

Electronic Signatures.

According to a report issued by the UK Office of Fair Trading in March 2008, internet retailing is growing at about 30% each year.

In the non virtual world, a paper based signature can provide evidence that data originated from the signer, that the signer intended to adhere to the document on which the signature is written and that the signed data has not been altered after signature.

One of the issues that constantly arises in the context of internet retailing is to provide for an electronic signature system which could replicate a paper based signature.

The EU recognised this issue some time ago and in 1999, an EU system for the regulation of electronic signature based products and services was adopted as the Electronic Signatures Directive 1999/93 (the Directive).

There have been a number of issues with the Directive. First the Directive is very technical and indeed arising from a recent report published for the Commission, judges still struggle with understanding the different levels of electronic signatures (basic, advanced and qualified) and how to assess the fulfilment of the technical criteria for creating a legally valid electronic signature.

Second, there is a lack of definition of the whole set of electronic signature products, a lack of referenced standards outside the standards related to Annex II(f) (trustworthy systems and products) and III (requirements for secure signature creation devices) of the Directive and a lack of formal standards in the area of electronic signatures. eSignature related standards that are referenced in the Official Journal are not necessarily harmonised standards but in some cases are based on CEN workshop agreements.

Indeed the Commission report I just referred to, recommended that the Commission update by way of decision, the list of generally recognised standards which ensure compliance with Annex II (f) and Annex III of the Directive and further that the Commission issue a mandate to the European Standardisation Organisations asking them to draft a guidance paper on the use of relevant standards including their legal relevance in the context of the Directive.

We understand as a result, that the Commission are likely to adopt before the end of 2008 an action plan on Electronic Signatures, which will address these issues.

As I mentioned above, the Directive defines three different types of electronic signatures, an **electronic signature** (ie a basic electronic signature)¹, an **advanced electronic signature**² and a **qualified electronic signature** (“QES”).

What is particularly important about an electronic signature which is a QES is, that it is the only type of electronic signature which the Directive states must be recognised as having the same legal value as a handwritten signature. In the case of a basic or advanced electronic signatures, Member States cannot deny their legal effectiveness and admissibility as evidence in court, solely on the ground that they are in electronic form or are not based on a qualified certificate etc. However the exact legal effect of an electronic signature in a particular context would be a matter for a court to decide in a given case.

The mandatory requirements for accepting a signature as a QES are i) that the electronic signature is an Advanced Electronic Signature, ii) the signature is supported by a Qualified Certificate and iii) the signature is created by using a secure signature creation device. The Qualified Certificate (“QC”) is an electronic attestation which links signature verification data to a person and which confirms the identity of that

¹ means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. The term authentication encompasses any legal purpose or function that the signature is considered to fulfil in each national jurisdiction.

² an advanced electronic signature is an electronic signature that meets the following requirements:

(i) It is uniquely linked to the signatory (ii) It is capable of identifying the signatory (iii) It is created using means that the signatory can maintain under his sole control and (iv) It is linked to the data to which it relates in such a manner that any subsequent change is detectable.

person. The Directive lays down detailed requirements for the contents of the **QC** and also in relation to the service provider who will provide the **QC**.

Accordingly, the first thing to be considered whether you are a supplier, or a customer (such as a government department) or for example, a provider of a financial service over the internet, is whether the law mandates the use of a QES in context.

However, even if the law does not mandate the use of a QES, the parties may decide to use a QES where the use of the QES is essential to prevent the occurrence of serious legal risks (for example the level of transactions involved in the application supported by an electronic signature mechanism is considerably high).

In these circumstances, it is not so much the higher legal value of the QES that is important, but rather the security and functional guarantees that are inherent from the creation of the QES that are important.

It is clear from the definition I gave above of an electronic signature, that it gives an entity seeking to rely on it very little comfort.

In a recent case in the UK, a director of a company the subject of a winding up petition, asked a member of staff to send an email to the solicitors acting for the plaintiff, to consider adjourning the winding up petition for one week in return for a personal guarantee. The email itself was not signed, but the head of the email showed that it came from the employee's address. There was no further reference to the email sender's name in the body of the email. The proposal was accepted but then the employee did not honour the guarantee. The judge held that the email message satisfied the statutory requirement of writing, but could not be classified as a signature. It was not possible to hold that the automatic insertion of an email address was intended as a signature.

In the context of a closer user group, the parties may decide that a QES is not necessary and instead accept that members of the group will be bound by an electronic signature or an advanced electronic signature. However the structuring of the closed user group will require careful planning from a systems perspective and also will require that the parties agree on a comprehensive set of terms and conditions, so that the risks in context are properly managed.

9th of October 2008

Paul Foley
Partner
McKeever Rowan
pfoley@mckr.ie

Copyright Paul Foley October 2008 – all rights reserved