ELECTRONIC SIGNATURES AND ASSOCIATED LEGISLATION

This can be a complex subject and the following text offers a brief introduction to Electronic Signatures, followed by more background on the Register of UK Certification Service Providers.

Key legislation:

The Electronic Communications Act 2000

The Electronic Signatures Directive 1999/93/EC

The Electronic Signatures Regulations 2002

See also:

The Transposition Note for the Electronic Signatures Directive, available as a PDF from the Electronic Signatures section of BERR's Information Security web pages.

Electronic Signatures PDF – a guide to their use in business, is also available from the Electronic Signatures section of BERR's Information Security web pages.

A definition of electronic signatures

A rough definition of an electronic signature is that it is the electronic equivalent of a written signature. Electronic signatures can come in many forms:

- typewritten
- scanned in signature format
- an electronic representation of a hand written signature
- a unique sequence of characters
- a digital representation of characteristics e.g. fingerprint, retina
- a signature created by cryptographic means.

Signatures are as good as the business process and technology used to create them. High value transactions need better quality signatures. Such signatures need to be linked to the owner in order to ensure trust in the underlying commercial system. Better quality signatures can offer:

- authentication – linking the originator to the information
- integrity – allowing any modifications to the information to be detected
- non-repudiation – ensuring satisfaction (in a legal sense) as to the signature's origin.

Why use electronic signatures?

All parties involved in any commercial transaction or messaging activity need to have confidence (trust) that any communication that is sent reaches its destination without being changed in any way. There may also be a need for it to reach its destination without being read by anyone else. Trust is the basis of all commerce and can be enhanced by the use of electronic signatures.

Electronic signatures can:

- prove (authenticate) the origin of a message
- prove whether a message has been altered (integrity)
- keep messages secret (confidentiality) by the use of encryption.

Cryptographic techniques can be used to provide encryption for confidentiality and electronic signatures can provide authentication and integrity of communications.

There are 2 basic types of cryptographic encryption – symmetrical and asymmetrical – and many different coding mechanisms. Some are general purpose whilst others are targeted at specific business problems. All require a specific key or keys to encrypt and decrypt a message.

A symmetrical system, where the same key is used to encrypt and decrypt data, is termed a "private key system".

An asymmetrical system uses one key to encrypt data and another to decrypt it. This is termed a "public key system". Asymmetrical or public key systems overcome certain management issues connected with symmetrical systems but they do raise other issues. Technology can only assist in the creation and maintenance of trust between businesses and their customers. It provides the basis for security but cannot guarantee it. The appropriate business management and organisational processes must also be in place (and should be regularly reviewed). The international standard on information security management, ISO/IEC 27001, is a business-led approach to best practice in this area. For further information on the standard please check out the relevant section of our Business Advice Pages (follow the link on our Home Page).

Register of UK Established Certification Service Providers that issue Qualified Certificates to the Public

The following text and Register have been produced in response to Regulation 3 of the Electronic Signatures Regulations 2002, which implements Article 3.3 of the Electronic Signatures Directive 1999/93/EC.
This text is intended for guidance purposes only and is not a substitute for formal legal advice.

The Directive

What does the Electronic Signatures Directive do?

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures was published on 19 January 2000.

This is a framework Directive designed to assist in the proper functioning of the internal market of the European Union by ensuring the free movement of electronic signatures and supporting services and products.

Member States are required to implement the requirements expressed in the Directive in national legislation.

The Directive is implemented into UK law by the Electronic Communications Act 2000, and the Electronic Signatures Regulations 2002 (SI 2002 No. 318).

What is the legal status of electronic signatures?

Article 5.2 of the Directive provides for a harmonised and appropriate legal framework for the use of electronic signatures by ensuring the recognition of all electronic signatures as evidence.

This covers the full range of electronic signatures – no matter what their form or technology basis – from simple to advanced electronic signatures. The Directive does not mention simple signatures, but this is taken to be any signature that would have low evidential value.

Article 5.2 is implemented into UK law through Section 7 of the Electronic Communications Act 2000.

How does an electronic signature equate to a hand-written signature?

Article 5.1(a) of the Directive requires Member States to ensure that an Advanced Electronic Signature, which is based upon a qualified certificate and is created by a secure-signature-creation device, satisfies the legal requirements of a signature in relation to data in electronic form in the same manner as a hand written signature.

Such signatures are commonly referred to as Qualified Signatures – though this term is not expressly used in the Directive.

There is no specific UK implementation of Article 5.1(a) as, under the law in England, Wales, Scotland and Northern Ireland, a hand written signature is already capable of being satisfied by an electronic one, including an advanced electronic signature.

Article 5.1(b) requires Member States to ensure that qualified signatures are admissible in legal proceedings.

This repeats the requirement of Article 5.2 for any electronic signature, and is implemented into UK law through Section 7 of the Electronic Communications Act 2000.

What supervision of certification-service-providers does the Directive require?

Article 3.3 of the Directive requires Member States to ensure the establishment of an appropriate system that allows for supervision of **certification-service-providers (CSPs)** which are established on its territory and which issue **qualified certificates (QCs)** to the public.

Article 3.3 is implemented into UK law by Regulation 3 of the Electronic Signatures Regulations 2002 (see below for further details).

What liability is imposed on a CSP?

Article 6 of the Directive sets out a minimum level of liability that Member States must impose on CSPs which issue qualified certificates to the public. It also grants CSPs the right of placing limitations on the use of such certificates.

Articles 6.1 and 6.2 of the Directive are implemented by Regulation 4 of the Electronic Signatures Regulations 2002.

Article 6.1 of the Directive requires that where a CSP issues a qualified certificate to the public, or guarantees such a certificate, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate in respect of:

- completeness and accuracy at the time of issuance of all information
- assurance that the designated signatory held the signature-creation-data corresponding to the signature-verification-data given or identified in the certificate
- where the CSP generates both the signature creation data and the signature validation data, assurance that they work together - unless the CSP proves no negligence.

Article 6.2 of the Directive requires that, where a CSP issues a qualified certificate to the public, the CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate in respect of failure to register revocation of the certificate - unless the CSP proves it has not acted negligently.

Articles 6.3 and 6.4 require that Member States allow CSPs to place limitations on the use of QCs. These provisions are not implemented in the UK by specific legal provisions because CSPs can already exclude liability under tort and delict for these matters, subject to the applicable laws on the exclusion or limitation of liability.

Article 6.3 ensures that a CSP can indicate (in a QC) limitations on its use – provided the limitations are recognisable to third parties. The CSP is not liable if a certificate is then used in a manner that exceeds those limitations.

Article 6.4 ensures that a CSP can indicate in a QC a limit on the value of the transactions for which it can be used – provided the limit is recognisable to third parties. The CSP is not liable if that limit is then exceeded.

What Data Protection duty is imposed on a CSP?

Article 8 of the Directive requires Member States to ensure that CSPs and national bodies responsible for accreditation or supervision comply with certain data protection requirements.

Article 8.1 requires that CSPs, and the national bodies responsible for accreditation (known as “approval” in the UK) and supervision, comply with the requirements in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 95/46/EC has been implemented into UK law by the Data Protection Act 1998.

Article 8.2 goes further and requires that CSPs which issue certificates to the public collect personal data only directly from the data subjects or with their explicit consent and only in so far as is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purpose without the explicit consent of the data subject.
Article 8.2 of the Directive is implemented into UK law by Regulation 5 of the Electronic Signatures Regulations.

Article 8.3 requires Member States do not prevent CSPs from identifying a signatory in a certificate by using a pseudonym.

Article 8.3 has not been implemented into UK law by a specific provision. The right of a person to use a pseudonym in this way already exists.

Concepts used in the directive

Article 2 of the Directive and Regulation 2 of the Electronic Signature Regulations 2002 define a number of terms.

What is an Electronic Signature?

Article 2.1 of the Directive defines an electronic signature as data in electronic form which are attached to, or logically associated with, other electronic data and which serve as a method of authentication.

An electronic signature can be created by any means. It is thus wider in meaning than a number of other terms e.g. digital signature.

What is an Advanced Electronic Signature?

Article 2.2 of the Directive defines an advanced electronic signature as an electronic signature that is uniquely linked to a signatory, and capable of identifying the signatory, and created by means the signatory can maintain under his sole control, and linked to the data being signed such that any change of the data is detectable.

The Directive does not say how these requirements should be fulfilled – however the use of a secure-signature-creation device coupled with suitable technology could be one way.

Who is a Signatory?

Article 2.3 of the Directive defines a signatory as a person who holds a signature-creation device and acts on his or her own behalf or on behalf of the natural or legal person he or she represents.

What is a Signature-Creation Device?

Article 2.5 of the Directive defines a signature-creation device as configured hardware or software used to implement signature creation data. Examples of signature creation devices are a Smart Card and software running on a PC.

What is Signature-Creation Data?

Article 2.4 of the Directive defines signature-creation data as codes, or private cryptographic keys, which are used by the signatory to create an electronic signature.

This covers e.g. a signing key, or a signature private key.

What is a Secure-Signature-Creation Device (SSCD)?

Article 2.6 of the Directive defines a secure-signature-creation device as a signature creation device that meets the requirements of Annex III.

Annex III essentially requires, at a minimum, that the signature creation data be unique, capable of being kept secure, cannot be derived (e.g. reverse engineered), be protected against forgery, protected from the use of others, cannot alter the data to be signed, and cannot prevent the signed data from being presented to the signatory before it is signed.

The technology to be used and the form of an SSCD are not mandated. It can therefore be implemented as software, hardware or a combination provided it complies with the requirements of Annex III.

What is a Certification-Service-Provider (CSP)?

Article 2.11 of the Directive defines a certification-service-provider as an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

This is a wide ranging definition, and not all CSPs will be supervised under Regulation 3 of the Electronic Signatures Regulations 2002

What is a Certificate?

Article 2.9 of the Directive defines a certificate as an electronic attestation which links signature-verification data to a person and confirms the identity of the person.

A certificate is thus a block of data that represents the necessary information that helps to create the link. The items usually include the name of the issuing party, the name of the person being identified, what the certificate is to be used for, etc.

The confidence of a certificate may be increased when it is electronically signed by the issuing authority.

Certificates are usually not presented in plain text – they are read by an automatic process such as a computer programme and thus conform to a standard (X509 is the common standard for certificates).

What is Signature Verification Data?

Article 2.7 of the Directive defines signature-verification-data as data such as codes, or public cryptographic keys which are used for the purpose of verifying an electronic signature.

This includes, for example, a signature public key.

What is a Qualified Certificate?

Article 2.10 of the Directive defines a qualified certificate as a certificate which meets the requirements of Annex I of the Directive and is provided by a person (CSP) complying with Annex II of the Directive).

Annex 1 of the Directive is transposed into UK law by Schedule 1 to the Electronic Signatures Regulations 2000.

Qualified Certificates must therefore contain at least the following items:

- an indication that it is a qualified certificate,
- the identification of the Certification-Service-Provider (CSP) and the State in which the CSP is established,
- the name of the signatory or a pseudonym, which must be identified as such,
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose of the certificate,
- the signature verification data (such as the public key),
- an indication of the start and end date of validity,
- its identity code (e.g. serial number),
- the Advanced Electronic Signature of the CSP that issued it,
- any applicable limitations on its use (e.g. restricted to certain applications, or within a certain group of participants),
- any applicable limits on the value of transactions for which the certificate can be used (e.g. maximum transaction value).

Annex II of the Directive is transposed into UK law by Schedule II to the Electronic Signature Regulations 2002.

CSPs that wish to issue Qualified Certificates must therefore:

- show the necessary reliability for providing certification services,
- run a prompt and secure directory and a secure and immediate revocation service,
- ensure that the date and time of issuance and revocation can be determined precisely,
- verify the identity and any applicable attributes of the person to whom a qualified certificate is issued,
- employ personnel that are qualified and technically competent to run the services securely and apply administrative and management procedures which are adequate and correspond with recognised standards (e.g. ISO/IEC 27001),
- use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them,

- protect against forgery of certificates, and guarantee confidentiality during in-house signature-creation data processes,
- maintain sufficient financial resources to operate in conformity with the Directive, in particular to cover liabilities, for example by obtaining appropriate insurance,
- keep all relevant records (manually or electronically) concerning a qualified certificate for an appropriate period of time, in particular to provide evidence in legal proceedings,
- not store or copy signature-creation data (e.g. a private key) of any person to whom the CSP provided key management services,
- before entering into any contractual relationship for a certificate, inform anyone seeking certification services of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary approval scheme, complaints and dispute settlement procedures. Such information may be transmitted electronically, but must be in writing, and in readily understood language. Upon request, relying third parties must also have access to relevant parts of the information,
- use trustworthy systems to store certificates in a verifiable form so that only authorised persons can make entries or changes, information authenticity can be checked, certificates are publicly available for retrieval only where the certificate holder's consent has been obtained, and any technical changes compromising these security requirements are apparent to the operator.

How is Supervision carried out?

Method of Supervision:

Regulation 3 of the Electronic Signatures Regulations 2002, which implements Article 3.3 of the Directive, imposes a duty on the Secretary of State to:

- keep under review the carrying on of activities of Certification Service Providers (CSPs) established in the United Kingdom which provide Qualified Certificates (QCs) to the Public, and of the persons by whom they are carried on, with a view to the Secretary of State becoming aware of the identity of those persons and circumstances relating to the carrying on of those activities,
- establish and maintain a register of those CSPs,
- record in the register the name and address of the those CSPs of whom the Secretary of State is aware,
- publish the register in an appropriate manner,
- have regard to any evidence of the conduct of those CSPs, which is detrimental to users of QCs, with a view to publication of any evidence.

The Register (and thus supervision) only includes those organisations that sign qualified certificates issued to the public to support the use of advanced electronic signatures. The organisation's agents, distributors, and the like, along with registration authorities, are thus excluded.

To the public is not defined in the Directive or the Regulations, but the "public" in this context is taken to mean the general public together with classes of the public which do not have the characteristics of a closed user group.

Closed user group is not defined in the Directive or the Regulations, but recital 16 of the Directive notes that a regulatory framework is not required for one defined by voluntary agreements under private law between a specified number of participants – we consider this to be a "closed user group". It can be taken therefore that Supervision does not cover the issuing of certificates to persons in a defined group that has its own contractual arrangements, under which protections can be negotiated and agreed.

Prior authorisation is expressly forbidden in Article 3.1 of the Directive. When BERR becomes aware of the activities of a CSP issuing qualified certificates to the public it will act to include its details on the Register.

tScheme is the independent, industry-led, voluntary, self-regulatory scheme set up to create strict assessment criteria, against which it approves trust services:

- tScheme was created in response to Part I of the Electronic Communications Act 2000,
- tScheme can approve qualified certification services,
- tScheme approval is separate from the supervision activity.

Go to www.tScheme.org

BERR | Department for Business Enterprise & Regulatory Reform

REGISTER OF
UK ESTABLISHED CERTIFICATION SERVICE PROVIDERS
WHICH ISSUE QUALIFIED CERTIFICATES TO THE PUBLIC

REGISTER

	NAME	ADDRESS	COMMENTS
	British Telecommunications plc	BT Trust Services Helpdesk, PP2 Ty Cynnal, Watkiss Way, Cardiff CF11 0SW	

Details of CSPs to be added to this list should be sent to:

Communications Supply Policy Team
Department for Business, Enterprise and Regulatory Reform
Bay UG 28
1 – 19 Victoria Street
London SW1H 0ET

Published by the Department for Business, Enterprise and Regulatory Reform
www.berr.gov.uk