



Department for
Business, Energy
& Industrial Strategy

**ELECTRONIC SIGNATURES AND
TRUST SERVICES**

Guide

AUGUST 2016

Withdrawn

Contents

Introduction	3
What this guide explains	3
Background Information	4
Why are e-signatures and trust services important?.....	4
What is an e-signature and why should you use one?.....	4
What is a trust service and why should you use them?	5
What is electronic identification and why is it important?	5
Legislative Background	7
Electronic Signatures	7
Advanced Electronic Signatures.....	7
Qualified Electronic Signatures	7
Electronic Seals	8
Legal effect of electronic signatures, seals, time stamps, registered delivery services and electronic documents	8
Trust Service Providers	9
UK Trust Service Status List (TSL).....	9
How to check and authenticate the TSL.....	9
Data Protection	11
Supervisory Body – Information Commissioner’s Office	12
Annex A – Definitions	13

Introduction

What this guide explains

This guide is intended to assist individuals and businesses in understanding the changes made to the electronic signature regime introduced by Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

The changes made to UK law on electronic signatures are set out below and the requirements of the eIDAS Regulation are explained in general terms. This guide covers basic information about electronic signatures, the introduction of a new framework for trust services, and the supervisory regime. You should refer to the Regulations themselves for a full explanation of the requirements:

- UK Regulation: [The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 \(2016 No.696\)](#)¹ and [section 7 of the Electronic Communications Act 2000](#).²
- EU Regulation: [Regulation \(EU\) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC](#).³

Further requests for information or enquiries should be sent to:
uksinglemarketcentre@beis.gsi.gov.uk

¹ http://www.legislation.gov.uk/uksi/2016/696/pdfs/uksi_20160696_en.pdf

² <http://www.legislation.gov.uk/ukpga/2000/7/section/7>

³ <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN>

Background Information

Why are e-signatures and trust services important?

Businesses and individuals involved in commercial transactions or messaging activities need to have confidence in, and be trusting of, any communication that is sent in relation to that activity. This helps to ensure that documents sent electronically have not been altered in any way, that the sender can be easily recognised, and that the document has the necessary security.

Trust is the basis of business and commercial activity, and can be enhanced by the use of electronic signatures and trust services. Generally, electronic signatures and trust services can prove the origin of the communication or document, show whether a message has been altered and ensure messages remain confidential.

More and more businesses and individuals are using, or are seeking to use, electronic signatures and trust services and, with an increasing number of Government services available digitally, there will be continued growth in this market for some time to come.

What is an e-signature and why should you use one?

Electronic signatures deliver a way to sign documents in the online world, much like one signs a document with a pen in the offline world. 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 or retina scan
- 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 – these are uniquely linked to the signatory, are capable of identifying the signatory, and are linked to data within the signature that can detect any changes made.

- Qualified electronic signatures – an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Electronic signatures are only as secure as the business processes and technology used to create them. High value 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 signatory 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

What is a trust service and why should you use them?

In order to ensure the security and legal validity of an electronic activity, e-signatures are certainly important, but not always sufficient. Trust Services can offer:

- Electronic time stamping – this is data in electronic form which binds other electronic data to a particular time, providing evidence that such data existed at that time.
- Electronic seals – the electronic equivalent of a seal or stamp which is attached or incorporated into a document to guarantee its origin and integrity
- Electronic registered delivery service – this is a service enabling parties to exchange electronic data securely by protecting the data against risk of loss, theft, damage or any unauthorised alterations. The service also provides evidence relating to the handling of the transmitted data, including proof of delivery and receipt.
- Website authentication – a certificate that allows users to verify the authenticity of the website and its link to the entity/person owning the website

What is electronic identification and why is it important?

Online identification is becoming increasingly important as services move online. GOV.UK Verify is the new way to prove who you are online. It gives safer, simpler and faster access to government services like filing your tax or checking the information on your driving licence.

A range of UK Government services are now available for use with GOV.UK Verify. For more information, you can visit the [Verify webpage](#).⁴

Withdrawn

⁴ <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>

Legislative Background

Directive 1999/93/EC on a Community framework for electronic signatures ('Electronic Signatures Directive') established a legal framework for electronic signatures and associated certification services to ensure the proper functioning of the internal market. In the UK, the Directive was implemented into law by the Electronic Communications Act 2000 and the Electronic Signatures Regulation 2002 (SI 2002 No. 318).

The main objective behind the eIDAS Regulation is to update these rules and create a uniform regime for the mutual recognition of electronic identification and trust services throughout the EU.

In the UK, the eIDAS Regulation has been implemented into law by the [Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 \(2016 No.696\)](#)⁵ and [section 7 of the Electronic Communications Act 2000](#).⁶

The eIDAS Regulation is fundamentally split into two parts. The first section deals with electronic identification systems and establishes a legal framework that allows for mutual recognition of identification systems between Member States.

The second section of eIDAS deals with Trust Services and electronic signatures in particular. It clarifies existing rules and introduces a new legal framework for electronic signatures and seals, time stamps, registered delivery services and website authentication, offering greater legal certainty to services that follow eIDAS's rules, which are designed to improve the reliability and trustworthiness of these services.

Electronic Signatures

One important change to this regime is that an electronic signature can now only be used by individuals. Previously, under the Electronic Signatures Directive, an electronic signature could be used by both individuals and corporate organisations. The eIDAS Regulation makes a distinction between natural and legal persons.

Advanced Electronic Signatures

Another change from the new Regulation is the re-definition of the Advanced Electronic Signature, which allows unique identification and authentication of the signer of a document and enables the verification of the integrity of the signed agreement. This authentication is typically accomplished through the issuance of a digital certificate by a Certificate Authority. These certificates have existed for many years and now, under eIDAS, users are able to utilise mobile technology for this activity.

Qualified Electronic Signatures

⁵ http://www.legislation.gov.uk/ukxi/2016/696/pdfs/ukxi_20160696_en.pdf

⁶ <http://www.legislation.gov.uk/ukpga/2000/7/section/7>

The final type of signature defined under the eIDAS Regulation is the Qualified Electronic Signature (QES). While both Advanced and Qualified Electronic Signatures are uniquely linked to the signer, Qualified Electronic Signatures are Advanced Electronic Signatures created by qualified electronic signature creation devices, based on Qualified Certificates. Qualified Certificates can only be issued by a qualified trust service provider, which has been granted its qualified status by the Supervisory Body. The electronic signature creation data must also be stored on a qualified signature creation device such as a smart card, a USB token, or a cloud based trust service.

Electronic Seals

The eIDAS Regulation also introduces the recognition of electronic seals. These are similar to electronic signatures but only available to legal persons, such as corporate entities.

Legal effect of electronic signatures, seals, time stamps, registered delivery services and electronic documents

Articles 25, 35, 41, 43 and 46 of the eIDAS Regulation provides for a harmonised and appropriate legal framework for the use of electronic signatures, trust services and electronic documents, by ensuring the recognition of all as evidence in legal proceedings. Articles 25, 35, 41, 43 and 46 are implemented into UK law through section 7 of the Electronic Communications Act 2000.

Trust Service Providers

The eIDAS Regulation requires Member States to establish, maintain and publish trusted lists, containing information on qualified trust service providers (QTSPs) in their territory, together with information on the qualified trust services they provide.

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, consisting of a list of Trusted Providers that are established in each Member State of the EU (plus members of the European Economic Area).

Under the eIDAS Regulation this Trusted List mechanism has been expanded. These lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.

In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission has [published a central list with links to the national "trusted lists"](#)⁷ and the [central list itself can be found on the Commission's website](#).⁸

[tScheme Limited](#) 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, Energy and Industrial Strategy (BEIS).

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):
 - 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
 - Or a new certificate that is valid from 08/08/2014 to 08/08/2017:

⁷ <https://ec.europa.eu/digital-single-market/eu-trusted-list-certificate-providers-further-info-and-policy>

⁸ https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

- 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

The authenticity and integrity of the TSL should be verified by the relevant parties prior to any use. More information on the list and its authentication can be found on the [tScheme website](#).⁹

Withdrawn

⁹ http://www.tscheme.org/UK_TSL/index.html

Data Protection

Organisations/persons involved with providing trust services are required to comply with Directive 95/46/EC which has been implemented into UK law as the Data Protection Act 1998.

The Information Commissioner's Office is the regulator for the Data Protection Act 1998. A guide on data protection can be found on the [Information Commissioner's Office website](#).¹⁰

Withdrawn

¹⁰ <https://ico.org.uk/for-organisations/guide-to-data-protection/>

Supervisory Body – Information Commissioner’s Office

The UK’s implementing regulations, the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, designates the Information Commissioner’s Office (ICO) as the supervisory body for chapter III of the eIDAS Regulation, on the topic of Trust Services, and provides that it must carry out the tasks set out in Article 17 of the EU Regulation.

The ICO must:

- Take action if necessary in relation to Trust Service Providers if informed that they allegedly do not meet the requirements set out in the eIDAS Regulation. This could mean issuing an enforcement or assessment notice requiring an organisation to take a particular course of action or a fixed monetary penalty of up to £1000;
- Inform other European supervisory bodies and the public about breaches of security or loss of integrity;
- Submit a report to ENISA (European Union Agency for Network and Information Security) on its main activities and any breach notifications on an annual basis;
- Carry out audits on Trust Service Providers where there is a justified reason for doing so;
- Grant, withdraw and renew ‘Qualified’ status to Trust Service Providers; and
- Verify the existence and correct application of provisions on termination plans for Qualified Trust Service Providers including how information will be kept accessible.

Annex A – Definitions

Advanced Electronic Signature – means an electronic signature which meets the requirements set out in Article 26 of the EU Regulation, which specifies the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Certificate – a certificate is an electronic attestation that links signature-verification-data to a specific person and confirms the identity of that person. Under the eIDAS Regulation, certificates come in three forms:

- a 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
- a 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person; and
- a 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued.

Creator of a Seal – means a legal person who creates an electronic seal.

Electronic Seal – means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

Electronic Signature – means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

Electronic Signature Creation Data – means unique data which is used by the signatory to create an electronic signature.

Electronic Signature Creation Device – means configured software or hardware used to create an electronic signature.

Qualified Certificate for electronic signature – means a certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in

Annex I of the eIDAS Regulation. Qualified certificates for electronic signatures shall contain:

- an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;
- a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
- at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;
- electronic signature validation data that corresponds to the electronic signature creation data;
- details of the beginning and end of the certificate's period of validity;
- the certificate identity code, which must be unique for the qualified trust service provider;
- the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- the location where the certificate supporting the advanced electronic signature or advanced electronic seal is available free of charge;
- the location of the services that can be used to enquire about the validity status of the qualified certificate;
- where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

Qualified Electronic Signature – means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

Qualified Electronic Signature Creation Device – means an electronic signature creation device that meets the requirements laid down in Annex II of the eIDAS Regulation.

Qualified Trust Service Provider – means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.

Signatory – means a natural person who creates an electronic signature.

Trust Service – means an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

Trust Service Provider – means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.

For a full set of definitions, please refer to the [EU Regulation](#).¹¹

¹¹ <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN>

OGL

© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk. Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication available from www.gov.uk/bis

Contact us if you have any enquiries about this publication, including requests for alternative formats, at:

Department for Business, Energy and Industrial Strategy
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

Email: enquiries@bis.gsi.gov.uk

BEIS/16/15