ARTICLE
APRIL 2012

Electronic signatures: are we getting there?

Rob Sumroy and **Brett Sherrard** of **Slaughter and May** look at the law and practice of electronic signatures, and assess how it has developed alongside the growth in e-commerce.

The use of signatures in paper transactions has developed over many years as a means of achieving certainty of the identity and authority of the contracting parties. Parties to transactions receive comfort as to the authenticity and integrity of the transaction documents from the signatures, seals or other accepted marks applied to them (*see box "Manual signatures"*).

The challenge and the commercial imperative for the success of e-commerce has been to find the electronic equivalent of the signature. Yet, despite the availability of a wide variety of technology solutions which allow parties to use electronic signatures with a level of certainty comparable to that of using handwritten signatures, and the existence of a legal framework that recognises the validity of electronic signatures, the take up and use of electronic signatures within e-commerce in Europe remains relatively low.

This article looks at the current position on the law and practice of electronic signatures, and considers future developments in this field.

ELECTRONIC SIGNATURES

Before carrying out a transaction electronically, a trader will want to be able to identify reliably the other parties involved.

As with manual signatures, there are a number of ways of "signing" in the electronic world (*see box "Types of signatures"*). Some, like typing a name at the end of an email, or clicking a website button, provide little security or certainty as to the sender's identity. To achieve a level of certainty comparable to a handwritten signature, an electronic signature needs to be:

- Unique to the signatory.
- Created using means within a signatory's sole control.
- Capable of being linked to the relevant document or data in such a manner that any subsequent changes to that document or data would be detectable.

The most common methods of achieving an increased level of certainty in relation to an electronic signature are to use cryptography technology, or to have that electronic signature certified by an independent trusted third party.

Encryption

There are two main methods of cryptography used for the purposes of creating electronic signatures:

Symmetric cryptography. This ensures confidentiality through the encryption of a message using a software "key" based on a mathematical algorithm. The encrypted message can only be unscrambled, or decrypted, using that same key. In order to ensure confidentiality, the key must be kept secret between the two parties.

MANUAL SIGNATURES

Manual signatures play three important roles:

- They identify the signatory.
- They provide certainty as to the personal involvement of that person in the act of signing.
- They associate that person with the contents of the document.

Over time, various methods have developed for achieving these aims (*see box "Types of signatures"*).

The measure of certainty that the recipient will get as to the sender's identity depends on the method used. For example, the recipients of a letter from Slaughter and May may be satisfied that the sender is a Slaughter and May solicitor merely because the letter is typed on the firm's notepaper. It may be assumed that access to the firm's notepaper will be limited to those who have authority to use it. The addition of the sender's handwritten signature will give more certainty (particularly if it can be checked against one previously received). Even more certainty as to the sender's identity is achieved if the signature is witnessed under oath or notarised.

The level of certainty required by the parties (and therefore the mode of signing agreed on) will depend on the level of risk that each party is willing to accept regarding the identity of the other party and the authenticity of that party's actions.

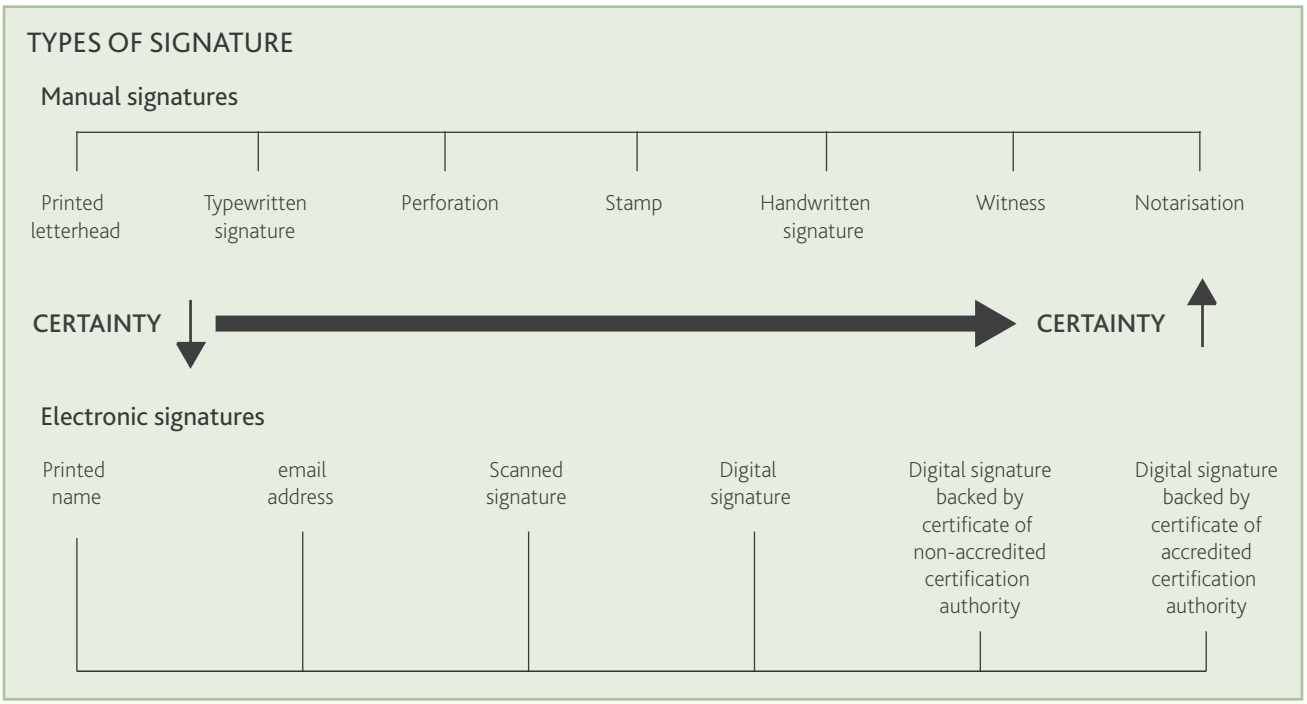
While this may be appropriate for the signature of an important or high-value contract, it will not be suitable for all circumstances. For example, a requirement for an e-commerce trader to share a secret key with each of his customers and suppliers is neither practical nor commercially viable.

Public key (or asymmetric) cryptography. By contrast, public key cryptography is ideal for the creation of electronic signatures (an electronic signature created within public key encryption technology is often referred to as a digital signature).

Public key cryptography uses two keys: a "private key" and a "public key", known as a key pair. Messages are encrypted with one key and can only be decrypted with the other key. As the names suggest, the private key is known only to the owner whereas the public key is made publicly available. The two keys are mathematically related but are constructed so that it is not technically feasible or is prohibitively expensive to calculate the private key when a party only has access to the public key.

When this technique is used for electronic signatures, the private key is used by the sender of a message to encrypt either the message itself or a computer-generated "fingerprint" of the message known as a "digest". It is common for just the message digest to be encrypted rather than the full message as this is a much smaller data file and is therefore quicker to encrypt. The encrypted message digest becomes the electronic signature and will be sent to the recipient with an unencrypted copy of the message (*see box "Creating an electronic signature"*).

Anyone with access to the public key (which might, for example, be available on a website or may be sent with the electronic signature) can use it to decrypt the message digest, so verifying that the message could only have been signed by someone with access to the private key. The recipient will also check that the message has not been altered or tampered with by generating its own message digest for the received message and comparing it with the decrypted message digest. Any alterations to the received message would mean that the two message digests no longer match (*see box "Validating an electronic signature"*).



Certification authorities

One disadvantage to encryption technology is that encryption key pairs may be forged, stolen or created by a fictitious identity.

Digital certification is one method used to manage this risk and to add an additional layer of authentication to an electronic transaction. A sender who wishes to provide certainty as to his identity can procure a digital certificate from a trusted third party known as a certification authority.

The certification authority will verify the identity of the sender (for example, for an individual through checking passport details, and for a corporate entity through checking corporate documents and returns) and will issue a digital certificate (signed with the certification authority's own digital signature for verification of its authenticity) which will verify that the sender is who they claim to be. That digital certificate can then be appended to a message or a digital signature to verify the identity of the sender.

An example of use

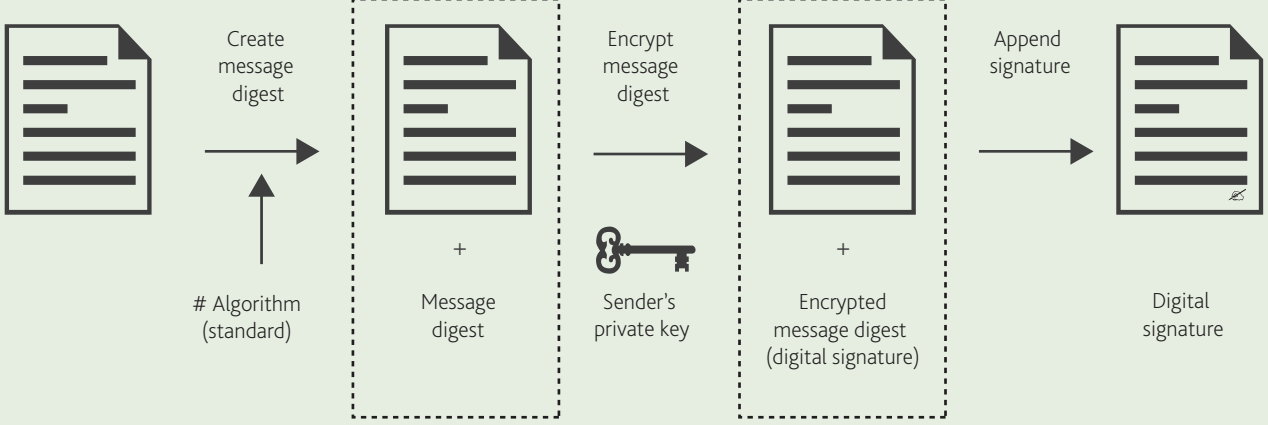
Though the take up of digital signatures and digital certification services has generally been lower than anticipated (*see "In practice" section below*), they have been used in the UK in the online banking and electronic payments sectors.

For example, Bacs, an electronic payment provider owned by the major banking groups in the UK, enables businesses to use digital signatures and digital certificates to authenticate instructions to Bacs to make electronic payment of their payrolls through its "Bacstel-IP" delivery channel. Bacs claims that currently over 90% of the UK workforce is paid via Bacs.

Bacs issues companies with a smart card which contains a chip embedded with the company's private key, public key and a copy of the company's digital certificate (issued to the company by a certification authority). The confidentiality of the private key and digital certificate is protected by a PIN. The company can authenticate a transaction with Bacs by logging on to Bacs' website with its credentials. Bacs will then send the company a random string of text.

The company can digitally "sign" the random string of text by entering its smart card into a smart card reader attached to a computer and entering its PIN. This will create a digital signature by encrypting the string of text using the company's private key. The digital signature, along with the company's public key and digital certificate, are then sent to Bacs which will validate the digital signature through decryption using the public key and validate the digital certificate by contacting the certification provider. If both

CREATING AN ELECTRONIC SIGNATURE



validations are successful then Bacs will process the requested payment.

Public key infrastructure

If there are doubts about the identity of the certification authority itself, then its digital signature can also be verified and certified by another certification authority. For example, the digital signature of a Slaughter and May client could be certified by Slaughter and May. Slaughter and May's digital signature (on its digital certificate) could be certified by the Law Society. In turn, the Law Society's digital signature may be certified by the Department for Business, Innovation and Skills, and so on until there is a level of certainty of the sender's identity which is sufficient for the recipient to conclude the online contract.

The resulting hierarchy of (often cross-certifying) certification authorities is called a public key infrastructure (PKI). According to Bacs (*see above*), Bacstel-IP is currently the world's largest PKI community.

LEGAL POSITION

The continued development of technology and prevalence of e-commerce transactions has meant that parties increasingly require comfort that the use of electronic signatures will be recognised by law.

The Directive on a Framework for Electronic Signatures (*99/93/EC*) (the Directive) is designed to ensure the free movement of electronic signatures and supporting products within the EU. The Directive was implemented into UK law by the Electronic Communications Act 2000 (2000 Act) and the Electronic Signatures Regulations 2002 (*SI 2002/318*) (2002 Regulations).

The Directive

The Directive's five key principles are as follows:

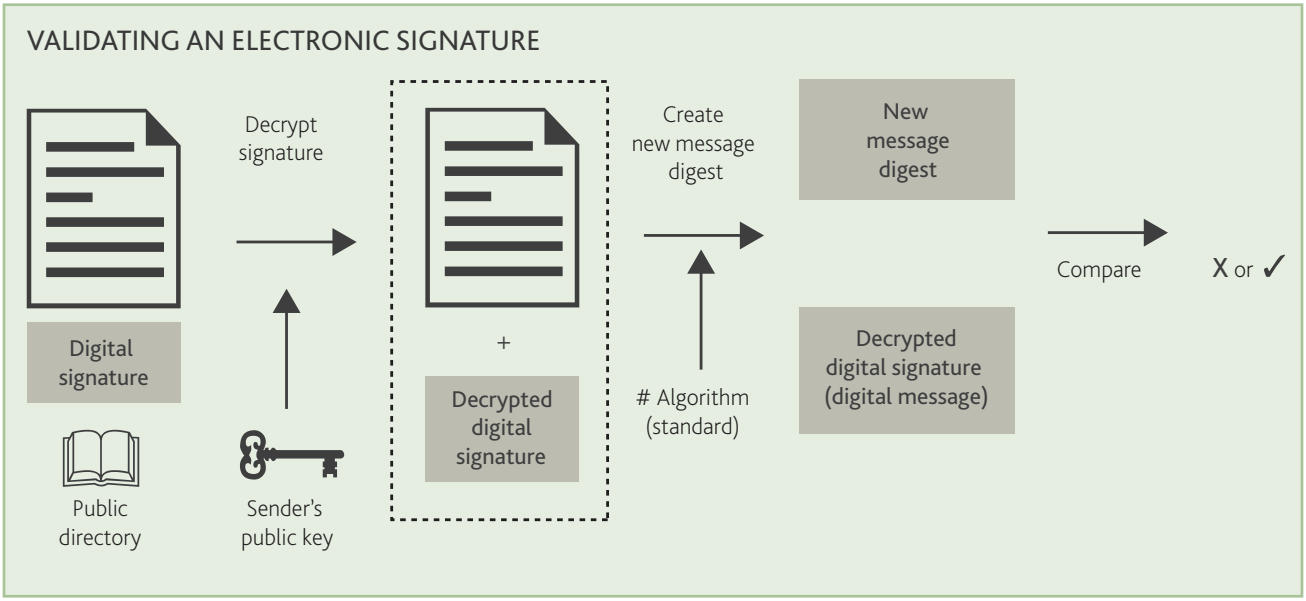
1. **Legal recognition and admissibility**. The Directive requires contracting states to ensure that a signature will not be inadmissible as evidence before the courts of that state merely because it is electronic rather than manual. However, this does not mean that an electronic signature will be admissible merely because it is electronic.

   The Directive distinguishes between electronic signatures and advanced electronic signatures. An electronic signature is an advanced electronic signature if 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.

The Directive provides that an advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device will be legally admissible as evidence in legal proceedings, and will satisfy the legal requirements for signing (*for more information on what constitutes a "qualified certificate" and a "secure signature creation device" see boxes "Requirements for qualified certificates" and "Secure signature creation devices"*).

An electronic signature that does not reach the standard of an advanced electronic signature will not be automatically admissible but, in line with the general principle of admissibility, it will also not be automatically inadmissible. In those circumstances, the evidential weight to be given to an electronic signature, as with a manual signature, will depend on all the circumstances of that particular signature.

2. **Technology neutral**. The Directive is drafted in a technology-neutral manner. The term electronic signature covers any data in electronic form that can serve as a method of authentication for other data to which the electronic data are attached or otherwise associated. Even the definitions for the advanced forms of electronic signature are drafted by reference to characteristics, rather than the technical means for achieving those characteristics.

Although the Directive's definitions appear to be describing digital signatures that are backed by certification authority certificates and are created by using public key cryptography, there is actually no reference to public key cryptography or any other specific technology in the Directive. The intention was for the Directive to be broad enough to be relevant to electronic signatures created by new technologies in the future.

3. **Voluntary approval of certification authorities**. Under the Directive, an EU member state is not permitted to require a certification authority to be authorised. However, the Directive recognises the benefit of voluntary accreditation schemes, through which a certification authority complying with minimum standards will receive accreditation for its certification services.

The Directive contains a set of minimum standards for the accreditation of certification authorities. While the Directive requires member states to permit any person to offer certification services, automatic admissibility before the courts will only be guaranteed by using a certificate from an accredited certification authority.

4. **Certification authorities' liability**. Under the Directive, certification authorities will be liable for any inaccuracies in the assurances given and the other information contained within a digital certificate published by it, but will not be liable for any inaccuracies in the document to which the signature is attached. A certification authority will also be liable for any losses resulting from its failure to revoke a digital certificate (for example, after its validity has expired).

   In each of these cases, under the Directive, a certification authority can limit its liability by showing that it has not been negligent, although the burden of proof rests with the certification authority. A certification authority can further limit its liability by restricting the uses to which a digital certificate may be put and the value of transactions for which a digital signature certificate may be used.

   What is not clear is the extent to which a certification authority may limit its liability to its customers by contractual provisions (for example, exclusions of liability for indirect or consequential loss) in the relevant contract terms. It may be the case that a certification authority is able to limit its liability to customers and other people relying on its certificates, where such certification authority has not been negligent.

   It should be noted that, in a supplier-consumer context, the Directive is subject to the provisions of the Unfair Contract Terms Directive (*93/13/EC*) which may render certain terms in certain consumer contracts invalid or subject to a reasonableness test.

5. **Mutual recognition**. The Directive stipulates member state responsibilities for achieving conformity and consistency of national laws and for removing any differences. It requires member states to recognise electronic signatures and certification authorities (and their certificates) that, in each case, comply with the laws of another state that is party to that law, without imposing any further legal or other restrictions or requirements.

   The Directive also recognises the European Commission's role in making proposals to member states for the effective implementation of standards and international agreements relating to certification services, and the negotiation of bilateral and multilateral agreements with third countries and international organisations.

UK regulation

The parts of the 2000 Act and the 2002 Regulations relevant to electronic signatures address four main areas:

1. **Legal recognition and admissibility**. The 2000 Act provides that electronic signatures and any certification of such electronic signatures by a certification authority or any other person are admissible in evidence in legal proceedings in relation to any question as to the authenticity of the communication or data or as to the integrity of that communication or data[1].

   The definition of electronic signatures is drafted widely and, from a technological perspective, neutrally. It includes anything in electronic form incorporated in or associated with an electronic communication or electronic data which purports to be so associated or incorporated for the purpose of establishing the authenticity or integrity of that communication or data.

   The effect of the 2000 Act is that all electronic signatures are admissible in UK legal proceedings (this differs from the Directive (*see above*)). The nature of a particular electronic signature will, however, determine the evidential weight attributed to that electronic signature in legal proceedings. A simple typed signature at the foot of an email would not, for example, carry the same evidential weight as an electronic signature certified by a certification authority.

[1] Section 7(1).

REQUIREMENTS FOR QUALIFIED CERTIFICATES

Annex I to the Electronic Signatures Directive (*99/93/EC*) (implemented into UK law by Schedule 1 to the Electronic Signatures Regulations 2002 (*SI 2002/318*)) provides that for a digital certificate to be a qualified certificate it must contain:

- An indication that the certificate is issued as a qualified certificate.
- The identification of the certification authority and the state in which it is established.
- The name of the signatory or a pseudonym, which shall be identified as such.
- Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended.
- Signature-verification data (for example, the public key) which correspond to signature-creation data (for example, the private key) under the control of the signatory.
- An indication of the beginning and end of the period of validity of the certificate.
- The identity code of the certificate.
- The advanced electronic signature of the certification authority issuing it.
- Limitations on the scope of use of the certificate, if applicable.
- Limits on the value of transactions for which the certificate can be used, if applicable.

2. **Statutory formalities**. Unfortunately, the 2000 Act introduced some uncertainty as to whether electronic writing or an electronic signature is sufficient to satisfy a requirement under a piece of UK legislation for a document to be "in writing" or "signed".

   It is estimated that there are 40,000 such references in current UK legislation. When the 2000 Act was introduced, instead of introducing a blanket deeming provision by which each of these references would be deemed to permit electronic writing and electronic signatures, the government instead opted for a legislation-by-legislation approach.

   Under the 2000 Act, the Secretary of State may by statutory instrument modify any such provision to permit electronic equivalents of writing or signatures as is considered appropriate, provided that the availability of records of things done must be no less satisfactory in cases where electronic methods are permitted than in other cases.

   To date, a number of statutory orders have been made in order to permit the use of electronic signatures under various pre-existing laws. For example, the Companies Act 1985 was amended by the Companies Act 1985 (Electronic Communications) Order 2000 (*SI 2000/3373*) to permit the use of electronic communication (the use of electronic communications is dealt with expressly in the replacement Companies Act 2006).

   As a result, there exists a risk that where parties purport to conclude a transaction which needs to be in "writing" and/or "signed" according to relevant legislation, by means of, say, an e-mail with an electronic signature, this might not be valid if secondary legislation has not been passed to allow for this.

In 2001, the Law Commission published an advisory paper examining the extent to which the statutory form requirements for "writing" and "signature" are satisfied by electronic means. It concluded that, although there was some lack of consensus on these issues, in its view statutory requirements for "writing" are generally capable of being satisfied by e-mails and by website trading, and statutory requirements for "signature" by the use of a digital signature, scanned manuscript signature, typing a name or initials, or clicking on a website button.

The Law Commission was of the opinion that it is function (namely, demonstrating an authenticating intention of the signatory), rather than form, which is determinative of the validity of a signature.

The question as to whether secondary legislation is required was not addressed in the guidance issued by the then Department for Business, Enterprise and Regulatory Reform (BERR) in 2009[2]. Interestingly, however, BERR explained that the reason UK law chose not to make a distinction between the legal validity of a "simple" electronic signature and an "advanced" electronic signature was because under UK law "a hand written signature is already capable of being satisfied by an electronic one". As explained above, this is due to the fact that the admissibility of a signature is primarily a matter of evidence.

Additionally, there is recent case law relating to guarantees which suggests that the courts will uphold the use of electronic signatures to satisfy a statutory requirement for a document to be "in writing" or "signed" where the relevant legislation has not been amended by a statutory order under the 2000 Act. The courts have followed a similar "function over form" approach to the Law Commission, examining whether the electronic signature in question provides sufficient evidence that the signatory intended to sign the communication.

By way of example, section 4 the Statute of Frauds Act 1677 requires a guarantee to be in writing and signed by or on behalf of the guarantor and is silent as to the validity of electronic signatures. In cases including *J Pereira Fernandes SA v Mehta*[3] (obiter) and *Golden Ocean Group Ltd v Salgaocar Mining Industries Pvt Ltd and another*[4], the courts suggest that an email containing an electronic signature would be sufficient to satisfy section 4.

Therefore, in the absence of government guidance (except in relation to certain areas of the law, for example property), we are left in a disappointingly uncertain position as to the validity of electronic writing and signatures where a statute has not been specifically amended. However, given the Law Commission's stance and the apparent openness of the English courts to this practical, functional approach, we consider the risk of an electronic signature failing to satisfy a requirement for a "written" contract or for that contract to be "signed" to be low.

For additional comfort, parties may wish to consider including a provision in their electronic agreement stating that such agreement is deemed to be in writing and the use of an electronic signature is deemed to be a signature. While the intent of the parties indicated by such a clause may not be sufficient to counter any statutory requirements, it may at least build a sufficient argument in a court that either party would be estopped from challenging the validity and enforceability of that electronic agreement on those grounds.

3. **Supervision and voluntary approval scheme**. Under the 2002 Regulations, the Secretary of State is required to keep under review the activities of certification authorities and to maintain and publish a register of certification authorities established in the UK.

   The "tScheme" has been set up as an industry-led, not-for-profit organisation with the purpose of registering, regulating and setting service standards for certification authorities in the UK. A full list of UK certification authorities can be found on the t-Scheme website.

[2] BERR (2009) *Electronic Signatures and Associated Legislation.*

[3] [2006] EWHC 813 (Ch)

[4] [2011] EWHC 56 (Comm)

SECURE SIGNATURE-CREATION DEVICES

Annex III to the Electronic Signatures Directive (*99/93/EC*) provides that to be a secure signature-creation device, the hardware and software used to create the signature-creation-data (for example, a private key) must ensure at the least that:

- The signature-creation-data used for signature generation can practically occur only once, and the secrecy of that data is reasonably assured.
- Such signature-creation-data cannot, with reasonable assurance, be derived, and the signature is protected against forgery using currently available technology.
- Such signature-creation-data can be reliably protected by the legitimate signatory against the use of others.
- In addition, secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory before the signature process.

The set of minimum standards for the accreditation of certification authorities contained in the Directive has also been implemented into UK law by the 2002 Regulations.

4. **Liability**. The 2002 Regulations implement the liability provisions of the Directive, so certification authorities will be liable for any inaccuracies in the information contained within a digital certificate published by it, but will not be liable for any inaccuracies in the document itself to which the signature is attached. A certification authority will also be liable for any losses resulting from its failure to revoke a digital certificate.

   In each of these cases, as is provided under the Directive, a certification authority can limit its liability by showing that it has not been negligent, although the burden of proof rests with the certification authority.

   The 2002 Regulations do not implement the provisions of the Directive that allow a certification authority to limit its liability further by restricting the uses to which a digital certificate may be put, and the value of transactions for which a certified digital signature certificate may be used.

IN PRACTICE

Public key cryptography technology and digital certification services have been available in a convenient and affordable manner for the provision of electronic signatures to businesses and consumers for a number of years.

US technology companies such as Entrust Technologies Inc. and VeriSign Inc. provide applications and services for both businesses and private individuals in relation to PKI, electronic signatures and digital certificates. Each has affiliates and partners throughout the world. In the UK, the tScheme has approved the provision of PKI, electronic signature and digital signature services by organisations including British Telecom (in conjunction with VeriSign) and The Royal Bank of Scotland plc.

Despite the availability of digital signature and digital certification services provided by certification authorities, the services have not become as widely used by businesses and consumers as was originally anticipated when the Directive and subsequent UK implementing legislation came into force. While such services have been successfully used within the banking and electronic payment sectors, the use of digital signatures and digital certification services in

general e-contracting by businesses and consumers remains relatively low.

There are a number of possible reasons behind this. One is the increased availability of alternative technology to authenticate the identity of a signatory. Many businesses, particularly in the online banking sector, have focused on the use of passwords and tokens as a means of authenticating identity. These are generally cheaper and simpler to use than PKI technology.

Another reason for the slow take up of electronic signature certification services is that many businesses and consumers have not seen the need to obtain the additional certainty provided by digital signatures or the certification services offered by certification authorities. In the UK, the 2000 Act will recognise and enforce any form of legitimate electronic signature, however simple.

Many businesses also continue to prefer to negotiate their key contracts in person and in paper format and, as such, have not required the use of digital signature or services provided by certification authorities. Key contracts will commonly be signed either in person at a negotiation meeting or counterpart copies will be signed and shared with each party by email or post.

THE FUTURE

The European Commission (the Commission) recognises that the adoption of electronic signature certification services may not have been as successful as anticipated, and that changes to the legislation may be required to foster an increased use of electronic signatures. It is particularly concerned that low levels of consumer and business confidence in electronic signatures is holding back the development of cross-border online commerce in Europe.

As part of its "Digital Agenda for Europe", the Commission carried out a public consultation on the Directive in early 2011 to seek views on how electronic signatures and other forms of electronic identity authentication can contribute towards the development of a single European digital market[5].

The results of the consultation were published in late 2011 following responses from around four hundred stakeholders including governments, industry associations, businesses and individuals, although, somewhat disappointingly, the results did not contain any commentary from the Commission itself.

The results confirm a widespread belief among stakeholders that the take-up of electronic signatures in Europe to date has been moderate to low. The reasons identified for this include:

- A limited number of services requiring electronic signatures.
- A lack of user-friendliness.
- The limited EU cross-border interoperability of electronic signatures.
- Costs.
- A lack of legal certainty.

Interestingly, the majority of respondents felt that the take up of electronic signatures would be helped if financial institutions opened up their electronic signature solutions (such as bank cards and one-time pass calculators) to wider application in other industries.

The overwhelming response to the consultation was that the current legislative framework for electronic signatures in Europe is not satisfactory, and further changes to the Directive are required to promote the cross-border use of electronic signatures. Respondents believe that future EU legislation should address the lack of standardisation of electronic signature technologies in Europe, unclear terminology in the Directive, and an inconsistent approach to the regulation of electronic signatures in member states.

[5] European Commission (February 2011) *Public Consultation on eSignatures and eIdentification*.

Suggestions for a European standardisation effort include the creation of a central European validation service or a government validation service in each member state.

The Commission has indicated that it intends to use the results of the public consultation to inform a number of revisions to the Directive.

In the UK, there is also likely to be a strong drive towards increasing the use of electronic signatures, particularly within eGovernment services. A new team within the Cabinet Office, the Government Digital Service, was launched in December 2011 and has been tasked with transforming government digital services, including the simplification and strengthening of digital government in order to improve the quality, and consequently use, of online channels.

Rob Sumroy is a partner and Brett Sherrard is an associate in Slaughter and May's IP and Technology Group. If you would like more information on any of the issues raised in this article, or would like to discuss IP or Technology matters generally, please contact Rob Sumroy, Brett Sherrard or your usual Slaughter and May contact.

This article was originally published in PLC magazine April 2012 and is reproduced with the permission of Practical Law Company Limited.