Law Society of Scotland

Guide on the use of Electronic Signatures

20 March 2020

Table of Contents

GUIDE ON THE USE OF ELECTRONIC SIGNATURES

Please note this is a working draft of a guide to the use of electronic signatures that the Electronic Signatures Working Group of the Technology Law and Practice Committee have drafted. The guide was being prepared prior to recent Covid-19 outbreak.

Although the guide is not completely finalised the Working Group felt that sharing the guide as a 'beta' version would be of use to the profession given the current practical difficulties they face at the present time.

The Working Group will continue to review and update the guide as necessary and users of the guide should be aware that amendments may be made in the future.

The Working Group hope that the guide is of some assistance and would appreciate any feedback that users have.

Please send any feedback you have to antonymcfadyen@lawscot.org.uk

1. Introduction

This guide has been prepared by the Electronic Signatures Working Group in conjunction with the Law Society of Scotland. It has been put together to assist the legal profession with the use of electronic signatures in commercial contracts, and to reflect best practice in this area.

The guide sets out the Scots law position. Where relevant, we have contrasted the position under English law. The law in other jurisdictions may of course be different.

There are a number of third party providers of e-signing platforms. Adobe Sign and DocuSign are two well-known ones. Some of the practical examples in this guide are based on the capabilities of these two providers. Each provider will, however, do things differently and offer different functionality. Nothing in this guide constitutes an endorsement of any third party provider.

This guide does not deal with the Scottish rules of evidence. Please see section 7 of the Electronic Communications Act 2000.

The guide reflects the views of the Working Group but is not, nor is it intended to be, a complete statement of the law and does not displace the legal responsibilities and obligations on solicitors to identify relevant matters of law. The Society welcomes any comments on the guide and would be pleased to hear from members with any suggested additions and amendments to it.

For assistance on the use of Smartcards, please refer to the Smartcard practical advice guide.

2. WHAT IS AN ELECTRONIC SIGNATURE?

2.1 Overview

An electronic signature is defined as *data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign*[1]. This simply means that some electronic data has been used by a person to sign or otherwise signify agreement or consent.

Electronic signatures can take a number of different forms. The three main types of electronic signature are discussed below.

2.2 Simple electronic signatures

- The most basic form of electronic signature is the simple electronic signature. We encounter these every day, for example:
- using a finger or stylus to sign on a pad when a parcel is delivered;
- clicking an onscreen button such as “I agree”, “Submit” or ticking a box saying “I accept the terms and conditions”;
- typing your name into an email[2];
- electronically pasting a signature (e.g. in the form of an image) into an electronic version of a contract, or
- an e-signature on an e-signing platform.

At the date of this guide, the form of e-signature provided by most service providers is a simple electronic signature.

2.3 Advanced electronic signatures

Advanced electronic signatures (AES) are more secure since the signatory has a greater level of control over their use and any change to the signature is detectable. They are:

- uniquely linked to the signatory;

[1] Article 3(10) eIDAS
[2] See *Neocleous v Rees* [2019] EWHC 2462 (Ch)

- capable of identifying the signatory;
- created using means that the signatory can maintain under their sole control; and
- linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.

In practice, the availability of AESs is limited and only available through a third-party service provider.

2.4 Qualified electronic signatures

The highest standard of electronic signature is a qualified electronic signature (QES). Under Scots law, a QES is self-proving (probative).

There are only limited situations where a QES will be available. The most common would be a signature applied by a Scottish solicitor using their Law Society Smartcard. As at the date of this guide, we are unaware of any provider in the UK of publicly available QESs for use by individuals. The other QESs available are closed loop systems where the QES is issued for a particular purpose (e.g. Register of Scotland ARTL E-Signatures).

In some countries QESs are more widely available, for example Belgium and Sweden.

2.5 EU regulations eIDAS

The use of electronic signatures is governed by Regulation (EU) No 910/2014 ("eIDAS"), along with the UK legislation set out at **Relevant legislation** (see 2.8). The effect of eIDAS is that:

- a qualified electronic signature has the same legal effect as a handwritten signature; and
- electronic signatures cannot be denied legal effect and admissibility solely on the grounds that they are in electronic form.

However, while eIDAS gives legal recognition to electronic signatures of all types, it does not provide what evidential weight might be attached to a particular type of signature (see paragraph 8.3 below).

Certain provisions of eIDAS have been implemented in UK legislation such as the Requirements of Writing Act and the Electronic Documents (Scotland) Regulations 2014. When the UK leaves the EU, eIDAS will become part of UK law under the European Union (Withdrawal) Act 2018.

2.6 What is an electronic document?

Electronic signatures can only be applied to electronic documents. The Requirements of Writing Act tells us that electronic documents are documents which, rather than being written on paper, are created in electronic form[3]. These are documents which are never printed in hardcopy but rather exist solely as, for example, Word documents, PDFs and/or emails.

Documents printed on paper are referred to as traditional documents.

2.7 What is not an electronic signature

If you print out a document, sign it in wet ink, then scan it in, that is not an e-signature. That is a signed traditional document of which a copy has been made.

By contrast if the document is not printed out, but some form of mark is applied electronically (e.g. a scanned version of a signature), that is a type of e-signature.

2.8 Relevant legislation

Requirements of Writing (Scotland) Act 1995 (NB this Act has been updated since 1995, including a new Part 3 which deals with electronic documents)

Legal Writings (Counterparts and Delivery) (Scotland) Act 2015

eIDAS - EU Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market

Electronic Communications Act 2000

The Electronic Documents (Scotland) Regulations 2014

The Land Register of Scotland (Automated Registration) etc. Regulations 2014 [These add Regulations 5-7 to the Electronic Documents (Scotland) Regulations 2014, in particular stipulating who is able to sign on behalf of different entities (mirroring the provisions of Schedule 2 to the 1995 Act)]

The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016

[3] Section 9A, Requirements of Writing Act

3. VALIDITY OF ELECTRONIC SIGNATURES

3.1 E-signatures and the Requirements of Writing Act

Section 1(2) of the Requirements of Writing Act sets out certain documents which must be made in writing. The requirements for valid execution in section 2 of the Requirements of Writing Act only apply to section 1(2) documents.

Section 1(2) documents must be signed with an AES to be valid and a QES to be self-proving[4]. However, wills and testamentary writings, and certain documents which are to be registered, must be created and signed in traditional form using wet ink signatures.

Unless there is a specific statute covering the particular type of document, there is no statutory requirement as to how non-section 1(2) documents should be executed. A simple electronic signature is a valid form of execution for those types of document not set out in section 1(2) of the Requirements of Writing Act.

For non-section 1(2) documents, Scots law requires evidence of offer and acceptance. A simple electronic signature may well suffice for this purpose – it depends how much evidential weight can be put on it. See **Verifying an electronic signature (see 8).**

Generally, the precise form of electronic signature used is not critical: being able to prove who signed and that they had an authenticating intention is more important.

3.2 Requirements for “in writing” outside the Requirements of Writing Act

Where there is a requirement by legislation outside of the Requirements of Writing Act for a contract to be made in writing, an electronic signature is a legally effective means of signifying agreement in writing. An example of this is a jurisdiction clause under the Recast Brussels Regulation[5].

There may however be a specific statutory requirement for a wet ink signature. An example (there may be others) is section 31(6) of the Patents Act 1977. This requires assignations of, or grants of security over, patents to be in writing and "subscribed". However, "subscribed" is a term used only in the provisions of Requirements of Writing Act dealing with documents that are in paper, parchment or other tangible medium. It is not clear whether the failure to update the wording in section 31(6) to reflect Requirements of Writing Act amendments was an oversight.

[4] Sections 2 and 3 of the Electronic Documents (Scotland) Regulations 2014

[5] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

3.3 Non-Scottish entities signing a document governed by Scots law (Rome 1 considerations)

Where a non-Scottish entity executes a document governed by Scots law, an electronic signature by that entity would be valid under Scots law. In these situations, advice from the local jurisdiction (e.g. an opinion from local counsel) should be obtained in case there are any local law requirements that would prevent, restrict or otherwise impact the ability of the entity to sign using an e-signature.

4. USING ELECTRONIC SIGNATURE PLATFORMS

Most e-signing platforms work by selling a licence to use the platform (e.g. to a legal advisor). The licensee may then make the platform available to clients and counterparties. Therefore the signatories themselves do not necessarily need to have the e-signing platform installed.

The considerations outlined in **The signing process (see 7)** will be relevant when solicitors (or their clients) intend to use an e-signing platform. Solicitors will have to advise on whether that is appropriate in the context of the transaction.

When working with counterparties, it is often simpler to use one platform. If that is not possible, consider the technical implications if the parties use different providers. Is it possible for one party to sign using platform A, send the electronic document to the other party, other party uploads to platform B, then applies his signature on platform B? Or would that cause the signature from platform A to disappear?

For some clients, there may be a business imperative to use their, and only their, e-signing platform. For example, there may be an internal requirement to have an audit trail showing that the contract was approved by various people before being passed on for signature.

If asked to use a provider different from the one you are used to, ask to try it out – interrogate the metadata and see how it compares to the metadata of the provider you are used to. Agree with the other side what metadata you want to be provided.

5. APPLYING AN ELECTRONIC SIGNATURE

5.1 Applying an e-signature without an e-signing platform

E-signatures may be applied without the use of an e-signing platform, for example using one of the methods set out in paragraph 2.2.

5.2 Applying an e-signature using an e-signing platform

Although each e-signing platform is different and platform services are continually being updated, in general each signatory would receive an email request to sign the relevant document. They would then access that document through a link provided in the email, and apply their e-signature to the document in the appropriate place.

For QESs and how to apply e-signatures using a Smartcard, please see this Law Society of Scotland guidance which can be accessed here.

5.3 Where to place the signature block when using an e-signing platform

Theoretically, it is not necessary for the signature block to be placed at the end of the body of an electronic agreement. The signature block could appear anywhere in that electronic document. Rather than subscription, section 9B of the Requirements of Writing Act talks about the electronic document being "authenticated by the granter" if that person's signature is "incorporated into, or logically associated with, the electronic document". However, it is not necessary to include any particular form of wording in the testing clause or signature blocks.

In practice we expect that electronic documents would be set up in the same way as traditional documents, with the signature block at the end of the body of the agreement. This would also allow the document to be signed in counterpart if necessary, as the electronic counterpart would be identical to the traditional counterpart.

6. SELF-PROVING STATUS

6.1 Witnessing an electronic signature

It is misleading under Scots law to refer to "witnessing an e-signature". Scots law does not recognise the concept of witnessing an e-signature in the same way that special status is attributed to the witnessing of a wet ink signature.

No type of electronic signature can be witnessed within the meaning of section 3 of the Requirements of Writing Act. Section 3 is only relevant to wet ink execution of traditional documents. Therefore a purported "witnessing" of any form of electronic signature does not create a self-proving signature.

For the purposes of the Requirements of Writing Act, a self-proving electronic signature can **only** be created by use of a QES. No witnessing is required. The QES, by itself, is self-proving[6].

[6] Section 3 of the Electronic Documents (Scotland) Regulations 2014

An AES or simple electronic signature **cannot** be self-proving.

Example 1 – John is a party to an agreement. He uploads a scan of his handwritten signature to the signature block. Jane stands beside him and watches him to do this. Jane then uploads a scan of her handwritten signature and applies it to the witness signature block. Although Jane's signature may be of evidential value, it is not self-proving in terms of the Requirements of Writing Act.

Example 2 – Ahmed receives a request from an e-signing platform asking him to execute an electronic document. He calls Alina over to witness his signing of the document via the platform. Alina watches him sign, and then applies her e-signature to the witness block in the e-signing platform. This does not make Ahmed's signature self-proving under the Requirements of Writing Act.

6.2 Comparison with England

In order for a document to be validly executed as a "deed" under English law, the attestation of a witness is required (for certain signatories). The Report on Electronic Execution of Documents by the Law Commission of England and Wales states that a deed must be signed in the physical presence of a witness, whether it is signed in wet ink or by electronic means. The report recommends further consultation be carried out to establish whether witnessing the electronic signature of a deed through a video link should be allowed.

This is not comparable to Scots law because the rules in the Requirements of Writing Act on self-proving signatures apply only to traditional documents (see paragraph 6.1).

6.3 Is a self-proving signature required?

If a self-proving signature is not legally required, consider whether the document needs to be signed in a self-proving (probative) manner. In certain sectors, the usual practice by solicitors is to seek to obtain a self-proving signature in the majority of cases. However, in many cases a valid signature would suffice and this could be considered on a case by case basis. Although certain agreements will require it (e.g. documents which need to be registered), there may be many circumstances where a self-proving signature is not necessary. For example, the parties may be satisfied to sign a low-risk contract in a valid rather than self-proving manner, in which case a simple electronic signature would suffice. For further considerations, see **Risk assessment (see 8.2).**

7. THE SIGNING PROCESS

Please note in developing this guide, we have looked to engage with the major e-signing platforms. We have had a demonstration and discussion with Adobe in relation to Adobe Sign but have not yet had a demonstration from DocuSign. Every e-signing platform is different, and you need to check the functionality and configuration options with your provider in advance.

7.1 Agreeing to sign electronically

In a practical sense, it is helpful if contracting parties agree in advance whether the document may be signed using e-signatures. However, it is not necessary to include a provision in the document referring to the parties' agreement to execute electronically. If all parties sign electronically using the one e-signing platform, then there is just one document and it is clear on the face of it how it has been executed.

Note that electronic signatures will not work for certain documents, for example where the document needs to be registered and the relevant registry does not accept electronic documents.

7.2 Date and place of signing

It is not necessary to include either the date or place of signing, although the date of signing may be useful in some circumstances.

The Requirements of Writing Act presumptions on date and place of signing (section 3(8)) do not apply to electronic documents. This suggests there is no great benefit in including them.

7.2.1 Place of signing

This might be embedded or discoverable from certain types of e-signature (e.g. where you can obtain the IP address of the signatory). However, that might not always accurately reflect the place where the signatory actually was.

For many kinds of contracts, including the place of signature will be of little practical value. Evidence of the place of signing might in rare cases be relevant e.g. if the contract purportedly shows that Mr. Smith signed in Edinburgh on 1 January 2019, but Mr Smith denies he signed it and can prove he was in Paris on that date.

7.2.2 Date of signing

This will be embedded in some types of e-signature (e.g. ones provided by e-signing platforms) but not others (e.g. if a party cuts and pastes a scan of their handwritten signature into a document).

In some e-signing platforms, the date of signature can be certified.

Where a contract is concluded in counterpart, the date of delivery for the purpose of the Counterparts Act is a key date. See **Documents which require to be delivered (see 7.3)** as to how this might be achieved through use of an e-signing platform.

7.3 Documents which require to be delivered

The following guide relates to documents which require to be delivered under Scots law, for example those signed in counterpart.

7.3.1 Legislative framework

In relation to the authentication of documents in accordance with the Requirements of Writing Act (i.e. section 1(2) documents or electronic documents that are to be self-proving), the framework for this is in section 9F of the Requirements of Writing Act:

(1) An electronic document may be delivered electronically or by such other means as are reasonably practicable.

(2) But such a document must be in a form, and such delivery must be by a means which (a) the intended recipient has agreed to accept, or (b) which it is reasonable in all the circumstance for the intended recipient to accept.

If using a single e-signing platform, it can be configured to notify everybody when the last signature is applied. In the absence of a contrary agreement, delivery would take place at that point. See **Holding documents as undelivered (see 7.3.3)** regarding delaying the delivery date.

See also **Dating the document (see 7.5)**.

7.3.2 When is delivery effected?

The essential requirement for delivery to have taken place is whether or not the granter of the document has deliberately put the document beyond their further control with the intention of becoming bound by it. The Counterparts Act does not deal with this.

The Law Society Smartcard practical advice guide refers to commentary supporting the view that the contract is concluded when the document is received by the recipient, not at the point of dispatch by the sender.

In practice, a receiving solicitor would normally wait for the email to arrive before advising a client that the contract has been concluded.

7.3.3 Holding documents as undelivered

This could be achieved either by:

- using functionality available on the e-signing platform; or
- having an email exchange between the parties

Using functionality on the e-signing platform

Some e-signing platforms can be configured so that, after the last signature, there is another step required (the "approval" step) before the document is confirmed as complete. That final step could be to require a nominated person to add the agreed effective date.

The parties could agree in advance that the nominated person would only add that date when all parties had agreed that they could do so.

The e-signing platform would record and certify that the final approval step had been taken,

This would enable the parties to control the date on which the electronic document comes into effect.

There would need to be a supporting email exchange which made clear how this would work so that everyone knew and agreed what this final approval step signified.

By email exchange

The parties/their solicitors could agree by email exchange that, notwithstanding the last date of signature, and whatever messages the e-signing platform sends out, the document will not come into effect until all the parties agree.

There would then need to be a further email exchange confirming that date.

In either scenario, the email chain would need to be stored with the electronic document.

7.4 Coming into effect

Certain documents do not require to be delivered under Scots law (e.g. mutual agreements) and the following guide relates to such documents. For documents which are subject to a delivery requirement (e.g. those signed in counterpart), see **Documents which require to be delivered (see 7.3).**

When using a single e-signing platform, the order of signatures is set up in the platform, which then sends it round to each party in order. Where there are multiple completion documents, an e-signing platform can assist by ensuring documents are sent out for signature in the correct order.

Once the last party has signed, the system can be configured to inform everyone that is it has been signed. In the absence of any indication to the contrary, the document would come into effect then.

7.5 Dating the document

7.5.1 Where all parties use the same e-signing platform

Under Scots law, when all parties use the same e-signing platform to sign the same version of the document, the effective date and/or date of delivery will be when the platform releases the signed version to everyone (unless otherwise agreed). See ***Documents which require to be delivered*** and **Coming into effect (see 7.4)**.

Where an e-signing platform has been used, it may be possible to configure the platform so that one party (e.g. the person sending the documents for signature) can insert an effective/delivery date at the end of the signature process.

7.5.2 Where counterparts are signed by both parties electronically

Documents signed electronically and exchanged in counterparts require to be delivered, and therefore a key issue will be agreeing the date of delivery.

If the parties have affixed a simple electronic signature to a Word or pdf document, and exchanged counterparts, it may not be possible to type the date in afterwards. It may be possible to print out the document, add the delivery date by hand, and scan it back in - but this will create a new copy of the original document which may not be desirable.

In practice, the parties' solicitors will need to agree in advance how they want to deal with evidencing the delivery date. If it is not possible to apply the delivery date to the actual document, it could be evidenced through an email exchange which is then kept with the counterpart.

As with all counterparts, care will need to be taken with any definitions of "Commencement Date" or "Effective Date" to ensure they do not cut across or become confused with the delivery date.

8. VERIFYING AN ELECTRONIC SIGNATURE

8.1 Is it an electronic signature?

The first thing to check is whether the signature really is an electronic signature.

If you have received a pdf of a document which has been printed out, signed by hand, then scanned in - that is not an electronic signature. That is a copy of an original. It may be that the party sending it is relying on section 4 of the Counterparts Act which allows delivery of a traditional document to be made by electronic means.

Note that whether or not the signature is electronic may not be obvious from the pdf. For example, the signatory could have applied a scan of their handwritten signature to the document. That would be a simple electronic signature. It may be prudent to check with the signatory directly.

8.2 Risk assessment

If the e-signature is not a QES and a self-proving signature is not required, you will need to carry out a risk assessment to determine how comfortable the contracting parties can be in relying on that signature.

You will be assessing:

- the risk of a contracting party in future disputing that they had signed at all (or that they had signed this particular document); and
- the impact of such a dispute.

Disputes of this nature could of course equally occur with wet ink signatures of traditional documents. Cases are relatively rare. However, they are costly and can be problematic to address if they do occur.

Depending on the above assessment, you will need to consider whether the electronic signature would suffice as evidence that the document was signed by the person purporting to have signed it.

Your approach will depend on:

- the type of electronic signature you have;
- the type of document you are dealing with (e.g. agreement, resolution, board minutes, etc.); and
- the nature of the transaction (e.g. value, risk) and the importance of the particular document within that.

8.3 Evidential weight

While eIDAS gives legal recognition to electronic signatures of all types, it does not provide what evidential weight might be attached to a particular type of signature.

That depends on the level of certainty that the electronic signature provides of the person's identity and their intention to form a contract.

The question is whether, if challenged, one can prove that the person you think authenticated a document did in fact do so. That is easier to do with an AES or QES compared with a simple electronic signature.

8.4 Reliance on simple electronic signatures

The level of reliance which a contracting party can place on a simple e-signature will vary depending on the type and the circumstances.

For example, if the document has been signed by uploading a scan of a handwritten signature, how was it sent to you? Was it emailed directly by the signing party or their solicitors? Or did it come via a third party? In the latter case, you might seek additional confirmation that the party actually applied (or consented to the application of) their signature to the document you have received.

There are significant risks to signing Word documents by inserting a JPEG of a scanned handwritten signature. Word documents can, unless suitably protected, be amended after the signature has been applied, meaning that such a document may not provide much in the way of evidence. There may be a high degree of trust between the contracting parties at the time so that they are willing to execute in this way, with an exchange of emails helping to provide an evidential trail of what was agreed. However, someone else may need to review or rely on that contract further down the line, and they may not have the same level of comfort (particularly if they do not have access to those emails).

The default functionality on most e-signing platforms does **not** amount to an advanced electronic signature (and certainly not a qualified electronic signature). It is a simple electronic signature only. The platform may only be able to tell you that the contract was "signed by [Provider]" - **not** by the individual contracting party.

If so, then potentially anyone with access to the signatory's inbox could have applied the signature. You need to look at the metadata to see if that gives you sufficient comfort that the person you thought was signing did in fact sign.

Some e-signing platforms offer additional security measures such as two-factor authentication using a pin code sent to a mobile number. This is still a form of simple electronic signature but provides more evidential weight.

Familiarise yourself with the way in which the e-signing platform works and check with the provider. It may be that they can offer advanced functionality which would satisfy the requirements for an AES.

8.5 Constitutional signing requirements

Contracting parties that are not individuals may have their own constitutional or internal requirements (e.g. byelaws, delegated authorities) that specify who can execute particular documents. For example, certain office holders may be designated as authorised signatories and authorised to sign contracts.

If electronic execution is proposed, those constitutional or internal requirements will need to be checked to identify whether they will meet the Requirements of Writing Act requirements.

9. WHAT IS THE ORIGINAL DOCUMENT?

The concept of "original" or "principal" really only works for traditional documents.

Where an electronic document is signed by an e-signature, the file to which those signatures are attached/associated is the "original". However, unlike traditional documents, it is possible to create multiple duplicate "originals" of electronic documents e.g. each time an email is forwarded to which the document is attached or by copying and pasting the document into a new folder.

If, however, someone were to open the document and click "Save as" a new document, that would create a copy rather than a duplicate "original". And, if the document was a Word document, doing this would cause the electronic signatures to disappear.

Note that printed hardcopies of electronic documents are merely copies, and not originals.

10. STORING DOCUMENTS THAT HAVE BEEN ELECTRONICALLY SIGNED

10.1 Solicitors storing their clients' electronically signed originals

The contracting parties and their solicitors should agree about storage in advance, as they would for traditional documents. Unlike traditional documents, however, where in order for each party to have its own "copy" the parties would need to execute multiple wet ink versions, "duplicate originals" of an electronically signed document can be created so that each party can have its own electronically signed document and store duplicates.

Each party should agree with its solicitors whether the solicitors will retain the electronic document and, if so, for how long. See the Law Society guidance on The Ownership and Destruction of Files and Law Society guidance on Scanning and Archiving Documents.

The approach to storage of electronically signed documents will vary depending on:

- the type of electronic signature being used;
- each firm's policies on storage and retention of client documents; and
- the terms of the relevant letter of engagement (which should make clear to the client where the responsibility lies).

For example, it is the policy of some firms not to hold principal (traditional) agreements for clients. If they have not already done so, firms will need to decide whether they are willing to be responsible for storing on behalf of the client electronically signed documents (e.g. in a sub-folder in the client file), including the costs of so doing, the duration for which it is retained, and the means of storage/access.

If a firm does agree to store an electronically signed document, check the impact of the firm's policies on automatic destruction or archiving of material held electronically.

If the solicitors are storing the electronic document, it should be stored on the client's electronic file. In addition, each contracting party should be provided with, and advised to retain, the electronic document.

10.2 Storing the e-signature data

Where a document has been signed using either a QES, AES or a third party e-signing platform, it is possible to create multiple duplicate "originals".

Note that certification data relating to the signatures may need to be obtained and retained by all those holding an electronic document that has been signed electronically.

For example, where a document is signed in Microsoft Word or Adobe Acrobat using a QES (e.g. a Law Society Smartcard), the signatory's electronic signature is attached to the document, and the relevant certificate can be viewed directly from the document itself. By right clicking on the signature, you can see the certificate provided by the trust provider.

However, in most e-signing platforms the electronic signature attached to the document (and the associated certificate) will be associated with the platform provider, not the signatory using the e-signing platform.

Although the print out of the metadata looks like you have the individual signatory's signature, if you hover over the actual signature in the document, it will say "signed by [provider]".

Information (metadata) connecting the signatory to that signature (i.e. date and time of signature, email address to which the request to sign was sent and the IP address of the device) will be collected by the e-signing platform and made available by the e-signing platform for signatories to download. However, it is not possible for a third party to directly access this information.

It is therefore necessary to consider each provider's system e.g.:

- how long does the provider retain the metadata?

- who exactly has access to the metadata necessary to interrogate the e-signature? Is it the individual signatory only? If so, consider whether other contracting parties or third parties will need access to this data in future (e.g. for due diligence purposes).

The simplest solution may be to download the signing metadata and for each party to store a copy of the certificate with the electronic document.

If the delivery date of the electronic document differs from the last date of signature, information about that will also need to be stored with the electronic document.Read **Documents which require to be delivered (see 7.3)**, **Date and place of signing (see 7.2)** and **Coming into effect (see 7.4)**).

10.3 Storing counterparts executed electronically and as traditional documents

This is where one party has executed a counterpart electronically and the other has signed a paper counterpart.

The electronically signed counterpart would be held in the client's electronic file. It would be sensible also to hold a scanned copy of the traditionally signed counterpart and indicate prominently in the file where that wet ink counterpart is stored.

The party retaining the wet ink counterpart should place a note with it explaining that the other counterpart was signed electronically and noting where that is electronically filed.

11. COUNTERPARTS SIGNED ELECTRONICALLY AND AS TRADITIONAL DOCUMENTS

Documents may be signed in both electronic and traditional methods when using counterparts.

Example:

Party A prints out a counterpart and signs in wet ink.

Party B applies its e-signature to another counterpart.

Each delivers their executed counterpart to the other party.

This is possible and envisaged by the Counterparts Act (section 3(1)).

Note 15 of the Explanatory Notes states: It also follows that it is competent for a document to be signed in various counterparts some by electronic signature and some in wet ink.

The counterparts are treated as a "single document" (section 1(3)) even though physically they reside in different media. Section 1(4) provides that the single document may be made up of (a)

both or all the counterparts in their entirety, or (b) one in its entirety, collated with the signature pages of the other(s).

What constitutes the “single” document where counterparts have been executed and exchanged in (i) mixed media (i.e. one with an electronic signature and one executed traditionally on paper) or (ii) using two different e-signing platforms?

In both situations, the single document comprises all counterparts – although each counterpart exists in a different environment. However, they do not need to be held together in the same place for them to constitute the single document "in its entirety".

Note that where one party sets up the document for signature in a single e-signing platform, and all signatories use that platform to sign, this is not execution in counterpart: there is a single document which each party signs electronically. In the case of mutual contracts, there would be no requirement for delivery under Scots law and the document would come into effect on the date the last person signed. **Coming into effect (see 7.4).**

12. QUICK LINKS

Report on Electronic Execution of Documents by the Law Commission of England and Wales

English Law Society and CLLS practice note on electronic signatures July 2016

Law Society guidance on The Ownership and Destruction of Files

Law Society guidance on Scanning and Archiving Documents

Law Society Smartcard practical advice guide