dti

ELECTRONIC SIGNATURES FACTSHEET

Electronic signatures mean that you can exchange information with others electronically and securely – safe in the knowledge that everyone is who they claim to be and that only the right people can access the information.

What are electronic signatures?
The benefits
The legal situation
The technology
Implementing electronic signatures
Further help and advice

What are electronic signatures?

Electronic signatures – sometimes known as digital signatures – are the electronic equivalents of written signatures; they allow businesses to sign documents and carry out business transactions electronically. They provide assurance that the authors and signatories of e-mails or electronic files are who they claim to be.

An electronic signature is not a picture of your handwritten signature; it is an electronic means of connecting individuals with important electronic documents and e-mails, which also verifies the sender's identity and ensures that the content is uncorrupted.

Where there might be doubt about the validity of your signature, you can add a digital certificate to authenticate the signature itself. A digital certificate vouches for information about your identity – your name, e-mail address and the name of your business, as well as the date the certificate was issued and by whom, and key data belonging uniquely to you.

The benefits

All businesses need to exchange information speedily, accurately and securely, both internally and externally. Doing this electronically, rather than on paper, provides significant advantages:

- Information arrives nearly instantaneously, regardless of distance.
- Once set up, the cost of sending each item is virtually nothing – no stamps, no post room, no envelopes, no fax machine, no fax paper.
- Information can move directly from individual to individual – desk to desk – without any other humans being involved.
- Information generally arrives uncorrupted, or there is a warning and retransmission easily follows – no more garbled faxes.

Examples of products and companies included in this leaflet do not in any way imply endorsement or recommendation by DTI. Bear in mind that prices quoted are indicative at the time it was published.

Electronic signatures

- The need to re-key data into other computer systems disappears as do all the attendant risks and costs of errors.
- Automatic logging of who sent what to whom and when, and even when the recipient received and read it.

But electronic exchanges, particularly ones with external parties, seem to lack the same legitimacy as paper exchanges with their printed letterheads and ink signatures. They seem too easy to produce, to alter and to copy and hence open to impersonation and ultimately fraud.

Electronic signatures solve these problems, providing the confidence that allows you to realise the benefits of secure electronic transactions for your business. Electronic signatures are not merely convenient alternatives to written signatures – they have the potential to offer much more to your business.

Improved security

Electronic signatures are more secure than their handwritten equivalents. They offer:

- Additional security – when used properly it is impossible for someone to copy your signature, and your electronic signature applies to the whole document and not just the last page.
- Protection for the integrity of the data – you can be sure nothing has changed or been maliciously altered.
- Proof of message transmission (time stamping) – businesses can use third party authorities to verify the transmission dates and times of critical electronic messages for legal and commercial purposes.
- Protection against repudiation – they provide strong evidence that a message and its contents was signed and sent. This means that, if a contractual dispute did arise, the sender could not deny knowledge of the message.

Additionally, with the cooperation of the recipient, the sender can optionally ensure that only the intended recipient can retrieve and read the message content.

Streamlining business

By removing the need for paper copies of documents, electronic signatures provide the final link in the e-business chain. This streamlining of processes offers numerous benefits:

- Increased efficiency – posting or sending contracts by courier takes time and costs money. Now simple contracts can be instantly set up online.
- Location is no longer a factor in signing contracts.
- Electronic orders can link directly into your office systems – this saves time spent on processing and fulfilling customer orders by removing the need for faxing, posting and re-keying information.
- Documents, files and orders can be tracked and managed online – for accurate record keeping, automated receipts and faster confirmation.

- Re-keying errors disappear, resulting in correct deliveries, fewer payment disputes and more satisfied customers.

- Enhanced trading opportunities for smaller businesses – electronic signatures are available cheaply and offer a level of security that should be acceptable to even the largest and most technically advanced organisations.

The legal situation

In the UK, binding contracts can result from oral exchanges, handshakes, faxes – just about anything that signals that both parties intend to abide by whatever they have agreed. Electronic signatures add to this list of possibilities. However, this flexibility does not apply in many other countries or to certain activities in the UK, for example signing wills or registering births. This has historically led to doubt as to where electronic signatures apply and where they do not.

The Electronic Communications Act of 2000 has made it clear that electronic signatures are admissible in evidence about the authenticity or integrity of a communication or data (see Section 7(1) of the Act). A European directive has ensured the effectiveness of electronic signatures across Europe. Legislation in the USA and in many other countries has done the same elsewhere.

The use of electronic signatures and associated security measures means that companies can now do business more effectively with customers and suppliers as well as file their tax and accounts, distribute annual reports and allow shareholders to vote online.

The technology

An electronic signature can be attached to anything recorded digitally – a document, an image, an e-mail, a web page – all it takes is a mouse click and a few keystrokes using some purpose-built software. Purpose-built software can also verify the correctness and completeness of anything signed. Some standard software, for example Microsoft's Outlook Express, includes the appropriate functions.

As with any document (paper or electronic), simply signing it does nothing to conceal its contents from unwanted eyes. But unlike paper signatures, electronic signing can be accompanied by encryption to make the document's contents unintelligible to all but the intended recipient.

Any document can be signed and sent to someone you have never corresponded with before but, to send encrypted information to someone, you'll need certain information from them first. Equally, if a recipient wants to verify an electronic signature (rather than just reading the contents of the signed information and noting that it is signed) then they have to have special information about the sender (the person signing). The required information is held in an individual's digital certificate. And something known as a public key infrastructure (PKI) provides the means to support these certificates in a reliable way. Again, standard software can hide all the details of this once it's set up and activated.

This guide looks at the application of electronic signatures to information exchanges between businesses and between businesses and government. So it's about signing e-mails, contract documents, statutory returns and the like – and not about websites and the internal workings of specialist applications.

The use of electronic signatures, supported by digital certificates, is growing rapidly, encouraged by the Government's campaign to pioneer secure access to online services such as filing tax returns and business accounts via the Government Gateway (www.gateway.gov.uk for further information).

There are already several technologies for electronically signing documents:

Secure e-mail
E-mails, signed with an electronic signature supported by a digital certificate and encrypted, are a cost-effective way of exchanging information securely with existing trading partners.

For one method of signing and encrypting your messages, you and your correspondent each need:

- an S/MIME-compatible e-mail programme (a standard feature of most modern e-mails and browsers
- a digital certificate – these are available for around £50 per year for ones accepting reasonable liability and for much less for ones accepting little or no liability, but you will need one per person or e-mail account
- simple instructions on how to install your certificate and how subsequently to operate signing and encryption

Signing documents
Having agreed the terms of any agreement, all parties to the agreement have to sign it. Often the contract terms are too long and complicated to express in the message text of an e-mail and are more suited to a word-processed file which can be attached to the e-mail. Just as with paper, each party can in turn add their electronic signature to the file, returning a fully signed copy to each of the parties at the end for retention and later consultation.

There is standard software available to perform the signing task and any later verification. As with e-mail, digital certificates typically support the signing process.

Obtaining digital certificates
A digital certificate acts much like an electronic passport, verifying your identify and confirming your rights to access particular electronic information and services.

- You can obtain a digital signature from any of a number of certificate authorities (CAs) – preferably a properly approved one. These organisations are sometimes known under the umbrella title of trusted third parties.

- Certificates are available for both individuals and businesses; and higher reliability ones typically cost around £50 per year and last for one or two years.

- You need a separate digital certificate for each e-mail account you want to send signed e-mails from.

Digital certificates are available online and, depending on the level of security you want, should be e-mailed to you within a day of submitting the necessary information to prove your identity.

Check with www.tscheme.org for details of approved suppliers of digital certificates.

Off-the-shelf software packages

These offer robust security for signing and encrypting files, instant messages and web pages, plus additional options such as control over message history, multiple user signing and alteration checking. In other words, the extra functions that make signed electronic exchanges even easier and exploit all the benefits of electronic transactions.

Most packages start at around £70 and can be used either with digital certificates provided as part of the software or with digital certificates explicitly obtained and imported by you. Some companies offer a range of solutions to suit most business purposes. While they claim that no technical knowledge is needed to operate them, you may well need support to implement the systems successfully. Adobe Acrobat 6 also incorporates a SelfSign function and integrates easily with several third party signing systems (www.adobe.com). It is often the case that recipients of signed information can use freeware (no charge) software to read what they receive. In other words, businesses that send out encrypted sensitive data or electronically signed contracts to many parties need not be concerned about imposing undue costs on their business partners.

Naturally, you will need to ensure that your intended recipients have access to, and knowledge of, the software you are using.

Security considerations

To be certain that you, and you alone, signed an e-mail or a document then there has to be a way of linking something unique about you to your signature. With pen and ink, we rely on the fact that you alone can direct the pen accurately in a precise combination of movements – even though we know that this is not 100% reliable, we consider it good enough. With electronics, we instead rely on:

- something that you know – usually a pass-phrase which is a longer version of a password
- something that you are – for example, a scan of your fingerprint, of your iris or of the movements that form your physical signature
- something that you have – for example, a smart card or a portable storage module or even just physical access to a particular PC or
- some combination of these.

You present this ‘something’ each time you perform an electronic signature. The assumption is that no one else but you can do this. Your signature remains safe only for as long as your ‘something’ remains solely under your control. This is a very important consideration.

Implementing electronic signatures

Research & analyse

Set objectives
Understand what you want to achieve and ensure that it's realistic.

With whom do you wish to exchange signed information online?

Do they already operate this way?

If they do, does the way that they do it suit you?

If they don't, can you motivate them to join with you?

Cost/benefit analysis
Understand the projected total costs and the benefits that you are likely to accrue.

Consult with colleagues and partner organisations to establish cost models.

Obtain estimates from possible suppliers, covering additional hardware, software, staff training, implementation, maintenance, support, ongoing services and upgrades.

Include the cost of any necessary modifications to interface your existing application systems correctly to your prospective electronic exchanges.

Identify the benefits in terms of reduced staff time, speedier turnarounds, fewer errors, reduced risk of information compromise, expanded market reach, enhanced image and so on.

Which electronic signatures solution?
Set the parameters for the implementation that you have decided upon.
Identify the target applications that you want.
Identify your partners.
Identify your participating staff.
Identify the affected business processes.

Consult

Professional advice
If you lack the skills in-house, contact a Business Link adviser (or equivalent if you are in Scotland, Wales or Northern Ireland), in the first instance, for help on how best to: define your exact requirements establish how much you will need to pay scope the project create an implementation plan undertake implementation provide training and software support.

Talk to your trading partners and similar organisations
Attend conferences and exhibitions on the subject.
Gain as much knowledge as possible from those who have already done it.
Give extra weight to the opinions of those who have businesses like yours.

Plan & test

Try before you buy

Experiment with the low cost or free versions of what you may want to implement properly later.
Before you commit to a particular solution, ask around.
What do others in your industry use?
What does your trade or professional association think?

Plan the roll-out phase

Depending on the complexity of the solution you are introducing, you will want to provide staff training or familiarisation at this point. Decide who needs training and allow time for them to adjust to the new system.

Do not expect to run too soon – you are probably altering some of the fundamentals of how your business communicates with the rest of the world and this demands great care.

Act

Implement

Encourage staff involvement and feedback, this will help smooth implementation, as staff buy-in can make or break a technology project.

Remember that comprehensive testing is essential.

Do not abandon the old ways until you are completely certain of the new way.

Evaluate

Monitor and review the impact on your business and against your objectives.
Get feedback from staff, collaborators, customers and suppliers on the changes.

Evaluate the impact after 6 months and 1 year.
Have you achieved your objectives?
Establish how you could improve things further.

Further help and advice

Legislation and regulations
Electronic Communications Act 2000
www.opsi.gov.uk/acts/acts2000/20000007.htm

Electronic Commerce (EC Directive) Regulations 2002
www.opsi.gov.uk/si/si2002/20022013.htm

The Electronic Signatures Regulations 2002
www.opsi.gov.uk/si/si2002/20020318.htm

Electronic Signatures Directive. (Full title: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures). The Official Journal reference is OJ L13 19.1.2000.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

Electronic Signatures Directive Transposition Note
www.dti.gov.uk/sectors/infosec

The use of digital technologies in business.
www.cabinetoffice.gov.uk/e-government

Securing electronic transactions
For more background on securing electronic transactions, read *'The tScheme Simple Guide to Securing Electronic Transactions'* available from: www.tscheme.org

General
DTI Information Security Health Check Tool
www.securityhealthcheck.dti.gov.uk

DTI Information Security Home page
www.dti.gov.uk/sectors/infosec

DTI Information Security Business Advice pages
www.dti.gov.uk/sectors/infosec/infosecadvice/page10059.html

DTI Information Security
Publications (available to order or download)
www.dti.gov.uk/sectors/infosec/infosecdownloads/page9935.html

Published by the Department of Trade and Industry. www.dti.gov.uk