Explaining Electronic Signatures

August 2021

Author: Ben Semple, Pinsent Masons LLP

OPEN IDENTITY EXCHANGE

The Open Identity Exchange (OIX) is a technology agnostic, non-profit trade organisation of leaders from competing business sectors focused on building the volume and velocity of trusted transactions online. OIX enables members to expand existing identity services and serve adjacent markets. Members advance their market position through joint research and engaging in pilot projects to test real world use cases. The results of these efforts are published via OIX white papers and shared publicly via OIX workshops. OIX members work together to jointly fund and participate in pilot projects (sometimes referred to as alpha projects). These pilots test business, legal, and/or technical concepts or theory and their interoperability in real world use cases. OIX operates the OIXnet trust registry, a global, authoritative registry of business, legal and technical requirements needed to ensure market adoption and global interoperability.

Contact:

Nick Mothershaw, Chief Identity Strategist

nick.mothershaw@openidentityexchange.org

PINSENT MASONS LLP

Pinsent Masons is a full-service international law firm. We respond to the pressures and opportunities facing businesses globally with legal excellence and innovation.

With office locations on four continents, wherever your commercial interests take you, we have the footprint and expertise to provide support. We recognise that giving a first class service goes beyond just legal excellence. A deep understanding of local cultural and commercial issues, and an innovative approach, underpins all of our advice. We understand the key political, economic, commercial and regulatory issues, helping to minimise risk and maximise opportunities.

We provide a strong local presence with an excellent understanding of the local market, backed up by our innovative technologies and global resources.

Contact:

Pippa Whitmore, Legal Director

Pippa.Whitmore@pinsentmasons.com

THE INVESTING AND SAVINGS ALLIANCE

The Investing and Saving Alliance's (TISA) is a unique industry-wide membership organisation. Our mission is to bring the UK financial services savings industry together to promote collective engagement, to deliver solutions and to champion innovation for the benefit of citizens, our industry and the nation.

We do this by focusing on good consumer outcomes and harnessing the power of our broad industry membership base to deliver practical solutions, new digital infrastructure and by devising innovative, evidence-based strategic proposals for government, policy makers and regulators. This holistic approach to address the major consumer issues uniquely positions TISA to deliver independent insight, promote innovation and facilitate good practice. TISA's rapidly growing membership is representative of all sectors of the financial services industry. We have over 200-member firms involved in the supply and distribution of savings, investment products and associated services, including the UK's major investment managers, retail banks, online platforms,

insurance companies, pension providers, distributors, building societies, wealth managers, third party administrators, Fintech businesses, financial consultants, financial advisers, industry infrastructure providers and stockbrokers.

Contact:

Harry Weber Brown, Executive Director

Harry.weber-brown@tisa.uk.com

TABLE OF CONTENTS

BACKGROUND

Prior to the outbreak of the COVID-19 pandemic in March 2020, where parties to a transaction were not physically present at the same meeting to sign documents, common practice was for the lawyers involved to arrange a 'virtual signing' via email. This typically involved the relevant document being sent to the signatory/ies or their lawyers as a .pdf, the signatory/ies printing the document to sign a hard copy document in wet ink, converting the document and signature into electronic form by scanning them and returning the signed document by email. However, with social lockdowns being implemented across the globe to tackle the spread of the novel Coronavirus, resulting in many people being forced to work from home without access to a printer or scanner, this virtual signing process has been rapidly replaced with the use of electronic signatures created using dedicated electronic signature software platforms.

Regulation (EU) No. 910/2014 ("**eIDAS**") defines an electronic signature as "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". Put simply, it is two **connected** sets of data:

- one set of data that comprises the electronic document or contract (e.g. a Word document, a .pdf, html behind a web page); and

- another set of data that is created by someone "signing" that document.

The data created to sign a document can take many different forms, from an electronic representation of a handwritten signature to a digital representation of biometric characteristics, for example, a fingerprint or a retina scan.

Using a dedicated electronic signature software platform allows a company or an individual to send important documents to anyone in the world using a computer or smartphone through trusted electronic signature software. Once received, the recipient can input their signature, accept the terms, and send it back in less than a minute. In comparison, the traditional means of collecting signatures via mail and even the virtual signing process via email can require a great deal more time, money, and paper. Stacks of paper must be printed, copied, distributed, and stored for safekeeping. The entire process can be costly, time-consuming, and environmentally unsustainable. With electronic signatures, companies can save valuable time and money that would have otherwise been spent collecting physical signatures using more traditional methods.

Furthermore, businesses and individuals involved in commercial transactions need to have confidence in, and be trusting of, any communication that is sent in relation to that activity. Trust is the basis of business and commercial activity and can be enhanced using electronic signatures and trust services. Generally, electronic signature software platforms and trust services can prove the origin of the communication or document, show whether a message or contract has been altered and ensure information remains confidential. 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.

These are just a few of the reasons why the use of electronic signatures and trust services by businesses and individuals around the world has grown exponentially since the outbreak of the COVID-19 pandemic. Electronic signatures had been increasingly common in the market before 2020 but, as office spaces across the globe were closed, businesses transitioned to using dedicated electronic signature software platforms, such as DocuSign or Adobe Sign, to execute their documents in extraordinary numbers. With working practices having perhaps changed permanently and with an increasing number of government and business services available digitally, it is likely that there will be continued growth in this market in the coming years. It is therefore increasingly important that the market has a sound understanding of the practical and legal implications when using different types of electronic signatures.

TYPES OF ELECTRONIC SIGNATURES

eIDAS sets the standard for three different types of electronic signature: Simple, Advanced and Qualified. eIDAS includes additional options to the Advanced electronic signature in terms of how the identity of the signatory is established (by use of a Qualified Certificate ("**QC**")) and in the cryptographic process used to create the electronic signature (by use of a Qualified Signature Creation Device or QSCD). If both options are employed then eIDAS defines this as being a Qualified electronic signature. From a legal standpoint, there is a significant gap between Qualified electronic signatures and Simple electronic signatures. In practical and technological terms too, there is a marked difference. Qualified Certificates have strict regulatory constraints in terms of how the identity of the signatory is verified and, similarly, QSCDs have to be certified by National Technical Authorities (such as CESG). Simple and Advanced signatures offer a probative value for certain use cases, but a Qualified electronic signature is the only electronic signature type to have special legal status in the UK (as well as EU member states) offering a legal equivalent of a traditional wet signature. Whilst eIDAS stated in Article 25 that electronic signatures shall not be denied admissibility as evidence in legal proceedings, recital 49 made it clear that it is for national law of the participating member states of the EU to dictate the legal effect and evidential weight of different types of electronic signatures.

Simple Electronic Signature

This is the most basic form of electronic signature and habitually used in the UK market. Electronic signature software platforms, such as DocuSign and Adobe Sign, are predominantly used in the UK to create simple electronic signatures.

Other forms of simple electronic signature include email auto-signatures, typing a name at the foot of an email, typing a name into an electronic form of a document, using a finger or stylus to sign on a pad (e.g. when receiving a parcel) and electronically pasting a signature in the form of an image into a soft copy version of a contract in the appropriate place.

Although it is not strictly required, parties will often take several precautions to minimise risk and give as much probative value to a simple electronic signature as possible, particularly when signing important documents. For example, it is common practice when using electronic signature software platforms to send a PIN to the signatory by telephone call or by text which must be entered to access the document. A PIN provides two-factor authentication to combat the risk of a signatory's inbox being compromised. This adds a degree of protection in that (in many cases) the party sending the document will not only use the signatory's phone number to contact them but may also recognise the signatory's voice, adding to the certainty that it was the correct signatory who signed. If the PIN is relayed by text, this adds to the electronic evidence trail, and may provide clarity as to the identity of the signatory if the validity of signature were to be challenged.

Advanced Electronic Signature

This is more secure than a simple electronic signature because it requires a connection with the individual signing the document – some sort of identity authentication. This is defined in eIDAS as:

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

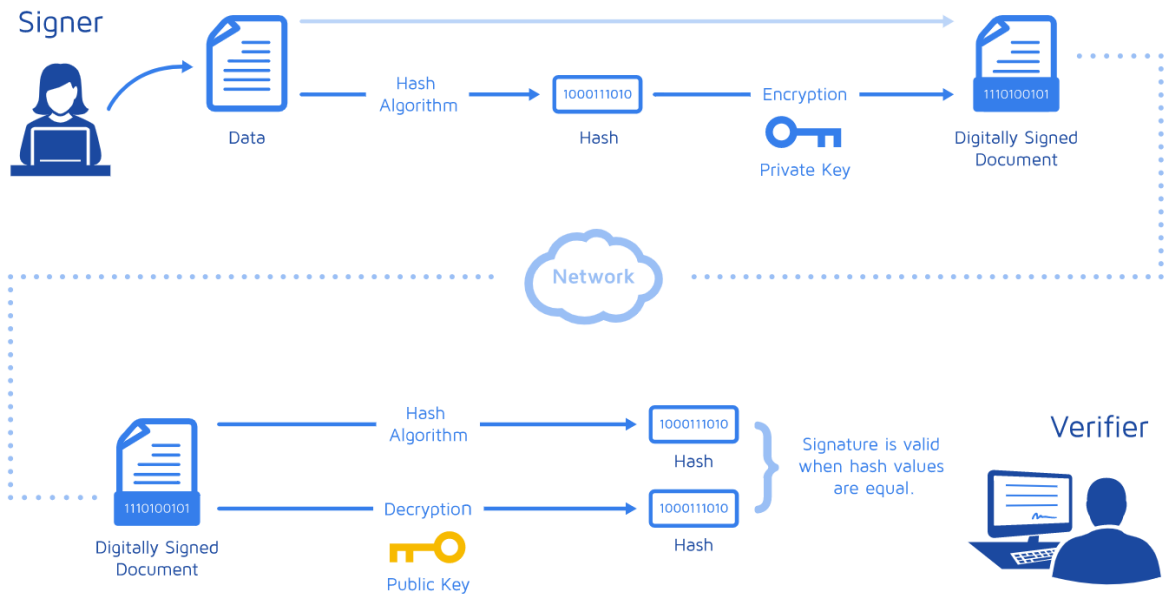
The most common form of advanced electronic signature are digital signatures based on Public Key Infrastructure (PKI), which satisfy all the above requirements.

Digital signatures rely upon advanced cryptography to produce results by using a secret value (key) that cannot easily be guessed or discovered by trying possible answers one at a time – it would just take too long. There are two kinds of cryptography available – symmetric (the same key encrypts and decrypts) and asymmetric (two different keys: one to encrypt and one to decrypt). Symmetric is faster and more efficient (it is used in online secure transactions indicated by the padlock symbol) but it is obviously very difficult to share securely. In asymmetric cryptography, one key is kept secure (i.e. private) and the other can be shared (i.e. public).

If you are trying to keep information confidential and only want the recipient to be able to read it then imagine that they provide online 'padlocks', anyone can then use one of these padlocks safe in the knowledge that only the recipient has the key to unlock it. If you are using digital signatures then the analogy is reversed and you provide online keys so that when you sign (or padlock) a document the recipient knows it was signed by you because they can only unlock it with one of your keys. Don't worry about the potential for confusion though as each of these online keys and padlocks come with a certificate that says who it belongs to and whether it is a key or a padlock – this certificate service is all provided by a Public Key Infrastructure made up of trustworthy Certificate Authorities ("**CA**").

When a signatory electronically signs a document, it is chopped up into equally sized chunks that are repeatedly compressed (using a known hashing algorithm like SHA-256) until a single chunk is left – the hash or digest of the message, which along with the date and time is then encrypted using the signatory's private key, which must be securely kept by the signatory. The recipient then performs the same hashing function and also produces the hash of the message and if this matches the received hash (after it has been decrypted using the signatory's public key) then you can be confident that the message is from the signatory and has not be altered.

As an example, Jane signs an agreement to sell a timeshare using her private key. The buyer receives the document. The buyer who receives the document also receives a copy of Jane's public key. If the public key can't decrypt the signature (via the cipher from which the keys were created), it means the signature isn't Jane's, or has been changed since it was signed. The signature is then considered invalid.[1]



[2]

As mentioned earlier, to protect the integrity of the signature, the process requires that the keys be created, managed and stored in a secure manner, and requires the services of a reliable CA. A CA can be the digital signature provider themselves or a trusted independent third party. PKI also enforces additional requirements, such as a digital certificate[3], end-user enrolment software, and tools for managing, renewing, and revoking keys and certificates. Although electronic signature software platforms, such as DocuSign and Adobe Sign can be used to create Advanced electronic signatures they are less prolific in the present market due to the added financial and administrative costs required to all the requirements listed above.

Qualified Electronic Signature

This is the most secure type of electronic signature because it carries additional cybersecurity beyond that of an advanced electronic signature and the authentication process for

[1] DocuSign Inc, 2021, accessed 11 July 2021, < https://www.docusign.co.uk/how-it-works/electronic-signature/digital-signature/digital-signature-faq>

[2] Ibid

[3] A "digital" or "public key" certificate provides a safe way for an entity to pass on its public key to be used in asymmetric cryptography. A digital certificate can be thought of as the digital equivalent of a passport. It is issued by a trusted organization and provides identification for the bearer. A trusted organization that issues public key certificates is known as a Certificate Authority or, to use eIDAS terminology, a 'Trust Service Provider' ("**TSP**"). The CA can be likened to a notary public. To obtain a certificate from a CA, one must provide proof of identity. Once the CA is confident that the applicant represents the organization it says it represents, the CA signs the certificate attesting to the validity of the information contained within the certificate.

signatories is carried out by a Qualified Trust Service Provider ("**QTSP**"), which are strictly regulated under eIDAS. The authentication process for Advanced electronic signatures is much less rigorous and is often delegated by the CA to a separate body to carry out the ID check. As mentioned above, Qualified electronic signatures are the only electronic signatures to which eIDAS gives the same legal effect as a handwritten signature.

A Qualified electronic signature is an advanced electronic signature - with all the features outlined above - that is also:

- based on a QC for electronic signatures, provided by a service provider that has been audited and certified by an accreditation provider under eIDAS. A QC can only be purchased from a CA that is certified as a QTSP[4]; and

- created by a Qualified Signature Creation Device ("**QSCD**"). This might be a USB token, a SmartCard, or a cloud-based trust service.

Qualified Certificates - The Identity Verification Process

Before a user can create a Qualified electronic signature they will need to be issued with a QC, and for that they will need to pass through an Identity verification process. This is conducted by the relevant QTSP in accordance with national law in conformance to eIDAS regulation.

There are myriad ways in which the QTSP can verify the identity of the user. Traditionally the process has relied on a face-to-face check of the user's ID document (usually a passport, driving licence or identification card) alongside a signed personal statement and other secondary documentation (proof of address)[5].

In eIDAS there is a distinction between a signature, which is produced by a natural person, and a seal, which is produced by or on behalf of a legal person – although they both use the same cryptographic process. If an individual is applying for a QC on behalf of an organisation then information verifying the organisation's identity, address and the individual's affiliation with that organisation will also be required.

In recent times more QTSPs use video conferencing, which negates the requirement for the physical meeting, but does present some dependencies such as an appointment booking and availability of an agent to conduct the process. Some of the more innovative QTSPs have gone a step further again and are able to meet the eIDAS requirements to create a Qualified

[4] A QTSP is accredited by a supervisory body in the Member State where it is established. In the UK, a QTSP is given that status by the Information Commissioner's Office. While a Qualified electronic signature based on a QC cerified by a QTSP established within an EU Member State is legally recognised in the other 26 Member States and in the UK, it should be noted that a QTSP established in the UK is not currently recognised in the EU.
[5] European standards for identity proofing processes have been aided by the publication of ETSI Technical Specification 119 461, which was published in July 2021. This document aims to specify policy and security requirements for a 'trust service component' providing identity proofing of trust service subjects.

electronic signature via an automated end-to-end remote customer journey without any need for video conferencing.

There is also an obligation on the QTSP to ensure that the claimed identity of the user is a real person and is the same person as the one creating the account. Therefore, a liveness check using liveness detection software will also be required. The entire process is facilitated differently depending on the QTSP in question but must be conducted in accordance with Article 24 of eIDAS. Once the user identity has been verified and the liveness check has been carried out the QTSP can issue the QC to the user.

Qualified Electronic Signatures – Signing Methods and Authenticators

Qualified electronic signatures can be generated in two different variants, which differ mainly in regard to where the signatory's private key is stored and whether a QTSP needs to be involved:

1. Local Qualified Electronic Signature

The private key for a local Qualified electronic signature is hosted on the signer's device. These signatures can be generated on a cryptographic card, through a USB token or by using cryptographic signature software. This type of Qualified electronic signature works in most operating systems and browsers since it is installed on the signer's device previously.

The token or smart card is bound to the signatory so that when they are required to sign a document the device has the assurance that it is them. The private key must be appropriately protected and reliable and therefore must be kept safe and secure. Keeping them thus can be burdensome. Factor in the time and financial expenditure required to revoke and replace a device if it is lost and one begins to understand why adoption in the UK for Qualified electronic signatures has been relatively low (particularly given there is limited legal need for anything more than a simple or advanced electronic signature).

2. Remote Qualified Electronic Signature

The private key is located in a single repository on a secure and supervised server called a Hardware Security Module ("**HSM**").

This second type of Qualified electronic signature is more commonly used by organisations rather than individuals; it is more versatile, the signatory can access it from any computer or mobile device with internet access and has sole control over the private key.

A remote Qualified electronic signature allows the signing process to be carried out remotely with a two-factor authentication of the signatory once the signature request is triggered. In effect presenting a virtual smart card solution. Whilst the technology and cryptography of a QTSP's service may be far too complicated for many to comprehend, for the user the process of signing a document is now very straight-forward. With cloud-based software, QTSPs use HSMs to hold keys on behalf of their users, as opposed to storing the keys on physical hard-

ware tokens. A signatory who uses a QTSP offering this service, uses the HSM to securely hold the signing keys, so there is a much lower risk of them being lost or stolen. Signatories can securely sign documents using their smart phone, tablet or another electronic device, which they are much less likely to lose or forget and means that the physical tokens aren't required to be re-issued making for a better experience for all involved and a more sustainable model. The use of HSMs is likely to be an important factor in galvanising the market as is the ability of QTSPs in being able to verify the identity of the signatories remotely.

Table

The information detailed above can be summarised in the following table:

Types	SES			AES	AES with QC	QES
Methods	Hard Copy Signed - Scanned and Emailed	Signing Platform	Signing Platform - Use of 2FA	Signing Platform – Uniquely identifying the individual		
Uniquely linked to an individual				✓	✓	✓
User verified to defined standard (eIDAS)					✓	✓
User issued with electronic signing mechanism						✓

THE LAW IN ENGLAND, WALES & NORTHERN IRELAND

Summary

There is no legislation or case law in England, Wales or Northern Ireland specifically confirming the validity of, or evidential weight relating to, electronic signatures, and only a handful of cases which focussed on the use of electronic signatures.

An electronic form of words meets the requirement to be "in writing" (per the Interpretation Act 1978) and therefore can be used to evidence offer, acceptance and agreed terms. What constitutes a signature is generally flexible and (save for some statutory exceptions) there is no prescribed type.

In 2019 the Law Commission published a report on electronic execution of documents. Based on common law principles the Law Commission were of the view that electronic signatures can be used to validly execute a document, including a deed, if:

- the person signing the document does so intending to authenticate it; and
- any formalities relating to execution of that document are satisfied. Those formalities might be, for example, that the signature is witnessed or in a particular form. The formalities might be required, for example, by statute, by private contract or by an entity's constitution.

Law Commission report and JWP Guidance

The Law Commission's report specifically endorsed the views expressed in 2016 guidance on the use of electronic signatures produced by a joint working party of the Law Society Company Law Committee and The City of London Law Society Company Law and Financial Law Committees (the "**JWP Guidance**"). A statement by the UK Government in March 2020 endorsed the Law Commission's findings.

Importantly, the Law Commission's report stated:

"*An electronic signature may satisfy a legal requirement for a document to be "signed" and it can be admitted in evidence in legal proceedings. However, parties will also need to consider the evidential weight (or probative value) which may be given to that signature if there is a dispute about, for example, who in fact signed the document, whether they intended to be bound, or about the content of the document.*"

Whilst the Law Commission's report does not create or state the law, it would be influential in a court and therefore was instrumental in establishing market practice on the use of electronic signatures.

Here are links to the Law Commission report, the government's statement and the JWP Guidance:

- Law Commission Report
- Government statement on Law Commission Report
- JWP Guidance

Validity for simple contracts – England, Wales, and Northern Ireland

As outlined in the JWP Guidance above, the risk that a court will find a simple electronic signature created using an electronic signature software platform to be incapable of creating a contract is minimal, unless there is statutory authority stating otherwise. However, while certain contracts may be lawfully executed using a simple electronic signature note should be taken that certain registry bodies will not accept them and continue to insist on the use of a wet signature. While most public bodies have permitted the use of electronic signatures during the COVID-19 pandemic some do not, e.g. the Office of the Public Guardian in relation to Lasting Power of Attorney forms.

Validity for deeds – England & Wales

This is a step further than the first risk, namely the challenge that whilst a contract can be created using an electronic signature software platform, a deed cannot. The Law Commission believed a simple electronic signature can be used to create a deed but recognised difficulties around whether someone can witness an electronic signature.

In their guidance, the Law Commission stated that deeds could be signed using electronic signatures but also noted that witnesses to that signature must be *physically* present. Witnessing via video conferencing will not be accepted as a valid method for observing the signature being applied. During social lockdowns this has obviously been somewhat difficult. It may be possible in certain circumstances if those signing have an adult member of their household physically with them and that adult household member is not in any way involved in the transaction, for that adult household member to act as witness. However:

- Some documents which are required to be witnessed cannot be witnessed by family members (e.g. some Governmental forms and powers of attorney)[6];

- Many financial institutions are nervous about using non-connected parties as witnesses - not just for their own signatories, but also for other parties. Some organisations may also have policies prohibiting family members from acting as a witness for bank signatories so as not to disclose the home address of staff members; and

- There are additional security and confidentiality issues with witnesses signing on electronic signature software platforms. For example, stopping a witness from

[6] The Law Society issued guidance in January 2021 with useful tips on witnessing documents being signed using an electronic signature.

receiving a full copy of the execution document, although the witness only needs to witness the signature on the signing page.

For Companies and LLPs, a deed can be created without the need for a witness: if two authorised signatories sign (e.g. two Directors, two Members). This sidesteps the concerns around witnessing electronic signatures. On 27 July 2020, HM Land Registry announced that they would accept dispositionary deeds (such as transferring, creating leases and securing mortgages) that have been signed by way of a witnessed electronic signature. This announcement was published alongside very prescriptive requirements on electronic signatures which are detailed (as at August 2020) in their guidance and in their execution practice guide here.

In short, while witnessing a deed that has been signed using an electronic signature is technically possible, under the current restrictions and requirements of HM Land Registry and other registry bodies it is incredibly cumbersome.

Validity for deeds – Northern Ireland

When it comes to executing documents, the law in Northern Ireland generally tends to reflect the law in England & Wales. However, there is an old case from the 16th century that is creating some uncertainty around the validity of using electronic signatures to sign deeds in Northern Irish law.

Goddard's Case (*Goddard v Denton* [1584] 76 ER 396) established that the "essence and substance" of a deed must be made in writing and cannot be made orally. There were additional requirements established in that case, including that a deed must be written on paper or parchment or vellum and not on any other substance, including wood, stone, slate, linen, cloth, leather or steel. These additional requirements were understandably abolished by the Law of Property (Miscellaneous Provisions) Act 1989 (LP(MP)A 1989). The difficulty arises because this piece of legislation does not apply to Northern Ireland and so the rather antiquated requirements of Goddard's Case still apply there as no legislation has been passed abolishing the rather antiquated requirements in that jurisdiction.

Documents created, signed and delivered using an electronic signature software platform are of course not written or signed using paper or parchment and so their validity is uncertain. Furthermore, the Land Registry in Northern Ireland does not accept deeds signed using electronic signatures like the Land Registry in England and Wales. While market views differ as to whether such an old piece of law would be upheld in court given the drastic changes to the law and to business practice since the 16th century, deeds in Northern Ireland continue to be signed using the traditional wet ink method to minimise the risk being assumed by the signing parties.

THE LAW IN SCOTLAND

Summary

The law on electronic signatures in Scotland is set by statute. Electronic signatures can be used to create valid contracts. An Advanced electronic signature supported by a QC and, by extension, a Qualified electronic signature are self-proving, other forms of electronic signature are not. Some electronic documents[7] require an Advanced electronic signature to be valid and must be self-proving to be registrable. In practice, Registers of Scotland do not yet accept most electronic documents[8]. This means that electronic signatures should not be used for any documents which may require to be registered in the Land Register, the Sasine Register or the Books of Council and Session.

Law Society of Scotland Electronic Signatures Guide

The Law Society of Scotland has published a guide on electronic signatures.

Legislation governing electronic signatures

Electronic documents and electronic signatures in Scotland are dealt with in the Land Registration etc. (Scotland) Act 2012 (the "**2012 Act**") and the Electronic Documents (Scotland) Regulations 2014 (the "**2014 Regulations**"). The 2012 Act amends the Requirements of Writing Act (Scotland) Act 1995 (the "**1995 Act**") to permit electronic documents to have equivalent status and standards of validity and authenticity to paper documents[9]. The legislation uses the term "authenticating" a contract rather than "signing" a contract. This should not be confused with the process for authenticating a signatory's identity as discussed above, the term authenticating in the legislation refers solely to the act of signing a document.

Self-proving documents

Electronic documents executed using a simple electronic signature or advanced electronic signature that is not supported by a QC will not be self-proving. If their validity were challenged, you would need to prove that there was an offer, acceptance, agreed terms and an intention to be bound.

A self-proving document shifts the burden of proof. Self-proving documents are assumed to be valid unless it is proven otherwise (e.g. by establishing fraud, undue influence or duress).

---

[7] Set out in section 1(2) of the Requirements of Writing (Scotland) Act 1995. Whilst section 1(2) includes the making of any will, testamentary trust disposition and settlement or codicil, it is not possible to sign these electronically because the relevant statutory enabling provisions are not yet in force for testamentary writings (Land Registration etc (S) Act 2012 (Commencement No. 2 and Transitional Provisions) Order 2014 (SSI 2014/41), art 3 and Sch).

[8] Registers of Scotland will accept electronic signatures on documents submitted to them via the Automated Registration of Title to Land (ARTL) system and on electronic discharges. However, some larger firms in Scotland do not use the ARTL system or the electronic discharge system primarily because ARTL caters for only very limited types of transactions and the electronic discharge system is geared to residential rather than commercial transactions.

[9] Testamentary writings are excepted because the enabling legislation is not yet in force.

Validity – Scotland

The Requirements of Writing (Scotland) Act 1995 requires agreements which must be registered in the Land Register (for example a Standard Security) to be self-proving. Self-proving means that the document is presumed to have been signed by the signatory. If a document is self-proving the burden of proof is on the party disputing that a signatory signed the document. It is for the challenger to prove the contract was not validly executed.

Documents required under s.1(2) of the 1995 Act need an Advanced electronic signature for validity and a Qualified electronic signature to be self-proving. Simple electronic signatures, such as those generated routinely using an electronic signature software platform can be used to sign other (non s.1(2)) contracts but they will not be self-proving and should not be used for documents that are required to be executed in accordance with s.1(2). For parties using simple electronic signatures there would be an additional evidential burden – on the balance of probabilities – to show that a contract was formed, should that be challenged by the counterparty.

Table

The information detailed above can be summarised in the following table:

Types	SES			AES	AES with QC	QES
Methods	Hard Copy Signed - Scanned and Emailed	Signing Platform	Signing Platform - Use of 2FA	Signing Platform – Uniquely identifying the individual		
Legal Equivalent to Wet Ink Signature						✓
E&W Valid for Simple Contracts	✓	✓	✓			
E&W Valid for Deeds	Yes – but practical challenges with witnessing					
NI Deeds*	✗	✗	✗			
Scotland					Achieves Self Proving Status	

*As mentioned above, there remains uncertainty in Northern Ireland due to *Goddard's Case*. While it is common practise to have Northern Irish law deeds signed with wet ink as the safest mode of execution, it is not unheard of for Northern Irish law deeds to be signed using electronic signatures as the ruling in *Goddard's Case* is several centuries old.

ELECTRONIC SEALS

eIDAS introduced electronic seals as a solution for legal entities, allowing them to protect authenticity and integrity of electronic documents and data. An electronic seal is based on the same technology as an electronic signature and can be simple, advanced (with or without a QC) and qualified.

Some commentators have equated the electronic seal with an electronic signature for companies. But that is technically inaccurate. An electronic seal is not a substitute for a common seal and will not satisfy the statutory requirements for execution in s44 of the Companies Act 2006 or s74 of the Law of Property Act 1925. The purpose of an electronic seal is to validate the origin and integrity of an electronic document (e.g., an electronic invoice), rather than to sign it. Thus, where a company executes documents (including deeds) on an electronic signature software platform, it relies on authorised signatories to apply their own electronic signature.[10]

eIDAS states that a Qualified electronic seal shall enjoy the presumption of integrity of all data and of correctness of the origin of that data to which the Qualified electronic seal is linked. Like regular handwritten signatures, a Qualified electronic seal is recognized in the European Union - a Qualified electronic seal, based on a qualified certificate issued in one Member State, shall be recognized as a Qualified electronic seal in all other Member States.

In practice, however, there is still a lot of uncertainty around the use of electronic seals in the United Kingdom. This is reflected by their general lack of use in the market. This uncertainty is the product of several factors:

- Companies governed by the Companies Act 2006 must (a) have their name **engraved** on the seal[11] and (b) **affix** their seal[12]. Both words evoke physical connotations and don't lend themselves to the electronic application of a seal. It is unclear whether the wording of the law is permissive enough to allow Companies in England, Wales and Northern Ireland to execute deeds using a seal[13].

- For corporations that are not governed by the Companies Act 2006, s74 of the Law of Property Act 1925 states that an instrument is duly executed if the "seal purporting to be the corporation's seal purports to be affixed to the instrument in the presence of and attested by…". The wording in this statute also uses the word 'affixed', which would logically follow the rationale explained above relating to the Companies Act.[14]

[10] Richard Oliphant, 'Land registry: Digital transformation', (March 2021 #385) Property Law Journal, https://www.lawjournals.co.uk/2021/03/02/property-law-journal/land-registry-digital-transformation/, accessed 2 March 2021

[11] See s45(2) of the Companies Act 2006

[12] See s44 of the Companies Act 2006

[13] This issue was raised by the Bar Council and referenced at 6.125 of the Law Commission Report on Electronic Execution of Documents. It simply says that this "appear[s] to preclude" electronic seals".

[14] Although, it may be argued that the words "purports to be" is more permissive than s44 of the Companies Act.

- s.74(6) of the LPA 1925 states, "Notwithstanding anything contained in this section, any mode of execution or attestation authorised by law or by practice or by the statute, charter, articles, deed of settlement or other instrument constituting the corporation or regulating the affairs thereof, shall (in addition to the modes authorised by this section) be as effectual as if this section had not been passed." On this basis, it can be argued that Corporations Aggregate can execute deeds with an electronic seal so long as their constitution expressly permits it and the execution of documents has followed the rules set out in the constitution.

- The Land Registry in England and Wales has set out at section 1.2 of "Practice Guide 80: Coronavirus (COVID-19): useful information for conveyancers" that until further notice, they will accept execution of a deed by a local authority when it certifies that it is, under its constitution, able to validly execute a deed other than in accordance with their special arrangements. This would include in circumstances where the seal has been applied electronically if this is permitted by the council's constitution.

The information above simply emphasises the fact that electronic seals remain legally uncertain and are not presently a replacement for a corporate seal being physically affixed to a document. This uncertainty is reflected in the market where electronic seals remain almost completely unused, even while the use of electronic signatures became an extremely popular method for executing documents when countries went into lockdown in 2020.

WHERE IS THE UK MARKET AT IN AUGUST 2021?

While electronic signatures in general have become increasingly popular over the course of the last 15 months, they have not been adopted uniformly across the market and there are many different factors limiting their use.

Qualified electronic signatures remain relatively uncommon in the UK, largely because of the expenditure required to acquire a qualified signature, but also due to a lack of understanding of the benefits over Simple electronic signatures, the relative absence of QTSPs established in the United Kingdom and the challenge in obtaining a QC in the current environment. However, in July 2021 the Information Commissioner's Office approved GlobalSign as the UK's first QTSP under the UK eIDAS Regulations. GMO GlobalSign Ltd is the first company to have gone through this process in the UK and is now a QTSP for QCs for both Qualified electronic signatures and seals.[15] It remains to be seen whether this marks the beginning of a significant turn toward the use of Qualified electronic signatures across the UK market, but it is certainly an important first step.

There is already a market for Qualified electronic signatures in real estate transactions in Scotland, where it is commonplace for conveyancers to complete missives using qualified signatures. Historically this has been achieved using SmartCards issued by the Law Society of Scotland, but the market is now shifting towards more digital offerings.

Advanced electronic signatures remain mostly unused in the UK because of the increased time costs and administrative work required to verify the signatory's identity in comparison with Simple electronic signatures, in addition to there being limited legal need for an escalation in signature type.

As a result, Simple electronic signatures remain the prevalent form of electronic signature used in the United Kingdom. That is the case notwithstanding the fact that Simple electronic signatures provide a lower degree of evidential weight should the signature be challenged and this probably reflects the fact that challenges to the validity of a contract due to its method of signing are rare.

The JWP Guidance gave most electronic signature users the confidence to use Simple electronic signatures wherever legally possible (which is extensive, particularly under the laws of England, Wales and Northern Ireland), because they are the cheapest and most flexible way to apply an electronic signature to a document. Financial institutions and other businesses insist on the use of two factor authentication and email chains to create an audit trail that would go some way to verifying the signatory did in fact sign the document if a Simple electronic signature should ever be challenged; however from an evidentiary perspective this does not achieve the level of protection of an Advanced electronic signature or a Qualified electronic signature.

The requirements of the different Land Registries in each of the UK jurisdictions means that wet ink signatures are still being widely used for most documents and deeds requiring registration. Electronic signing is not an option for documents to be registered with the NI

[15] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-approves-the-first-uk-eidas-regulations-qualified-trust-service-provider/

Land Registry or Registers of Scotland. Standard securities in Scotland cannot be signed electronically as the security is not "created" until registered in the Land Register and the Land Registry won't accept electronic documents for registration.

In July 2020, HM Land Registry in England announced that they would accept certain deeds that have been signed with a witnessed electronic signature. However, they would only accept documents signed electronically which met very prescriptive requirements[16]:

STEP 1 – The conveyancer controlling the signing process:

- uploads the final agreed copy of the deed (including any plans) to the platform
- populates the platform with the name, email address and mobile phone number of the signatories and the witnesses. Where the platform allows, the details for a witness can be populated later, either by the signatory entering the details for their witness or the conveyancer doing so, provided this is done before STEP 5
- highlights the fields that need completing within the deed and indicates by whom they are to be completed, setting out the order (so the witness is after the signatory whose signing they are witnessing).

STEP 2 – The platform emails the signatories to let them know the deed is ready to sign.

STEP 3 – To access the deed on the platform via the email they have received, the signatories are required to input an OTP sent to them by text message by the platform. The OTP must contain a minimum of six numbers.

STEP 4 – The signatories enter the OTP and sign the deed in the physical presence of the witness, with the date and time being automatically recorded within the platform's audit trail.

STEP 5 – Once the signatory has signed the deed, the witness will receive an email from the platform inviting them to sign and add their details in the space provided in the attestation clause. The witness inputs an OTP sent to them by text message by the platform, signs and adds their address in the space provided, with the date and time being automatically recorded again.

STEP 6 – Once the signing process has been concluded, the conveyancer controlling the signing process dates the deed within the platform with the date it took effect. (There will be a gap between this step and the previous one if, as will often be the case, the deed is signed by all the signatories and witnesses some time in advance of completion.)

As a result of these detailed and complex requirements most documents that are being registered with the Land Registry continue to be signed using wet ink using the 'virtual signing' method described at the beginning of this paper. Furthermore, none of the requirements listed above solve concerns around levels of security and confidentiality when using electronic signatures, particularly on witnessed documents. For example, ensuring that a witness does

[16] To read the requirements in full see paragraph 13.3 of Practice guide 8 from HM Land Registry.

not receive a full copy of the document via an electronic signature software platform (when it only needs to witness the signature on the signing page)? Many financial institutions are uncomfortable with security and confidentiality aspects of electronic witnessing. Additionally, certain organisations are not willing for witnesses or signatories using unsecure personal email addresses to receive their copy of the document, as it increases risks of hacking and documents being viewed by parties not involved in the transaction.

While Brexit has had a tremendous impact on many parts of the UK market it has not made significant alterations to the law surrounding electronic signatures. eIDAS became part of UK domestic law under the European Union (Withdrawal) Act 2018, subject to some amendments. While UK law does not mirror eIDAS entirely – it amends or omits provisions that are no longer required, such as changes to terminology – the crux of the legislation remains the same. Importantly, the UK continues to recognise Qualified electronic signatures based on QCs issued by EU registered QTSPs, which means that UK organisations can continue to use EU based trust services although caution needs to be exercised where the signatory is a UK citizen as to whether the identity has been verified in accordance with UK law. The approved trust providers that appear in the eIDAS trusted list immediately before the end of the transition period were carried over. The Secretary of State has appointed the Information Commissioner's Office to be responsible for the awarding of Qualified status to TSPs in the UK and for supervising their activities. tScheme is currently contracted to carry out the maintenance and publication of the trusted list in the United Kingdom.

However, while much has not changed, a significant change since the end of the transition period is that the EU no longer recognises UK-registered QTSPs. This means that Qualified electronic signatures based on QCs issued by those QTSPs will not be treated as a Qualified electronic signature under EU law. This may have consequences for the recognition of those electronic signatures and validity of documents in EU member states and is a clear incentive for UK businesses to work solely with QTSPs established in the EU.

WHAT IS THE FUTURE OF ELECTRONIC SIGNATURES IN THE UK?

The Land Registries within the UK are all currently considering the implementation of Qualified electronic signatures for documents requiring registration. This will be a significant transformation in market practice and is likely to sound the starting pistol for wider use of Qualified electronic signatures in the UK market.

Qualified electronic signatures are more commonly deployed in Europe and other nations with codified laws, therefore cross border transactions would often be eased with the use of a qualified signature, ensuring cross border applicability of documentation.

The use of such signatures in place of witnessing will require a legislative change for which there appears currently to be limited momentum.

A recent development in the European Union that may influence the UK's approach to electronic signatures in the future is the European Commission's recent proposal for an EU-wide digital identity framework. This framework would allow businesses and citizens to link their national digital identities with other forms of identification such as a driving licence and share electronic documents from their European Digital Identity Wallets ("**EDIW**") with the click of a button on their phone. The proposal defines a EDIW as "a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals."

The new EDIW will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. The Commission said individuals would have full control over the data they shared and that the EDIW could be used to prove someone's identity when opening a bank account, filing tax returns, proving your age, renting a car or checking into a hotel. It will sit in an electronic wallet accessible through any type of mobile device or laptop. Perhaps the most important point to note for the purposes of this paper is that one of the mandatory features of the EDIW would be to enable users to qualify for a QC to sign documents using Qualified electronic signatures and seals and will be free of charge to natural persons. Other tools such as electronic timestamps and electronic registered delivery services could also be integrated into the wallet.

The framework would be introduced through the form of a regulation, which the commission has published in draft form. The commission said that it hoped to have agreed on a toolbox to implement the European Digital Identity framework by September 2022, with the toolbox published in October 2022. The technical framework would then be tested in pilot projects.[17]

It is at present unclear how the UK Government will move forward on electronic signatures now that we are no longer obliged to remain equivalent to the EU. The Trade Agreement concluded with the EU on 31 December does however require that neither the UK nor the EU

[17] For more information on the EDI see the following Outlaw article by Angus McFadyen, technology law expert at Pinsent Masons LLP.

will deny the legal effect and admissibility as evidence in legal proceedings of an electronic document or an electronic signature solely on the ground that it is in electronic form. In February 2021 the Department for Digital, Culture, Media & Sport published 'the UK digital identity and attributes trust framework' (the "**UK Trust Framework**"). Like the European digital identity framework, the UK Trust Framework proposes a form of digital "wallet" which allows UK citizens to contain to store various trusted pieces of information or "attributes". The framework is still taking feedback and remains a prototype but the updated version of the document published in August 2021 does cover some ground in relation to electronic signatures. The document provides that if an organisation wishes to provide a service under the UK Trust Framework they must follow the guidance under GPG 44 and GPG 45 to ensure their authentication process is secure. The document states that, "if someone has already been through an identity verification process to use another service you provide, you might be able to develop this into a trust framework service. For example… an identity proofing and verification process has bound an identity to an qualified electronic signature by a qualified trust service provider."

While both the European and UK frameworks are yet to be finalised there are already questions regarding the issue of equivalence between eIDAS and GPG 45 and how these two frameworks might be made interoperable. The answers to these questions remain a long way off but it is clear that electronic signatures are here to stay; what form they will take and how the market will evolve will be of great interest to many.