



A guide to eSignatures

Introduction

With an ever-increasing demand for remote document signing and customer onboarding processes that help speed up completions and reduce the risk of identity fraud, the use of Electronic Signatures is becoming the norm for many businesses and is now a legally accepted and globally recognised way to complete transactions over the internet. However, some confusion still remains about where, how and when eSignatures can be used.

This guide has been written to explain the background to eSignatures standards and the legal and regulatory position behind them.

What is an Electronic Signature (eSignature)?

In its most basic form, an “electronic signature” or “eSignatures” is a digital record of a transaction or process which replaces the need for a wet ink signature and, when logically associated with other data in electronic form, is used by the signatory to sign. This type of signature has the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation under which it was created e.g., eIDAS in the UK / European Union, NIST-DSS in the USA or ZertES in Switzerland.

In law, the use of Electronic Signatures is deemed to be reliable enough to prove a high degree of “intent” by the signer and therefore provides a more reliable way to confirm such intent by delivering a “digital record” or “digital fingerprint” that can evidence a link between any document, matter or process with the signer(s). Such digital records may be used as evidence in a court of law.

Electronic Signature can be used with many kinds of day-to-day business transactions and two enhanced versions have been developed to provide a much higher degree of eSignature authentication, identity proofing and security which help eliminate risk and detect potential fraud.

What is an Advanced Electronic Signature (AdES)

Advanced Electronic Signature is an electronic signature that has met the requirements set forth under EU Regulations No 910/2014 (e-IDAS regulation) on electronic identification and trust services for electronic transactions. AdES incorporates a number of controls that must be capable of authenticating and linking the signatory to a document, transaction or process in such a way that any subsequent changes to such document, transaction or process can be detected. The signature must be made using an electronic signature creation device that the signatory makes under his or her sole control and has provided satisfactory evidence of this. The use of specific authentication rules is applied to the process which increases the level of authenticity and verification of the signer.

What is a Qualified Electronic Signature (QES)

Qualified Electronic Signature (QES) is an electronic signature that is compliant with EU Regulation No 910/2014 (e-IDAS regulation) on electronic identification and trust services for electronic transactions which uses AdES standards and, in addition, is capable of providing a qualified digital certificate that has been created by a qualified signature creation device (QSCD). For an electronic signature to be considered as a qualified electronic signature, it must comply with the following key requirements;

1. The signatory must be linked and uniquely identified to the eSignature.
2. The data used to create the eSignature must be under their sole control.
3. The ability to detect if any data changed since the eSignature was applied.

4. The ability to ensure the signatory has control over their private key.
5. The ability to keep data confidential and protected from forgery.

Specialised software and the use of Near Field Communications (NFC) based technology with anti-tamper and anti-spoofing face identity checking with liveness detection is used to assist with eSignature validation and identity verification process.

What does the law say about eSignatures?

Since the introduction of the Electronic Communications Act 2000, electronic signatures have been recognised as a legally admissible means of authenticating signatures linked to documents or other matters. The United Kingdom adheres to the European Union's eIDAS regulations, meaning that the UK is aligned with all EU member states and compliant within the European legal framework. An electronic signature that is signed in the UK is recognised in the EU and vice versa.

Section 7 of the Electronic Communications Act 2000 states that in any legal proceedings, "an electronic signature incorporated into or logically associated with a particular electronic communication shall be admissible as evidence in relation to any question as to whether the communication or signature data is authentic".

The signing of documents and deeds electronically will require the use of an operating system or **VirtualSignature** platform that manages the electronic signing process, including the creation, authentication and verification of the electronic signature.

The Law Society of Great Britain has published a number of practice notes and members can obtain copies online at: <https://www.lawsociety.org.uk/topics/in-house/electronic-signatures-the-essentials>

Further information about eIDAS can be found at:
<https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/>

Can a deed be electronically signed & witnessed?

At this time, and to be certain that a deed has been executed properly, a witness must be physically present to witness the act of signature (whether that signature is applied electronically or otherwise) by the person signing the deed. So long as the witness is physically present and, at a distance or not, able to see the signatory sign the document, these are all valid forms of signing and witnessing.

Both the Law of Property (Miscellaneous Provisions) Act 1989 and the Companies Act 2006 (CA 2006) require the "presence of a witness", but they do not specify "physical" presence, so it is not clear that the requirement may be satisfied by remote forms of witnessing such as by video link. However, in a statement published by the Law Commission in September 2019 it states that: "With specific regard to deeds and the witnessing requirements thereof, a deed must be signed in the physical presence of a witness who attests the signature. This is the case even where both the person executing the deed and the witness are executing/attesting the document using an electronic signature."

Can a Will be legally signed & witnessed electronically?

UK estate planning laws that dictate the requirements of a legal Will are written into the 1837 Wills Act. and, therefore, electronic signatures are not legally accepted. Currently,

testamentary wishes written by email, in an app, video Wills, faxed, scanned, or any other electronic copy of a document are all invalid Wills. In July 2017, the Law Commission announced that the signing of Wills needed to be updated to reflect modern technology available today.

Are eSignatures accepted by the UK HM Land Registry?

HM Land Registry accept eSignatures and the Law Commission concluded that an eSignature was capable, in law, of being used to execute a document or deed. The Law Commission also concluded that an electronic signature could be witnessed in the same way as a wet ink signature, provided the witness could attest to seeing the signatory adding their signature to the document or deed via a suitable electronic device.

In July 2020 HM Land Registry announced its decision to allow the use of eSignatures on deeds and published its guidance for solicitors and conveyancers. HM Land Registry are presently in the process of drafting their **“Safe Harbour”** standards in order to provide a benchmark against which legal firms can check that their procedures are aligned with minimum eSignature verification and security requirements. HM Land Registry will, for the time being, accept for the purposes of registration certain deeds that have been electronically signed in accordance with the requirements set out below:

1. All the parties agree to the use of electronic signatures and a platform in relation to the deed.

2. All the parties have conveyancers acting for them, except that only the lender in the case of a mortgage, discharge or release, the personal representatives in the case of an assent and the donor in the case of a power of attorney need have conveyancers acting for them. If any party is unrepresented (other than in the situations just outlined), including a party who is not signing themselves, electronic signatures cannot be used by any of the parties involved. Where a deed is to be signed electronically by a party's attorney, and the deed is one other than the power of attorney itself, a conveyancer must be acting in respect of the execution, but it does not matter for the purposes of these requirements whether the conveyancer was instructed by the party or by the attorney.

3. A conveyancer is responsible for setting up and controlling the signing process through the platform.

HM Land Registry permit the following;

- **A deed that effects one of the dispositions referred to in section 27(2) and (3) of the Land Registration Act 2002.**
- **A discharge or release in form DS1 or form DS3.**
- **Equivalent deeds in respect of unregistered land.**
- **An assent of registered or unregistered land.**
- **A power of attorney other than a lasting power of attorney.**

In addition, they will accept a deed of substituted security in respect of registered land, incorporating a discharge or release and a grant of a new charge, that has been electronically signed in this way, even though the discharge or release will not be in form DS1 or form DS3, provided there is nothing to prevent the deed from being regarded as sufficient proof of satisfaction of the charge (rule 114 (4) of the Land Registration Rules 2003).

The signing and dating process follows a defined procedure as set out in Practice Guide 8 / 13.3: <https://www.gov.uk/government/publications/execution-of-deeds/practice-guide-8-execution-of-deeds#our-requirements>

Further information from HM Land Registry can be found at: <https://www.gov.uk/government/news/hm-land-registry-to-accept-electronic-signatures>

What is the position between the UK and European Union for eSignatures?

EU regulation no longer applies in the UK. However, the UK government has incorporated the eIDAS rules into UK law. Thus, electronic trust service providers operating in the UK will need to comply with eIDAS rules under the UK eIDAS Regulations.

The Information Commissioners Office (ICO) explains: “following withdrawal from the EU, the EU eIDAS Regulation was adopted into UK law, amended by Part 1 of the UK exit regulation. In addition, the existing UK trust services legislation is also amended by Part 1 of the UK exit regulation. Taken together, these amended texts are referred to in this guidance as the UK eIDAS Regulations.”

This guide outlines the eSignatures standards, typical use and eSignature platform requirements.			
eSignature Standards	Standard eSignatures	Advanced eSignatures (AdES)	Qualified eSignatures (QES)
Transaction Risk	Low	Medium	High
Description	A Standard Electronic Signature refers to data in an electronic format that is logically associated with others. Applying an eSignature to a document, matter or transaction is legally accepted in law as the signers intent or acknowledgement to its content. However, Standard eSignatures do not require any type of signer identification.	An Advanced Electronic Signature (AdES) uniquely links the eSignature to a document, matter or transaction through a series of authentication processes that give it legitimacy and validity. The eSignature creation device ensures that the content cannot be modified or tampered with and that the signer has control over the process.	A Qualified Electronic Signature (QES) uses AdES standards together with the most advanced NFC-based identity certification technology that is capable of proving that the signer is who they say they are. In addition, the signer must have access and control of an internet enabled device (mobile phone) that can be identified and has the capability of generating an electronic certificate.
Regulatory Governance	ICO-eIDAS	ICO-eIDAS/LSGB/HMLR	eIDAS/LSGB/HMLR
Typical Use	All general consent forms, standard contracts and agreements.	Most licences agreements,*deeds and online bank data / funds transfer	As Advanced eSignature standards + Commercial & residential property transactions**
eSignature Creation Device Requirements			
Signer Authentication	No	Yes	Yes
Anti-Tamper Technology	No	Yes	Yes
Signer Identity Certification	No	No	Yes

*Please refer to regulatory practice notes at all times. **HMRC restrictions apply.