Editorial

As we enter the digital world, so the importance of electronic signatures will begin to take hold amongst lawyers, people in business, the public services and members of the public. Millions of people around the world use what is probably the most popular form of electronic signature in daily use: that of their name typed into an electronic document, mainly in an e-mail. Another form of electronic signature that is used frequently is the electronic equivalent of the manuscript form of a cross – the 'I accept' or 'I agree' icon, used on web sites and software to indicate the signatory intends to enter into a contract or accepts the terms of a licence. Of interest, is that most of the people that use these forms of electronic signature, including those who espouse the use of digital signatures, are not aware that they are using an electronic signature.

Politicians have rushed into drawing up laws in relation to electronic signatures, often in ignorance of the concept, having been drawn into the promises made that digital signatures can solve issues, to the exclusion of other forms of electronic signature that have proved to be more popular and robust than imagined. In a desperate attempt to indicate they are 'digitally savvy', politicians have also pressed ahead with expensive and ambitious plans to encourage or enforce individuals to use digital signatures when corresponding with e-government services. In the same breadth, politicians have placed a heavy burden on those individuals that communicate with e-government, because the government refuses to verify the digital signature that is used. This places an onerous burden on the individual, because it many instances when an individual obtains a digital signature and uses it, it is assumed that they have either used or authorized the use of the signature. It is no wonder that the people of Denmark have failed to take up the offer of obtaining a digital signature, as described by Jan Hvarre in his article.

The use of electronic signatures poses the usual threat to any person or organization relying on a signature: how do you verify the signature is of the person it purports to be and can it be trusted. The concept of a digital signature is supposed to resolve this conundrum, but does not. Whatever the format an electronic signature takes, the evidential issues will remain the same if the signature itself is in dispute. Lawyers will have to rely on experts to investigate the digital evidence to determine whether an electronic signature was used. In such circumstances, the evidential weight to be attached to an electronic signature may well depend upon the digital audit trails that can be adduced to demonstrate the use of the signature. Even if an electronic signature can be proved to have been used, it will not follow that the person actually caused the electronic signature to be affixed. Once the risks attached to the use of electronic signatures are more widely understood, it is possible that more people might challenge the formation of contracts in their name. This will, if such a circumstance comes to pass, cause major problems for everybody relying on electronic signatures to enter legally binding contracts electronically.

This journal seeks to bring into focus the legal and practical issues relating to electronic signatures, in the widest sense. This includes lawyers, academics, cryptographers, technicians and vendors of practical solutions. Without the support of everybody connected with electronic signatures and the variants of signature available, there will be a failure to more fully understand the range of problems that need to be discussed and overcome. This journal seeks to provide a platform to encourage an open and honest debate on the issues.

The editor wishes to thank the contributors of this inaugural edition of the journal, and hopes to see some exciting and meaningful articles and debates in future editions.

This journal seeks to bring into focus the legal and practical issues relating to electronic signatures, in the widest sense

Editorial

Few end users of technology understand the security issues, and even fewer numbers of people understand the problems relating to digital forensics

It is becoming increasingly common for both commercial and public organizations to use computers that are connected to internal and external networks. As a result, users have begun to alter the way they conduct business. There is nothing new in this, as the reader will readily note. However, the electronic environment presents a range of problems that are little understood by end users. Few end users of technology understand the security issues, and even fewer numbers of people understand the problems relating to digital forensics. Of course, the media regularly reports on criminal acts that are perpetrated by using a computer and a connection to the internet, and the proliferation of unsolicited bulk e-mail, viruses and spyware are also reported in accordance with the space available when a story is considered to be worthy of reporting. However, reporting on the problems that regularly occur will not resolve how people interact with computers, especially when they are connected to an external network, such as the internet.

Of interest is the way the move towards the electronic environment has caused a wider range of people to become more fully aware of issues that they would not be involved with in the normal course of events. One example is how to store electronic documents, images and databases that increase in size each day. In the past, somebody in the organization would have been responsible for ensuring that documents were retained in accordance with the law, regulations and best practice. This person would also dispose of the documents in due course, or haul them off to a store somewhere in the blue yonder. This problem is now affecting the IT manager and a larger number of people in the organization than hitherto. This is because fewer documents are filed in cardboard folders and put into filing cabinets. They are stored in computers.

Another issue that has yet to be more fully understood relates to the authentication of electronic documents – principally correspondence sent by e-mail, although the problem is the same for all documents transferred electronically. As observed in the case report from Greece, and the case note from France Société Chalets Biosson v M. X., when people are made aware that typing their name into an e-mail is a form of electronic signature, their first response is to ask the question 'Is it safe?' The reply to this question is: 'You have asked the wrong question'. Nobody asks the question 'Is it safe?' when presented with a manuscript signature on a letter with the name of a firm, company or public body printed on the paper. Yet the entire letter may be a fabrication. The manuscript signature and the name of the firm or company may be forged or not even exist. The real question to be asked of any signature (whether in electronic format or a manuscript signature) is this: 'Is there sufficient evidence to trust the signature?' If not, the recipient needs to ask themselves what action they should take to confirm the signature is that of the person whose signature it purports to be.

To a certain extent, many of the articles in this issue of the Journal address this very issue. The problem is usually considered from the point of view of the digital signature. Where a person or organization intends to use a digital signature, the focus should be on the accuracy of the registration process, and a number of articles discuss this point.

The digital signature presents a number of very serious issues in contract and tort that are addressed elsewhere. Considered to be an answer to the problem of authenticating a sender, the public key infrastructure (PKI) as it is called, does not succeed very well. However, the use of digital signatures can succeed within a closed PKI, such as Identrus and, more recently, the new system introduced under the name BACSTEL-iP, mentioned in the News section of the Journal. This is a good example of a semi-closed multiple PKI, where the rights and duties of the various parties are enforced by way of contract. This use of a PKI mechanism illustrates what can be achieved using a PKI model. In effect, a closed PKI system can enforce security procedures on end users and educate them to the practical problems at the same time.