not take very much notice of how we entered contracts, because we thought we knew what a signature was. As far as English law is concerned, a signature can take many forms, because it is the function a signature performs that makes it effective, not whether it is in the correct form. This article considers the types of electronic signatures that are currently in use, and considers some practical issues of proof.

Before the use of electronic signatures, successive judges in England and Wales, as well as other common law countries, took the view that the form a manuscript signature takes is not relevant, providing the function the signature performs is clear from the evidence. This pragmatic view of the imperfections of human behaviour has enabled judges to widen the concept of a signature, so that a signature can be evidenced in a variety of ways, such as a partial signature, the use of initials, a stamp, and a cross, to name but a few examples.

Forms of electronic signature

There are various types of signature, all of which can demonstrate the intent of the signing party to authenticate the document. The different types are:

- When a person types their name on to a file in electronic format, such as a letter, e-mail or other form of document, the text added is a form of electronic signature. This was the subject of discussion in England and Wales in the case of Hall vs. Cognos Limited. In this case, the chairman of the tribunal determined that a name typed into an e-mail was a form of signature. Although no relevant case law was mentioned in this instance, the decision was consistent with decisions made by judges in England and Wales since the seventeenth century, illustrating that the function of a signature overrides the form it takes. Case law applying electronic signature statutes in the United States of America indicates the acceptance of this form of electronic signature, as does a recent case in Singapore.
- The 'click wrap' method of indicating intent, namely clicking the "I accept" icon to confirm the intention to enter a contract when buying goods or services electronically.
- A personal identification number (PIN), used to obtain money from cash machines or to 'sign' a credit card with a PIN.

The form of an electronic signature will have a bearing on its legal and evidential effect.

- A biodynamic version of a manuscript signature; a special pen and pad measure and record the actions of the person as they sign. This creates a digital version of the manuscript signature. The file can then be attached to electronic documents.
- A scanned manuscript signature; a manuscript signature is scanned and transformed into digital format, which can then be attached to an electronic document.
- The digital (or hash cryptographic) signature, which uses cryptography. A very simple explanation serves to illustrate how a digital signature works: 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.

The form of an electronic signature will have a bearing on its legal and evidential effect. However, it should also be observed that the elements that make up the definition of an electronic signature, and the presumptions that apply, will also affect its legal acceptance in a given jurisdiction. It should be noted that there is no world-wide accepted definition of what constitutes an electronic signature. Furthermore, there is no agreement about the elements of an electronic signature, nor is there any agreement about the functional equivalence of an electronic signature. Finally, there is no clarity about the evidential presumptions relating to the use of electronic signatures.

The functions of a signature

Of interest is the way electronic documents are authenticated. The role of the notary public is less well known in common law countries, although it is interesting to note that the National Notary Association of the United States of America has appointed a Director of eNotarization. The approach taken by the State Bar of Notaries in Austria demonstrates that it is possible to provide for the authentication of documents electronically, given the legal framework established in Austria. It will be interesting to observe whether greater use of such services will become ubiquitous.

Invariably, the authentication of a document will depend on the function a signature performs. In summary, a signature can serve a number of functions, some of which are set out below, each of which can have varying degrees of importance:

- The primary evidential function, serving to provide admissible and reliable evidence

that the signatory approves and adopts the contents of the document, and to demonstrate that is shall be binding upon the parties and shall have legal effect.

- Secondary evidential functions, for instance where a signature is capable of authenticating the identity of the person signing the document.
- Cautionary function, where the signature acts to reinforce the legal nature of the document.
- A protective function, in that there is tangible proof of the source and contents of the document.

Enforceability

Several factors will have a bearing on the enforceability of an electronic signature. They include the elements that define the signature, provisions relating to form and any presumptions that apply. Each will be treated briefly in turn.

Elements

The elements that make up the definition of an electronic signature can demonstrate difficulties for the international acceptance of a particular form of signature. For instance, the UNCITRAL Model Law on Electronic Commerce provides, in article 7(1)(a) for methods that are used to identify a person, and to indicate their approval of the information contained in the message. Whilst not precluding any other form of electronic signature, this definition presupposes that only a digital signature will suffice. This is reinforced by the provisions of article 7(1)(b), which discusses the issue of reliability and whether the form of signature is appropriate in the circumstances. The problem is that reliability does not demonstrate a link between the owner of the signature and the act of affixing or linking the signature to the data message.

The same comments can be made in relation to the EU Electronic Signature Directive, in that the electronic signature under the provisions of article 2(1) serves as a method of authentication. Unfortunately, this definition fails to link the need for the electronic signature to authenticate the data to which it is attached or logically associated. It is not clear whether the authentication relates to the origin of the data, or acts to verify the identity of a person or entity.

By contrast, the United States has approached the definition by taking a functionalist approach, as set out in section s106(5) of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7003 2000:

"(5) ELECTRONIC SIGNATURE. - The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

The definition provides a number of elements, the most important of which is that the signature is "adopted by a person with the intent to sign the record." This part of the definition permits any form of electronic signature to effect the function of demonstrating intent.

In summary, the elements of an electronic signature differ from jurisdiction to jurisdiction. Whether this will ever have an effect on trade is another matter. At present, there is little evidence that such differences have any bearing on international trade in practice. However, given that the use of e-mail has become common, it is probable that contracts are formed every day with the exchange of e-mail communications, both by individuals and business, and across international boundaries. Where a challenge is made over the use of an electronic signature, care must be made to become more fully aware of the intricate details of the relevant statutes relating to electronic signatures. An example is the Greek case of No 1327/2001 – Payment Order, before the Court of First Instance of Athens. In this case, a Czech agent concluded a service agreement with a Greek travel agency by way of an exchange of e-mail correspondence. A dispute occurred, and the judge upheld the complaint of the Czech agent by recognising the validity and the binding effect of the legal acts that were exchanged through the e-mail communications. The judge accepted the probative force of the e-mail exchange in this instance.

Provisions relating to form

A document may only be acceptable for certain types of transactions if it conforms to a particular form. Examples include the formation of a will, the sale or lease of land, or the assignment of intellectual property rights. Whether a transaction complies with the necessary form will depend on the applicable law, or both the applicable law and any relevant rules of evidence. Rules of evidence may be express or implied, and such rules may serve to limit the ability to use the evidence of an electronic signature to demonstrate either the attrition of a message to its purported originator, or whether an electronic signature is an appropriate method to meet the formal legal requirements of a signature.

The interpretation of form varies between jurisdictions. The liberal approach is illustrated by an example from the United States of America in the case of a breach of contract. In Cloud Corporation vs. Hasbro, Inc, the defendant denied placing orders. The parties communicated by way of e-mail, and the appeal court held that the sender's name in an e-mail satisfied the signature requirement of the statute of frauds. In the Columbian case of Juan Carlos Samper Posada vs. Jaime Tapias, Hector Cediel and others, the defendants sent unsolicited commercial e-mails to Mr. Samper. Mr. Samper sent e-mails to the defendants asking them to stop sending him spam. The defendants repeatedly assured Mr. Samper that they would take him off the e-mail list, but failed to do so.

He had to take legal action to stop the unwanted e-mails. Of interest was the assertion by the defendants that the court was not empowered to hear the matter, because both parties lived in Bogotá. However, the learned judge indicated it was rather ironic that defendants who used cyber space should argue over the venue for a court case. In addition, the defendants argued that the court proceedings were not valid because they did not include the use of digital signatures. In response, the judge indicated that where regulations require the information to be sent in writing, an e-mail is sufficient, provided the parties are able to obtain access to the e-mail at a later date.

The French courts have taken a more restrictive approach, although it should be noted that the case mentioned below pre-dates the introduction of the French law on electronic signatures, and the decision may well be different now. In the case of Société Chalets Boisson vs. M. X the council of the Society Chalets Boisson entered an appeal before the Cour d'Appel of Besançon against a decision of a Conseil de prud'hommes (employment tribunal). The notice of appeal was sent to the office of the clerk of the court by e-mail, bearing an electronic signature. The defendant sought to have this appeal declared invalid, because the electronic signature was deemed not to identify the signatory. The Cour d'appel of Besançon accepted this argument and then declared this appeal inadmissible. The Cour de Cassation approved the Cour de Besançon decision. For an order to be valid, an appeal must be signed by its author and that an electronic signature, at the material time of these events, was deemed insufficient to identify the author. The comments by Philippe Bazin bear repeating:

"…. judges at the time (and unfortunately still today) did not have any technical understanding about what these notions concretely represent. These that they know, they have practised for a long time, and they have to do with paper, not the electronic environment.

In the 30th April 2003 decision, the Court adopted a systematic position of mistrust with respect to the electronic signature. It confirms that – culturally – it is the paper, and only the paper, that constitutes the only solid legal guarantee."

In some jurisdictions, it may well be that this attitude might persist for some time.

Presumptions

Where an electronic signature is considered as a functional equivalent of a manuscript signature, some countries have included a number of presumptions in the legislation, such as article 3 of the Japanese Law Concerning Electronic Signatures and Certification Services (Law No.102 of 2000). The recently enacted Electronic Signatures Law of People's Republic of China has a similar presumption, as set out in Article 9, which is subject to a number of conditions:

- A data message is deemed to be sent by the originator if any of the following conditions has been met:
- It was sent under the authorisation of the originator;
- It was sent automatically by the originator's information system;
- The addressee verifies and ascertains the data message by a method ratified by the originator.
- If the parties have agreed otherwise, such agreement prevails.

To a certain extent, the presumptions illustrated above demonstrate that the same presumptions apply in the digital world as they do in the real world in relation to manuscript signatures. The difference may be with respect to the costs of proof: evidence in digital format is more expensive in terms of the expertise required to analyse a computer or computer network. In this respect, lawyers, to fully advise their clients when dealing with international contracts, must be aware of the differences between jurisdictions with respect to the legal presumptions that apply to difference forms of electronic signature.

Concluding remarks

As demonstrated in this article, it is necessary to be aware of the presumptions relating to the use of electronic signatures across jurisdictions. What might be acceptable in one jurisdiction will not necessarily be enforceable in another, unless due care has been taken to establish whether the format of a particular form of electronic signature is enforceable. It is too early to predict how electronic signatures in a formal context will develop, but the rush by legislators across the world to provide for the complexity of digital signatures as a functional equivalent of a manuscript signature was somewhat premature. Click wrap signatures did not require any form of legislation, yet this particular form of signature remains a form of electronic signature, despite the imposition of a highly technical response by way of legislation to what is a relatively simple legal issue. For lawyers, the central issue will be how to prove the nexus between the application of the signature, whatever form it takes, and the person whose signature it purports to be. Even where there is a presumption that the person used a digital signature whose signature it was issued to, there remains in the legislation the possibility of challenging such a presumption.

Stephen Mason is the author of Electronic Signatures in Law (LexisNexis Butterworths, 2003), UK and is general editor, Digital Evidence Journal incorporating the eSignature Law Journal.

Contact Stephen Mason,
stephenmason@stephenmason.co.uk