

## Electronic (or Digital) Signatures

July 2007

**Electronic Signatures - also known as Digital Signatures - are becoming more popular.**

**They can be used as a means of both proving that an electronic document hasn't been tampered with, and as a legally binding "signature" to a contract.**

**Our E-Business Advisers discuss:**

### 1. What is an Electronic (or Digital) Signature?

As the range of business opportunities and possibilities for customer services offered by the Internet increases, security becomes ever more important.

In particular, to create a legal contract, firms need to be sure that information is from who it is supposed to be from, and hasn't been altered enroute.

For example, they need to be certain that an electronically transmitted invoice is from who it says it's from, and hasn't been altered.

If you're buying from a web site, you also need to be sure that the firm is who it says it is.

This verification process hence needs 4 elements to be present to enable a legal contract:

1. "Authentication" - you need certainty about the identity of the sender.

2. "Integrity" - you need certainty that that the information has not been altered enroute, either accidentally or deliberately.
3. "Confidentiality" - you need certainty that only the real recipient is able to get the information sent.
4. "Non-Repudiation" - you need certainty that the person who sent the document can't deny having sent the message, nor can the recipient deny having received it

To ensure that all the above four points are met, a standardised methodology must be used.

This is what electronic signatures achieve. They provide the electronic equivalent of a hand-written signature, and this can be checked.

Legislation - the Electronic Communications Act 2000 - means that an electronic signature is as binding legally as an ordinary signature would have been.

### 2. How does it work?

Electronic signatures work by using "digital certificates".

A process known as "public key cryptography" is used.

This has two electronic "keys" - one public, one private. The key is a unique number, which, when combined with the data you are "signing", produces an encrypted version of the data.

The same process works in reverse to decrypt



# Fact Sheet

the data too.

The public key is freely distributed, but your private key is held secretly by you.

This hence makes for a secure way of transferring data back and forth.

The public and private keys are mathematically related, but it is not feasible to derive one key from the other.

Typically, you may see 40-bit to 128-bit encryption: the higher the "bits" the stronger the encryption.

There are different types of digital certificates for different usages - for example, e-commerce web sites and emails.

### 3. How do I get a digital certificate?

To meet the four requirements for verification, you need to use an industry standard, recognised encryption methodology.

The most common way of doing this is by buying a digital certificate from an organisation known as a "Trusted Service Provider" or "Trusted Third Party".

Buying a certificate from a Trusted Service Provider allows digital signing of a wide range of data.

After making sure that you are who you say you are, they provide the certificate, along with a mechanism for distributing the public keys.

For your web site, your web hosting company will normally allow you install a digital certificate.

If you are selling online via your web site, you will need a digital certificate to fulfill the requirements of security if you want customers to enter their credit card details.

If you use a Third Party Payment Provider (such as WorldPay, SecPay, NetBanx etc) to take credit card details and process payment for you, it is likely that you will be using their certificate.

This would be provided as part of the contracted service with the firm.

### 4. Useful Links

There are many Trusted Service Provider digital certificate providers.

These include:

Thawte - [www.thawte.com](http://www.thawte.com)

Verisign - [www.verisign.com](http://www.verisign.com)

AddTrust - [www.addtrust.com](http://www.addtrust.com)

GlobalSign - [www.globalsign.net](http://www.globalsign.net)

*Disclaimer: we have no commercial links with these companies, and their appearance in this fact sheet is not an endorsement.*