THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

# Profession Practice Advice for the Profession

The Society has recently introduced Smartcards for the Scottish legal profession.

If you have queries in relation to the administrative process for obtaining and activating a Smartcard you will find helpful advice here www.lawscot.org./smartcard.

## Practical Advice Guide

The purpose of this guide is to provide further practical advice to using your Smartcard after it has been activated.
This guide and corresponding FAQs will to continue to evolve as members begin to use their Smartcard and as legislation and practice develops.

Smartcards provide the opportunity to use digital signatures within the profession. While the advent and use of digital signatures is not new, it is still relatively underutilised and untested within legal practice and so this guide is designed to support solicitors by providing some further explanation and resource around using the Smartcard digital signature facility.

This guide 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. It is hoped however that this guide will assist solicitors in accessing and using their Smartcard

The Society welcomes any comments on the guidance and would be pleased to hear from members with comments or useful additions and amendments to it.

| **VERSION CONTROL** | | | |
|---|---|---|---|
| **Version number** | **Date approved** | **Approved by** | **Superseded** |
| v1.2 | 29 August 2014 | NS | V1.1 |
| v1.3 | 03 June 2014 | NS | V1.2 |
| *NB. During the early stages of deployment we will be updating this guidance regularly to best support. Please always check you are using the latest version by checking the version number against our website at www.lawscot.org.uk/smartcard* | | | |

The Law Society of Scotland
26 Drumsheugh Gardens
Edinburgh EH3 7YR

T +44(0) 131 226 7411
F +44(0) 131 225 2934
E smartcard@lawscot.org.uk

www.lawscot.org.uk/smartcard

@lawscot TheLawSocietyofScotland The Law Society of Scotland

THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

## THE STRUCTURE OF THIS GUIDE

### A. INTRODUCTION AND BASICS

- The purpose of the Smartcard
- Electronic Signatures
- What is a secure digital signature?
- How is the digital signature created?
- How do I apply my Smartcard digital signature?
- How does a signature appear on the document?
- How do you know if you can to trust a digital signature?
- Are digital signatures legally binding?

### B. USING YOUR SIGNATURE

- Why might I use a digital signature?
- What sorts of things are digital signatures used for?
- Should I sign emails with my digital signature?
- Can I change the file name of a digitally signed document?
- My client and I would like to use digital signatures but the solicitors on the other side do not wish to. Can the Society do anything about this?
- I would like to use digital signatures and Smartcards in my next transaction. What do I need and what should I be considering?
- It's fairly common in our firm's busy office that other solicitors, trainees and secretaries will PP documents or apply signatures on behalf of those who are absent from the office on other business matters. Provided I give direct authority and direction can I utilise the digital signature and Smartcard in the same way?
- Does the digital signature in the Smartcard provide any greater or enhanced certainty or security over a manual or wet signature?
- When is a bargain concluded when I issue an electronic document?
- Can a document be digitally executed by one party but wet or manually signed by another?

- Should multiple copies of all digital documents be executed to create multiple signed original copies one for each party?
- Is it the case that a digitally signed document is evidentially 'worthless' if printed off? i.e. a hardcopy print does not have the same probativity as the soft copy because the hardcopy cannot demonstrate the certification authority chain?
- What about digital signatures of clients acquired from third-party providers which do or do not meet legislative requirements?
- How does appending a digital signature interact with the practice of certifying documents as true and accurate copies?
- When applying a digital signature to a 200 page document with a plan and 30 appendices do I sign once applying a signature to the entire document or do I have to sign multiple times?
- At a practical level, will the system allow signatures to be added to all types of documents, regardless of the package on which they were created – for instance can a Word document be digitally signed as well as a PDF? Will a range of PDF packages work?

**C. DIGITAL SIGNATURES IN CONVEYANCING TRANSACTIONS**

- What steps should solicitors take to preserve a copy of digital missives or indeed in any digitally executed contract ?

**D. DIGITAL SIGNATURES IN COURT MATTERS**

- How do you submit a digitally executed document to a Court?

**E. GLOSSARY (working definitions)**

THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

# A. INTRODUCTION AND BASICS

The Smartcard is issued by the Law Society of Scotland and in the future will replace the existing practising certificate. The Smartcard will operate as:

(1) a form of photographic ID

(2) live electronic ID and

(3) as a secure digital signature.

The Society's services will increasingly use and accept digital signatures, and over the coming years, further functionality will be delivered using the Smartcard.

### The purpose of the Smartcard

The practicalities of the Smartcard operating as a photographic ID and allowing for easier access to courts and prisons, for example, are self-evident as is the operation of the Smartcard providing real time confirmation of the credentials and status of a solicitor since the inclusion of a signature in an email or a document confirms that the person was, at the time of sending, a practicing Scottish solicitor.

However, the area where understanding may be less clear relates to the use of the Smartcard secure digital signature facility. This guide endeavours to explain this process further as well as answer some of the queries that use of the Smartcard digital signature gives rise to.

### Electronic and digital signatures

The use of electronic or digital signatures is not new and has developed globally over the years. The Society's strategic technology partner for the project has issued digital signatures to lawyers for over a decade and through over 70 bar associations in Europe. Notwithstanding that electronic signatures are utilised by the public, banks and retailers in many everyday transactions, its use within the legal profession in Scotland is still relatively small.

An electronic signature, or e-signature is considered a fairly generic term which simply provides approval to a process or transaction. Many electronic signatures have the ability to ensure the identity and authenticity of the document as well as the individual.

As a generic term electronic signatures vary widely in their sophistication and use. They can extend to signing a handwritten signature on an electronic pad, for example signing for mail, or for shopping to be delivered. It might be interpreted as clicking a 'submit' or 'buy' button on a website or using a four-digit PIN to withdraw cash from an autoteller. It might also be an electronic or digital signature which is cryptographically tied to a digital identification or certificate.

THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

**What is a secure digital signature?**

There are generally considered to be a hierarchy of three main types of electronic signature, each considered to be of increasing certainty and security, all of which are acknowledged in the EU Directive on electronic signatures:

**1) The electronic signature**

This is data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication.

**2) The advanced electronic signature.**

This is data which meets the following requirements:

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

**3) The qualified digital signature**

This is data which must in particular include:

- an indication that it is issued as a qualified certificate;
- the identification of the certification service provider;
- the name of the signatory;
- provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- signature-verification data corresponding to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate;
- the identity code of the certificate; the advanced digital signature of the issuing certification service provider.

***Electronic vs digital*** – in this document we tend to use electronic signature to mean the wide group of electronic signature that people may use, and digital signature to mean the qualified digital signature issue by the Law Society of Scotland and applied by using your Smartcard.

***What does the 'qualified' element of this term mean?*** It means it is a signature which 'qualifies' by meeting certain stringent legal requirements which includes a publicly available certification policy, covering certain key matters, so that anyone can check the status of the signature. It is the highest level of signature and security recognised in most jurisdictions.

The Law Society of Scotland
26 Drumsheugh Gardens
Edinburgh EH3 7YR

T +44(0) 131 226 7411
F +44(0) 131 225 2934
E smartcard@lawscot.org.uk

www.lawscot.org.uk/smartcard

@lawscot TheLawSocietyofScotland The Law Society of Scotland

***Why are 'certificate' and 'signature' both used as terms?*** The 'qualified certificate' is the document that proves ownership of a public key. The public key is used to check that a digital signature (created using a private key) is valid. So, ownership of a qualified certificate is what lets you apply a qualified digital signature.

It is a qualified certificate or digital signature which the Law Society of Scotland has chosen to provide to all practising solicitors.

**How is the digital signature created?**

The digital signature is created with asymmetric codes (also known as asymmetric cryptography or public key system). These are commonly called the public and private keys. Although different, the two parts of this key pair are mathematically linked.

The private key, which is known only to the signatory, is used to create the digital signature and to change the message into encrypted form.

The public key is used by a receiving party to verify the digital signature and decrypt the message.

**How do I apply my Smartcard digital signature?**

The signature can be applied using mainstream business IT packages such as Word and Adobe. The functionality is built into these programmes (although you will need to ensure your settings and installation choices mean this functionality is live).

*A technical guide on how to apply a signature is available at: www.lawscot.org.uk/Smartcard*

**How does a signature appear on the document?**

It may appear on printed versions or on screen as a box detailing who signed the document, their email address, the date and timing of the signature and some other information.

In some packages, a user can also set an image to represent their digital signature, and this could be a version of their wet signature or corporate seal. Hovering over or clicking the signature will reveal the digital signature attributes, as will use of the relevant menus within the particular package (like Word or PDF). Solicitors will need to consider how they examine all types of "signature" on electronic documents to ensure they understand its status.

However, it is important to understand that visual representation is NOT the signature.

The signature will be a clickable link – within the menu, title bar or document which links through to a range of information on the digital certificate/signature. Again, our technical guide (available and

www.lawscot.org.uk/smartcard) covers this for the most commonly used software packages. However, solicitors should note it is that data, and not any visual representation on the 'face of' the document which they need to check.

**How do you know if you can to trust a digital signature?**

This is an important question which links to queries around 'how to do you know if a signature was really signed by the person who says they signed it?', and 'how do you know the document hasn't been changed'.

It is worth noting that even when using manual signatures, uncertainty can arise as to the validity and identity of the signature and the authenticity of the document so such concerns are not exclusive to electronically signed documents.

Nevertheless, there is a number of ways of enhancing certainty and security and the Smartcard provides for a digitally secure signature which can provide the highest level of assurance.

The main components of creating certainty and trust around the digital signature can be broken down into four elements:-

1. ***Authentication*** *– How did the individual verify their identity within the 'transaction'?*
   The digital signature should be unique to the signatory and created by a means that only the signatory can operate. For example, a strong authentication process will not simply permit a user to click a button without first entering a password or a code and using a 'physical token' which should only be in their possession (in this case, the Smartcard).

   The Smartcard authentication process seeks to ensure confidence, confidentiality and authenticity by using cryptography technology.

2. ***Vetting*** *- How was the identity of the individual assessed by the regulatory authority and system?*
   The Smartcard process requires a face to face meeting with every solicitor at which that solicitor's identification and photograph are checked against our database thus providing far greater certainty than simply accepting a photograph posted to the Society or by filling in an online form. Those seeking to rely on a digital signature provided by a member of the Society can be reassured that the Society has implemented the highest levels of authentication and identity in implementing the Smartcard.

3. ***Registration and Certification –*** *How do I know I can trust the vetting system and the integrity of the authentication?*

   To be a qualified digital signature there must be a Certification Authority which publishes a Certification Policy which meets certain legal requirements (for your Smartcard, the Certification Authority is Abogacía Certification Authority / ACA, operated by RedAbogacía). The signature must then be issued by a recognised Registration Authority (for your Smartcard, the Society itself is the Registration Authority).

   The Society holds a live register of its members. If practice is suspended or cancelled then the Society can also instantly terminate the signature (like with a bank card, when the person next inserts their card in a machine the signature will be suspended/cancelled before any other transaction can take place).

   Signing systems such as the one being used by the Society through Smartcard offer one of the highest levels of assurance available.

4. ***Certainty and Integrity*** *- How do I know when the digitally signed document was signed and that the digitally signed document has not been altered in some way since it was signed?*

   The Society has adopted cryptographic calculations which operate a mathematical calculation within the software. Essentially this operates as a key which gives only the person signing the document access. The date stamp applied to the signature is generated by the communication with e Certification Authority and cannot be altered.

   By using this technology, a certificate is produced which adds a further layer of certainty and authentication to the signature.

All these elements create a ‘circle of trust’ which is fundamental to the operation of a digital signature infrastructure.

THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

**Are digital signatures legally binding?**

Electronic signatures are widely used and legally binding in the majority of countries worldwide. The European Directive 1999/93/EC of 13 December 1999 established a community framework for the use of digital signatures on electronic contracts in the EU. The signatures are legally admissible as evidence in legal proceedings and enforceable in the European Union. There are key issues to consider around signature authentication, but broadly using a digital signature is legally binding. In the UK the UK Electronic Communication Act 2000 establishes the legality of digital signatures. Regard should also be given to the Requirements of Writing (Scotland) Act 1995.

The question does raise further queries around how a third party such as a court or fellow solicitor might receive and respond to a document verified through digital signatures and this is considered in further in the FAQ's.

The Law Society of Scotland
26 Drumsheugh Gardens
Edinburgh EH3 7YR

T +44(0) 131 226 7411
F +44(0) 131 225 2934
E smartcard@lawscot.org.uk

www.lawscot.org.uk/smartcard

@lawscot TheLawSocietyofScotland The Law Society of Scotland

# B. USING YOUR SIGNATURE

**Why might I use a digital signature?**

There are many reasons why a solicitor might adopt this process. It may be more efficient and make for faster workflow. It may be driven by client demand. Making use of a digital signature which is self-proving (which the Law Society of Scotland Smartcard signature is) may provide more efficiencies for your business. Some may consider it provides greater integrity within the document and it may prove to be a positive technological development within a firm.

Using the digital signatures facility in your Smartcard is not mandatory and solicitors should use professional judgement as to the convenience and appropriateness of doing so.

It is also clear that this is an area of law that is relatively untested within Scotland and it is only with practice and experience that further case law and knowledge will be developed.

The degree of certainty and mode of signing adopted by solicitors will depend on the degree of authenticity and level of risk assessed for the transaction and the client and it will be for solicitors to form a judgement as to whether circumstances merit the use of a digital or a manual signature. It is recognised that not all situations may be suitable for using a digital signature but in others it may provide significant benefits in terms of cost and time.

**What sorts of things are digital signatures used for?**

In many respects and digital signature can be used in the same way that you manually sign a document. It might be applied to:-

- Contracts
- Conveyancing transactions
- Trust Deeds
- Financial instruments and share dealings
- Confirmation advice has been given on a compromise agreement (employment)
- Commercial contracts and leases
- Company documents (acting as secretary or company director)
- Statements to police / investigating authorities
- Licences on behalf of clients
- Trademark/patent applications on behalf of clients
- Submissions to local authorities on behalf of clients – planning, licensed trade, etc.

This guide provides some further questions which have been grouped as general questions about using digital signatures in documents generally. Thereafter the guide considers the use of digital signatures in conveyancing and in relation to court and litigation matters.

**Should I sign emails with my digital signature?**

For a formal legal letter, document or contract it is recommended that solicitors create a Word or PDF document and sign this. This creates a standalone document, which reduces the risk of confusion from long email chains, conflicts arising from email footer/disclaimer information and so provided greater clarity on what is being signed.

However, quickly signing and email, with a statement such as 'this signature is only attached to provide confirmation of my identity and status as a practising solicitor' is a quick and easy way to absolutely verify your details to another solicitor. This can be done within the body of an email text. .

**Can I change the file name of a digitally signed document?**

No. In most cases this is not possible, as all attributes of the contract are 'locked' to ensure an original version. If the file is saved under a different name the signature is likely to be invalidated. To manage this within cases management systems there are a number of options – such as creating a folder following your normal filing convention and then saving the actual file, with the name unchanged, into that folder, or saving the email, with the document attached, as changing the name of the email will not affect the document.

**My client and I would like to use digital signatures but the solicitors on the other side do not wish to. Can the Society do anything about this?**

Using digital signatures are not mandatory and the Society has no locus to intervene in a matter such as this. It would be a matter for negotiation amongst the solicitors and parties involved. You may wish to share this guide with them to further their understanding of the process.

**I would like to use digital signatures and Smartcards in my next transaction. What do I need and what should I be considering?**

Firstly, you should consider with your client and with the other parties to the transaction whether they are agreeable to this and consider any matters that require clarifying. The Smartcard is being rolled out in a gradual process and not all Scottish practitioners will have a Smartcard at the present time. You should also consider the matter with the client and consider if there is any further legal advice the client requires in this regard.

On a practical level, you will receive a card reader when you activate your Smartcard and this will enable you to put a digital signature on relevant documents.

You should also consider the longer terms aspect of the transaction and account in your Terms of Engagement for how matters will be dealt with.

You should consider including clarification on items relating to digital signature and storage, for example:

a)how original documents are retained by the practice unit;

b) risks associated with electronic retention;

c) the practice unit's policy in relation to retention of electronic documentation, for example, whether the electronic or scanned documents will be retained beyond the Society's recommended retention periods or not; and

d) providing the client with advice that the client should also retain the document electronically and without alteration.

**It is fairly common in our firm's busy office that other solicitors, trainees and secretaries will PP documents or apply signatures on behalf of those who are absent from the office on other business matters. Provided I give direct authority and direction can I utilise the digital signature and Smartcard in the same way?**

No. This would be a misuse of the card and could give rise to fraud and is not permitted

**Does the digital signature in the Smartcard provide any greater or enhanced certainty or security over a manual or wet signature?**

A wet or manual signature, on its own, does not guarantee the identity or the professional status of the person signing the document. There are different risk issues around wet or manual signatures and digital signatures, and their use in different circumstances, but in many settings a digital signature will offer great certainty and security. The signature also 'locks' the document and prevents any amendment, compared to a paper contract where a page could, for example, be careful removed and replaced depending on the method used to secure pages together.

**When is a bargain concluded when I issue an electronic document? Is it when I dispatch a digitally executed document by e-mail or is it when it is received by the recipient? Supplementary questions in that regard arise should there be any error in the e-mail address which might still mean that it is delivered to the correct business but not to the individual recipient?**

There is no law on what constitutes the point of delivery of an electronic document. However, commentary on creation of contracts by electronic means refer to "transmission" and "delivery" which supports the view that the contract is concluded when the document is received by the recipient, not at the point of dispatch by the sender.

This approach is in line with the general rule that "an acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror" - *Article 18 of the UN Convention on Contracts*

*for the International Sale of Goods (1980) provides as a general rule that "an acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror"*

In the interests of certainty, it would be advisable to state within the contract itself when the parties intend for delivery to be effected

**Can a document be digitally executed by one party but wet or manually signed by another?**

Once The Legal Writings (Counterparts and Delivery) (Scotland) Bill is enacted in its current form a document can be digitally executed by one party and wet/ manually signed by another but only in counterparts as defined in the said Bill.

Electronic documents in terms of ARTL will continue to be dealt with in terms of that specific regime.

**Should multiple copies of all digital documents be executed to create multiple signed original copies one for each party?**

This is still new and untested, however, once The Legal Writings (Counterparts and Delivery) (Scotland) Bill is enacted in its current form a document can be digitally executed by several parties in counterparts. This may be the most straightforward method of multiple execution of electronic documents.

If there are several signatories and an electronic document is not being executed in counterparts then, if Adobe is used, there is a function to set up the number of signatories. It is recommended that the parties agree the sequence of execution. The first signatory would sign and lock the document with the private key. The second would unlock it with the public key, check that it has not been amended, sign it with his or her private key and send it on to all. Each signatory can then check it and add his or her signature in turn, without it showing as an amendment, email on to all, and then the next one can be added. The most recently signed document should be regarded as the “original” in these circumstances. It is recommended that documents state the mechanism for completion.

Note that ARTL does not anticipate multiple execution of electronic documents.

**Is it the case that a digitally signed document is evidentially ‘worthless’ if printed off? i.e. a hardcopy print does not have the same probativity as the soft copy because the hardcopy cannot demonstrate the certification authority chain?**

The document is not evidentially worthless but the hard or pdf copy will not have the same self-proving status as the “original/authenticated version” which can only be accessed electronically. As such, the best means of verifying the document is to access it electronically.

As a result, members may wish to consider lodging with the Court a certified hard copy of the document.

If a document is signed using an electronic signature other than the LSS Smartcard then members should take steps to verify whether the signature is an advanced digital signature.

Even if the electronic signature is not an advanced digital signature then it is still admissible in Scottish legal proceedings. It will be for the Court to decide in a particular case whether a digital signature has been correctly used and what weight it should be given against other evidence.

A digital signature and its certification are admissible in any legal proceedings as evidence in respect of any question as to the authenticity or integrity of an electronic communication.

A person can certify that the signature, a means of producing, communicating or verifying the signature or a procedure applied to the signature is a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

In these circumstances, members should also consider lodging with the Court at the same time any public key information, a print-out from the Law Society website “Find a Solicitor”, certification authority documentation and any other certification available as set out above.

On the basis that the current draft Bill on Legal Writings (Counterpart and Delivery) (Scotland) Bill enters into force unchanged, the same comments will apply in relation to counterparts executed by digital signature.

**What about digital signatures of clients acquired from third-party providers which do or do not meet legislative requirements?**

If a solicitor uses a third party provider of electronic signatures (whether an advanced digital signature or not) then he/she will not be able to rely on the “circle of trust” provided by the LSS Smart Card system. As a result, recipient members will wish to see certification of the third party provider. Only a document signed using an advanced digital signature with a qualified certificate will benefit from having a self-proving status.

The same comments apply in relation to clients that use electronic signatures. It should also be remembered that clients may have agreed with each other how they will treat each other’s electronic communications.

**How does appending a digital signature interact with the practice of certifying documents as true and accurate copies?**

**(e.g. Would it be acceptable practice to scan a document, add a 'true and accurate' docquet to the PDF and then append a digital signature to the whole PDF?). Are there any practice rules on this?**

There is no law on this but in principle there would seem to be no reason why this could not work. To certify a copy of an original document as a true copy requires:

- The signatory to have seen both the original document and the copy and seen that the latter is a copy of the former.
- A docquet to be applied to the copy to the effect that it is a true copy of the original.
- The docquet to be signed by the person who has inspected the original and the copy.

There would seem to be no reason why the "copy" should not be a pdf, rather than a hard copy photocopy, since an advanced digital signature is as valid a way of signing something as a manual signature.

**When applying a digital signature to a 200 page document with a plan and 30 appendices do I sign once applying a signature to the entire document or do I have to sign multiple times?**

A single digital signature is all that is required, provided all the annexations have been referred to in the document, are identified as being the annexations referred to in the document and are annexed to the document before the digital signature is applied to the combined document and annexations.
*Note – This is provided by Regulation 4 of The Electronic Documents (Scotland) Regulations 2014.*

**At a practical level, will the system allow signatures to be added to all types of documents, regardless of the package on which they were created – for instance can a Word document be digitally signed as well as a PDF? Will a range of PDF packages work?**

The signatures work on a range of generally used business packages like Word and Adobe – there are details on the website (www/lawscot.org.uk/smartcard) of the ones most commonly used and where the Society will offer technical support, or you can check the details of your own product.

THE LAW SOCIETY of SCOTLAND
www.lawscot.org.uk

Smartcard

**How and to what extent do LSS members need to interrogate the validity and nature of a qualified digital signature?**

The digital signature is a dynamic process. It occurs in the online environment and checks the Registration Authority and Certification Authority at the time when the private key is applied.

The Law Society of Scotland is the registration authority - performing the necessary ID checks, issuing cards and digital signatures, and providing accurate information to the certification authority. The Certification authority is Abogacía Certification Authority (ACA, operated by RedAbogacía). It meets all key EU and international standards required of certification authorities, holding the required information to allow the issuing and use of a qualified digital signature.

Members should not rely on a printed version of a document. Members should access the electronic document and use that to access the digital signature. That will confirm whether the digital signature was valid when it was applied.

Members are not permitted to allow others to apply their digital signature.

The Law Society of Scotland
26 Drumsheugh Gardens
Edinburgh EH3 7YR

T +44(0) 131 226 7411
F +44(0) 131 225 2934
E smartcard@lawscot.org.uk

www.lawscot.org.uk/smartcard

@lawscot TheLawSocietyofScotland The Law Society of Scotland

## C. DIGITAL SIGNATURES IN CONVEYANCING TRANSACTIONS

**What steps should solicitors take to preserve a copy of digital missives or indeed any digitally executed contract?**

Solicitors should comply with existing LSS guidance on Ownership and Destruction of Files, Scanning and Archiving, Electronic Communications, Outsourcing and Cloud Computing. This Guidance is currently being reviewed and will be updated.

All outsourcing providers should be made aware of that guidance and required to comply with it.

In the event that the digital documents are to be destroyed, the intent to do so should be intimated in writing to the client. Tacit consent by accepting terms of engagement may be acceptable, but is a matter of law.

The normal duties of care and confidentiality in the storage of clients' papers in terms of the rules would, for the avoidance of doubt, apply to electronic and scanned material. Offsite copies of the electronic and scanned archive should form part of the practice unit's contingency planning strategy.

Although documents which have only ever existed electronically and are appended by digital signatures have the same legal status as 'manual signature' documents, and given the fact that probative status only adhibits to the electronic version, great care should be taken to ensure that the electronic documents be retained in original electronic format and backed up appropriately. Whilst a hard copy will not have the same self-proving status as the "original/authenticated version" which can only be accessed electronically, it would be best practice to print hard copies of these for retention in the event that the digital files are lost, altered, corrupted or the software becomes superseded

**Where missives are concluded by an exchange of digitally signed documents, this means both parties will be in possession of a copy of an original. Does that mean that there are in fact two principal sets of documents either of which is evidentially as valid as the other?**

It is necessary to recognise the distinction between electronic documents, which are "created" in electronic form, and exist virtually, and traditional documents which are written on paper and which exist actually.
Each party has access to each "original" digitally executed document, held on their system, each of which is equally valid.

## D. DIGITAL SIGNATURES IN COURT MATTERS

### How do you submit a digitally executed document to a Court?

Unless the Court directs otherwise, it will be necessary for a hard copy of the digitally executed document to be lodged. Some Courts may allow productions to be lodged electronically in pdf format, but this is will be a matter of policy and practice which is likely to develop as Courts become e-enabled.

If a document has been signed by a member using the LSS Smart Card, the hard copy or pdf document will contain a printed version of the members' public key and the date/time stamp of signature. However, the hard or pdf copy will not be an "original/authenticated version" of the document which can only be accessed electronically.

On the basis that the current draft Legal Writings (Counterpart and Delivery) (Scotland) Bill enters into force unchanged, the same comments will apply in relation to counterparts executed by digital signature.

## E. GLOSSARY

**This section provides working definitions which may be of further assistance in using this guide, but the explanations are not legal definitions.**

| | |
|---|---|
| **Advanced Digital Signature —** | The middle level of signature recognised under the relevant EU Directives - This is data which meets the following requirements:<br>▪ it is uniquely linked to the signatory;<br>▪ it is capable of identifying the signatory;<br>▪ it is created using means that the signatory can maintain under their sole control;<br>▪ it is linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.<br>▪ |
| **Certification Authority –** | In the LSS system the Certification Authority is Abogacía Certification Authority (ACA, operated by RedAbogacía). It meets all key EU and international standards required of certification authorities, holding the required information to allow the issuing and use of a qualified secure digital signature. This process removes the cost, resource commitment and risks of The Law Society of Scotland attempting to become a certification authority in its own right within a small market like Scotland, something which we did not consider as viable or desirable when we designed the project specification in 2013 and tendered the project. |
| **Counterparts –** | Historically, contracts under Scots law have been concluded by both parties signing the same physical copy. If proposed legislation passes in 2014 then execution in counterpart will become possible. Signing in counterparts is where parties sign a separate physical copy of a document. Once the parties have all signed their respective counterparts, these are exchanged between them, and the contract takes effect from that point. |
| **Cryptographic device –** | This is the 'chip' contained on your Smartcard, which looks similar to those on your bank card. In this case, the chip is actually a computer which processes information meaning your private key never leaves the card, but is matched to you public key, when in a reader, within in the computing capability of the chip itself |

| | |
|---|---|
| **Cryptography –** | In this context, the creation of asymmetric codes (in a PKI system, one public, one private) which are related mathematically but not in a way which can be determined by only having access to one of the codes. This can then be used to encrypt a message or to apply a digital signature by embedding the private key within a document. |
| **Digital Signature –** | The lowest level of signature recognised under the relevant EU Directives - This is data in electronic form which is attached to or logically associated with other electronic data and which serve as a method of authentication |
| **Manual Signature -** | A hand written signature |
| **PKI (Public Key Infrastructure) –** | Cryptography could have two keys, neither of which are 'public' to allow communication between two individual who have set the system up in advance. However, where one of the keys is public the system is usually referred to as PKI |
| **Private Key –** | The private key, which is known only to the signatory, is used to create the digital signature and to change the message into encrypted form. It is essentially a very long list of numbers and characters, that have an mathematical association with the public key. |
| **Public Key –** | The public key is used by a receiving party to verify the digital signature and decrypt the message. It is essentially a very long list of numbers and characters, that have an mathematical association with the private key. |
| **Qualified Digital Signature –** | The highest level of signature recognised under the relevant EU Directives (and the type of signature used by the LSS Smartcard) - this is data which must in particular include:<br>▪ an indication that it is issued as a qualified certificate;<br>▪ the identification of the certification service provider;<br>▪ the name of the signatory;<br>▪ provision for a specific attribute of the signatory to be included if |

| | |
|---|---|
| | relevant, depending on the purpose for which the certificate is intended;<br>▪ signature-verification data corresponding to signature-creation data under the control of the signatory;<br>▪ an indication of the beginning and end of the period of validity of the certificate;<br>▪ the identity code of the certificate;<br>▪ the advanced digital signature of the issuing certification service provider. |
| **Registration Authority** | For this project, the Law Society of Scotland is the registration authority - performing the necessary ID checks, issuing cards and digital signatures, and providing accurate information to the certification authority. |
| **Wet Signature -** | A hand written signature |