Contents

1. What is an electronic signature? ................................................................. 3
2. Why should I use an electronic signature? ............................................. 3
3. Security ...................................................................................................... 4
4. Register of UK Established Certification Service Providers (CSPs) that issue Qualified Certificates (QCs) to the public (see Annex B) ............................................................. 4
5. What is the Electronic Signatures Directive? ........................................... 4
6. What is the legal status of an electronic signature? ................................. 4
7. How does an electronic signature equate to a hand-written signature? ... 5
8. How are certification-service-providers (CSPs) supervised? ................... 5
9. Liability ...................................................................................................... 5
10. Data Protection .......................................................................................... 6
11. UK Trust-service Status List (TSL) ............................................................. 6
12. How to check and authenticate the TSL .................................................... 7

Annex A: Definitions ................................................................................... 9

Annex B: Register of UK Established Certification Service Providers that issue Qualified Certificates to the Public .......................................................... 11
1. What is an electronic signature?

An electronic signature is the electronic equivalent of a written signature. Electronic signatures come in many forms, including:

- Typewritten
- Scanned
- An electronic representation of a handwritten signature
- A unique representation of characters
- A digital representation of characteristics, for example, fingerprint, retina
- A signature created by cryptographic means

Electronic signatures can be divided into three groups:

- **Simple electronic signatures** - these include scanned signatures and tickbox plus declarations
- **Advanced electronic signatures** - can identify the user, is unique to them, is under the sole control of the user and is attached to a document in a way that it becomes invalidated if the contents are changed
- **Qualified electronic signatures** - an advanced electronic signature with a digital certificate encrypted by a secure signature creation device e.g. smart card

Electronic signatures are only as secure as the business processes and technology used to create them. High value or more important transactions need better quality electronic signatures - signatures used for these transactions need to be more securely linked to the owner in order to provide the level of assurance needed and to ensure trust in the underlying system.

Better quality electronic signatures can offer:

- **Authentication** – linking the originator to the information
- **Integrity** – allowing any changes to the information provided to be detected more easily
- **Non-repudiation** – ensuring satisfaction (in a legal sense) about where the electronic signature has come from

2. Why should I use an electronic signature?

Those involved in a 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 and that the sender can be identified. There may also be a need for it to reach its destination without being read by anyone else.

Trust is the basis of business and commerce and can be enhanced by the use of electronic signatures. Some types of electronic signatures can:

- prove the origin of the message
- show whether a message has been altered
- ensure messages remain confidential
3. Security

More information on this issue can be found in the document: “The tScheme Guide to Securing Electronic Transactions” that can be found at:

http://www.tscheme.org/library/tSi0256_1.0%20The%20tScheme%20Guide.pdf

_tScheme is the independent, industry-led voluntary, self-regulatory scheme set up to create strict assessment criteria against which it approves trust services. tScheme can approve certification services; approval is separate from the supervision activity.

For further information go to: http://www.tscheme.org/index.html

4. Register of UK Established Certification Service Providers (CSPs) that issue Qualified Certificates (QCs) to the public (see Annex B)

The Secretary of State is required to:

- review the activities of CSPs established in the UK that provide QCs to the public
- establish and maintain a register of those CSPs
- publish the register
- have regard to any evidence of the conduct of CSPs, which is detrimental to users of QCs, with a view to publishing that evidence

Note: the Register (and thus supervision) only includes those organisations that sign QCs issued to the public to support the use of advanced electronic signatures and excludes their agents, distributors etc along with any registration authorities.

5. What is the Electronic Signatures Directive?

- Directive 1999/93/EC on a Community framework for electronic signatures was published on 19th January 2000. The Directive is designed to help the proper functioning of the internal market by ensuring the free movement of electronic signatures and supporting services and products. Member States are required to implement the requirements set out in the Directive in their national legislation.
- In the UK, the Directive is implemented into law by the Electronic Communications Act 2000, and the Electronic Signatures Regulations 2002 (SI 2002 No. 318)

6. What is the legal status of an electronic signature?

- 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 used – from “simple” to “advanced” electronic signatures. (The Directive does not mention simple electronic signatures but, in practice, this is taken to mean any signature that would
have a low evidential value.) Article 5.2 is implemented into UK law through section 7 of the Electronic Communications Act 2000.

7. How does an electronic signature equate to a handwritten 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 handwritten signature.
- Such signatures are commonly referred to as Qualified Signatures although this term is not 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 handwritten signature is already capable of being satisfied by an electronic signature, 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 requirements of Article 5.2 for any electronic signature and is implemented into UK law through Section 7 of the Electronic Communications Act 2000.

8. How are certification-service-providers (CSPs) supervised?

- Article 3.3 of the directive requires Member States to ensure the establishment of an appropriate system that allows for the supervision of certification-service-providers (CSPs) that are established in its territory and issue qualified certificates (QCs) to the public. Article 3.3 is implemented into UK law by Regulation 3 of the Electronic Signatures Regulations 2002.

9. Liability

- Article 6 of the Directive sets out a minimum level of liability that Member States must impose on CSPs that issue qualified certificates to the public. It also allows CSPs to place 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 that reasonably relies on the certificate in respect of:
  - completeness and accuracy of all information at the time of issue
  - 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 can prove it has not acted negligently.

• Articles 6.3 and 6.4 of the Directive 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 for these matters, subject to the applicable Lawson the exclusion or limitation of liability.

• Article 6.3 of the Directive ensures that a CSP can indicate (in a QC) limitations on its use – provided the limitations are recognisable to third parties. The CSP is then not liable if that limit is then exceeded.

10. Data Protection

• 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 of the Directive 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 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 of the Directive goes further and requires that CSPs that issue certificates to the public collect personal data only directly from the data subjects or with their explicit consent and only insofar 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 2002.

• Article 8.3 of the Directive requires that 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.

11. UK Trust-service Status List (TSL)

• Directive 2006/123/EC on services in the internal market (the Services Directive) was published on 12 December 2006 and Article 8 of the Services Directive allows for relevant procedures to be completed electronically and remotely. As a result, a trust mechanism has been put in place in order to provide confidence when completing these procedures online.

• tScheme Limited (see: http://www.tscheme.org/index.html) is the UK’s Trusted List Scheme Operator (TLSO) and creates, hosts and maintains the UK’s Trust Service-status List (TSL) on behalf of the Department for Business, Innovation and Skills (BIS). Every Member State has its own TSL and each of these is referenced from a central list that is maintained by the Commission (see: EU Trusted list certificate providers - further info and policy).
• The key requirements of a TLSO are to provide:
  o the tools to create and manage the TSL
  o a secure means to provide the location of and updates to the TSL
  o information for all related web pages needed to support the UK’s TSL.

12. How to check and authenticate the TSL

• The digest information related to the certificate that supports the electronic signature of the machine-processable and human-readable versions of the UK’s TSL is presented here together with digest information on a new certificate that can be used to electronically sign the TSL in case of expiry or compromise of the current certificate. Only one of the two certificates below is applicable at a time.
• The digital certificate can be authenticated through one of the following digests (sometimes referred to as the thumbprint):
  o The current certificate, which is valid from 20/02/14 until 20/02/2017:
    ▪ SHA-1 digest (Hex) value: 17 9c 15 26 47 92 53 eb b3 39 c2 12 62 73 38 1d e2 77 38 14
  o Or a new certificate that is valid from 08/08/2014 to 08/08/2017:
    ▪ SHA-1 digest (Hex) value: 56 45 69 46 82 b0 e5 8f f8 38 bb 55 96 2f 6e e1 a1 2d e3 b5

Note: the authenticity and integrity of the TSL should be verified by relying parties prior to any use. (More information on authentication can be found at: http://www.tscheme.org/UK_TSL/index.html

Key Legislation:

• The Electronic Signatures Directive 1999/93/EC
• The Services Directive 2006/123/EC
• The Electronic Communications Act 2000
  (see: http://www.legislation.gov.uk/ukpga/2000/7/contents)
• The Electronic Signatures Regulations 2002

See also:

• The Transposition Note for the Electronic Signatures Directive, which is available at: http://www.tscheme.org/library/file34341.pdf
• Electronic Signatures PDF – a guide to their use in business is also available at: http://www.tscheme.org/library/file34339.pdf

Subject to some specific exceptions, the Regulation will apply from 1\textsuperscript{st} July 2016. Further advice on EIDAS will be issued during implementation.
Annex A: Definitions

Article 2 of the Electronic Signatures Directive and Regulation 2 of the Electronic Signatures Regulations 2002 define a number of terms, including:

What is an electronic signature?

An electronic signature is data in electronic form that are attached to, or logically associated with, other electronic data and that serve as a method of authentication. An electronic signature can be created by any means and so is wider in meaning than a number of other terms e.g. digital signature.

What is an Advanced Electronic Signature?

An advanced electronic signature is an electronic signature that is:

- uniquely linked to a signatory
- capable of identifying the signatory
- created by means the signatory can keep and maintain under their sole control
- is 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 met but the use of a secure-signature-creation-device coupled with suitable technology would be one way.

Who is a signatory?

A signatory is a person who holds a signature-creation-device and acts on their own behalf or on behalf of the natural or legal person they represent.

What is a signature-creation-device?

A signature-creation-device is configured hardware or software used to implement signature creation data, examples include a smart card and software running on a PC.

What is signature-creation-data?

Signature-creation-data are codes or private cryptographic keys that are used by the signatory to create an electronic signature, for example, a signing key or a signature private key.

What is a secure-signature-creation-device (SSCD)?

An SSCD is a signature-creation-device that meets the requirements of Annex III of the Directive. Annex III of the Directive requires that, at a minimum, the signature creation data is:

- unique
- capable of being kept secure
- cannot be derived e.g. reverse engineered
• protected against forgery
• protected from the use of others
• unable to alter the data to be signed
• 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 specified – it can therefore be implemented as software, hardware or a combination of both provided it complies with the requirements of Annex III.

What is a certification-service-provider (CSP)?

A CSP is 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?

A certificate is an electronic attestation that links signature-verification-data to a specific person and confirms the identity of that person.

It is a block of data that represents the necessary information that helps to create the link to that person and usually includes: 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 not usually presented in plain text – they are read by an automatic process such as a computer programme and so conform to a standard (X.509 is the common standard for certificates).

What is signature-verification-data?

This is data such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature, including, for example, a signature public key.

What is a Qualified Certificate (QC)?

A QC is a certificate that meets the requirements set out in Annex I of the Directive and is provided by a person (CSP) that complies with the requirements set out in Annex II of the Directive.


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

<table>
<thead>
<tr>
<th>Number</th>
<th>Name of Company</th>
<th>Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>British Telecommunications plc</td>
<td>BT Trust Services Helpdesk PP2 Ty Cymnal Watkiss Way Cardiff CF11 0SW</td>
<td></td>
</tr>
</tbody>
</table>

Details of CSPs to be added to this list should be sent to: uksinglemarketcentre@bis.gsi.gov.uk