Law Society of Scotland

Guide to Electronic Signatures

3rd edition

In association with

denovo

Whole Practice Management Software

Contents

1. Introduction

This guide has been prepared to assist the legal profession with the use of electronic signatures in commercial contracts, and to suggest 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 eSignature are two well-known ones and the Working Group is very grateful to them for their assistance in preparing this guide. 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 is not a complete statement of the law and does not displace the legal responsibilities and obligations on solicitors to identify relevant matters of law. 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 here.

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 electronic signature on an e-signing platform with audit trail capability. At the date of this guide, the standard functionality provided by most e-signing platforms 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;
- Capable of identifying the signatory;
- Created using means that the signatory can maintain under their sole control; and
- Linked to the data to which they relate in such a manner that any subsequent change in the data is detectable.

AESs are available through some e-signing platforms (see Qualified electronic signatures (2.4)) and other third party providers.

2.4. Qualified electronic signatures

The highest standard of electronic signature is a qualified electronic signature (QES). This is the most secure type of signature and involves the signatory's identity being verified by a qualified trust service provider before the signatory is issued with a QES. Under Scots law, a QES is the only type of electronic signature that is self-proving (probative) (see Self-proving status (7)). The Law Society Smartcard enables Scottish solicitors to apply a QES to documents. The 'out of the box' standard functionality of e-signing platforms does not usually provide AES or QES functionality. Providers such as Namirial, Intesi Group, DocuSign eSignature and Adobe Sign (and other e-signing platforms) do offer AES and/ or QES functionality

at an additional cost. In some countries (including some in continental Europe with civil law systems) QESs are more widely available. For example, some countries have them built into national identity cards.

2.5. Digital signatures

Often the terms "digital signature" and "electronic signature" are used interchangeably. However, a digital signature is generally intended to refer to an electronic signature where advanced cryptography is used (for example, an AES or QES that uses cryptography). A simple electronic signature is not a digital signature.

2.6. UK eIDAS

The use of electronic signatures is governed by UK eIDAS along with the other UK legislation set out at Relevant legislation (2.9). UK eIDAS is the version of Regulation (EU) No 910/2014 (eIDAS) that has been incorporated into UK law following the UK's exit from the European Union. The effect of UK 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 UK 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 Evidential weight (9.3)).

Certain provisions of UK eIDAS have been reflected in UK legislation such as the Requirements of Writing (Scotland) Act 1995 and the Electronic Documents (Scotland) Regulations 2014. While UK eIDAS and eIDAS are similar, creating parallel regimes in the UK and EU, the relationship is asymmetric. UK law recognises a QES issued by a qualified trust service provider under eIDAS , but eIDAS does not recognise a QES issued by a qualified trust service provider registered in the UK under UK eIDAS.

When dealing with international matters, check which qualified trust service provider has provided each QES, to establish whether the QES is recognised under Scots law. You can use this eIDAS dashboard to check if a QES has been issued by a qualified trust service provider under eIDAS.

2.7. 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 not 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'.

2.8. 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 electronic signature. That is a signed traditional document of which an electronic 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 electronic signature

2.9. Relevant legislation

Requirements of Writing (Scotland) Act 1995 - This Act was updated in 2014 to introduce 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 (eIDAS) as incorporated into UK law upon the UK's exit from the European Union

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 – These Regulations made certain consequential amendments to UK law as a consequence of eIDAS (now UK eIDAS) coming into force

The Registers of Scotland (Digital Registration, etc.) Regulations 2022 - These amend the Electronic Documents (Scotland) Regulations 2014, in particular the requirements regarding annexations to electronic documents. They also permit PDFs of QES signed electronic documents to be registered in the Books of Council & Session.

[1] Article 3(10) eIDAS.
[2] See Neocleous v Rees [2019] EWHC 2462 (Ch).
[3] Section 9A, Requirements of Writing Act.

3. Validity of electronic signatures

3.1. Electronic 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 include certain documents relating to land (such as missives, dispositions and leases), gratuitous unilateral obligations except those undertaken in the course of business, and "truster as trustee" trusts. 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 documents that are not covered by section 1(2) should be executed. A simple electronic signature is a valid form of execution for those types of document. See also Self-proving status (7) and Verifying an electronic signature (9). Generally, the precise form of electronic signature used is not critical: being able to prove who signed and that they intended to be bound is more important.

3.2. Requirements for 'in writing' outside of 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 the Requirements of Writing Act dealing with documents that are in paper, parchment or another 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.

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 (of the appropriate type) 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 (a) prevent, restrict or otherwise impact the ability of the entity to sign using an electronic signature; or (b) affect whether or how the contract could be enforced against the non-Scottish entity, particularly if overseas assets could be involved.

3.4. Documents governed by a law other than Scots law

This guide only covers Scots law. If the document to be signed is governed by another law, advice from the local jurisdiction should be sought as to whether and how electronic signature may be used.

[4] Regulations 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.

4. Using electronic signature platforms

Most e-signing platforms work by selling a licence or subscription to use the platform (e.g. to a legal advisor). The licensee can then use the platform to initiate the signing process without the signatories themselves having to have an account. The e-signing platform is browser based and will not require installation of software. The considerations outlined in the signing process (8) 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 simpler to use one platform and the parties should agree in advance which one that should be (if different parties use different platforms). Whichever e-signing platform is used, all participants to a signing process should receive the final signed document(s). Participants should also make sure that they receive from the originator of the signature process the accompanying audit trail (metadata and any certificates provided) if this is not provided to them automatically. See Storing the electronic signature data (11.2).

5. Applying an electronic signature

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

Electronic 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 electronic signature using an e-signing platform

Although each e-signing platform is different and platform services are continually being updated, in general each signatory receives an email request to sign the relevant document. They then access that document through a link provided in the email and apply their electronic signature to the document. For how to apply a QES using the Law Society of Scotland's Smartcard, please see the Law Society of Scotland guidance.

5.3. Where to place the signature block

It is not necessary for the signature block to be placed at the end of the body of an electronic document. The signature block can 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". It is not necessary to include any particular form of wording in the testing clause or signature blocks but, to ensure ex facie validity, the capacity of the signatory (e.g. director, secretary, authorised signatory) should be evident from the face of the electronic document. In practice electronic documents are typically set up in the same way as traditional documents, with the signature block at the end of the body of the document. Paragraph 6 explains how to ensure that annexations are regarded as incorporated into an electronic document.

In particular, note that for AES and QES-signed electronic documents each signatory only requires to apply their AES/QES once to the document, without the need to also apply their AES/QES to any annexations (provided that any annexations are annexed to the document before the AES/QES is applied – see paragraphs 6.1 and 6.2c). If a signatory of an electronic document "over-signs" (by applying their electronic signature to more places within the document than is necessary, or to an annexation when it is not required), that will not invalidate the signing of the document.Where an electronic signature is being applied under Scots law, solicitors should remove any references to witnesses. Witnessing an electronic signature does not create a self-proving signature. It may be confusing for anyone looking at the document in the future if parts of a signature block appear to be incomplete even though they did not need to be completed. See Witnessing an electronic signature (7.1).

6. Annexations

The type of electronic document will determine how an annexation to it is to be regarded as incorporated in that document. Under Regulation 4(1) of the Electronic Documents (Scotland) Regulations 2014, the general rule is that, unless an enactment expressly provides otherwise, an annexation to an electronic document is to be regarded as incorporated in the document if it is-

a. referred to in the document, and
b. identified on its face as being the annexation referred to in the document,

without the annexation having to be authenticated.

However, there are two exceptions to that general rule – where an annexation is annexed to an electronic document listed in section 1(2) of the Requirements of Writing Act; and where an electronic document which is not listed in section 1(2) but which relates to land has an annexation to it which describes or shows all or part of the land (see 6.1 and 6.2).

Where parties wish to annex/ incorporate something to/into an electronic document that does not fall within the two exceptions (and will be signed using a simple electronic signature), since section 1(2) does not apply, there is no requirement for formal writing and so, for such documents, the parties might choose not to follow the general rule for annexations to electronic documents set out in Regulation 4(1) and to rely instead on the usual contractual principles for incorporation by reference. Exactly how they incorporate by reference will be up to the parties. For example, the parties may choose to incorporate a separate document (B) into an electronic document (A) before document A is signed (in which case document B forms part of document A). In the main body of document A they may refer to (the newly incorporated) document B as being 'annexed to' document A and they may identify (the newly incorporated) document B on its face as being the document which is referred to in the main body of document A. Alternatively, if that is not feasible (e.g. size or file format issues), the parties could keep document B separate from document A but incorporate it by document A referring to document B by name/date/version number etc. It would be good practice to also identify document B on its face as being the document referred to in document A. Incorporation could also be achieved when using an e-signing platform, by including document B in the same envelope as document A, or a separate envelope, as long as document B is clearly referred to in document A. It would be good practice to also identify document B on its face as being the document referred to in document A. Further evidence of incorporation may be provided by applying electronic initials to document B (a feature available on some e-signing platforms). In practice, for electronic documents not falling into either of the two exceptions (see 6.1 and 6.2), the crucial question will be what did the parties agree and are they able to evidence that?

6.1 Exception 1: Electronic documents listed in section 1(2)

Regulation 4(2) of the Electronic Documents (Scotland) Regulations 2014 states that an annexation (e.g. schedule or plan) to an electronic document listed in section 1(2) of the Requirements of Writing Act (see Electronic signatures and the Requirements of Writing Act (3.1)) will be regarded as incorporated if **and only if** the annexation is:

c. referred to in the document,
d. identified on its face as being the annexation referred to in the document, and
e. annexed to the document before an electronic signature under Regulation 2 (i.e. an AES) or Regulation 3 (i.e. a QES) is incorporated into or logically associated with the document and the annexation.

It is unclear what is meant in Regulation 4 by an "annexation" and how in practice an annexation is to be annexed to the electronic document before the electronic signature is incorporated into or logically associated with the document and the annexation. If you are authenticating a document listed in section 1(2) with an AES or (to make it self-proving) a QES then, whether you are using a Law Society Smartcard (or similar signature creation device) or an e-signing platform, the prudent approach is to incorporate all the annexations into the same electronic file (i.e. into the same Word document or PDF) prior to attaching the electronic signature. However, for large documents, file size issues may make this problematic. By complying with Regulation 4 (2), the effect is that the whole document, including the annexations, will be regarded as having been signed by each signatory.

6.2 Exception 2: Electronic documents not listed in section 1(2) but which relate to land and have an annexation which describes or shows all or part of that land

For electronic documents not listed in section 1(2) of the Requirements of Writing Act (see Electronic signatures and the Requirements of Writing Act (3.1)) but which relate to land and have an annexation which describes or shows all or part of that land, the annexation is to be regarded as incorporated in the document if **and only if** the annexation is:

f. referred to in the document,
g. identified on its face as being the annexation referred to in the document, and
h. it satisfies one of two extra conditions set out in Regulation 4(4) of the Electronic Documents (Scotland) Regulations 2014, namely:

- (when using an AES or a QES)

the annexation is annexed to the document before the AES or QES is incorporated into or logically associated with the document and the annexation; or

- (when using a simple electronic signature) the simple electronic signature is applied to (i) each page, where it is a plan, drawing, photograph or other representation, or (ii) the last page, where it is an inventory, appendix, schedule or other writing. (Note: this condition reflects the level of security provided by a simple electronic signature, as compared with that provided by an AES or QES, and mirrors the provisions for traditional documents in section 8(2)(c) of the Requirements of Writing Act).

As is the case for traditional documents, where there is more than one granter, the requirement under Regulation 4(4) (b) (ii) of signing on the last page is complied with (provided that at least one granter signs at the end of the last page) if any other granter signs on an additional page.

7. Self-proving status

7.1 Witnessing an electronic signature

It is misleading under Scots law to refer to 'witnessing' an electronic signature. Scots law does not recognise the concept of witnessing an electronic signature in the same way that special status is attributed to witnessing a traditional document. 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] . 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 electronic 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.

7.2 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 Witnessing an electronic signature (7.1)).

7.3 Is a self-proving signature required?

In certain sectors, the usual practice by solicitors is to seek to obtain a self-proving signature even if that is not legally required. Whether this is necessary should be considered on a case by case basis. Although certain documents will require it (e.g. those which need to be registered), there may be many circumstances where a self-proving signature is not necessary in which case a simple electronic signature would suffice. At the time of writing it is not possible to register electronically signed documents in the Land Register of Scotland, or the Register of Sasines. However the Register of Deeds (in the Books of Council and Session) is now able to accept electronically signed documents, with effect from 1 October 2022. Such deeds require to be self-proving. For further considerations, see Risk assessment (9.2).

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

8. The signing process

Please note in developing this guide, we had assistance from major e-signing platforms. However, every e-signing platform is different, and you need to check the functionality and configuration options with your provider in advance.

8.1 Agreeing to sign electronically

In a practical sense, it is helpful if contracting parties agree in advance whether the document may be signed using electronic signatures. However, it is not necessary to include a provision in the document referring to the parties' agreement to execute electronically. 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].

8.2 Sending electronic documents to a party who is not your client

8.2.1 Sending electronic documents to another law firm's client

Where a document is being set up for electronic signing, the document should not be sent directly to another law firm's client for signature without an agreement between the solicitors to do so being in place. The Law Society of Scotland Standards of Conduct B1.14.2 states: "You may only communicate with a person known or believed to be the client of another regulated person ("the other regulated person") if: (a) The other regulated person has agreed to the communication". If using an e-signing platform, the easiest way of complying with this is to obtain the other law firm's agreement to your sending the document directly to their client via the platform. You are likely to be agreeing the signing process with that law firm anyway and you can obtain consent as part of that. If for any reason consent is not given – for example the other firm wants to review the document within the signing platform before their client signs it – you will need to include an additional step in the signing process. Check the platform's functionality but, broadly speaking, the signatory's lawyer should be placed before their client in the signing order. The signatory's lawyer should be asked to 'approve' the document before the platform will release it to their client for signing. This allows the solicitor to check and confirm that the document uploaded for signing is the agreed, final form version. The solicitor's approval and the signing order will be recorded in the signing certificate.

8.2.2 Sending electronic documents to an unrepresented party

In the same way as when organising the signature of hard copy documents, the Law Society of Scotland Rule B2.1.7 applies to sending electronic documents for signing by unrepresented parties. Remember that solicitors must inform such parties in writing that:

a. their signature may have certain legal consequences, and
b. they should seek independent legal advice before signing.

8 .3 Date and place of signing

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. However, the date and place of signing could be used for evidentiary purposes should a dispute occur regarding the identity of the signatory or the circumstances of the signing process.

8.3.1 Place of signing

This might be embedded or discoverable from certain types of electronic 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. Including the place of signing might 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. Including the place of signing might also be relevant for tax purposes. Therefore, parties may wish to include the place of signing for evidential purposes. Alternatively, where there is no requirement for the place of signature to be established, parties may choose to omit reference to it in the signature block of a document to be signed electronically.

8.3.2 Date of signing

If using an e-signing platform, the date of signing will be recorded and stored within the electronic document. The date will not be visible if the electronic document is printed, but e-platforms will include the date of signing in the audit trail certificate that they provide. The date of signing will not be recorded in the document where an electronic document is signed using other types of simple electronic signatures (e.g. if a party cuts and pastes a scan of their handwritten signature into a document). Parties may wish to include the date of signing for evidential purposes. Some e-signing platforms offer a date/time field which automatically inserts the date/time but check before using this whether this reflects the appropriate time of signature (e.g. this could reflect the time when the recipient first views the document rather than the time of signing, or the date/time could be that on the signatory's local

[7] The only electronic documents signed with electronic signatures which can currently be registered in the Land Register of Scotland are residential electronic discharges, submitted via the Digital Discharge Service. The Register of Deeds now accepts electronically signed documents provided they are self-proving.

computer). An e-signing platform may offer the option to insert a text field which can be completed during the signing process with the date on which the signatory signed. If the date inserted in this field conflicts with the date recorded by the platform, this may create doubt around the actual date of signing. Where there is no requirement for the date of signature to be established, parties may choose to remove reference to it in the signature block of a document to be signed electronically.

8.4 Documents which require to be delivered

Paragraphs 8.4.1 to 8.4.5 relate only to documents which require to be delivered under Scots law (e.g. an intimation of assignation). For documents which do not require to be delivered (e.g. mutual agreements), see Documents which do not require to be delivered (8.5).

8.4.1 Documents which require to be delivered - 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.

8.4.2 Documents which require to be delivered - 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 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. If using an e-signing platform, the order of signatures can be set up in the platform, which then sends the documents round to each party in order. The platform can be configured to notify everybody when the last signature is applied. In the absence of a contrary agreement, delivery would take place at the point of notification.

8.4.3 Documents which require to be delivered - Holding documents as undelivered

It is possible to hold a signed document as undelivered until such time as the signatory confirms it is delivered, or until some condition has been satisfied. This could be achieved either by:

- Using functionality available on the e-signing platform; or
- Having an email exchange between the parties

Care should be taken with any defined terms relating to date to ensure that they do not cut across or become confused with the delivery date.

8.4.4 Documents which require to be delivered - Using functionality on the e-signing platform to control delivery

In some e-signing platforms, the signing process can be set up to assign a final role to a solicitor, which allows them to date the document after the last signature has been applied and before the signed document is released to the signing parties. For example, the final step in the signing order could be to require a solicitor to add the agreed date of delivery. The parties could agree in advance that the solicitor would only add that date when all parties had agreed that they could do so. There would then need to be a further email exchange confirming that date. Alternatively, the parties could agree in advance that the solicitor would add a specified agreed date. The e-signing platform would record and certify that the final step had been taken. This would enable the parties to control the date on which the electronic document that requires to be delivered is treated as delivered. All email chains should be stored with the electronic document.

8.4.5 Documents which require to be delivered - Using email exchange to control delivery

Where a document is signed electronically without using an e-signing platform, the parties/ their solicitors could agree by email exchange that the document will not be treated as delivered until all the parties agree. There would then need to be a further email exchange confirming that date. Alternatively, the parties/their solicitors could agree by email exchange that the document will not be treated as delivered until a specified date. Parties must be diligent in storing the supporting email exchanges with the signed electronic document as the risk is that this email evidence becomes separated from the signed document over time. Using an e-signing platform to control the delivery date of the document (as described in 8.4.4) means this risk is avoided. If the document contains an entire agreement clause, consider whether that clause extinguishes the previous agreement regarding the delivery date made by the parties over email. If so, the clause wording may need to be amended to exclude this agreement.

8.5 Documents which do not require to be delivered

Paragraphs 8.5.1 to 8.5.3 relate only to documents which do not require to be delivered under Scots law e.g. mutual agreements. (For documents which require to be delivered, see Documents which require to be delivered (8.4)) For a document that does not require to be delivered under Scots law, the default position is that it will come into effect when the last party has signed it. 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. Once the last party has signed, the system can be configured to inform everyone that it has been signed by all parties. In the absence of any agreement to the contrary (see 8.5.2 or 8.5.3 below), the document would come into effect when it is last signed. If the parties do not want this to happen, their solicitors will have to agree in advance how to control the date when the document comes into effect. It is possible for contracting parties to do this. One of the essentials for a contract is an 'intention

to be bound': the parties may not intend to be bound when the last party signed the document but to be bound, instead, with effect from a later point. If the parties agree to delay the coming into effect of such a document, this agreement must be made before the last party signs the document. See Documents which do not require to be delivered – delaying their coming into effect (8.5.1).

8.5.1 Documents which do not require to be delivered - delaying their coming into effect

This could be achieved either by:

- Using functionality available on the e-signing platform; or
- Having an email exchange between the parties.

Care should be taken with any defined terms relating to date, to ensure that they do not cut across or become confused with the date which the parties agree the document will come into effect. In particular, it should be made clear that the date of signature by the last party to sign is not the same as the date the document comes into effect.

8.5.2 Documents which do not required to be delivered - Using functionality on the e-signing platform to control coming into effect

In some e-signing platforms, the signing process can be set up to assign a final role to a solicitor, which allows them to date the document after the last signature has been applied and before the signed document is released to the signing parties. For example, the final step in the signing order could be to require a solicitor to add the agreed date of the document coming into effect. Solicitors for the contracting parties will need to consider what adjustments need to be made to the document's operative wording in order to achieve this. One option is to include an additional operative clause in the document to confirm the parties' intention with respect to the date on which the document should come into effect. The clause could appear immediately before the testing clause/signature blocks, and state that notwithstanding the date when the document is signed by all the parties, it does not come into effect until the date set out in the testing clause. The parties could agree in advance that the solicitor would only add that date when all parties had agreed that they could do so. There would then need to be a further email exchange confirming that date. Alternatively, the parties could agree in advance that the solicitor would only add a specified agreed date. A text box would be inserted at the appropriate place in the document for the solicitor to add the date on which the document comes into effect. The e-signing platform would record and certify that the final step had been taken. This would enable the parties to control the date on which the electronic document comes into effect. All email chains would need to be stored with the electronic document.

8.5.3 Documents which do not require to be delivered - Using email exchange to control coming into effect

Where a document is signed electronically without using an e-signing platform, the parties/ their solicitors could agree by email exchange that the document will not be treated as coming into effect until all the parties agree. There would then need to be a further email exchange confirming that date. Alternatively, the parties/their solicitors could agree by email exchange that the document will not come into effect until a specified date. Any such agreement must be made before the last party signs the document. Parties must be diligent in storing the supporting email exchanges with the signed electronic document as the risk is that this email evidence becomes separated from the signed document over time. Using an e-signing platform and the best practice method in 8.5.2 above to control the date when the document comes into effect means this risk is avoided. If the document contains an entire agreement clause, consider whether that clause extinguishes the previous agreement regarding when the document becomes effective made by the parties over email. If so, the clause wording may need to be amended to exclude this agreement.

8.6 Dating the document

8.6.1 Where all parties use the same e-signing platform

Under Scots law, when all parties use the same e-signing platform to sign a document, the effective date and/or date of delivery will be either (for documents which do not require delivery) when it is last signed or (for documents which require delivery) when the platform releases the signed version to everyone (in each case unless otherwise agreed). See Documents which require to be delivered (8.4) and Documents which do not require to be delivered (8.5). 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.

8.6.2 Where an electronic document is executed in counterpart

See When are electronic documents signed in counterpart (12.3)

9. Verifying an electronic signature

9.1 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 Legal Writings (Counterparts and Delivery) (Scotland) Act 2015 which allows delivery of a traditional document to be made by electronic means. When opening a PDF in Adobe Acrobat or Adobe Reader, if the document has been signed using an e-signing platform, a 'signature panel' may appear at the top corner. That will provide validating information about the signature, the content of which will depend on the type of electronic signature applied. For example, the signature panel will state that it is a "qualified electronic signature" if a QES has been used. If no signature panel appears, then it may be that the document has been signed without using an e-signing platform and using another kind of simple electronic signature, such as a scan of a handwritten signature. It may be prudent to check with the signatory (or their solicitor) directly if you are not sure what kind of signature has been applied to the document you are looking at. Where an e-signing platform has been used, another source of validation of an electronic signature is the audit trail (for example, the Certificate of Completion in DocuSign eSignature or the Audit Report in Adobe Sign) that often accompanies the electronically signed document and/or is present in the e-signing platform that was used to sign the document. Different levels of information may be available for an electronic signature depending on the type of electronic signature (e.g. simple, AES or QES) and on the options that the user of the platform may have set on the electronic signature platform. For documents signed with a Smartcard, see the Law Society Smartcard practical advice guide for QES information.

9.2 Risk assessment

If the electronic 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 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.

In many cases a simple electronic signature (e.g. using the standard functionality provided by an e-signing platform) suffices. While AES and QES provide a greater level of assurance in relation to the identity of the signatory, consider industry practice, regulatory requirements and the likelihood of litigation, together with the user experience/ease of use and costs when deciding whether that type of signature is needed.

9.3 Evidential weight

While UK 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 may be easier to do with an AES or QES compared with a simple electronic signature, but a simple electronic signature applied through an e-signing platform coupled with the audit trail can often provide an adequate level of certainty.

9.4 Reliance on simple electronic signatures

The level of reliance which a contracting party can place on a simple electronic 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 standard 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. A user should consider what type of metadata is stored with the electronic signing platform to see if it provides sufficient evidence that the person you thought was signing did in fact sign (e.g. date, user account who signed, location of signature, etc.). Some e-signing platforms offer additional security measures such as two-factor authentication e.g. 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 e.g. how robust is the information provided, can you rely on the platform in future, how does the platform authenticate the signatory) and check with the provider. It may be that they can offer advanced functionality which would satisfy the requirements for an AES or QES.

9.5 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 impact or prevent electronic signing. To ensure ex facie validity, the capacity of the signatory (e.g. director, secretary, authorised signatory) should be evident from the face of the signed electronic document.

10. 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 electronic 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. Because it is possible to have and share duplicate originals of an electronic document, there should be little or no need to create 'certified copies'. If, however, a certified copy is required (e.g. a registration requirement where the registrar cannot accept electronically signed documents or there is a requirement to provide the document in hard copy form), a certified copy of an electronic document may be created. Consider what form of wording would be appropriate for the certification statement.

11. Storing documents that have been electronically signed

11.1 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. Where a document has been executed through an e-signing platform (or the parties have otherwise all applied their electronic signatures to a single electronic document), there is one electronic document. Where an e-signing platform is used, all participants to the signing process can access the electronic document on the platform, and they also automatically receive the completed signed document for their records. They should also receive the audit trail certificate, which provides the meta data collected by the e-signing platform in relation to each signature. Where a document has been executed by electronic means, 'duplicate originals' of that document can be created so that each party can have its own electronically signed document and store duplicates. For example, a party or their solicitor might download a copy of the document from the e-signing platform and save it to their own document management system, or, where an e-signing platform has not been used, the signed electronic document could be circulated among the parties. 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) documents 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. As mentioned above, where an e-signing platform has been used, each signatory will already have their own 'original' of the document. 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 along with the metadata on the signature provided by the e-signing platform (see Storing the electronic signature data (11.2)). In addition, each contracting party should be provided with, and advised to retain, the electronic document.

11.2 Storing the electronic signature data

Where a document has been signed electronically, it is possible to create multiple 'duplicate originals'. Where an e-signing platform or Smartcard has been used, certification data relating to the signatures should be obtained and retained by all those holding the electronic document. For example, where a document is signed in Microsoft Word or Adobe Acrobat using a QES (e.g. a Law Society Smartcard) or the signatory's QES has been applied to a document using an e-signing platform, 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 where an electronic signature other than a QES is being used, 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 printout 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 in the form of an audit trail certificate or report. 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 electronic 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 parties agree

to delay the delivery date or the coming into effect of the electronic document, information about that will also need to be stored with the electronic document. Read Date and place of signing (8.3), Documents which require to be delivered (8.4) and Documents which do not require to be delivered (8.5).

11.3 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.

12. Counterpart signing and electronic documents

12.1 Can some counterparts be signed electronically and some in wet ink?

This is possible and envisaged by the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015 (section 3(1)). Note 15 of the Explanatory Notes to the Act 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 requisite type of electronic signature would need to be applied. For examples of when this can arise, see When are electronic documents signed in counterpart (12.3).

The Register of Deeds accepts mixed media documents [8].

12.2 What constitutes the "single" document?

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 (i) in mixed media (i.e. at least one with an electronic signature and at least 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". At the time of writing, it does not appear to be possible to merge counterparts from different electronic sources into a single file without losing the e-signature metadata. Therefore, in this situation it is not possible for the single document to consist of one counterpart in its entirety, collated with the signature pages of the other(s). All electronic counterparts in their entirety will make up the single document.

[8] See the 'QES guidance for customers' section in the Register of Deeds guidance on the Registers of Scotland Knowledge Base

12.3 When are electronic documents signed in counterpart?

There are four scenarios, outlined below. Scenarios 1 and 2 do not constitute counterpart signing. Counterpart signing occurs in Scenarios 3 and 4.

Scenario 1: Signing via a single e-signing platform

Where an electronic document is set up 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. (But if one party selects the print and sign option in the platform, that results in execution by counterpart – see scenario 3.)

Scenario 2: Single electronic document, sequential execution

Where a single electronic document is signed electronically by each party in turn without the use of an e-signing platform, this is not execution in counterpart. For example, a single PDF document may be circulated among the parties for sequential execution by each party applying a JPEG scan of their signature. This is a single document which each party signs electronically.

Scenario 3: Multiple electronic counterparts, separate execution

These scenario 3 examples constitute counterpart execution. Counterpart execution would occur when separate electronic counterparts of the same document are sent to the signing parties. For example: (a) Two or more electronic counterparts are circulated separately, with at least one party receiving its own counterpart for signature. The counterpart may be signed for example by each party affixing a simple electronic signature to their own separate counterpart; (b) Contract parties sign identical counterparts using different e-signing platforms; or (c) Identical counterparts are sent for signing via a single e-signing platform but in a separate envelope for at least one signatory; or (d) Identical counterparts are sent for signing via a single e-signing platform in a single envelope using a separate counterpart for at least one signatory.

Scenario 4: "Mixed media" (at least one in electronic form and at least one in traditional (hard copy) form)

This scenario 4 example constitutes counterpart execution. Parties can execute in "mixed media". One party receives (or prints out) a hard copy to sign in wet ink while the other applies their electronic signature to an electronic document. Mixed media execution occurs when an e-signing platform is used if one party selects the "print and sign" option (they will print out a copy and sign in wet ink) while the other applies their electronic signature within the platform.

12.4 Consequences of counterpart execution where at least one counterpart is an electronic document

Counterparts must be delivered in order to become effective. The parties will need to agree in advance how to effect, manage and evidence the date of delivery.

For example, if a party has affixed an electronic signature to a Word or PDF document, and exchanged it as a counterpart, 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. 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 complete signed document. Care will need to be taken with any definitions of date to ensure they do not cut across or become confused with the delivery date. See Documents which require to be delivered (8.4).

In the case of mixed media counterpart execution, the counterpart in traditional form can be delivered electronically in accordance with section 4 of the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015. This section allows the delivery requirement to be satisfied by delivery of part of the document (which must include the signed signature page). For guidance in relation to the delivery of electronic documents see paragraph 8.4.2.

For counterparts in electronic form, there is no provision in the Act allowing delivery of part. This should be borne in mind where large file sizes are involved e.g. because of multiple annexations.

13. Quick links

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

Law Society of England & Wales and CLLS Note on the execution of a document using an electronic signature October 2022

Law Society Guidance on The Ownership and Destruction of Files

Law Society Guidance on Scanning and Archiving Documents

Law Society Smartcard practical advice guide

Authors

This guide was written by the Electronic Signatures Working Group of the Law Society of Scotland's Technology Law and Practice Committee.
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.

Please send any feedback to: antonymcfadyen@lawscot.org.uk

In association with Denovo

Denovo's whole practice management solution, CaseLoad, incorporates Case Management, Legal Accounts and Cashroom Services into one integrated system, with the ability to have all data available and shared between the different areas of your law firm. Denovo's aim is to provide smart, simple, time-saving and bespoke solutions to fit your needs, while being flexible enough to change and grow as you and your team evolves. Their case management system allows law firms to operate in a realistic fashion – customisable to the way your practice works.

The inclusion of e-signature in CaseLoad means that you can now complete approvals and agreements in minutes or hours – not days. Experienced users are reporting that, from sending the onboarding pack out electronically, 65 per cent of clients are responding within the first two hours and 85 per cent within 24-48 hours. The best bit... CaseLoad allows you to bypass the challenges firms face while setting up e-signature yourself, no hassle and 100 per cent compliant with the legal requirements of electronic signing processes. Meaning Denovo partner with e-Signature platforms that provide a qualified electronic signature (QES), the most secure type of signature as it involves the signatory's identity being verified by a qualified trust service provider before the signatory is issued with a QES. Allowing you to send documents out for signature in seconds, to single or multiple signers and even use their Smart Events feature or workflows to automate a whole package of documents in the one action. Information clients add to the documents can also be sent back to the case management system, not only are the signed documents returned to the file automatically, you can also collect data from the client which goes straight into the file.

For more information visit:
www.denovobi.com

Or contact us at: info@denovobi.com Phone: 0141 331 5290

denovo
Whole Practice Management Software

Law Society of Scotland

The Law Society of Scotland
Atria One
144 Morrison Street
Edinburgh
EH3 8EX
T:+44(0) 131 226 7411

www.lawscot.org.uk