C/M/S/
Law.Tax

Electronic Signatures & E-Signing Platforms

Begin >

The definitive UK legal guide

November 2020
Version 1.01

Contents

Foreword

Introduction

Why did the Law Commission consult on electronic execution in 2018?

Electronic signatures, documents and seals

Digital signatures: advanced and qualified electronic signatures

Legal validity and admissibility of electronic signatures

Electronic signatures: simple contracts and deeds

Special Cases: When should you proceed with caution?

Why use an e-signing platform?

Engaging with e-signing platforms: due diligence and practical risk mitigation

Impact of Brexit

About CMS

1. Foreword

Digital transformation is high on the corporate agenda. Businesses need to think, plan, and build digitally in a way that will enable them to be agile, flexible, and ready to grow. Finding the optimal blend of technologies to create new or reinvent existing business processes, accelerate operational efficiency and deliver new or improved customer experiences, products and services to drive enterprise-wide growth is now a 'do or die' priority.

Some process changes aren't glamorous or exciting, but can save costs, drive improved compliance and auditability and simply make what would otherwise be time-consuming tasks much easier. The adoption of e-signing platforms is a good example of this.

Remote working, negotiation and execution of **transactions**[1], whether local or cross-border has increasingly become a business necessity in recent years. The COVID-19 pandemic and social distancing rules have accelerated this trend, further upending 'traditional' methods of doing business in person. Currently, face-to-face signing of documents and deeds in wet-ink is no longer practical and poses a risk to public health.

Mercury-compliant 'virtual signings' (where the signature page of a hard copy document is signed in wet-ink and a PDF of the signed signature page is typically sent by email to the signatory's lawyer) are the preferred method for many businesses remotely executing transaction documents.

> *An electronic signature is capable in law of being used to execute a document (including a deed) provided that (i) the person signing the document intends to authenticate the document and (ii) any formalities relating to execution of that document are satisfied.*

Paragraph 1 of the Statement of Law (Law Commission Report on the Electronic Execution of Documents).

However, while the use of electronic signatures in the UK, and for cross-border transactions is gaining increasing traction in the market, adoption of e-signing platforms (particularly by law firms) has been slower than expected. This is set to change.

The use of online platforms and electronic identification and trust services are at the heart of the European Commission's **digital strategy** and it specifically calls out the use of electronic signatures to sign contracts as a use case. There are clear indications that the COVID-19 pandemic is accelerating adoption of e-signing platforms by businesses in every vertical market and across the public sector. The opportunity e-signing platforms offer to save costs, reduce your environmental impact, drive improved compliance and auditability and generally improve the signing process and experience is huge.

The relatively low adoption rate to date has often been attributed to uncertainty over whether an electronic signature is a valid means of executing documents (rather than any aversion to digital technology).

This interactive guide is designed to help businesses and their lawyers address and overcome their concerns relating to the use of e-signing platforms as they look to accelerate their digital transformation. It aims to demystify the technical and practical aspects of using, and assist businesses evaluate their use cases for and approach to implementing, e-signing platforms.

In it we explain the e-signing process and identify what types of documents it is suited to, in addition to providing guidance on the legality and admissibility of electronic signatures and the differences between 'simple' electronic signatures and the more technologically sophisticated digital signatures. We also provide guidance on undertaking due diligence on, and taking risk mitigation in connection with the use of, e-signing platforms and examine the main contractual and compliance issues businesses must navigate when negotiating terms with e-signing platforms.

Ian Stevens
November, 2020

2. Introduction

This guide is designed to provide guidance on the law governing electronic execution of **deeds** and documents in all UK jurisdictions. While the position under the laws of England and Wales ("**English law**") and Northern Ireland are essentially the same, there are a number of differences in Scots law. In particular, Scotland has a separate statutory regime with less scope for uncertainty and mandates the use of **digital signatures** for some transactions. Where you are interested in electronic execution under Scots law, please refer to the appropriate operative section of this guide, where you will find a separate heading to address the Scottish position. Where this guide refers to the UK, this will encompass provisions under both English and Scots law.

Understanding the function and key features of the digital **audit trail**[2] generated by an **e-signing platform** is essential for businesses and their advisors. These audit trails typically record information about the person who signed the document, including the email and **IP address** they used, the timing of the signature, the geo-location of the signing (derived from the signatory's IP address and/or GPS) (where this option is selected), and any additional authentication factors (such as a one-time password). In a dispute over the authenticity or integrity of a document signed via the e-signing platform, the **electronic signature** and digital audit trail are admissible in evidence in **legal proceedings**[3]. An explanation of the practical steps and technical workflow for creating electronic and digital signatures can be found by clicking the 'e-signing workflow' button in the toolbar above. We provide guidance on the **different types** of electronic signatures and their **legal validity and admissibility**. We discuss some of the **practical and contractual considerations** when selecting a platform provider and assess the **implications** of Brexit for e-signing in the UK.

We commented previously on the Law Commission 2019 Statement of Law in June 2020, which is available **here**. The up to date HMLR position is contained in this Guide.

If you are interested in finding more about the use of electronic signatures in commercial contracts in jurisdictions outside the UK, please refer to our international expert **guide**.

3. Why Did The Law Commission Consult On Electronic Execution In 2018?

*The **2018 Consultation** was an acknowledgement by the Law Commission (of England and Wales) of the need to:*

- *Facilitate the **digital transformation** of transactions: '**Individuals, consumers and businesses demand modern, convenient methods for making binding transactions. Technological developments have changed the ways in which these transactions are made and will continue to change at an ever-more-rapid pace**[4]'; and*
- *Address concerns around the electronic execution of documents that were hindering the use of new technology where legislation requires a document to be 'signed'.*

The Law Commission's 2001 Advice to Government

At the turn of the twenty-first century, the rapid growth of e-commerce was the trigger for the Law Commission's **2001 Advice** on '*Electronic Commerce: Formal requirements in commercial transaction*'. The Law Commission concluded that where English law requires '*writing*', a '*signature*' or a '*document*', this could be satisfied electronically:

> *'Digital signatures, scanned manuscript signatures, typing one's name (or initials) and clicking on a website button are, in our view, all methods of signature which are generally capable of satisfying a statutory signature requirement. We say that on the basis that it is function, rather than form, which is determinative of the validity of a signature. These methods are all capable of satisfying the principal function: namely, demonstrating an authenticating intention.'*

Paragraph 3.3 of the 2001 Advice.

The 2001 Advice was a step forward, but it did not definitively settle the matter. Focused on the international sale and carriage of goods, it failed to dispel the general unease many lawyers still harboured about the validity of electronic execution, particularly in regard to deeds. Post-2001, lawyers continued to favour **wet-ink** signatures.

3. Why Did The Law Commission Consult On Electronic Execution In 2018?

By 2016, the emergence of web-based e-signing platforms prompted calls for new guidance. This culminated in a joint working party of the Law Society Company Law Committee and the City of London Law Society Company Law and Financial Law Committees ("**Law Society**") issuing the **Law Society 2016 Practice Note** on the '***Execution of a document using an electronic signature***[5]'.

The Law Society 2016 Practice Note unequivocally endorsed the use of electronic signatures to execute commercial contracts under English law. In its key findings, the Law Society confirmed that:

— simple contracts and deeds may be concluded using an **electronic signature**[6]; and

— an electronic signature will satisfy a statutory requirement for an English law document to be in writing and/or signed and/or made **under hand**[7]:

(a) a contract represented on a screen (including a desktop, laptop, tablet or smartphone) in a manner which enables a person to read its terms properly, will be 'in writing' at that point;

(b) to constitute a valid signature the mark which appears in the document must be inserted in order to give, and with the intention of giving, authenticity to it. If the signatory inserts an electronic signature into the appropriate place (e.g. next to the relevant party's signature block) in a document with the intention of authenticating the document, a statutory requirement for that document to be signed will be satisfied. Neither the manner of insertion of the electronic signature (e.g. typing in your name, or using a stylus to write it or pasting in a copy of your signature or clicking to have it inserted using an e-signing platform), nor its form (e.g. a handwritten signature, a generic handwriting font, a typed font, etc.) need to meet any set specific criteria; and

(c) the insertion of an electronic signature with the relevant authenticating intention is sufficient for a document to have been executed under hand.

Perhaps surprisingly, the Law Society 2016 Practice Note did not prove to be the watershed for e-signing platforms that many hoped it would be. Market practice in law firms remained largely unchanged. Parties to transactions continued to use wet-ink signatures and in-person signing, or follow the protocols for virtual-signing laid out in the Law Society 2010 Practice Note on the '*Execution of documents by virtual means*' (which involve the exchange of scanned or photograph copies of signature pages by **e-mail**[8]).

3. Why Did The Law Commission Consult On Electronic Execution In 2018?

The purpose of the 2018 Consultation was to:

> *'ensure that the law governing the electronic execution of documents, including electronic signatures, is sufficiently certain and flexible to remain fit for purpose in a global, digital, environment.'*

Paragraph 1.3 of the 2018 Consultation.

In its terms of reference, the Law Commission said it had been asked by the Ministry of Justice to assess whether current English law was impeding use of electronic documents by commercial parties and consumers with regard to **electronic signatures, witnessing and delivery**[9]. The Law Commission noted that there was confusion about using electronic signatures in transactions where there is a *'statutory requirement'* for a signature. It acknowledged, too, that there was doubt in some quarters over whether the **formalities** for a deed (to be signed, witnessed, attested and delivered) could be satisfied **electronically**[10].

During the consultation period in 2018-19, the Law Commission canvassed the views of lawyers, technology experts and other respondents. The **2019 Report** was published in September that year and found that the current law generally accommodates the use of electronic signatures; but the Law Commission acknowledged that there are situations in which English law is more prescriptive as to the type of signature required.

The scope of the 2018 Consultation was far-reaching. It covered electronic execution of commercial and consumer documents, and deeds such as powers of attorney and trust **deeds**[11]. However, the creation of wills and the registrable disposition of land (under the **LRA 2002** and the **LRR 2003**) were **excluded**[12]. The formalities for making a will had already been considered in a separate Law Commission **project** in 2017. Registrable dispositions were the subject of HMLR's own **consultation** on electronic conveyancing and registration in 2017.

The 2019 Report contained a detailed exposition of the law relating to electronic execution, and suggested options for reform. These included legislative changes to codify English law in a single statement clarifying the legal effect of **electronic signatures**[13], and to permit video witnessing of deeds; as we will see **later**, the Law Commission's firm view is that the current law requires the witness to be physically present and observe signature of the **deed**[14].

3. Why Did The Law Commission Consult On Electronic Execution In 2018?

On 3 March 2020, the Government published its **response** to the 2019 Report. It accepted the Law Commission's analysis of the current law and its recommendations, and the conclusion that formal primary legislation is not currently necessary to reinforce the validity of electronic signatures.

The Government acknowledged that, notwithstanding the position in law, there remain issues around the security and technology of electronic signatures that require further consideration. It confirmed that a multi-disciplinary industry working group will be set up to look at the practical and technical issues raised in the 2019 Report including the question of video witnessing of electronic signatures.

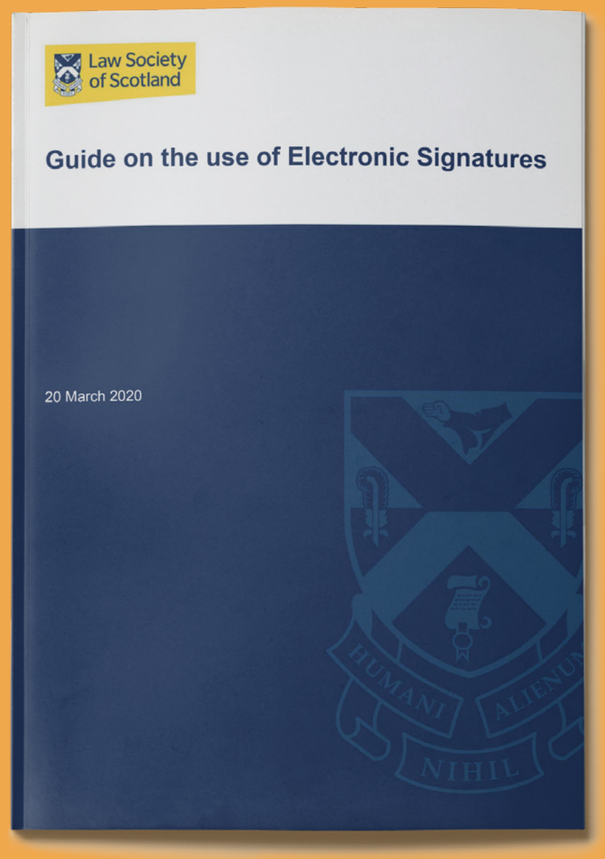
> *'I endorse the Commission's draft legislative provision as set out in the report, as reflecting the Government's view of the legal position on electronic signatures. They are permissible and can be used in confidence in commercial and consumer documents.'*

Rt. Hon. Robert Buckland (Lord Chancellor and Secretary of State for Justice), 3 March 2020.

3. Why Did The Law Commission Consult On Electronic Execution In 2018?

Law Society of Scotland

The Law Commission's 2019 Report, as a review of the use of electronic signatures under English law, is not directly relatable to the separate regulations under Scottish law. The Scottish framework is arguably more transparent on the use of electronic signatures and has not therefore, been subject to consultation. However, in March 2020, the Law Society of Scotland published a draft **Electronic Signatures Guide** to assist users with the regulations. The draft has been updated since March but – at the time of writing – has not been finalised.



4. Electronic Signatures, Documents And Seals

Electronic signatures

The Regulation on Electronic Identification and Trust Services in the Internal Market (910/2014/EU) ("**eIDAS**") came into force on 1 July 2016 and established an EU-wide legal framework for electronic signatures and other **trust services**.

eIDAS applies throughout the UK. It establishes three categories of electronic signature: electronic (often referred to as a 'simple electronic signature'), advanced and qualified.

An electronic signature is *'any 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'* (Article 3(10), eIDAS).

Article 3(9) of eIDAS defines 'signatory' as a natural person who creates an electronic signature. A legal person, such as a company, cannot use an electronic signature. What this means in practice is that execution by a company of a document or deed governed by:

— the law of England and Wales or Northern Ireland must be done in accordance with sections 43 or 44 of the Companies Act 2006 ("**CA 2006**") acting by one or more signatories, each of whom signs with their own electronic signature (see **here** for more detail on executing simple contracts and deeds).

— the law of Scotland must be done in accordance with section 48 of the CA 2006, which requires it to be signed or subscribed by one or more signatories, each of which 'authenticates' the document by the application of their own electronic signature in accordance with the provisions of the Requirements of Writing (Scotland) Act 1995 ("**ROWSA**[15]").

The statutory definition of 'electronic signature' is broad. It means the electronic equivalent of a wet-ink signature and may take many different forms. These include:

— Typing a name or initials at the bottom of an electronic document such as an email, or in the signature block of a Microsoft Word document.

— Pasting a signature (in the form of an image) into an electronic contract (commonly referred to as 'scanned manuscript signatures').

— Clicking an 'I accept' or 'I agree' button on a **website**[16].

— Using a stylus or finger to sign an electronic document via a touchscreen or digital pad.

— Using a password or PIN (for example, to authorise a credit card transaction rather than signing a paper receipt).

— Using biometrics such as fingerprints or retinal scans to verify the signatory's identity. If this information is *'attached to or logically associated with'* an electronic document, it may constitute a signature.

— Using a web-based e-signing platform to generate:

  – an electronic representation of a handwritten signature; or

  – a digital signature using **public key cryptography** which is backed by a **digital certificate** from the platform (or a **TSP**) to verify the signatory's identity and link the signatory to their public key.

This guide is concerned only with the final example – electronic and digital signatures generated by e-signing platforms.

The standard product licensed by Adobe Sign, DocuSign, HelloSign, Namirial and other leading e-signing platforms meets the definition of an 'electronic signature' under Article 3(10) of eIDAS. An e-signing platform typically allows the signatory to write their signature directly on to the document (with a stylus or mouse) or to select a computer-generated signature from a variety of fonts and styles. The standard product tends not to involve any independent third-party verification of the signatory's identity (as the premium products that support QES typically do – see **here**). The basic method of authenticating the signatory is to use their email address. This is sufficient for most use cases governed by English law; but an email address may be easily spoofed for **malicious use**[17]. If the parties to a transaction want more security, they can use multi-factor authentication such as an SMS, one-time password or knowledge-based authentication (KBA) to augment the process for verifying the signatory's identity (see **here** for the Scottish provision).

Although it does not affect the legal validity of an **electronic signature**[18], lawyers should always consider just how trustworthy, secure and reliable is the technology used to create it. For example, it is easy to forge a typed name at the end of a document. Similarly, anyone with access to a scanned manuscript signature may affix it to a document. The point is well made in the Department for Business, Energy & Industrial Strategy's guide to electronic signatures ("**2016 BEIS Guide**"):

> *'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.'*

Page 5, 2016 BEIS Guide.

4. Electronic Signatures, Documents And Seals

Electronic signatures generated by e-signing platforms demonstrate three fundamental properties:

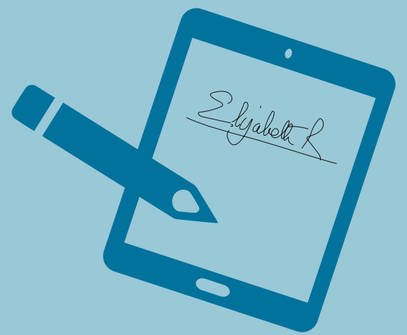
— **Authenticity**
Whether an electronic document comes from a particular person or other source.

— **Integrity**
Whether there has been any tampering with or alterations to the electronic document after signature.

— **Non-repudiation**
That the signatory cannot deny that they signed the electronic document.

Our level of trust in the e-signing platform used to generate an electronic signature, as well as our trust in the electronic signature itself and its evidential weight, primarily depends on how the electronic signature (and digital audit trail) embody these three properties.

printer/scanner



touchscreen/stylus

mobile device taking photo of document

biometrics

typing on signature

clicking "OK"

4. Electronic Signatures, Documents And Seals

The legal status of an electronic document

Article 3(5) of eIDAS defines an electronic document as any content stored in electronic form, in particular text or sound, or audio-visual recording (see also section 7C of Electronic Communications Act 2000 ("**ECA 2000**")).

Article 46 of eIDAS provides that an electronic document '*shall not be denied legal effect and admissibility as evidence*' in legal proceedings solely on the grounds that it is in electronic form.

Section 7C of the ECA 2000 also confirms that an electronic document is admissible in legal proceedings throughout the United Kingdom. However, it differs from Article 46 of eIDAS by not *expressly* stating that an electronic document shall not be denied legal effect. This omission from section 7C is puzzling but should not have any adverse consequences as, owing to the primacy of EU law, eIDAS takes precedence over the ECA 2000.

In its 2001 Advice, the Law Commission indicated that information stored in electronic form was a '*document*' and would satisfy a statutory requirement for a document. This view was corroborated by the 2019 Report and has also been confirmed in **case law**[19].

4. Electronic Signatures, Documents And Seals

Electronic seals

Article 3(25) of eIDAS introduced a new concept: the **electronic seal**[20]. As with electronic signatures, there are advanced and qualified electronic seals offering additional benefits to basic electronic seals.

Some commentators have equated the electronic seal with an electronic signature for companies. In its **guide to eIDAS**, the Information Commissioner's Office states that *'electronic seals allow companies and other corporate bodies to 'sign' electronic documents and certify them as genuine, in the same way as an individual can use an electronic signature.'*

Notwithstanding this, there is some consensus in the legal community that the correct interpretation is that an electronic seal cannot be used to execute a document or deed. An electronic seal is not a form of, or substitute for, a common seal and will not satisfy statutory requirements of section 44 of the CA 2006 or section 74 of the Law of Property Act 1925. The European Commission has **made clear** that a company may use an electronic seal for the purpose of validating the origin and integrity of an electronic document, rather than signing it. Accordingly, an electronic seal should be admissible in court as evidence of the integrity of a document in the same way as an electronic signature is admissible as evidence of execution. However, an electronic seal is not binding alone, and requires another document or act.

Electronic seals have not been widely adopted. Nevertheless, some companies are beginning to use **DocuSign's electronic seals** as a way of guaranteeing the authenticity of invoices that they send to their clients by electronic means. By verifying the electronic seal on the invoice, the client has further assurance that the invoice originated from the company and has not been modified after transmission.

4. Electronic Signatures, Documents And Seals

Scotland

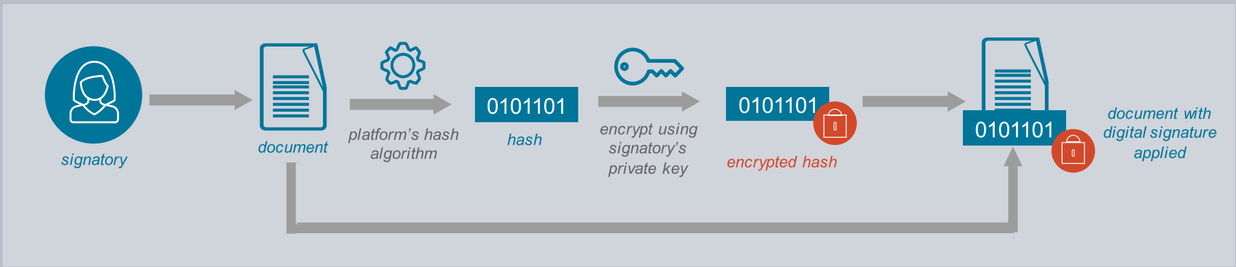
Scottish Companies
Similarly to the English law provision, in accordance with section 48 of the CA 2006, a company executes a document where it is signed or subscribed by or on behalf of the company through the agency of one or more signatories, each of which 'authenticates' the document by the application of their own electronic signature in accordance with the provisions of **ROWSA**[21].

Use Cases in Scotland
For some use cases governed by Scots law, an advanced electronic signature (AdES) is required for legal validity and this standard product will not be sufficient (see **here** for more detail).

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Before we look at **advanced electronic signatures** (**AdES**) and **qualified electronic signatures** (**QES**), we must consider the terms **digital signature** and **public key infrastructure (PKI)**.

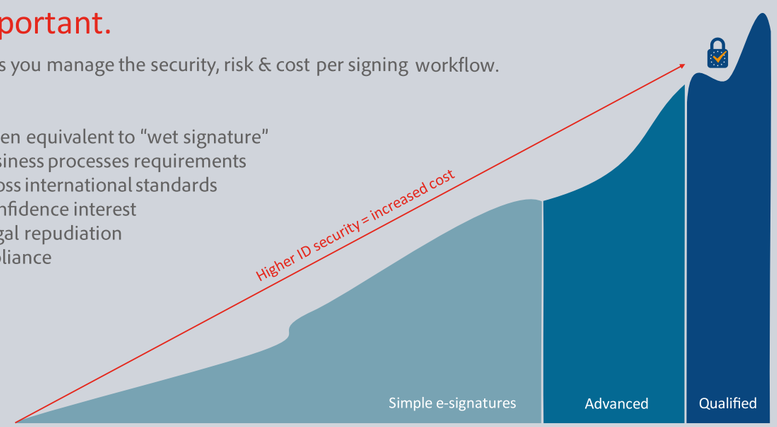
A digital signature is a more secure and technologically sophisticated form of electronic signature. The 2018 Consultation defined digital signature as ***'a type of electronic signature produced using asymmetric or public key cryptography[22]'***.



Why a trusted ID is important.

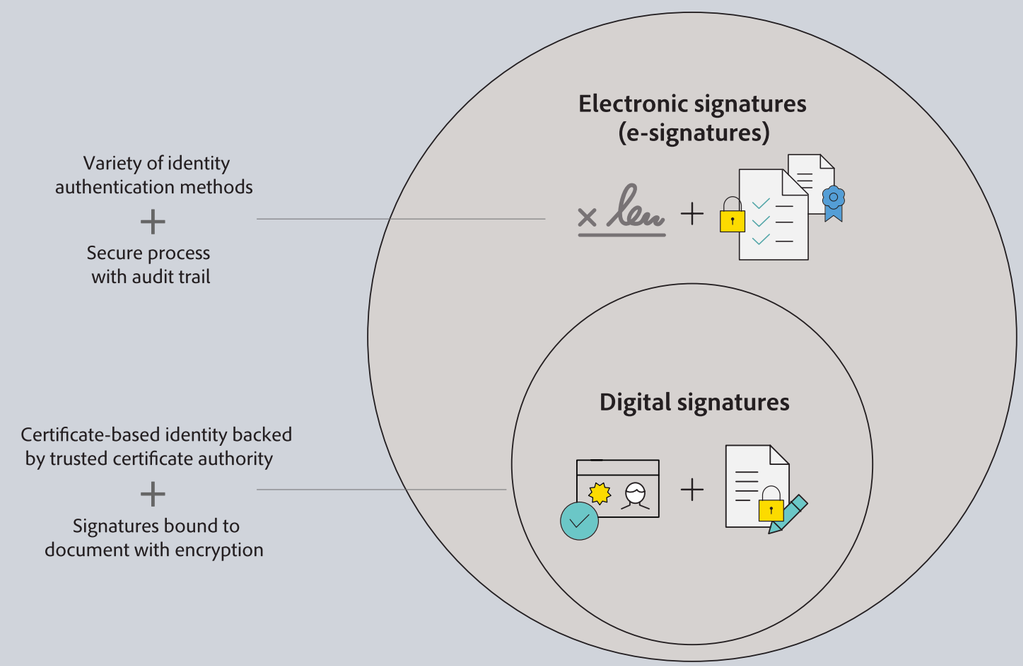
Increased identity (ID) assurance helps you manage the security, risk & cost per signing workflow. Trusted IDs help ensure:

- Legal validity, higher assurance often equivalent to "wet signature"
- Compliance with regulatory or business processes requirements
- Future alignment/equivalency across international standards
- Cultural or other business trust/confidence interest
- Mitigation of overall risk, risk of legal repudiation
- Regional, geo, or other legal compliance
- Cross-border enforceability (EU)
- Security of signing workflows



Graphic reproduced by kind permission of Adobe Sign.

Electronic vs. digital signatures



Note: certificate authority is another term for TSP

Graphic reproduced by kind permission of Adobe Sign.

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Public key cryptography and PKI

Public key cryptography (also known as 'asymmetric cryptography') involves the use of a private/public **key pair** to create and verify a digital signature. A cryptographic **hash function** is used to compute a '*hash*' of the document being signed. The signatory's private key encrypts the hash. The encrypted hash is the digital signature which is attached to the document and can be sent to the recipient.

The digital signature is verified by the recipient (also called the 'relying party' in eIDAS) using the signatory's public key. The original hash is retrieved by decrypting the digital signature with the public key and the recipient uses the same hash function to compute a new hash of the document. If the new hash is identical to the original hash, it means that neither the document nor the digital signature were modified (*integrity*), and that the signature could only have been created with the corresponding private key, so that the signatory cannot subsequently deny that they created the signature (*non-repudiation*).

Public key cryptography – on its own – provides assurance that the document has not been modified after signature (*integrity*); but it offers no certainty that the public key belongs to the signatory (*authenticity*). This problem is resolved by PKI technologies and the use of a third-party trust service provider (TSP, also known as a 'certification authority' or 'CA') to verify the signatory's identity.

Having verified the identity of the signatory and associated them with a public key, the TSP makes that information the subject of a digital certificate. The digital certificate is digitally signed by the TSP and certifies the link between the signatory and their public key (it can also include other information about the signatory, their organisation and the TSP).

As a consequence, the digital certificate can be used to verify the signatory associated with a public key when requested.

When the signatory uses their private key to sign the document, the digital certificate provided by the TSP is cryptographically bound to the signed document.

PKI technologies enable the creation, management, use, storage and revocation of digital certificates, as well as a public/private key pair for digital signatures. TSPs either generate a public/private key pair on behalf of a signatory or associate an existing public key provided by the signatory to that signatory. The TSP verifies the identity of the signatory and issues a digital certificate (typically based on **X.509 standards**[23]) confirming the signatory's name (or pseudonym) and linking the signatory's identity to their public key. The public key is uniquely associated with the private key which the signatory uses to digitally sign a document.

The digital certificate is embedded into the digital signature and provided to the recipient who uses the public key (available from the certificate) to validate the signature.

Using PKI provides a higher level of assurance than a standard electronic signature as to the authenticity and integrity of an electronic document.

The TSP holds a directory of the digital certificates it has issued enabling third parties to validate whether a certificate has been genuinely issued to that signatory and thereby fostering a high degree of trust in the system.

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Advanced electronic signatures (AdES)

The first type of digital signature, the AdES, is defined by Article 26 of eIDAS as an electronic signature that is:

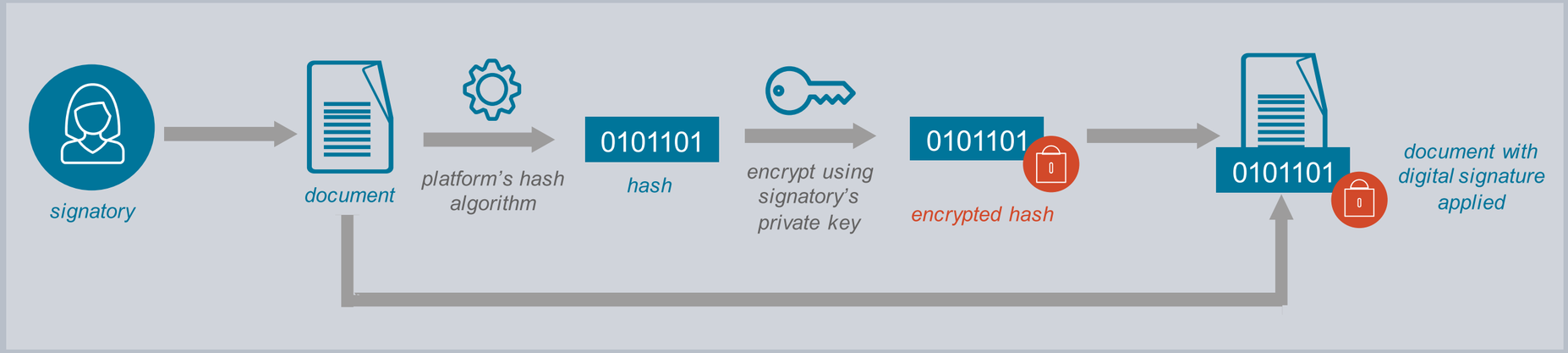
— Uniquely linked to the signatory.

— Capable of identifying the signatory.

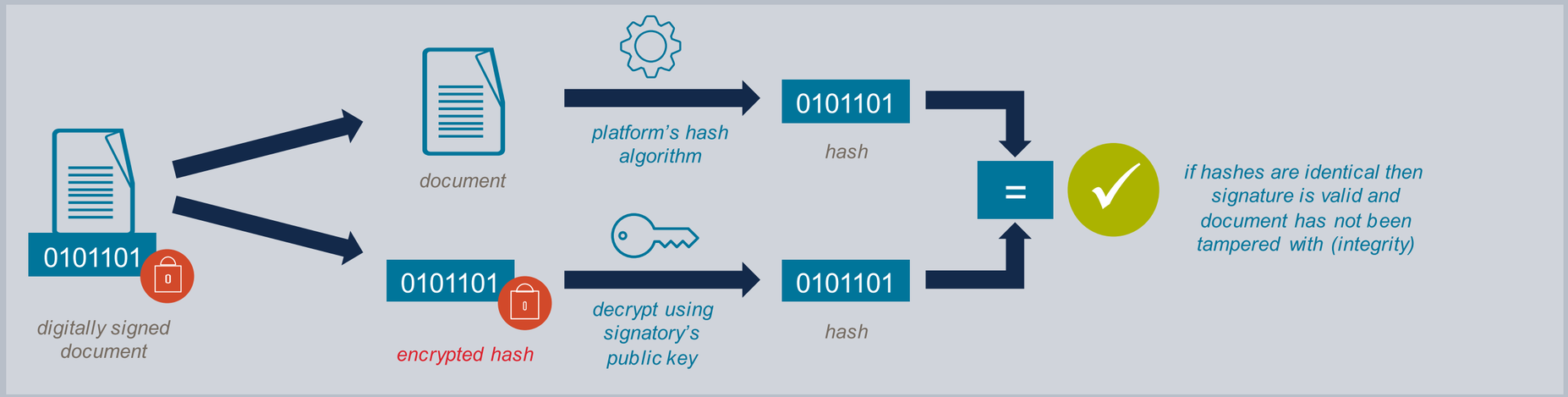
— Created using electronic signature creation data (in other words, a private encryption key) that the signatory can, with a high level of confidence, use under their sole control.

— Linked to the signed data in such a way that any subsequent change in the data is detectable.

eIDAS is '***technology-neutral***[24]'. It does not prescribe *how* the requirements for an AdES should be met. To date there has been no guidance from EU courts, but the Forum of European Supervisory Authorities for Electronic Signatures issued a **working paper** in October 2004, which noted that an AdES is usually achieved by using PKI technology. More than fifteen years later, this is also borne out by market practice. The leading e-signing platforms all use PKI to create digital signatures and certificates. The platform or a third-party TSP will verify the signatory's identity and issue a digital certificate which is provided with the **AdES**[25]. This enables the recipient to verify the authenticity of the AdES since the public key is available from the digital certificate.



AdES – Signing



AdES – Verification

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Qualified electronic signatures (QES)

The third category of signature recognised by eIDAS (and the second type of digital signature) is the QES. A QES is an AdES that fulfils two additional requirements:

- It must be supported by a **qualified certificate** issued by a **qualified TSP**, whose credentials have been recorded in a **trusted list**[26] published by an EU member state (Article 22, eIDAS).
- It must be created by a **qualified electronic signature device** (Article 3(23), eIDAS).

As is the case with an AdES, the qualified TSP must verify the identity of the signatory prior to the issuance of the digital certificates. The digital certificate is a qualified certificate providing the highest level of assurance that the signatory is who they purport to be and certifying the link between that signatory and their public key.

Annex I of eIDAS specifies the profile requirements for qualified certificates. They must contain the identity of the qualified TSP, the identity of the signatory (either a name or pseudonym), the signatory's unique public key, and indicate that the certificate is issued as a qualified certificate.

A QES provides the highest level of admissibility in EU courts and has equivalent legal standing to a handwritten signature (Article 25(2), eIDAS). A QES based on a qualified certificate benefits from mutual recognition across EU member states and the EEA.

The QES is therefore the 'gold standard' in terms of authenticity, integrity and non-repudiation (see **here** for more detail).

Historically, the qualified electronic signature device was a physical smartcard or USB token limited to desktop usage. This was inflexible and not particularly user-friendly. To date, QES has not seen wide adoption in the UK. But nascent technology is now enabling signatories to create and validate digital signatures in the cloud with a mobile device such as a tablet or smartphone. eIDAS expressly envisages the use of 'remote' or cloud-based signatures, obliging the TSP to:

> *'apply specific management and administrative security procedures and use trustworthy systems and products… …in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory.'*

Recital 52, eIDAS.

In 2019, the European Telecommunication Standards Institute (ETSI) released **a set of three technical specifications**[27] for cloud-based digital signatures supporting mobile devices; the latter of which builds on the Cloud Signature Consortium specification which was pioneered by Adobe Sign and establishes the protocols for secure communication between the different components needed to create a secure cloud-based digital signature, such as a QES.

It is likely that the use of cloud-based QES and qualified certificates for executing transaction documents will grow in the UK as lawyers and compliance professionals become more conversant with QES technology, particularly in relation to cross-border transactions.

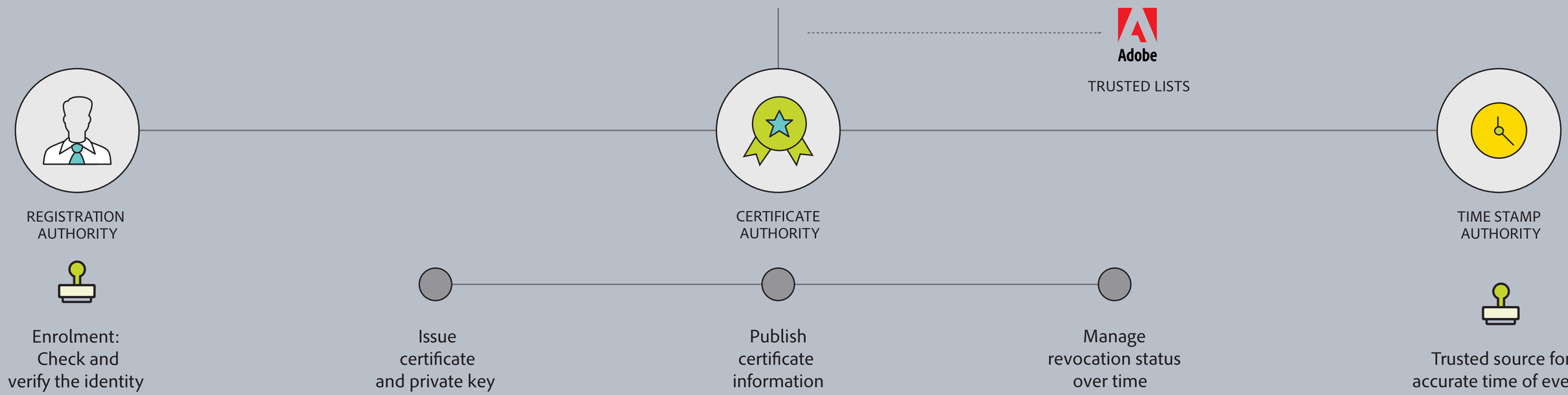
The leading platforms – notably Adobe Sign – work with a wide network of qualified TSPs. The qualified TSPs appear in the **European Union Trusted List**[28] which means they are accredited to provide qualified certificates, QES (and other qualified trust services) in compliance with eIDAS. The qualified TSP is responsible for verifying the signatory's identity or it may delegate this activity to a third party 'registration authority'. The procedure varies but a signatory requesting a qualified certificate typically uploads a copy of their passport or driving licence to the qualified TSP's digital platform and is authenticated in a video call (Article 24, eIDAS).

The key pair and qualified certificates are generated and hosted by the qualified TSP in the cloud on a certified hardware security module ("**HSM**"). The HSM is a 'qualified electronic signature device' that has been certified against the requirements laid down in Annex II of eIDAS. The qualified certificate may be used by the signatory to sign documents that are uploaded to the e-signing platform. This workflow, including the authentication process, can be found by clicking the 'e-signing workflow' button in the toolbar above.

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Trusted authorities and lists

Trusted authorities



Note: certificate authority is another term for TSP.

Graphic reproduced by kind permission of Adobe Sign.

5. Digital Signatures: Advanced And Qualified Electronic Signatures

Scotland

Digital signature discretion in Scotland

Where a document is **not required to be in writing under ROWSA**, the law in Scotland permits the parties to a transaction to choose which form of electronic signature is appropriate for use in any particular case, any form of which will be considered a valid signature. Where the use of a digital signature is not a legal requirement, the respective risks and benefits of a simple form of electronic signature or a **self-proving form** need to be weighed up. The Law Society of Scotland's draft **Electronic Signatures Guide** contains some guidance on the risk assessment process that should be carried out in making this decision.

Cloud-based digital signatures provided by e-signing platforms are being used in Scottish transactions, but their use is not yet widespread.

Law in practice: how Scottish lawyers use Smartcards

An alternative form of electronic signature which is self-proving is available through the Law Society of Scotland Smartcard issued to practising solicitors under its jurisdiction. This innovation enables solicitors to sign electronic documents and authenticate them with a QES in accordance with ROWSA. Section 12(3) of ROWSA provides that an agent may authenticate an electronic document on behalf of the granter (see **here** for more detail).

In practice, Scottish solicitors rely on this section to authenticate on behalf of their clients and use their Smartcards to apply a QES to the document. The Smartcard is used with a card reader and is protected by a PIN code to ensure that only the named solicitor, whose identity has been verified by the Law Society of Scotland, may use the Smartcard.

The Smartcard scheme has not proven popular with the legal profession. In 2020, solicitors and their clients predominantly sign transaction documents in wet-ink, but cloud-based QES and digital certificates overcome the limitations of Smartcards. Section 12(3) of ROWSA laid the foundations for Scottish solicitors to authenticate on behalf of their clients, but the Smartcard lacked the flexibility of the cloud-based platforms available. By upgrading to cloud-based digital certificates for QES, solicitors could authenticate transaction documents on behalf of their clients anytime and anywhere using a mobile device.

6. Legal Validity And Admissibility Of Electronic Signatures

Legal validity of electronic signatures in English law

The Law Commission concluded in its 2019 Report that '***an electronic signature is capable in law of being used to validly execute a document (including a deed)***[29]'. This is subject to two caveats: first, that the signatory intends to authenticate the document (that is, intends to sign and be bound by the document); and second, any statutory or contractual formalities relating to the execution of the document are **satisfied**[30].

In its 2001 Advice, the Law Commission suggested that the courts should apply a purely objective test to determine whether there is an intention to authenticate the document: '***would the conduct of the signatory indicate an authenticating intention to a reasonable person?***[31]' The 2019 Report endorsed this approach.

A significant advantage of using an e-signing platform is that – in the absence of fraud – the digital audit trail provides solid evidence of the signatory's intention to authenticate the document.

When arranging for a document to be signed in wet-ink or by electronic means, you must have due regard to the relevant formalities. If a contract or deed is signed with an electronic signature, but the relevant statutory formalities (such as witnessing and attestation) are not complied with, that document is not validly executed.

It is rare for statutory formalities to prevent the use of an electronic signature to execute a transaction, but there are two prominent exceptions:

- The Law Commission indicated in its 2017 consultation paper '**Making a Will (No 231)**' that '*the formality rules most likely preclude the electronic execution of wills*' under section 9 of the **Wills Act 1837**[32].
- HMLR has paved the way for digital conveyancing and land registration. Changes to the LRR 2003 introduced in 2018 have laid the legal foundation for registrable dispositions to be made digitally using an **AdES**[33]. Currently, this option is only available for digital mortgages, but the Chief Land Registrar has **recently consulted** and subsequently issued guidance on the use of electronic signatures in light of the **COVID-19** pandemic.

Formalities may be contractual as well as statutory. A common example is where a contract stipulates that any amendments are to be made in writing. Unless the contract provides otherwise, an electronic signature will be capable of satisfying this requirement.

Where the signatory is a corporate entity, it is prudent to check the constitutional documents (such as the articles of association) to ensure there is no bar on using an electronic signature.

The current law on electronic signatures derives from a mixture of EU and domestic legislation, as well as case law.

6. Legal Validity And Admissibility Of Electronic Signatures

eIDAS

eIDAS came into effect on 1 July 2016 and replaced the **eSignatures Directive 1999**[34]. As an EU Regulation, eIDAS had direct effect in the UK, but was supplemented by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016. This was necessary to designate the Information Commissioner's Office as the **supervisory body** for the UK and to make some minor, consequential amendments to the ECA 2000 (see **here** for more detail on the ECA 2000).

eIDAS defines three categories of electronic signature: **simple electronic signature**, and two digital signatures, **AdES and QES**.

Article 25(1) of eIDAS is the key provision. It states that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings *solely* on the grounds that it is in an electronic form. This is sometimes referred to as the 'non-discrimination' principle. A court may not discard an electronic signature as evidence solely because it is in electronic form; but the court must still check whether there are any execution formalities under EU and national law that apply to the document in question. If those formalities are not met, the document may have no legal effect.

Article 25(2) and (3) also established the QES as the highest grade of electronic signature: a QES has the equivalent legal standing of a handwritten signature in all 27 **EU member states**[35]. This reflects the European Commission's strong desire to promote QES as a common technical standard across the EU and boost the digital single market.

Recital 49 to eIDAS states that – save for the requirement that a QES is legally equivalent to a handwritten signature – '*it is for national law to define the legal effect of electronic signatures.*' This is amplified in Article 2(3) which provides that eIDAS '*does not affect national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form.*'

What this means is that a transaction document signed with an electronic signature is not automatically valid under eIDAS. Valid execution depends on whether the formalities for that class of transaction (and type of document/deed) have been satisfied under national law. For example, consider the status of an English law deed that is signed by an individual with an electronic signature, but the signature is not witnessed and attested: clearly, the failure to satisfy the formalities for a deed executed by an individual under English law would result in defective execution and the deed would be invalid as a **deed**[36].

6. Legal Validity And Admissibility Of Electronic Signatures

ECA 2000

The ECA 2000 applies across the whole of the UK. It transposed the eSignatures Directive into UK law and was subsequently amended in 2016 when eIDAS came into effect.

Section 7(1) of the ECA 2000 provides that in any legal proceedings:

(a) an **electronic signature**[37] incorporated into or logically associated with a particular electronic communication or particular electronic data; and

(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the *authenticity* or *integrity* of the communication or data.

Where a claimant alleges that an electronic document is inauthentic (for example, it was not signed by the person who had purportedly done so) or it has been tampered with after signature, they would have to prove this allegation on the balance of probabilities.

There is occasionally some confusion over the meanings of '*authenticity*' and '*integrity*' in section 7 of the ECA 2000. The explanatory notes to the legislation shed some light on what the parliamentary draftsmen intended:

> *'An electronic signature is something associated with an electronic document that performs similar functions to a manual signature. It can be used to give the recipient confirmation that the communication comes from whom it purports to come from ("authenticity"). Another important use of electronic signatures is establishing that the communication has not been tampered with ("integrity").'*

Explanatory notes to the ECA 2002, para 5.

When a transaction is executed using an e-signing platform such as Adobe Sign, DocuSign or HelloSign, a digital audit trail is generated. This records who signed the document (including their email and IP address), any additional steps taken to authenticate the signatory (such as a passcode sent to the signatory's mobile phone) and it is time-stamped. The digital audit trail is admissible in evidence under section 7(1) of the ECA 2000. This adds substantial evidential weight in the event of a dispute concerning an electronic document that was authenticated using that platform.

Although the ECA 2000 dealt with the admissibility of electronic signatures, it did not directly address their legal validity. The Law Commission suggested in its 2018 Consultation that this omission was because, '***the common law was considered to be sufficiently flexible to allow for electronic signatures***[38].' That may be so, but this flexibility has arguably contributed to the uncertainty many perceive to be hindering the adoption of e-signing platforms.

Case law

The failure to address legal validity in the ECA 2000 meant that it has fallen to the courts to determine whether an electronic signature satisfies a statutory requirement for a signature under English law.

A slender body of case law has established that an electronic signature is *generally* capable in law of being used to execute a document, including transactions where there is a statutory requirement for a signature.

Recent judgments from the Court of Appeal and the High Court typify a pragmatic approach which is more focused on the function, rather than the form, of an electronic signature. The courts look at all the surrounding circumstances to objectively assess whether the electronic signature demonstrates an intention to **authenticate**[39] the document.

Chapter 3 of the 2018 Consultation summarises the leading cases. The courts have held that the following types of electronic signature were valid for the purpose of fulfilling a statutory requirement for a signature:

— A name at the bottom of an **email**[40]

— Clicking an 'I accept' tick box on a **website**[41]

— The header of a SWIFT **message**[42]

The recent case of ***Neocleous v Rees***[43] reaffirms the purposive approach of the courts in interpreting whether an electronic signature can satisfy a statutory requirement for a signature. In this case, the Manchester county court invoked the 2019 Report in its judgment and ruled that an automatically generated email footer containing the name and contact details of the sender constituted a signature for the purposes of section 2(3) of the Law of Property (Miscellaneous Provisions) Act 1989 ("**LP(MP)A 1989**").

The common denominator in each of these cases is that the signatory *intended* to authenticate the document. Although untested by the UK courts, there is a strong argument that the digital audit trail from an e-signing platform should be admissible in legal proceedings and deliver compelling evidence of the signatory's intention to authenticate the document. This presumption of admissibility – and the evidential weight – will be greater where the signatories use multi-factor authentication or a digital signature.

Scotland

Legal Validity of Electronic Signatures in Scotland

There is some overlap between the two legal systems. For example, the ECA 2000 enacted the eSignatures Directive 1999 into UK law which means that Scots law also recognises electronic signatures and their admissibility in legal proceedings to determine any question as to the authenticity or integrity of an electronic communication (section 7(1)).

A recurrent theme of the 2019 Report is the Law Commission's preference that English law be '*technology-neutral*' and should not favour any particular technology to execute documents electronically. This contrasts starkly with the approach taken in Scotland where the law mandates the use of digital signatures for those documents which must be in writing under ROWSA and to secure self-proving status.

Scotland has specific legislation (ROWSA and the **Scottish Regulations** made under ROWSA) in relation to electronic documents and electronic signatures. ROWSA prescribes the use of an AdES for the valid authentication of certain kinds of Scots law documents. Additionally, a QES will be required where the parties to an electronic document wish to benefit from a statutory presumption that it has been (properly) signed (or 'self-proving'). An electronic signature and an AdES cannot be self-proving. In March 2020, the Law Society of Scotland published a draft **Electronic Signatures Guide** to assist users with the regulations.

Requirements of Writing (Scotland) Act 1995

In 2012, the Requirements of Writing (Scotland) Act 1995 ("**ROWSA**") was amended to explicitly allow certain documents, which had to be written tangibly under section 1(2), to take electronic form as an alternative to a **paper document**[44]. The amended ROWSA did not contain an express statement of validity for electronic signatures; it did, however, give legal effect to documents signed electronically where they meet certain requirements.

ROWSA provides that a written contract is not required (in paper or electronic form) except in specified cases. These include:

— A contract or unilateral obligation for the creation, transfer, variation or extinction of a real right in land (for example, a contract to sell a property)

— A gratuitous unilateral obligation, except those undertaken in the course of **business**[45]

— The constitution of a trust whereby a person declares himself to be the sole trustee of his own property (or any property which he may acquire)

— The making of a **will**[46]

— Assignations of, or grants of security over, **patents**[47]

These arrangements or obligations must either be contained in a 'traditional document' which complies with section 2 of ROWSA or an 'electronic document' which complies with section 9B of ROWSA.

Section 9B(1) provides that an electronic document required to be in writing is not valid unless it is authenticated by the 'granter' and meets the requirements prescribed by the Scottish Regulations. These regulations stipulate that the authentication must be by means of an AdES. The characteristics of an AdES are explained **here**. In short, if an electronic document is used for a contract that must be in writing under ROWSA, the granter must authenticate using an AdES to ensure valid execution.

7. Electronic signatures: simple contracts and deeds

Simple contracts

The general rule under English law is that a contract does not need to be made in any particular form. Most commercial and consumer contracts can be made informally and are not subject to a legal requirement for signature at all. In fact, in many instances they can be concluded orally or by conduct, provided the essential elements for an enforceable contract are present: offer and acceptance, consideration, certainty of terms and an intention to be legally bound.

Most simple contracts which the parties choose to record in writing may be validly executed with an electronic signature because there is no legal requirement for a signature in the first place.

In addition to verifying that the essential contractual elements are present, lawyers advising corporate clients should check that:

— The **articles of association**[48] (or other constitutional documents) do not prohibit electronic execution or specify what type of electronic signature is required (such as an AdES or QES).

— There is no board resolution restricting the use of an electronic signature.

— The designated signatory has the actual or ostensible authority to enter into the contract on behalf of the company.

7. Electronic signatures: simple contracts and deeds

Statutory formalities

Other types of document, however, may be subject to statutory formalities which the parties must observe if their contract (or transaction) is to be valid and enforceable. Formalities vary, but they typically require that the contract be recorded 'in writing', 'signed' or executed as a deed. Common examples include:

— Guarantees, which must be made in writing, or evidenced by writing, and signed by the guarantor (section 4, Statute of Frauds 1677).

— Contracts for the sale of land, which must be in writing, incorporate all the terms that the parties have expressly agreed in one document (or, where contracts are to be exchanged, in each document) and be signed by or on behalf of each party (section 2, LP(MP)A 1989).

— Transfers of registered securities, using a stock transfer form that complies with section 1 of the Stock Transfer Act 1963.

— Regulated credit agreements under the Consumer Credit Act 1974, which must be in writing in a prescribed form.

— Powers of attorney, which must be executed as a deed by the donor of the power (section 1(1), Powers of Attorney Act 1971).

— Copyright assignments, which must be in writing and signed by or on behalf of the assignor (section 90(3), Copyright Designs and Patents Act 1988).

— Unilateral promises, which must be made by deed to be enforceable.

7. Electronic signatures: simple contracts and deeds

Documents to be made 'in writing', 'signed' or 'under hand'

Two questions arise: first, can an electronic document satisfy a statutory requirement that a document be made 'in writing' or 'under hand'? Second, if it is authenticated with an electronic signature, has it been 'signed'?

Case law provides the answer to these questions:

- Electronic documents will, in general, satisfy a statutory requirement for **writing**[49].
- Electronic signatures are capable of satisfying a statutory requirement for a document to be 'signed' where there is evidence that the signatory intended to authenticate the **document**[50].

Drawing upon the relevant case law, the Law Society 2016 Practice Note concluded that an electronic contract or deed that is executed with an electronic signature is capable of satisfying a statutory requirement to be in writing or signed.

The Law Commission's 2019 Report is less bullish but echoes the Law Society's conclusion. It states that an electronic signature is capable in law of being used to validly execute a document (including a deed) subject to two important caveats:

> *'The person signing the document must have intended to authenticate the document. Any formalities relating to execution of that document must be satisfied.'*

Paragraph 3.6, 2019 Report and paragraph 1, Statement of Law.

The Law Commission based its **conclusion** on the provisions of eIDAS, the ECA 2000 and on case law relating to electronic signatures and signatures more generally.

7. Electronic signatures: simple contracts and deeds

Deeds

A deed is a document executed with a high degree of formality, and by which an interest, right or property passes or is confirmed, or a binding obligation is created or confirmed.

Deeds may be required by statute or common law. Examples include registrable transfers of land, mortgages, appointment of trustees, powers of attorney and unilateral promises.

Even where it is not mandatory under English law, parties may voluntarily execute a document as a deed to benefit from the longer limitation period of 12 years under the **Limitation Act 1980**[51].

A deed must fulfil any formal requirements prescribed by statute and common law, which include the key requirements that the deed be validly executed and delivered by the parties.

When are deeds required?

Documents which must be executed as deeds under English law include:

a) the transfer or creation of an interest in land (including a mortgage or charge); if it is not, it will be void for the purpose of conveying a legal estate under section 52 of the Law of Property Act 1925;

b) leases for a term of more than three years under section 52 of the Law of Property Act 1925;

c) a legal mortgage or charge by way of a legal mortgage over land under sections 52(2), 85(1) and 86(1) of the Law of Property Act 1925;

d) the appointment or discharge of a trustee under section 159 of the Trustee Act 1925;

e) a power of attorney (including powers of attorney used in a commercial context such as some inter-creditor deeds, and those used in a personal capacity such as lasting powers of attorney);

f) an agreement without consideration (unilateral promise); and

g) the release of a debt, liability or obligation where is no adequate consideration.

7. Electronic signatures: simple contracts and deeds

Deeds executed by an individual

Section 1(3)(a) of the LP(MP)A 1989 provides that for an individual to validly execute a deed, the instrument must be signed in the presence of a witness who attests the signature.

The statutory requirements for signature and attestation may be satisfied using an electronic signature provided that the witness is physically present when the individual signs the deed (see **here** for more detail on how to witness and attest an electronic signature using an e-signing platform).

Deeds executed by a company under the CA 2006

The formalities governing the execution by UK companies of deeds governed by English law are dealt with by sections 44 and 46 of the CA 2006.

Section 46 provides that a deed is validly executed for the purposes of section 1(2) of the LP(MP) A 1989 if it is duly executed by the company and delivered as a deed.

Section 44(2) specifies two ways in which a company may validly execute a deed (other than by affixing its common seal):

- By the signatures of two authorised signatories (either two directors or a director and secretary of the company) (section 44(2)(a)).
- By the signature of a director of the company in the presence of a witness who attests the signature (section 44(2)(b)).

In its 2019 Report, the Law Commission confirmed that where a deed is executed by the signatures of two authorised signatories in accordance with section 44(2)(a), there is no requirement for the signatures to be applied at the same time. Furthermore, each signatory can sign the deed electronically either in counterparts, or on the same soft copy of the **deed**[52].

The key takeaway is that section 44(2)(a) of the CA 2006 obviates the need to witness and attest the deed. Social distancing measures for managing the COVID-19 pandemic have made it harder to comply with the witnessing requirement; it is therefore advisable for corporates to sidestep this requirement wherever practicable by executing deeds using the signatures of two authorised signatories in accordance with section 44(2)(a).

Delivering a deed by electronic means

The final formality which is necessary for a deed to become binding on the parties is the requirement for delivery.

The purpose of delivery is to signify that the maker of the deed intends it to come into effect and be bound by it. The deed becomes binding on the date of delivery rather than the date of execution.

In practice, parties satisfy the requirement for delivery in various ways, for example, simultaneous execution and delivery, or passing onto a party's lawyer to 'hold to order', or including a clause in the deed which states the date of delivery.

Both the Law Society 2016 Practice Note and the 2019 Report agree that the requirement for delivery is no impediment to the electronic execution of deeds; but it is important to ensure the deed makes clear when delivery takes place.

7. Electronic signatures: simple contracts and deeds

Witnessing and Attestation

Witnessing involves observing the execution of a document by a signatory. *Attestation* involves a further step of recording on the document itself that the witness has observed the execution.

The 2019 Report discussed the statutory requirements in section 1(3)(a) of the LP(MP)A 1989 and section 44(2)(b) of the CA 2006 for a deed to be '*signed in the presence of a witness who attests the signature*'. The Law Commission deliberated over the meaning of the word 'presence', and whether it might be interpreted broadly to include 'remote' or 'virtual' presence (such as a video link) to account for advances in technology. A number of consultees had argued that it would be open for a court to decide that remote or virtual witnessing would satisfy the relevant statutory requirements. While acknowledging this possibility, the Law Commission concluded that formalities do require the witness to be physically present in the same location as the executing signatory and to observe the electronic signing of the deed (paragraph 8, Statement of Law).

How to witness and attest an electronic signature via an e-signing platform

The witness must be physically present and observe the signatory insert their electronic signature into the signature block of the electronic deed. The signatory must nominate a witness and fill in their name and email address. An email is then sent from the platform to the witness. The witness is prompted to provide their address and occupation, and to sign the attestation clause in the document with their own electronic signature. If the witness has an account with the platform, they will have access to the basic audit trail (what DocuSign calls the 'Envelope History'), but no access to the e-signed deed.

The complete digital audit trail (what DocuSign calls the 'Certificate of Completion') will record the IP address of the witness when they attest the deed. The theory goes that the IP address of the signatory and witness should match and constitute evidence that the witness was physically present when the electronic signature was affixed to the deed. But this is not always the case. For example, if the signatory uses a Wi-Fi network to sign the deed but the witness uses a mobile network to complete the attestation process on their own device, their IP addresses will differ despite being in the same physical location. Conversely, if the signatory and witness are not physically present in the same location but use the same virtual private network (VPN) to get online, it may appear as if they are working from the same IP address. The IP address may therefore not provide definitive proof that the witness was physically present when the deed was executed.

To avoid a discrepancy between the IP addresses of the signatory and witness, it is prudent for the signatory and witness to complete the execution and attestation process using the same device. A further advantage of this approach is that the witness can only see the execution block and not the contents of the document (which may be sensitive or confidential).

The 2019 Report has recommended, and the UK Government has agreed that an industry working group should be tasked with examining the '*practical and technical obstacles to video witnessing of electronic signatures on deeds and attestation*'. The Law Commission has also proposed that, following the work of the industry working group, the Government should consider amending the ECA 2000 to expressly permit video witnessing. COVID-19 underscores the urgency for this legal reform. We understand that the leading e-signing platforms are already exploring how to integrate the requisite functionality into their standard products in a way that will satisfy the legal requirements and preserve the simple workflow. In the meantime, if the parties wish to provide further evidence of the physical presence of the witness, the witness could be asked to provide separate written confirmation.

7. Electronic signatures: simple contracts and deeds

Consenting to sign documents with an electronic signature

It is not strictly necessary to include a reference to electronic signatures in an English law document itself for it to be validly executed using an **electronic signature**[53], but other jurisdictions may require some form of consent to do business electronically.

The leading e-signing platforms often have consent built into the workflow so there is no need to include an explicit consent in the document itself. Nevertheless, it may be desirable to do so, particularly where that document is used in cross-border transactions and will be signed by an overseas party. A specimen clause is set out below:

'*This Agreement may be executed: (i) by electronic signature (whatever form that electronic signature may take); and (ii) in any number of counterparts and by the parties to it on separate counterparts, each of which shall be an original, but all of which together shall constitute one and the same instrument. This Agreement shall not be effective until each of the parties has executed at least one counterpart. Execution by electronic signature shall be conclusive evidence of the executing party's intention to be bound by this Agreement in the same way as if it were executed with a wet-ink signature*[54].'

7. Electronic signatures: simple contracts and deeds

Scotland

Other than the **ROWSA requirements for written contracts** and other statutory exemptions (for example, the assignation of certain **intellectual property rights**[55]), there is no general rule in Scots law that requires contracts to be made in writing or signed by the parties. However, parties often choose to document their contractual arrangements in writing for evidential purposes.

Statutory Presumption

In Scots law there is no requirement for a human to witness an electronic signature, as remains required for certain types of execution of English law deeds. In this respect, the Scottish approach aligns more closely with the law of much of the rest of continental Europe, than it does with that of England and Wales.

ROWSA makes a distinction between a document which is (merely) formally valid and one which has been signed in such a way as to benefit from a statutory presumption that it has been (properly) signed ('authenticated') by the **granter**[56]. In order to benefit from this statutory presumption (i.e. to be self-proving or 'probative') ROWSA requires that the document be authenticated by means of a QES.

The statutory presumption is important for two reasons: first, from an evidential standpoint as it effectively means that the electronic document may be relied upon in a contractual dispute over whether it was validly executed; in other words, any party founding on that document in court is relieved of having to lead evidence as to its validity; second, certain registries require a document to be signed in self-proving form for registration purposes, including the Land Register of Scotland (although at present some of these registers do not accept electronically signed deeds at all or only accept limited categories of electronically signed deeds).

Self-proving ('probative') status of electronic documents in Scotland

An electronic document must fulfil the requirements of section 9C of ROWSA for it to be presumed to be self-proving:

— It must appear to have been authenticated by the granter, and nothing in the document or in the authentication indicates that it was not so authenticated.

— It must conform with the Scottish Regulations. As mentioned, Regulation 3 of the Scottish Regulations specifies that to secure self-proving status, an electronic document must be authenticated by a QES, backed by a qualified certificate from a qualified TSP.

8. Special Cases: When Should You Proceed With Caution?

Although the 2019 Report strongly endorses electronic signatures, there may be circumstances in which it is not appropriate to use them. This may arise where the applicable law prescribes the type of electronic signature for a document or where electronic execution is otherwise ill-advised.

*As noted **here**, statutory formalities rarely preclude use of an electronic signature, except in respect of the two notable exceptions of the creation of wills, and registrable dispositions under LRA 2002 and LRR 2003 explained below.*

HMLR requirements

Prior to the COVID-19 pandemic, HMLR would not accept an electronic document with an electronic signature as a dispositionary deed for registration in England and Wales unless it complies with the provisions of the LRA 2002 and rules 54A to D of the LRR 2003. Section 91 of the LRA 2002 confirms that an electronic document will be regarded for statutory purposes as a deed if it is executed with an AdES. But this is still dependent on the Chief Land Registrar issuing a notice under rule 54C of the LRR 2003 to specify which type of registrable dispositions may be made electronically. This is currently restricted to electronic mortgage deeds which are executed using HMLR's **digital mortgage service**. A further requirement is that the signatory uses HMLR's own purpose-built PKI solution for generating and certifying the AdES.

In light of the pandemic, HMLR announced that it will, until further notice, register a transfer or certain other deeds that have been executed in accordance with the 'option 1' **virtual signing** procedure set out in the Law Society 2010 Practice Note. HMLR has also permitted some Land Charges applications to be made by email from 1 April 2020.

HMLR published guidance to govern the use of electronic signatures and further information on digital signatures. From 27 July 2020 until further notice, HMLR will accept what it calls "witnessed electronic signatures" that comply with its **practice requirements**. While its requirements refer to signing in the presence of a witness, they also cover a deed being signed on behalf of a company by two authorised signatories under section 44(2)(a) of the CA 2006 with the requirements being read accordingly.

While HMLR believe that a number of businesses that currently provide electronic signatures should be able to quickly meet its requirements, there are some **concerns** that most e-signing platforms commonly used do not wholly conform.

HMLR consider that the use of witnessed electronic signatures is only an interim solution. They are currently working on how they might allow conveyancers to rely on section 91 of the LRA 2002 in carrying out transfers and other dispositions, in addition to just digital mortgages. HMLR is exploring the potential introduction of QES. HMLR believe that QES is the right long-term component of a wholly digital conveyancing process, because the added security and the digital nature of the resultant document enables joined-up and automated processing throughout the transaction.

HMLR envisage that the document would be uploaded by the conveyancer, the signatory would access the document but would need to meet the identification requirements of the qualified TSP before signing. The signed document is then made available to the conveyancer to access and submit to HMLR.

HMLR's intention (stated in a **blog** from HMLR's General Counsel on 2 October 2020) is to work with the property sector to bring QES in as an option as soon as possible, but with the expectation that it will be used alongside witnessed electronic signatures for some time to come. HMLR will at some point review the use of witnessed electronic signatures, but not until QES has shown how it performs in practice for the various different uses within the property market. That may take some time – possibly a couple of years or more. In the meantime, HMLR will continue to support the growing use of both types of signature. HMLR is close to having draft practice guidance for QES and the guidance will evolve according to feedback. It may then take a few months for the QES providers to tailor their services to meet the conveyancing sector's needs.

HMLR is also exploring whether digital identity checking technology used in other sectors can be encouraged in the conveyancing industry to increase resilience against fraud and improve the ease of buying and selling.

8. Special Cases: When Should You Proceed With Caution?

Summary of HMLR's practice requirements for witnessed electronic signatures

Until further notice, HMLR will accept for registration transfers and certain other registrable dispositions and deeds that have been electronically signed, provided that the requirements set out below are satisfied.

1. All the parties agree to the use of electronic signatures and an e-signing platform (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 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. 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.

4. The signing and dating process is as follows:

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 a one-time password (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 – Having observed the signatory sign 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.

5. The conveyancer who lodges the application with HMLR does so by electronic means and includes with the application a PDF of the completed deed. However, where the application is for first registration, a print-out of the PDF, certified to be a true copy of the completed deed, can be lodged.

6. The conveyancer lodging the application (including an application for first registration) provides the following certificate: "I certify that, to the best of my knowledge and belief, the requirements set out in practice guide 8 for the execution of deeds using electronic signatures have been satisfied." This certificate will be read by HMLR as referring to the requirements as they are at the time the deed is signed. The certificate is to be given by an individual conveyancer, not on behalf of the law firm. **Practice Guide 8** is HMLR's practice guide for execution of deeds and contains an example of an acceptable certificate at Appendix 3.

While not a requirement, HMLR state that the parties' conveyancers are advised to retain with their conveyancing file a copy of the completion certificate or audit report produced by the platform at the end of the signing process. Such a certificate or report should give an audit trail of the signing, including the time and date of the signatures, email addresses the document was sent to, the OTP method used, the fields that were completed and the IP addresses of the devices that were used.

HMLR permit "mixed signing". If it is necessary for one party to a deed to sign in wet ink (either in the conventional way or as part of the *Mercury*-signing process, see **here**) and another to sign with an electronic signature, this can be done by way of counterpart deeds. Parties can also sign counterpart deeds each using a different electronic signature platform provided that, in each case, HMLR's requirements are observed.

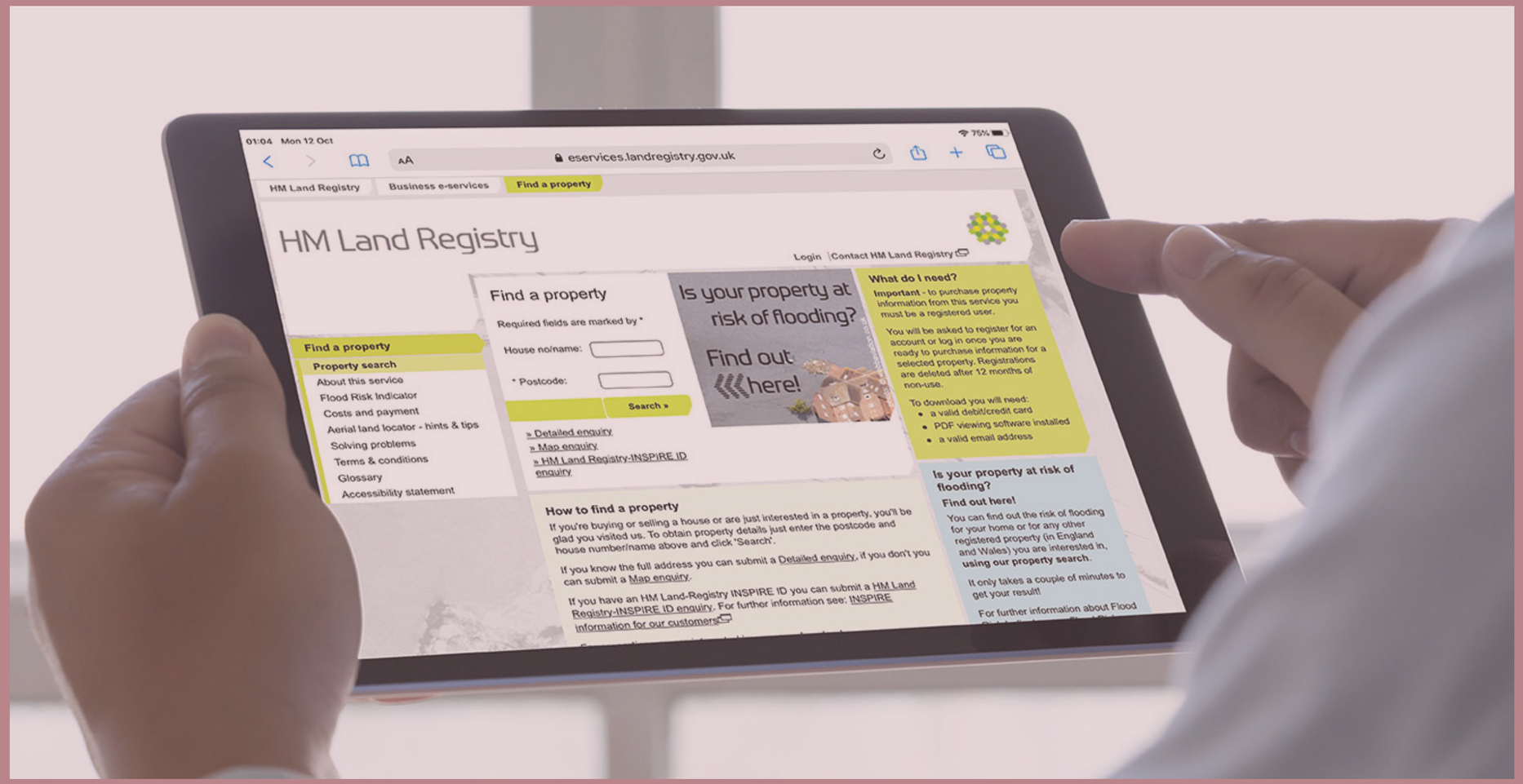
8. Special Cases: When Should You Proceed With Caution?

Concerns with HMLR's practice requirements

The key concerns relate to witnesses and to signatories unknown when the document 'envelope' (or equivalent on the relevant platform) is being populated by the conveyancer:

The requirement for the conveyancer to include at the outset the details of the signatories will prevent the use of functionality available on certain platforms that enable electronic signatures to be used when the specific identity of the signatory is unknown when the platform is populated. For example, an envelope can be sent to a company's signing administrator, who will then allocate the deed for signing to one or two signatories out of a pool of signatories.

The witness is required to input an OTP sent to them by text message by the platform to access the deed. Such two-factor authentication for witnesses is not possible on every platform. While to overcome this limitation, a witness may be treated as a signatory, this would mean that the witness will automatically receive a copy of all completed documents in the envelope, which may be inappropriate from a confidentiality perspective. This HMLR requirement may limit the use of e-signatures for deeds requiring witnessing.



8. Special Cases: When Should You Proceed With Caution?

Wills and lasting powers of attorney

The Law Commission has indicated that formalities under the Wills Act 1837 'most likely' prohibit electronic wills (see **here** for more detail).

A lasting power of attorney is used by an individual (the "**donor**") to confer authority on another person to make decisions about the donor's personal welfare, and/or property and affairs. The lasting power of attorney must be executed as a deed and in a prescribed form.

The requirements include a certificate by a third party who confirms that the donor of the power understands the purpose and scope of the document and that no fraud or undue pressure is being used to induce **them**[57].

The Law Commission's interpretation of the law is that, like most deeds, a lasting power of attorney could be in theory be executed electronically. But the document must be registered with the Office for the Public Guardian and it will only accept a wet-ink signature.

8. Special Cases: When Should You Proceed With Caution?

Negotiable instruments

Negotiable instruments, such as bills of exchange, promissory notes and chattel mortgages granted by individuals must exist in physical form. This has engendered some debate over whether they can be executed electronically and still comply with the relevant statutory formalities governing the instrument in question. In relation to bills of exchange, the leading text on the subject expresses the view that:

> *'Despite the ubiquity and sophistication of digital communications it remains the case that a bill of exchange within the meaning of the [Bills of Exchange Act 1882] can only be created as a physical document in which the obligations are embodied…. To date there have been no proposals to introduce electronic bills of exchange. There are problems inherent in seeking to achieve by way of electronic means, the legal effect of a paper bill of exchange. The physical piece of paper lies at the heart of the 19th century philosophy of the negotiability and transfer of bills. Any proposal to introduce an electronic instrument would require a fundamental departure from the 1882 Act as it exists at present.'*

Byles on Bills of Exchange and Cheques (29th edition, Sweet & Maxwell), Chapter 2, Form of Bills and Notes.

It is important to confirm that the signatory has the requisite authority, the company has the capacity and that there are no restrictions.

8. Special Cases: When Should You Proceed With Caution?

Registration requirements

It is often necessary to register transaction documents after execution. If a public registry only accepts wet-ink signatures, an electronic signature is not an option – regardless of whether this would be a valid means of execution under English law.

The direction of travel is supportive of electronic signatures as more and more registries look to modernise their business processes and facilitate online filings:

- Companies House generally accepts electronic signatures across the UK. It operates an online filing service which allows most forms and notices to be signed and delivered electronically.
- The Intellectual Property Office, the Civil Aviation Authority and the UK Ship Register generally accept electronic signatures for online filings from across the UK.
- HM Revenue & Customs normally expects to stamp a wet-ink version of a document where stamp duty is payable, such as a stock transfer form. However, it has temporarily relaxed its rules from 25 March 2020 across the UK to mitigate the impact of the COVID-19 pandemic. It now insists that instruments of transfer are not submitted by post and instead accepts emails attaching an electronic copy (for example, a scanned PDF).

Place of execution

If the place of execution of the document is important (for example, in relation to payment of tax or stamp duty), the parties may prefer a physical signing ceremony.

But the leading e-signing platforms have the functionality to record the signatory's geo-location in the digital audit trail. This could be adduced as proof of where the document was executed in the event of a dispute.

Restrictions in a company's constitutional documents

Where the executing party is a corporate entity, it is important to confirm that it has the requisite authority and capacity and there are no restrictions in its constitutional documents on using electronic signatures. The risk to the counterparty is tempered by some statutory protection in sections 39 and 40 of the CA 2006.

8. Special Cases: When Should You Proceed With Caution?

Cross-border implications

Trade and commerce traverse national borders. UK parties regularly conclude transactions with overseas parties and those transactions may or may not be governed by English (or Scots) law. It is vital, therefore, that the transactional documents are executed in a manner that ensures their recognition, registration or potential enforcement in the relevant jurisdiction. This may give rise to issues that will require advice from local counsel. For example:

(1) **Where any litigation, or other action, in relation to a document governed by English law may take place, or be required, outside England and Wales**. This may arise where: (i) there is a foreign jurisdiction clause in an English law contract; (ii) an English judgment needs to be enforced overseas; (iii) a claim needs to be made in a non-English insolvency proceeding; (iv) a document needs to be notarised or apostilled; and (v) a registration needs to be made at a non-English registry.

(2) **Where a document is governed by a law other than English law**. Whether a document can be validly executed using an electronic signature is a matter for the governing law and, in some jurisdictions, the impact of the law of the forum where the contract is relied upon. Such issues are beyond the scope of this guide. You may find the information in Appendix 2 to the 2018 Consultation helpful; it considers legislative schemes governing electronic signatures in a several overseas jurisdictions, including New York, Australia and Hong Kong.

(3) **Where an overseas company[58] signs an English law document. The Rome I Regulation[59]** will apply (in most cases) to any litigation brought in the English courts. For matters falling within the scope of the Rome I Regulation, an English court will typically uphold a document governed by English law as validly executed so long as it has been validly executed as a matter of English law. However, this can be affected by cross-border issues such as whether the execution was illegal in the location of the execution.

Section 44(1) of the CA 2006, as modified by the Overseas Companies (Execution of Documents and Registration of Charges) Regulations 2009, provides that, as a matter of English law, a document (including a deed) can be validly executed by an overseas company in the following ways:

— By affixing the company's common seal.

— In any manner permitted by the laws of the territory in which the company is incorporated for the execution of documents by such a company.

— By the signature of a person who, in accordance with the laws of the territory in which the company is incorporated, is acting under the authority (express or implied) of the company where the document is expressed (in whatever form of words) to be executed by the company.

Therefore, if a document governed by English law is executed on behalf of an overseas company with an electronic signature, it will be validly executed as a matter of English law *provided that* the relevant signatory is (as a matter of the laws of the territory in which the company is incorporated) acting under the authority (express or implied) of that company and the contract is expressed to have been executed by the company.

The question of the authority of a signatory, including any limitations on the scope of that authority and the manner in which the company binds itself (that is, whether electronic signature is excluded), is a matter of the laws of the territory in which the company is incorporated. The same principle applies to the question of that company's capacity. This is a complex area and it would therefore be advisable to seek an opinion from local counsel to confirm these matters.

8. Special Cases: When Should You Proceed With Caution?

E-notarisation and e-legalisation

International or cross-border transactions often require documents to be **notarised**[60] and **legalised**[61] , especially if the transaction involves a civil law jurisdiction such as France or Germany. A common example is where a power of attorney is notarised in England and used to sign documents overseas.

The technology already exists for documents to be notarised and legalised electronically, rather than in paper form. The DocuSign **eNotary service** is now used in many US states. However, there are scarcely any English notaries that provide 'e-notarisation' services, and the Foreign & Commonwealth Office does not currently issue e-apostilles for legalising documents.

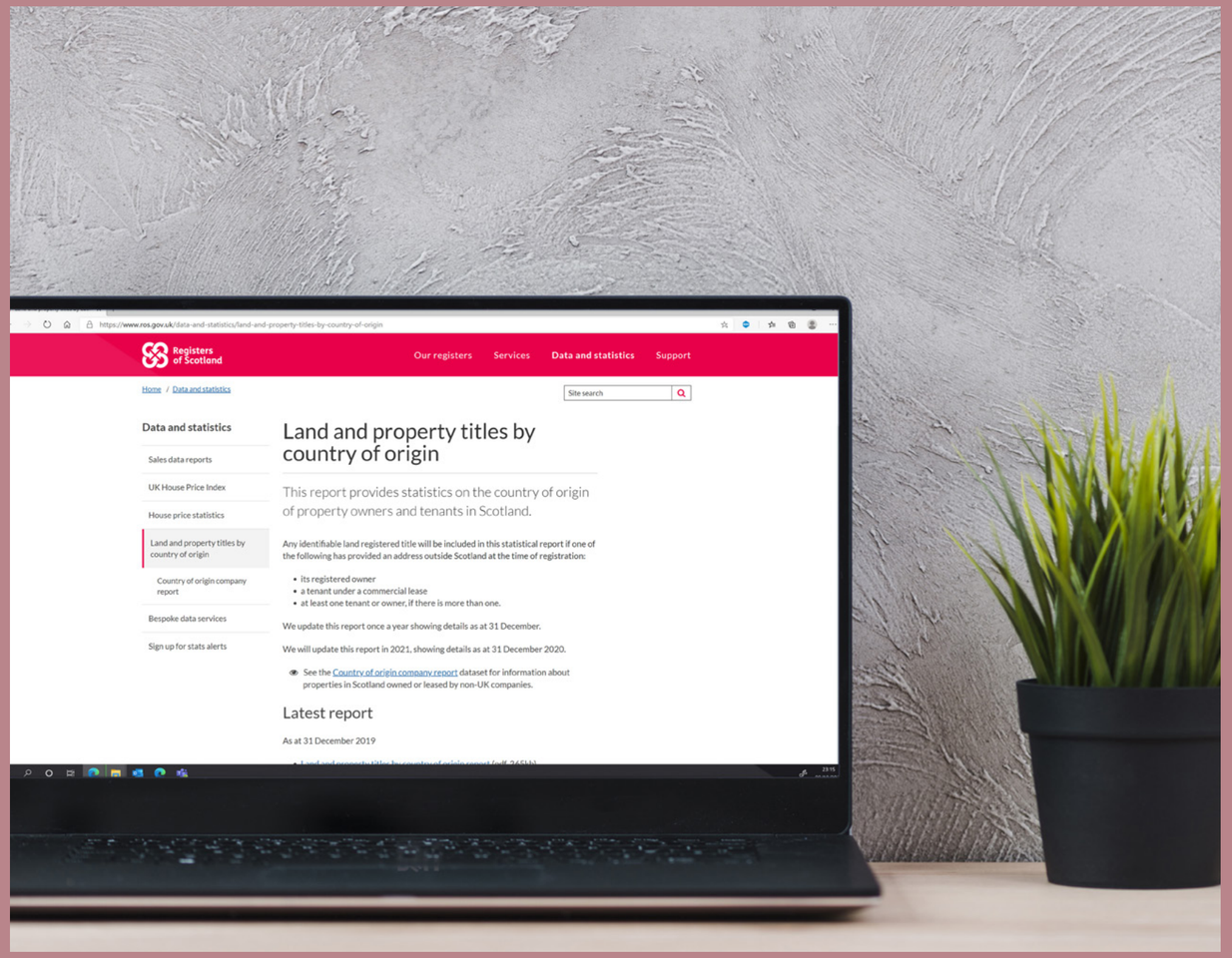
Many notaries are not comfortable with issuing a notarial certificate to an electronic document. Some may be willing to certify a print-out of an electronic document where they can verify its authenticity (normally by contacting the issuing body). But it is generally recommended to proceed on the basis that where a document requires notarisation or legalisation, it should be executed with a wet-ink signature.

8. Special Cases: When Should You Proceed With Caution?

Scotland

Registration at the Land Register of Scotland
Electronic documents are not registrable in the registers under the management and control of the Keeper of the Registers of Scotland, including the Land Register of Scotland unless they are probative (which in electronic terminology requires that they have been authenticated by QES). Registration is also subject to regulations made by the **Scottish Ministers**[62] (and indeed permissive regulations are needed to open up registration of different categories of documents in each of the registers). The Scottish registers will only be opened up gradually to electronically-signed documents over time to allow the necessary systems and practices to be developed. At present, regulations only allow for registration of very limited categories of documents, and even then only in very limited circumstances which means that virtually all commercial documents that require to be registered are not presently suitable for electronic signature.

The Scottish Ministers made the Registers of Scotland (Digital Registration, etc.) Regulations 2018, which came into force in March 2018 and facilitate the launch of new digital registration services that may be provided by the Registers of Scotland in due course. It is significant, too, that the regulations include a presumption in favour of the use of the digital registration services. Like its English counterpart, HMLR, the Land Register of Scotland is using digital signatures as a tool for modernising its approach to conveyancing and land registration albeit rather more slowly. **But unlike HMLR**[63], the Land Register of Scotland requires the highest level of authentication – the QES – for registering electronic documents.



9. Why Use An E-Signing Platform?

Facilitating the electronic execution of transactions is an enabler of digital transformation for many businesses. Set out below is a summary of some of the key practical and technological benefits of using e-signing platforms to authenticate documents with an electronic signature, in which we discuss the principal limitations and risks associated with the use of e-signing platforms and some of the steps that can be taken to mitigate them.

Agility
An e-signing platform speeds up workflow and execution of documents, especially where the parties are in different hemispheres and time zones. An authorised signatory just needs an email address and a smartphone or other device with internet capability and connectivity to sign from any location for standard electronic signature products.

Printing, faxing, scanning, and sending documents by post or courier is inefficient and expensive. DocuSign has estimated that each four-drawer filing cabinet contains 11,000 documents on average; this represents an annual maintenance cost of around £1,600.

Environmental footprint
Going paperless is eco-friendly. Investment in environmental sustainability is not just 'the right thing to do', it also reaps commercial and reputational **benefits**[64]. Businesses are increasingly looking for new ways to do things differently and help address the climate crisis. Reducing the volume of printing – and hence energy and paper consumption – is a step in the right direction.

Superior user experience
Advances in cloud and mobile technology mean users can sign and retrieve copies of their documents anytime, anywhere and from any device (desktop, tablet or smartphone). All they need is an email address and an internet connection.

Digital audit trail
The digital audit trail records who signed the document, including their email and IP address, when the document was signed and sometimes where. The audit trail also indicates what steps were taken to authenticate the signatory. In any legal proceedings where the authenticity or integrity of an electronic document is disputed (for example, it is alleged that the document was produced fraudulently), the audit trail is admissible (Article 25(1) of eIDAS; section 7 of the ECA 2002). Platform providers are also willing to stand behind their technology; they will often make their experts available to testify in proceedings and help their customers prove the legal validity of the e-signed document.

GDPR and regulatory compliance
The digital audit trail can help data controllers strengthen their regulatory compliance, particularly in relation to data privacy, security and retention. Article 5(2) of **GDPR** introduces the so-called 'accountability principle'. This has two elements. First, the data controller is responsible for complying with the data protection principles set out in Article 5(1) of the **GDPR**[65]; second, the data controller must be able to demonstrate that their data processing activities comply with those principles.

Accountability also means keeping a record of your processing activities (Article 30, GDPR). E-signing documents undoubtedly makes it easier to demonstrate compliance with the accountability principle. The digital audit trail is evidence of what was signed when, and by whom.

A data controller must also put in place appropriate security measures when handling personal data, and ensure the confidentiality, integrity and availability of the systems they use to process personal data. Many documents signed via an e-signing platform contain personal data. The signed documents are encrypted and (unless otherwise agreed with the provider) stored at the provider's data centres. The use of a reputable e-signing platform will help the data controller to comply with the accountability principle and satisfy other statutory duties under GDPR (for example, to record consent as the lawful basis of processing any personal data).

Secure cloud storage
Documents will be encrypted and (unless otherwise purged by the customer) stored securely at the provider's data centre(s). Providers are acutely aware that their credibility is dependent on their storage solution being resilient and keeping data secure and confidential, both in transit and at rest. Accordingly, the leading providers design their technical and organisational security measures with that in mind and will generally work with customers to get them comfortable that their storage solutions meet requirements.

Legal effect of electronic signatures
As the 2019 Report attests, an electronic signature can validly execute most commercial, consumer, corporate, financial and HR contracts under **English law**[66]. But caution is needed where documents are to be filed with public registries in the UK or overseas.

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

Security | Function | Legal

For an organisation that has become comfortable with the legal validity of electronic signatures and is persuaded that an e-signing platform will prove beneficial to its operations, the next steps will include:

- *undertaking due diligence on the available solutions and the extent to which they meet, or can be adapted to meet, your needs;*
- *electing an e-signing platform; contracting for the provision of the platform services; implementing the platform;*
- *and updating your technical and organisational measures, policies and procedures to reflect who can use the platform, when it is appropriate for them to do so and how they must do so.*

There are several platforms in the market to consider. This section of the guide looks at the practicalities of selecting a platform and the questions you may wish to ask the providers, the considerations that may be relevant to your selection, and systems and controls you may need to put in place within your organisation to make optimal use of the platform.

Security

Note: When making security inquiries, it may be appropriate to engage internal IT, information security and compliance/risk teams to understand how the security and resilience measures offered by the platform compare to you existing policies, standards and requirements of third party suppliers.

Leading e-signing platforms such as Adobe Sign, DocuSign and HelloSign typically offer a public cloud service known as 'Software as a Service' or 'SaaS'. The technical operation of, and associated security measures implemented in relation to, a SaaS platform are not controlled by the customer as it is not installed 'on premise' in the customer's IT environment. As a consequence, it is important to conduct due diligence focussed on the information security and risk management certifications, policies and practices of the provider and any third party cloud infrastructure or data centre hosting provider they use to host the platform.

? What measures does the platform use to secure my documents and data?

? Where are the services provided from and where are my documents/data held?

? Can I delete any documents or data the platform holds?

? Where is the provider and its group established? Do any intelligence, law enforcement agencies or other governmental bodies have rights under local law to access customer data? Do those laws have extraterritorial effect?

? What sub-contractors does the platform use?

? Is the platform compliant with its statutory obligations?

? What are my options for increased user authentication?

What measures does the platform use to secure my documents and data?

The appropriate level of security for a platform should be considered in light of the sensitivity and significance of the data and documents it will handle and store. External certifications (for example, compliance with the ISO 27001 standard for 'information security management systems' and SOC 2 Type 2-compliance) may be useful indicators. There is now an ISO standard for protecting personal data in the (public) cloud (ISO 27018:2019). AWS, Microsoft Azure and Dropbox are all audited for compliance with this standard. In view of the critical importance of GDPR and data privacy for customers, we anticipate that the leading e-signing platforms will in due course also seek certification to this ISO standard.

Where are the services provided from and where are my documents/data held?

Consider whether these services comply with your document retention and data protection policies (see **here** for more detail on the data protection implications). If you have any concerns in this regard, you might also inquire as to whether there are any alternative options available for storage (for example, whether the platform can use data centres in different locations). Consider, too, whether any data (including metadata) is to be transferred outside the UK and EEA and what cross-border mechanism is used by the provider to legitimise this transfer (e.g. the European Commission's Standard Contractual Clauses, the **EU-US Privacy Shield Framework**[67] and Binding Corporate Rules).

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

Can I delete any documents or data the platform holds?
If you make appropriate backups of executed documents, you may wish to automatically purge copies from the platform (although the digital audit trail, or metadata will always be retained for evidentiary purposes). Most leading e-signing platforms allow users to set a document retention policy whereby documents are automatically deleted after a period of time. Requiring the platform to delete documents may be particularly important if you have any reservations about the platform's security, or storage infrastructure or location. You may be more comfortable with the mechanics of a solution whereby you are responsible for keeping your own copy of executed documents, with the platform retaining only the digital audit trail.

Where is the provider and its group established? Do any intelligence, law enforcement agencies or other governmental bodies have rights under local law to access customer data? Do those laws have extraterritorial effect?
The leading platforms servicing the European market are committed to storing their European customers' data on servers in European data centres. This ostensibly makes it easier to comply with restrictions under GDPR on transferring personal data to a non-EEA country (Article 44, GDPR). However, the leading platforms are American which exposes them to the further risk that US intelligence and law enforcement agencies will require access to data under the provider's 'custody, control or possession'. This may give rise to an irreconcilable conflict of laws: the US platform may be obligated to respond to a warrant under the CLOUD Act 2018 (which has extraterritorial effect) but GDPR states that their customers' personal data may only be transferred to a non-EEA country including the US under an international agreement such as a 'Mutual Legal Assistance Treaty'. This could potentially put the customer (as a 'controller' of the personal data) in breach of GDPR.

When conducting due diligence on an American provider, it would also be prudent to ask about their policy for reconciling a warrant issued under the CLOUD Act 2018 with the conflicting requirements set out in GDPR, and whether they will agree to:

(i) notify you immediately on receipt of any such request (to the extent permitted by applicable law); and

(ii) delete all copies of your documents (including back-up copies, but excluding the audit trail metadata) within a short period. The period could be set so as to simply allow you to take, and verify that you have taken and backed up, an accurate copy of your signed documents (which you would schedule on a regular basis). In that way, the risk of confidential documents being accessed by external agencies without your consent can, to a degree, be mitigated.

Plans are in motion to develop Europe-based competition to the US-dominated cloud services market **GAIA-X Project**; if and when a European data infrastructure becomes viable, some of these concerns may change shape.

What sub-contractors does the platform use?
Consider who will have access to your data/ documents and what exactly they will have access to (for example, executed documents or metadata only). Is your consent required to changes in sub-contractors? How much visibility of sub-contracting do you need from an operational risk management perspective? You may need to do due diligence on, and potentially pre-approve, key subcontractors such as cloud infrastructure service providers. You may also need to consider this through a data protection lens (see **here** for more detail on the data protection implications).

Is the platform compliant with its statutory obligations?
E-signing platforms have independent obligations under GDPR and the EU Cybersecurity Directive (implemented in the UK by the Network and Information Systems Regulations 2018). The platform provider should be able to warrant its compliance with these obligations.

What are my options for increased user authentication?
Some platforms offer extra layers of security or two-factor authentication; for example, the option to use access codes or SMS to verify identity.

Consider whether these might be appropriate in the context of your organisation and your intended use cases for the platform.

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

Function

? What types of digital signature functionality does the platform offer?

? Can the platform integrate with my other applications (proprietary or off-the-shelf)?

? What is the audit trail on my signed documents?

What types of digital signature functionality does the platform offer?
Determine what type of electronic and digital signatures you require (see **here**) and check whether the e-signing platform offers this functionality. It is worth considering the nature and sensitivity of the documents that will be executed using the platform, whether any transactions will be cross border, and whether an AdES or QES might be required for additional certainty or, where the document is made under Scots law, to comply with legal requirements for the use case. **Often**, a simple electronic signature will suffice.

Can the platform integrate with my other applications (proprietary or off-the-shelf)?
If this is a requirement of the organisation, for example integration through APIs with your document management system, check that it is functionally possible (although note that while e-signing platform providers offer many API integrations, they **typically do not provide legal warranties** regarding this functionality).

What is the audit trail on my signed documents?
Ensure that, if required, you can retrieve not only the signed document but details of which verified signatory signed and when and using what IP address, and (if required) the location of the signatory. The audit trail is normally appended to the signed document for ease of reference.

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

Legal

Note: E-signing platforms are generally offered as a commoditised service, and this is typically reflected in the applicable terms of service. Terms tend to favour the platform provider and accept minimal risk or liability, often in return for offering an affordable price point. In this context a customer's negotiating power may be limited, although platforms may be more flexible depending on the subscription volumes proposed by the customer. Organisations will need to weigh the risks and make their own judgement as to whether the risk/reward balance is acceptable.

- ? How can I audit and enforce the security measures in place on the platform?
- ? What are the data protection implications?
- ? What is the platform provider's policy for reconciling a warrant issued under the CLOUD Act 2018 with the conflicting requirements set out in GDPR?
- ? Who else has the power to access my documents on the platform?
- ? What warranties does the platform provider offer?
- ? What is the platform provider's limitation of liability?
- ? Does the platform offer a service level agreement?
- ? Does the services agreement need to be FS regulatory compliant?
- ? Do I have suitable insurance cover for my use of the platform?

How can I audit and enforce the security measures in place on the platform?
Even if you are satisfied as to the audit and security measures an e-signing platform has in place, these will not necessarily be recorded as contractual obligations (some leading e-signing platforms commit contractually only to employing reasonable security measures). Entire agreement clauses are likely to prevent reliance on and enforcement of any pre-contractual statements, representations made in marketing materials or on the platform's website, proposals or even responses to due diligence inquiries. It would be prudent to check the way the platform commits to maintaining these measures and whether they can be reviewed, audited or enforced (especially any security measures that are particularly critical from your client's perspective). Does the provider commission regular comprehensive third-party security audits? If yes, can you obtain a copy of them and will the provider commit to implementing any material recommendations arising from a report in a reasonable time frame?

What are the data protection implications?
Data protection law requires appropriate contractual provisions between you and an e-signing platform (the platform will almost always act as your data processor). As part of your due diligence you should check whether the provider uses sub-processors, or if any aspects of the services (such as remote hands IT support) are provided from overseas (whether or not by sub-contractors) (see **here** for more detail). If so, you will also need to consider whether the terms of service appropriately capture the platform's obligations regarding sub-contractors, and whether adequate safeguards are in place to govern overseas transfers of personal data. Check also if the provider retains copies of any metadata containing personal data for its own purposes after your subscription ends (in which case the provider may consider it is acting as a controller of that data and you may wish to include protective provisions in the agreement).

What is the platform's policy for reconciling a warrant issued under the CLOUD Act 2018 with the conflicting requirements of GDPR?
See **here** for more detail.

Who else has the power to access my documents on the platform?
In some jurisdictions, government or law enforcement bodies may have legal rights to access your documents where they are held on the e-signing platform. These rights may arise by virtue of where the data is held, or where the platform provider is incorporated. One way to mitigate any concerns around this is to have in place a robust system to internally back up documents, so they can be promptly deleted from the e-signing platform (see **here** for more detail on internal backups).

What warranties does the platform provider offer?
Typically, e-signing platform providers will not provide comprehensive warranties. In particular,

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

providers will not warrant that an electronic signature provided via the platform will create a valid or enforceable contract, that additional authentication services will provide the certainty sought by customers, that the platform complies with technical standards or all applicable laws (such as eIDAS), or that any integrations with other enterprise applications will function correctly. If these are missing, you should seek to negotiate where it is reasonable to do so.

What is the platform's limitation of liability?
Platforms tend to cap their financial liability to the customer by reference to fees paid (for example, in the 12-month period preceding a claim, although some platforms seek to limit their liability as low as only 3 months of fees) and they also tend to exclude liability for loss or corruption of data. In both cases, there may be flexibility to negotiate (for example, to extend the platform's limitation of liability to the equivalent of fees paid over the life of the contract, or to include the platform's liability for loss or corruption of data on the basis that it amounts to a breach of contract). In light of increased fines under GDPR, platforms may also be willing to negotiate a separate liability cap in respect of a breach of data protection laws (typically between two and five times the deal value).

Does the platform offer a service level agreement?
Platforms will not usually volunteer service level agreements, and so you should seek to negotiate one where possible. The core principle of a service level agreement will be the availability of the platform; given that the leading e-signing platforms host and replicate data across multiple data centres, they should be able to commit to a high level of availability (99.9% or even higher).

Does the services agreement need to be FS regulatory compliant?
Platform services agreements are not typically designed to be compliant with **financial services regulatory requirements**[68], for contracts relating to the provision of material, important or business critical services or cloud services. If you intend to use the platform in a way that will trigger those requirements you will need to explore with the provider what additional commitments they are able to provide to enable you to put a compliant agreement in place.

Do I have suitable insurance cover for my use of the platform?
Check that your professional indemnity insurance covers (or does not preclude) your intended use of e-signing platforms, and whether there are any steps you need to take to ensure the cover is valid.

Once you are satisfied that an e-signing platform will meet your needs:

Internal policies and procedures – have a policy around use of e-signing platforms, including:

- the types of documents within the organisation that will typically be signed using the e-signing platform, and those for which the platform should not be used;
- which types of digital signature are required for which types of document/transaction;
- who will be responsible for setting up the signing process itself using the platform;
- any other corporate or policy documents with relevant considerations;
- the way documents will be dated; and
- whether there is a particular order of signing that should be built into the e-signing process.

Internal policies and procedures – have a clear, "one stop shop" policy around use of e-signing platforms in your organisation. Consider including detail on:

- the types of documents within the organisation that will typically be signed using the e-signing platform, those for which the platform should not be used and those where the assistance of legal should be sought before using the platform to sign them;
- which types of digital signature are required for which types of document/transaction;
- who (individual/role) will be responsible for setting up the signing process itself using the platform;
- what approvals process the transaction and relevant documents to be executed have to go through before the documents are executed;
- what signing authorities apply, and whether you have any particular requirements (e.g. number, seniority or locations of signatories, execution under power of attorney);
- checking that the correct signature blocks have been applied to the document(s);

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

— any other corporate or policy documents with relevant considerations (for example, the articles of association may stipulate particular execution formalities);

— the way documents will be **dated**; and

— whether there is a particular order of signing (perhaps already established in wet-ink signing protocols) that should be built into the e-signing process.

Before signature, check the following:

— Is the document suitable for signing using the e-signing platform?

— Are the relevant individuals prepared to use the e-signing platform?

— Do any particular formalities apply and does the document contain the correct execution blocks for these?

— Have the signatories been provided with, and approved, an execution version of the document separately?

— Are you confident there are no errors in the document?

— Have signature protocols been agreed with the counterparty? In particular:

  – Who will take charge of the e-signing process and do they have all the required information?

  – Does anyone need to receive a copy of the document or approve it for execution before execution can proceed?

  – Has the correct execution version of the document been uploaded for signature?

  – Certificate of completion

— If a witness is required, is it appropriate that the witness should receive a full copy of the document?

Is the document suitable for signing using the e-signing platform?
While many contracts will be suitable for e-signing, it is worth checking that the contract is **not an exception**. E-signing platforms will typically exclude their responsibility for inappropriate use of an electronic signature. An electronic signature will not necessarily be valid or enforceable simply because the platform is used. The onus is on the customer to ensure that the use of the electronic or digital signature will be valid and enforceable under applicable laws.

Are the relevant individuals prepared to use the e-signing platform?
Check that signatories have signed up to the platform, if required (although often, a platform will not require this) that they are aware that the document will be signed electronically, and that they are trained in and comfortable with use of the platform. Note that the person setting up the document flow for signature also needs their own unique log-in, even if they are not a signatory.

Do any particular formalities apply and does the document contain the correct execution blocks for these?
Check for statutory formalities (for example, is a witness required, and if so, how will witnessing take place in practice? Is the signatory signing under a power of attorney?) and any requirements under your or your counterparty's articles of association or other policies (including any policy on using electronic signatures).

Have the signatories been provided with, and approved, an execution version of the document separately?
Although it is possible to review documents via e-signing platforms, they are unlikely to be the optimal medium for substantive review (particularly on mobile devices).

Are you confident there are no errors in the document?
An e-signing platform is not conducive to reading and reviewing a document (particularly on a small hand-held device). Where a platform is used to execute a transaction, it is clearly important to ensure that any legal advisers, and the signatories, have already read and approved the execution version of the document – even if this means printing a hard copy of the document and breaking an e-signing taboo. Once the document is uploaded to the platform, although the platform offers the signatory the opportunity to review, this may not be practicable, and the signatory is likely to simply click

10. Engaging with e-signing platforms: due diligence and practical risk mitigation

through the signature tags (or fields) to authenticate and execute the document. The signatory is unlikely to spot errors in the document at this point. It is therefore incumbent on the lawyer or other person coordinating the signing process to check – and double check – that the correct execution version is circulated to the transaction parties.

Have signature protocols been agreed with the counterparty (if necessary)?

It would be prudent to agree certain matters with the other side of a transaction, in particular:

— **Who will take charge of the e-signing process and do they have all the required information?**

– The individual in charge will need certain information (usually the name and email address of signatories) in order to set up the signature flow on the platform.

— **How will the document be dated?**

– Once you have agreed the approach to inserting a date into the document, check that the e-signing platform can accommodate this. Typically, platforms will automatically date the document once all signatories have executed. If a different signing protocol is agreed (for example, if you need to share signatures with the other side before you can agree to date) be aware that the platform may not release the executed document until all fields (including the date) have been completed, in which case perhaps you should not include the date as a required field on the platform. You may need to date the document manually once all parties have signed, and share final dated versions in hard copy or PDF (although this can undermine some of the benefits of a fully automated e-signing process).

— **Has the correct execution version of the document been uploaded for signature?**

– While this may not be a concern where you are in control of setting up the e-signing process, it may otherwise be difficult to check. Note that some platforms include the ability to send the document to a non-signatory first for approval, so that, for example, the counterparty (or their lawyers) may confirm that the correct version of the document has been submitted for signature before the document is sent to any signatories. It would be prudent to agree that those in control of the e-signing process will utilise this option, and that agreed execution versions are circulated and confirmed in advance via email in order to resolve any discrepancy.

— **Audit trail**

– If you have not set up the e-signing workflow, it would be prudent to request that the other side provides the digital audit trail for signature, which may be called the certificate of completion or the audit report.

— **If a witness is required, is it appropriate that the witness should receive a full copy of the document?**

– The workflow for witnessing varies from platform to platform. It is important to check whether the platform can be configured so that the witness (who may also have an account with the platform) does not automatically receive a copy of the signed document. It is generally advisable to avoid the witnessing formality wherever possible (for example, execute documents on behalf of a company through the agency of two directors or a director and company secretary). It is worth noting, too, that the introduction by HMLR of electronic signatures for registrable dispositions **will oblige conveyancers** to follow a prescribed workflow for e-signing and witnessing. While HMLR's requirements refer to signing in the presence of a witness, they also cover a deed being signed on behalf of a company by two "authorised signatories" under section 44(2)(a) of the CA 2006 with the requirements being read accordingly.

— **Are any of the parties incorporated overseas, or is the document governed by overseas law?**

– If so, it may be appropriate to check with local counsel to ensure that the relevant signatory has authority under local law and the company's constitutional documents to sign, and/or whether the proposed electronic signature process complies with the laws of the governing jurisdiction.

— **After signature, back up contracts internally**

– Although e-signing platforms will typically allow retrieval of copies of signed documents at a later date, it would be prudent to also store these in a separate, secure internal contract management system. This will be particularly important if you have set a document retention policy within the platform which means that the platform will not hold your documents after a certain point. Even if you do not set a specific retention policy, be aware that platforms may (after a grace period) delete all documents when a customer agreement expires or is terminated, and so a backup is needed for when you move off the platform. In addition, platforms may seek to exclude their liability for loss or corruption of data, in which case the customer may not have any legal recourse if the platform 'loses' or corrupts a document.

11. Impact of Brexit

The UK left the European Union ("**EU**") on 31 January 2020 ("**exit day**[69]"). Under the terms of the **EU-UK Withdrawal Agreement 2020**[70], the EU and the UK agreed a transitional arrangement from exit day which – unless extended – will end at 11:00pm on 31 December 2020 ("**transition period**").

During the transition period, the UK continues to be treated for most purposes as if it were still an EU member state. It participates in the EU customs union and single market, and the four freedoms (goods, services, persons and capital) also apply as before.

EU law in its entirety (including eIDAS) continues to apply to the UK. But at the end of the transition period, the UK becomes a 'third country' and a new body of 'retained EU law' is created under sections 2 to 4 of the European Union (Withdrawal) Act 2018, which:

— Retains EU-derived domestic legislation such as EU Directives

— Saves and converts into UK law most directly applicable EU Regulations including eIDAS

In January 2019, the UK parliament approved a statutory instrument to amend those provisions of eIDAS that are deemed 'inappropriate or redundant' with effect from 1 January 2021 ("**eIDAS SI**[71]").

Repeal of the electronic identification provisions of eIDAS

From 1 January 2021, the electronic identification ("**e-ID**") provisions of eIDAS will be repealed and the UK will lose access to the interoperability framework for e-ID. This scheme was intended to enable EU citizens to use their national e-ID to access public sector digital services in other member states. **GOV.UK Verify** had been notified by the UK as the national e-ID scheme on 2 May 2019 pursuant to Article 9 of eIDAS; but it had not completed the notification process and been formally approved by the European Commission.

The European Commission issued a notice on 26 May 2020 that GOV.UK Verify will no longer be recognised by member states as the UK's national e-ID from the end of the transition period. This aligns with the eIDAS SI which provides that retained EU law will no longer include the e-ID sections of eIDAS. It is tempting to dismiss this as inconsequential. But e-ID is highly valued by the European Commission as a key driver of its flagship digital single market strategy. By the end of 2019, there were already six EU member states that had completed the notification process and whose citizens may now use their national e-IDs for cross-border access to online public sector services. The use of national e-IDs will extend to the private sector. The UK's exclusion from the interoperability framework for national e-IDs may prove to be more damaging to the UK's digital economy than we presently imagine.

Preserving mutual recognition

The eIDAS SI preserves the mutual recognition and interoperability of electronic signatures and other trust services. It does this by allowing the technical standards and specifications in the retained EU law to mirror those in eIDAS. Thus, if a QES is issued by a qualified TSP in an EU member state, it will still be recognised as a QES in the **UK**[72].

This is good news as the market-leading e-signing platforms providing trust services to UK businesses and public sector bodies are all established in other EU member states (principally the Republic of Ireland). The eIDAS SI ensures that these EU trust services can continue to be used in the UK beyond the transition period.

By contrast, the European Commission's notice on 26 May 2020 made clear that one consequence of the UK becoming a 'third country' is that a QES and other qualified trust services provided by a qualified TSP established in the UK will no longer be recognised in the EU. Recognition of qualified trust services is dependent on the EU and the UK concluding an 'international agreement' in accordance with Article 14 of eIDAS. This will have a bearing on qualified TSPs who are registered on the **UK Trusted List** with aspirations to serve the EU market. The UK Trusted List is managed by tScheme on behalf of the Department for Digital, Culture, Media and Sport. Each national trusted list is notified to the European Commission and consolidated into the **EU Trusted List**.

Legal validity and admissibility from 1 January 2021

Brexit will not have any material impact on the legal validity and admissibility of electronic signatures under UK law. The ECA 2000 remains unchanged and the eIDAS SI has saved and converted Article 25(2) of eIDAS into UK law so that a QES retains the equivalent legal standing of a handwritten signature.

In view of the above, we do not expect Brexit to have any adverse practical implications for the use by UK businesses and the public sector of Adobe Sign, DocuSign, HelloSign, OneSpan, Namirial and other leading e-signing platforms.

Glossary

This section sets out the meanings of some of the key terms and abbreviations we use in the guide.

— **2001 Advice:** the Law Commission advice on **E-commerce: formal requirements in commercial transactions** published in December 2001.

— **2016 BEIS Guide:** the guide to **Electronic signatures and trust services** published by the Department for Business, Energy & Industrial Strategy in August 2016.

— **2018 Consultation:** the Law Commission **Consultation on electronic execution of documents (Law Com No 237)**, published on 21 August 2018.

— **2019 Report:** the Law **Commission Report on electronic execution of documents (Law Com No 386)**, published on 4 September 2019.

— **advanced electronic signature (AdES):** an electronic signature meeting the requirements set out in Article 26 of eIDAS.

— **Brexit:** the UK's withdrawal from the European Union (**EU**) on 31 January 2020 when the UK-EU withdrawal agreement came into force. From 31 January to 31 December 2020, the UK is in a transition period during which EU law including eIDAS continues to apply to the UK.

— **CA 2006:** the **Companies Act 2006**.

— **Certificate Authority** or **Certification Authority** is another term for trust service provider (TSP). See below

— **conveyancer:** an authorised person within the meaning of section 18 of the Legal Services Act 2007 who is entitled to provide the conveyancing services referred to in paragraphs 5(1)(a) and (b) of Schedule 2 to that Act, or a person carrying out those activities in the course of their duties as a public officer. It also includes an individual or body who employs or has among their managers such an authorised person who will undertake or supervise those conveyancing activities (rule 217A of the Land Registration Rules 2003). To come within the definition of conveyancer in rule 217A of the Land Registration Rules 2003 an individual must be authorised under the Legal Services Act 2007 to provide conveyancing services; in effect they must have a practising certificate.

— **COVID-19:** the disease known as coronavirus disease and the virus known as severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).

— **deed:** a document governed by the law of England and Wales which is executed with a high degree of formality, and by which an interest, a right, or property passes or is confirmed, or a binding obligation is created or confirmed.

— **digital certificate:** a certificate issued by a TSP which links a signatory to their public key and confirms at least the name or the pseudonym of that person.

— **digital signature:** an advanced electronic signature or qualified electronic signature meeting the requirements set out in eIDAS and produced using public key cryptography or PKI.

— **digital transformation:** the adoption of digital technologies such as data analytics or cloud computing to fundamentally transform an organisation's business processes, increase efficiency and improve the customer experience.

— **ECA 2000:** the **Electronic Communications Act 2000**.

— **eIDAS:** **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**.

— **electronic signature:** a signature in electronic form meeting the requirements set out in Article 3(10) of eIDAS.

— **English law:** the laws of England and Wales.

— **eSignatures Directive:** **Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures**.

— **e-signing platform:** a web-based platform such as Adobe Sign, DocuSign, HelloSign, OneSpan and Namirial providing an interface through which documents (including English law deeds) may be uploaded and sent to a recipient to sign with an electronic or digital signature. The platform generates an audit trail recording data such as who signed the document, their email and IP address and the time and date of each signature.

— **formalities:** a procedure which a party must follow in order to give legal effect to a transaction. Formalities include requirements that certain transactions are made 'in writing' or 'signed' or made by deed.

— **GDPR:** the **General Data Protection Regulation ((EU) 2016/679) of the European Parliament and of the Council of 27 April 2016**.

— **hash function** (also called a 'hash'): a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function – a computed hash cannot be reversed to find other files that may generate the same hash value.

— **HMLR:** HM Land Registry.

— **HSM:** The key pair and qualified certificates are generated and hosted by the qualified TSP in the cloud on a certified hardware security module.

— **IP address:** a numerical label allocated to each computer network that connects to the internet.

— **key pair:** the cryptographic keys used for producing digital signatures. The signatory uses the 'private key' to digitally sign the document. This may be verified by a recipient using the signatory's public key.

Glossary continued

- **Law Commission:** the Law Commission of England and Wales.
- **Law Society:** The Law Society Company Law Committee, The City of London Company Law and Financial Law Committees.
- **Law Society 2010 Practice Note:** the **Practice note on the execution of documents by virtual means** published by the City of London Law Society Company Law and Financial Law Committee on 16 February 2010, and updated on 7 May 2020 to take account of the COVID-19 pandemic.
- **Law Society 2016 Practice Note:** the **Practice note on execution of a document using an electronic signature** published by a joint working party of the Law Society of England and Wales and the City of London Law Society on 21 July 2016, and updated on 7 May 2020 to take account of the COVID-19 pandemic.
- **LP(MP)A 1989:** the **Law of Property (Miscellaneous Provisions) Act 1989**.
- **LRA 2002:** the **Land Registration Act 2002**.
- **LRR 2003:** the **Land Registration Rules 2003 (SI 2003/1417)**.
- **public key infrastructure (PKI):** the policies, standards, people, and systems that support the distribution of public keys and the identity validation of individuals or entities with digital certificates and a certificate authority. The e-signing platforms and their TSPs use PKI to generate digital signatures.
- **public key cryptography** (also known as 'asymmetric cryptography'): the process of encrypting and decrypting data using public and private keys.
- **qualified certificate:** a digital certificate issued by a qualified TSP which meets the requirements laid down in Annex I of eIDAS.
- **qualified electronic signature (QES):** an advanced electronic signature that is created by a qualified electronic signature creation device and based on a qualified certificate (Article 3(12), eIDAS).
- **qualified electronic signature creation device:** configured software and hardware used to create a qualified electronic signature and meeting the technical and security requirements laid down in Annex II of eIDAS. Traditionally this was a physical device such as a smartcard or USB token and restricted to desktop usage. But nowadays e-signing platforms work with TSPs who host and manage the digital certificate and the encryption keys remotely in the cloud using hardware security modules (HSM). An HSM enables digital signing from a web browser or mobile device.
- **qualified TSP:** a TSP which appears in an EU member state's trusted list and has been certified by a supervisory body to provide qualified certificates and/or other qualified trust services.
- **ROWSA:** the **Requirements of Writing (Scotland) Act 1995**.
- **Scottish Regulations:** the **Electronic Documents (Scotland) Regulations 2014 (SSI 2014/83)**.
- **Statement of Law:** the statement of law setting out the Law Commission's high-level conclusions regarding the validity of electronic signatures, summarised as a series of propositions in the Executive Summary in the 2019 Report.
- **supervisory body:** a supervisory body designated in each EU member state to supervise the activities of a qualified TSP (Article 17, eIDAS).
- **trusted list:** the national trusted list of qualified TSPs and their trust services established, maintained and published by each EU member state (Article 22, eIDAS). Each national trusted list is notified to the European Commission and consolidated into the **EU Trusted List**.
- **trust services:** the creation, verification and validation by a TSP of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services (Article 3(16), eIDAS).
- **trust service provider (TSP)** (also known as a '**certification authority**', '**certification authority**' or '**CA**'): an entity providing one or more trust services such as creating, verifying and validating electronic signatures and electronic seals (Article 3(19), eIDAS). A TSP also issues digital certificates (for digital signatures) confirming the link between an individual and their public key (see also **PKI**).
- **virtual signing:** the method of executing documents set out in Options 1 and 2 of the **Law Society of England and Wales 2010 Practice Note**. Final execution copies of documents are emailed to all parties. Each party prints and signs the signature page only and then sends a single email, to which is attached (i) the final version of the document and a PDF copy of the signed signature page (Option 1); or a PDF copy of the signed signature page (Option 2).
- **wet-ink** or **handwritten signature:** a signature affixed to paper using, for example, a pen or pencil. In this guide, we use the terms 'wet-ink' and 'handwritten' interchangeably, to refer to non-electronic signatures.

E-signing workflow: How to use an E-Signing Platform

What is the process for signing a contract via an e-signing platform such as Adobe Sign, DocuSign, HelloSign and Namirial?

The workflow to send, sign and manage a contract that will be signed with an electronic signature is broadly the same for the leading e-signing platforms. Here is a simple overview:

Step 1: Upload and send document(s) for electronic signature

— The sender logs into the platform and uploads a Word document or PDF from the dashboard. The document may be uploaded from a computer or from file-sharing sites like BOX, Dropbox and Google Drive.

— The sender enters the name and email address of: (i) each signatory, and may specify the order in which they should sign; and (ii) any other recipients of a copy of the document (pre-signing and/or post-signing).

— The basic method of authenticating the signatory is their email address. There is an option for two-factor authentication, such as requiring the signatory to enter a password or access code sent via SMS.

— The sender identifies the document in the 'message' field and may add an instruction such as 'please review and complete this document'.

— The sender drags and drops signing 'tags' or 'fields' to indicate where each signatory should sign, initial and date the document.

— The platform emails a link to each signatory (and other relevant recipient) which they can use to access the document.

Step 2: Review and sign the document with an electronic signature

— If a recipient must approve the document before it can proceed to execution, that person opens the email and clicks the link to review and approve the document (or not). Assuming the document is approved the document becomes available for execution.

— The signatory opens the email and clicks the link to review and sign the document.

— The document opens in a new browser window.

— If two-factor authentication was required by the sender, the signatory is prompted to supply the password or access code.

— The signatory may be required to check a box and consent to signing the document electronically.

— The signing process begins, and the signatory is guided to each tag (or field) requiring an action.

— When the signatory clicks the signature tag (or field), they are prompted to enter their name or adopt a signature style to sign the document with their electronic signature.

— Once the signatory has clicked all the tags (or fields) in the document, the document is complete.

— The signatory may download a PDF copy of the e-signed document.

— The sender automatically receives an email with the e-signed document attached. The document will also be available from their dashboard. Anyone else designated as a recipient of the executed document will similarly automatically receive an email with the e-signed document attached.

Step 3: Managing documents on the e-signing platform

— The sender can use the dashboard to check on the status of documents sent out for signature.

— This indicates which documents have been completed, cancelled or are still in progress.

— The platform generates a comprehensive digital audit trail for each document. This audit trail records who signed the document, including their email and IP address, additional authentication factors, when and, sometimes, where the document was signed.

— The audit trail is admissible under section 7 of the ECA 2000 and will carry substantial evidential weight in proving the authenticity or integrity of a disputed document. More generally, the audit trail can help businesses to strengthen their regulatory compliance, particularly in regard to data protection, accountability and data retention obligations under the GDPR.

E-signing workflow: How Does An E-Signing Platform Generate Cloud-Based Digital Signatures?

Before the advent of cloud technology, a signatory would create a digital signature by using a private key and digital certificate stored on a smartcard or USB token that plugged into a desktop computer. This was cumbersome, inflexible and expensive. It is perhaps unsurprising, therefore, that digital signatures were not widely adopted in the UK.

The combination of the cloud and PKI now makes it possible for a signatory to sign documents with a digital signature via a web browser or mobile application. The public and private keys and the signatory's digital certificate to prove the signatory's identity are all managed by TSPs in the cloud. This has simplified the process for authenticating the signatory and using platforms like Adobe Sign, DocuSign, HelloSign, OneSpan and Namirial to execute documents with a digital signature.

Let us consider the digital signature workflow using the Adobe Sign platform and its network of accredited TSPs as an **example**[73]:

1. When a document is ready for signature, it is uploaded to the platform.

2. To use a digital signature, the signatory must own or obtain a digital certificate from a third-party TSP to verify their identity. This requires proof of identity, such as a driving licence or passport. The TSP will deploy machine-learning to examine watermarks and security features to validate that the submitted ID document is authentic.

3. Adobe Sign then asks the signatory to provide a PIN (issued by the TSP) or a one-time password (OTP) for authentication purposes.

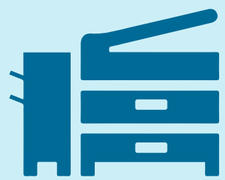
4. Once authenticated, the signatory activates the private key hosted by the TSP to encrypt a digital fingerprint of the document, called a 'hash'. The encrypted hash becomes the digital signature of the signatory and is cryptographically bound to the document.

5. The document is certified with a tamper-proof seal and Adobe Sign automatically sends a copy of the digitally signed document to the signatory and intended recipient. The recipient uses the public key to decrypt the digital signature and relies on the digital certificate to validate that the public key actually belongs to the sender.

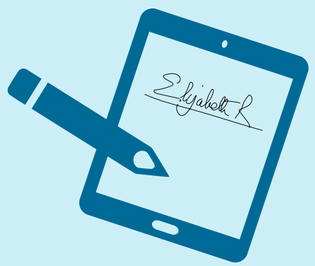
6. Finally, the platform generates a digital audit trail. This records who created and opened the document, who signed it, including their email and IP address, the timing of the signature, and (on compatible mobile devices) the geolocation of the signatory.

E-signing workflow: How Does An E-Signing Platform Generate Cloud-Based Digital Signatures?

Simple Electronic Signature



printer/scanner



touchscreen/stylus

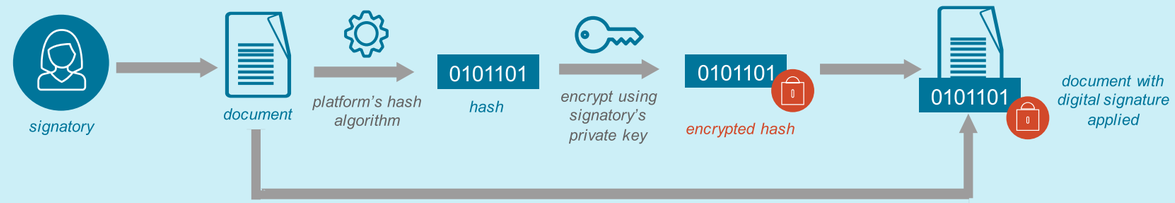
mobile device taking photo of document

biometrics

typing on signature

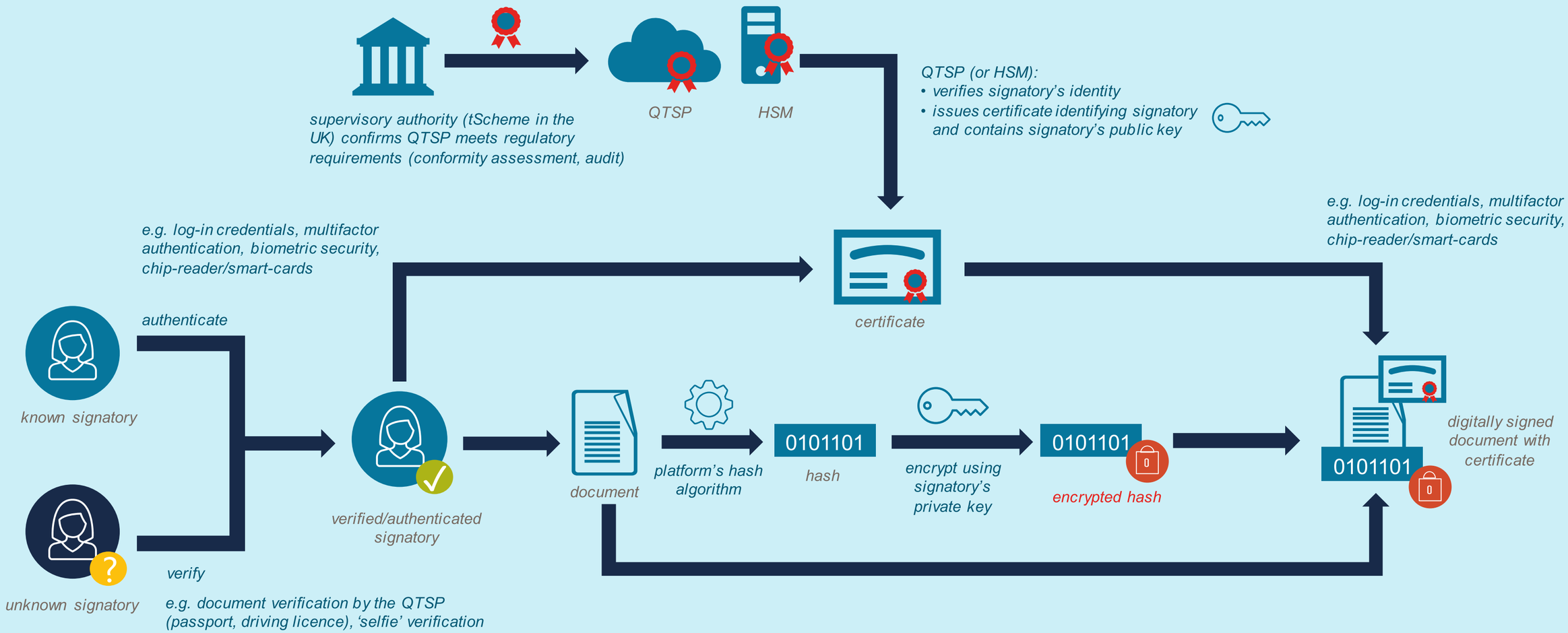
clicking "OK"

Advanced Electronic Signature



E-signing workflow: How Does An E-Signing Platform Generate Cloud-Based Digital Signatures?

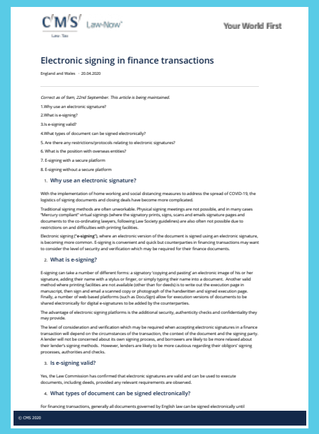
Qualified Electronic Signature – Signing



How we can help you

How CMS can help you:

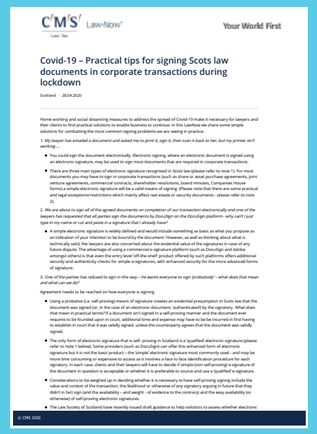
- Assist you to evaluate your requirements and determine whether a cloud-based or on-premise deployment of the e-signing platform is best for your organisation.
- Assist you to identify and refine the spectrum of domestic and international use cases that you wish to authenticate via any of the leading e-signing platforms.
- Advise you on selecting the right blend of electronic or digital signature for those use cases.
- Assist you to create in-house policies and procedures to manage your organisation's implementation and use of e-signing platforms, helping you understand the inherent risks and benefits.
- Assist you to undertake due diligence on, and negotiate and agree terms with, e-signing platform providers, with an emphasis on complying with GDPR and the EU Cybersecurity Act.
- Keep you up-to-date with the latest know-how, innovation and the changing regulatory landscape, across a wide range of industry verticals from conveyancing, energy and utilities supply and finance, to technology, media and communications businesses and public institutions.


Electronic signing in finance transactions

Electronic signing in finance transactions

Electronic Signatures in Real Estate Documents

Electronic signatures in Real Estate documents


Covid-19 – Practical tips for signing Scots law documents in corporate transactions during lockdown

Covid-19 – Practical tips for signing Scots law documents in corporate transactions during lockdown

Law Commission report on the electronic execution of documents

Law Commission report on the electronic execution of documents

CMS expert guide to e-signatures in commercial contracts

Key contacts

Commercial contracts, technology and data protection

English Law

Ian Stevens
Partner
T +44 20 7367 2597
E ian.stevens@cms-cmno.com

Richard Oliphant
Consultant
T +44 20 7367 3566
E richard.oliphant@cms-cmno.com

Libby Conole
Senior Associate (Qualified in New Zealand)
T +44 20 7367 2254
E libby.conole@cms-cmno.com

Scots Law

Duncan Turner
Partner
T +44 131 200 7669
E duncan.turner@cms-cmno.com

Corporate

English Law

Katie Nagy de Nagybaczon
Partner
T +44 20 7067 3519
E katie.nagydenagybaczon@cms-cmno.com

Scots Law

Caroline Wilson
Professional Support Lawyer
T +44 131 200 7368
E caroline.wilson@cms-cmno.com

Finance

English Law

Anne Chitan
Partner
T +44 20 7067 3485
E anne.chitan@cms-cmno.com

Simon Johnston
Partner
T +44 20 7367 2008
E simon.johnston@cms-cmno.com

Charlotte Choules
Associate
T +44 20 7367 3566
E charlotte.choules@cms-cmno.com

Scots Law

Jenny Allan
Partner
T +44 131 200 7618
E jenny.allan@cms-cmno.com

Real Estate

English Law

Warren Gordon
Senior Professional Support Lawyer
T +44 20 7067 3615
E warren.gordon@cms-cmno.com

Scots Law

Chris Rae
Partner
T +44 141 304 6137
E chris.rae@cms-cmno.com

Acknowledgements
Thank you to Adobe Sign for their kind permission to reproduce their diagrams for this Guide, with special mention to John Jolliffe, Andrea Valle and Lorie Groth for their technical input.

12. About CMS

Your World First – the CMS approach to delivering value

We have a phrase to sum up our promise to our clients: 'Your World First'. This phrase reflects our priorities of being client-centric, providing world vision and being performance driven.

Client-centric

You, the client, are at the heart of our business – whether you are a large or small organisation. Our emphasis is not just on being great technical lawyers, but really understanding your business and your key objectives. One way we do this is by organising CMS into sector groups that operate locally and internationally. CMS's international sector specialists take pride in understanding your industry and engaging with your company-specific issues.

We deliver added value services based on real client needs, such as Law-Now which provides easy-to-access, practical and timely knowledge that matters to your business. CMS expands to meet client needs, moving into countries where we can make a difference to your business. Recent examples include our new offices in Dubai and Mexico, which we set up to support our energy clients operating there.

World vision

Our sector insight means we immerse ourselves in the world of your business and we make sure we understand the global business issues you are facing. We have deep local expertise in your most significant jurisdictions as well as all the major global centres and we have established CMS in emerging markets in line with client needs. CMS professionals act as trusted partners, managing your global projects and transactions wherever you need us.

Performance-driven

We work with you to define what success means for you and your organisation and we focus on making it happen. CMS takes pride in first-class execution and project management – we deliver results, not just opinions. We will actively ask for your feedback to help us assess and improve our performance.

Delivering Client Service

We take the same approach to service delivery everywhere, based on a common training programme and a shared understanding of what our clients value most.

We provide you with management information to help you manage your account with us, covering areas such as invoicing, matter progress, fees, work in progress (WIP) along with bespoke reports on other factors specific to your business and your needs.

Your satisfaction with our performance drives our efforts to continuously improve our service. Through regular exchange of information and independent feedback we identify opportunities to reach higher levels of efficiency and effectiveness in service delivery and act upon them.

Staff **> 8,000**

Lawyers **> 4,800**

Partners **> 1,100**

49 NEW PARTNERS IN 2019, TAKING THE TOTAL TO OVER 1,100

Operating in **71** cities

Across **43** countries

EUR 1.426bn turnover for 2019

19 PRACTICE AND SECTOR GROUPS WORKING ACROSS OFFICES

- **#1 CEE, DACH, Germany** *(Mergermarket)*
- **#1 Germany, UK** *(Thomson Reuters)*
- **Top rankings in 2019 M&A League Tables** *(by deal count)*
  #1 by Bloomberg in Europe, Germany and UK
  #1 by Mergermarket in CEE, DACH and Germany
  #1 by Thomson Reuters in Benelux and Germany
- **#1 Europe, Germany, UK** *(Bloomberg)*

12. About CMS

CMS practice areas and sector groups

- Banking & Finance
- Commercial
- Competition & EU
- Corporate / M&A
- Dispute Resolution
- Employment & Pensions
- Intellectual Property
- Public Procurement
- Real Estate & Construction
- Tax
- Consumer Products
- Energy & Climate Change
- Funds
- Hotels & Leisure
- Insurance
- Infrastructure & Project Finance
- Life Sciences & Healthcare
- Private Equity
- Technology, Media & Communications

Locations worldwide

The Americas

Bogotá
Lima
Mexico City
Rio de Janeiro
Santiago de Chile

Europe

Aberdeen
Amsterdam
Antwerp
Barcelona
Belgrade
Berlin
Bratislava
Bristol
Brussels
Bucharest
Budapest
Cologne
Duesseldorf
Edinburgh
Frankfurt
Funchal
Geneva
Glasgow
Hamburg
Istanbul
Kyiv
Leipzig
Lisbon
Ljubljana
London
Luxembourg
Lyon
Madrid
Manchester
Milan
Monaco
Moscow
Munich
Paris
Podgorica
Poznan
Prague
Reading
Rome
Sarajevo
Seville
Sheffield
Skopje
Sofia
Strasbourg
Stuttgart
Tirana
Utrecht
Vienna
Warsaw
Zagreb
Zurich

Africa

Algiers
Casablanca
Johannesburg
Luanda
Mombasa
Nairobi

Middle East

Abu Dhabi
Dubai
Muscat
Riyadh

Asia-Pacific

Beijing
Hong Kong
Shanghai
Singapore

C/M/S/ Law-Now™

Law . Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335. It is a body corporate which uses the word "partner" to refer to a member, or an employee or consultant with equivalent standing and qualifications. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales with SRA number 423370 and by the Law Society of Scotland with registered number 47313. It is able to provide international legal services to clients utilising, where appropriate, the services of its associated international offices. The associated international offices of CMS Cameron McKenna Nabarro Olswang LLP are separate and distinct from it. A list of members and their professional qualifications is open to inspection at the registered office, Cannon Place, 78 Cannon Street, London EC4N 6AF. Members are either solicitors or registered foreign lawyers. VAT registration number: 974 899 925. Further information about the firm can be found at cms.law

© CMS Cameron McKenna Nabarro Olswang LLP

CMS Cameron McKenna Nabarro Olswang LLP is a member of CMS Legal Services EEIG (CMS EEIG), a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices. Further information can be found at cms.law

© CMS Cameron McKenna Nabarro Olswang LLP 2020

2006-0128426-20