ADLS Digital Signing Service Protocol

May 2020

These protocols may be updated without prior notification.

Background:

ADLS WebForms offers an integrated Digital Signing Service by which an electronic document may be signed electronically. This paper:

- gives a brief overview of electronic signing and explains how the Digital Signing business process links back to the electronic transactions law; and
- sets out suggested protocols for lawyers using the ADLS Digital Signing Service.

This paper is not legal advice. It is designed to help parties and their lawyers who wish to sign written contracts and sign deeds by electronic means rather than by a "wet signature" on a paper document. No duty of care or liability is accepted by ADLS or those involved in preparing this protocol to any company or individual who relies on material included in it.

This paper is ADLS' recommendation of good practice; while users are not required to follow the protocols, but we suggest that doing so will make it easier to interact with other parties using the ADLS Digital Signing Service.

It is important to note that the ADLS WebForms system enables both finalised WebForms documents, as well as PDF documents uploaded to WebForms, to be submitted for digital signing.

Contracts and Deeds

Contracts between parties may be entered into orally or in writing or by a combination of both.

A contract may be in writing because:

1. the parties elect to be bound by the information contained in a document (informal contract);
2. the contract is required by law to be in writing (formal contract); or
3. it is required to be in the form of a deed and therefore must be in writing, executed and delivered in accordance with that section (section 9 of the Property Law Act 2007).

Digital Signing allows both contracts and deeds to be signed electronically by the parties or signed by some of the parties electronically and "wet signed" by others. A party signing a document is either:

- signifying an intention to be legally bound by the contents of that document (primary party); or
- indicating that he or she was physically present and witnessed a party to the document signing the document (witness).

Legislation - Contract and Commercial Law Act 2017

The legislation facilitating the use of electronic technology, previously the Electronic Transactions Act 2002 and now the Contract and Commercial Law Act 2017 - Part 4, explains that its purpose will be achieved by providing that certain paper-based legal requirements may be met using electronic technology.

The facilitating legislation is technology neutral. The key definition for the purposes of the ADLS Digital Signing Service, is the definition of an electronic signature:

> *"**electronic signature,** in relation to information in electronic form, means a method used to identify a person and to indicate that person's approval of that information."*

The key elements of the definition are that it relates to:

- information in electronic form;
- a method used to identify a person; and
- a method used to indicate that person's approval of that information.

The ADLS Digital Signing Service enables the signatory to insert an electronic signature that may be the person's typed name or a graphic of the person's handwritten signature. The Service identifies the signatory and links that signatory to the insertion of the electronic signature.

The Service then seals the document, with a Digital Certificate, which enables any changes to a document after a person has inserted their electronic signature to be detected. This is the Digital Certificate that elevates the electronic signature to a digital signature and offers greater security.

Information in Electronic Form

A "document" or "instrument" can be described as a package that contains information. The persons who intend to be bound legally by the contents of that package indicate their acceptance of the information and confirm their intention to be bound by including their signature within the document. This act is useful evidence of intention but it is not always required for every contract type.

What is always required is that the packages of information be in a readable form.

There are three forms of readable document packages. An original paper document, an electronic document that can be read on screen using pdf or some other programme to convert digital bits into words. In addition, there is a scanned or printed copy of either of these two forms.

To prove that a paper document is (a) an original, and (b) has not been changed since it was signed by the parties, and (c) the signatures are the genuine signatures of the named parties, an expert forensic professional and/or handwriting expert is required to examine the document to confirm its validity.

Examining a scanned copy of the original is unlikely to prove its validity for there is no way of detecting if a clever forgery has occurred to change words that look original but were subsequently changed before scanning.

This applies whether the copy scanned was a paper or electronic document. It is possible to take a secure PDF, print it, then scan and save it as an ordinary PDF, convert to Word, change the Word document then save the amended Word documents as a PDF. Even if the scanned document contains a graphic of a wet or electronic signature the final changed PDF looks valid.

An electronic document that has been electronically signed using the ADLS WebForms Digital Signing Service can be verified without the intervention of a forensic professional. The document will contain a Digital Certificate – this is part of the signing box. This sets out the date and time and provides information regarding the signer. By clicking on the verification section of this box in the document's electronic form, the document, using hashing algorithms and PKI technology can return the statement that it was signed at a particular date and time and has not been tampered with since that date and time.

For this reason it is essential that you retain in electronic form a copy of the electronic document with the Digital Certificate (i.e. digital signature) imbedded. You can make electronic copies of the document and distribute these. The digital certificate remains imbedded and capable of verification in each document.

You may print and retain on your file a copy of the signed document. But this is not the electronic form that you might need to revert to if its validity is ever questioned. For this, you need an original electronic document with the Digital Certificate imbedded.

ADLS Digital Signing Service User Guide

ADLS has made available a Digital Signing User Guide (User Guide) that outlines in detail how to use the Digital Signing Service both for documents that are created in WebForms and for third party PDF documents that can be uploaded for Digital Signing.

Documents that cannot be digitally signed

Not all documents are permitted by Part 4 of the Contract and Commercial Law Act 2017. These are set out in Part 3 of Schedule 5 of the Act and include:

- affidavits, statutory declarations, or other documents given on oath or affirmation:
- powers of attorney or enduring powers of attorney:
- wills, codicils, or other testamentary instruments.

ADLS Digital Signing Service – Recommended Best Practice

The following information sets out some key elements of recommended best practice for lawyers utilising the ADLS Digital Signing Service. Please refer to the User Guide for an exact description of how to set up documents for digital signing.

A. Consent

> ***Contract and Commercial Law Act 2017***
>
> ***Section 220 Consent to use of electronic technology***
>
> *(1) Nothing in this subpart requires a person to use, provide, or accept information in an electronic form without that person's consent.*
>
> *(2) For the purposes of this subpart,*
>
> *(a) a person may consent to use, provide, or accept information in an electronic form subject to conditions regarding the form of the information or the means by which the information is produced, sent, received, processed, stored, or displayed:*
>
> *(b) consent may be inferred from a person's conduct.*
>
> *(3) Subsections (1) and (2)(a) are for the avoidance of doubt.*

This section overlies all use of electronic technology and requires that before utilising the ADLS Digital Signing Service the consent of all of the parties to the use of an electronic document and the acceptance of an electronic signature must be obtained.

The **first step** in the recommended best practice is therefore ensuring that all relevant consents have been obtained. This step is outside the scope of the Digital Signing feature available through WebForms and is entirely in the hands of the lawyers whose clients are signing.

Where there are multiple parties who are represented by different lawyers, the protocols suggest a process to obtain these confirmations. Each lawyer is free to determine whether consent is express or implied and how it is confirmed. The ADLS Digital Signing Service provides for documents to be partly electronically signed and partly wet signed. This ability for different signing methods does not override section 220 and all parties must consent to:

- accepting an electronic document; and
- accepting an electronic signature from the party providing it;
- and each party providing such a signature must consent to providing it.

It needs to be noted that choosing the option of partly digitally signing, and partly wet signing a document will result in a partially completed electronic signing log, as only the digital signatures can be captured in this log. The chain of signing evidence is therefore broken. The digital signing log for a document is an important record (the ultimate file note) for lawyers, as it provides a record of the date, time and details of each signing party invited to sign, and who have signed. A hybrid signing approach of digital signing with wet signing, is therefore not recommended.

B. Verification of identity

Contract and Commercial Law Act 2017

Section 226 Legal requirement for signature

(1) A legal requirement for a signature other than a witness's signature is met by means of an electronic signature if the electronic signature—

(a) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and

(b) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

(2) However, a legal requirement for a signature that relates to information legally required to be given to a person is met by means of an electronic signature only if that person consents to receiving the electronic signature.

Section 228 Presumption about reliability of electronic signatures

(1) For the purposes of sections 226 and 227, it is presumed that an electronic signature is as reliable as is appropriate if—

(a) the means of creating the electronic signature is linked to the signatory and to no other person; and

(b) the means of creating the electronic signature was under the control of the signatory and of no other person; and

(c) any alteration to the electronic signature made after the time of signing is detectable; and

(d) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(2) Subsection (1) does not prevent any person from proving on other grounds or by other means that an electronic signature—

(a) is as reliable as is appropriate; or

(b) is not as reliable as is appropriate.

The **second step** for recommended best practice is verifying the identity of the signatory.

The ADLS Digital Signing Service provides various means of capturing and retaining verification of identity. It is for each lawyer to determine the level of verification of identity required for each signatory to satisfy the test that it is *"as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required".*

It is also a matter for each lawyer to decide how verification of identity is recorded and for how long evidence of identity is retained. Please refer to the checklists provided at pages 14-16 of this Protocol that you may wish to use and retain on your client file.

B1. Contracts - Informal

Signing parties in the paper environment rarely provide detailed evidence of their identity. Depending on the nature of the contract, a party's identity may be determined by the circumstances. For example, it is standard for one lawyer to rely upon the implied representation or direct certification of another lawyer that the parties represented by the other lawyer are who they say they are.

Verification of identity generally has been raised to a higher level given the requirements of electronic land registration and AML/CFT legislation. Lawyers and their clients may elect whether or not to take additional steps to verify a party electronically signing a written document. They may chose not to verify if the identity of that party has previously been verified for another purpose.

B2. Contracts - Formal

Contracts that are required to be in writing may require verification of identity if the lawyer acting for the party has not previously acted for the signatory. It remains the lawyer's decision as to the extent of verification, if any, required.

It is good practice to require a reasonable level of evidence and verification of identity for a contract required to be in writing. If the law requires a higher level of evidence to confirm the contract, the lawyer should ensure a corresponding higher level of verification of identity.

B3. ADLS Digital Signing Service - Verification options

Optional methods by which a person may assert and a lawyer retain evidence of identity are offered in the ADLS Digital Signing Service. This includes an online assertion utilising a RealMe assertion of identity as well as on-line verification of evidentiary documents such as a New Zealand driver licence and passport.

In the case of documentary verification, you should read and understand the limitations of this method. For example, the verification may only confirm that the document and certain of its information is valid. This does not necessarily confirm that the person providing it to you is the correct holder of that identity document.

B4. Deeds and witnessing

An individual signing a deed and, in some cases a director signing a deed on behalf of a company, is required to have their signature witnessed.

The electronic transactions legislation confirms that a witness may also sign electronically. The witness must be physically present and watch the signatory carrying out the actions required for the signatory to attach his or her electronic signature to the document.

The ADLS Digital Signing Service provides for a witness to also attach his or her electronic signature to the document and confirm that this has been done for the purpose of witnessing the electronic signature of the signatory.

The lawyer may decide whether and to what extent there should be identity verification required of the witness. However this must be done outside of the ADLS Digital Signing Service as it currently only verifies the identity of signatories. Section 9 of the Property Law Act 2007 requires only, that if signing in New Zealand, the witness must add the name of the city, town or locality where he or she ordinarily resides and his or her occupation. The ADLS Digital Signing Service also requires the email address and a mobile phone number of the witness be included to enable the witness to sign the document electronically.

C. Linking the signatory to the verified identity

Section 228 (1)(a) and (b) of the Contract and Commercial Law Act 2017 require that the means of creating the electronic signature is linked to the signatory and is under the control of that person. It is at this step in the ADLS Digital Signing Service that the process becomes mandatory.

Only one lawyer will be involved in preparing the WebForms document (or uploading a third party document) for the purpose of using the ADLS Digital Signing Service. That lawyer will be required to indicate the following information for each signing party:

- full name;
- email address; and
- mobile phone number.

Where parties are represented by separate lawyers and a party requests that this information be kept confidential and not disclosed to the other party, the lawyer requiring confidentiality should request this by email and the lawyer setting up the document for digital signing should provide an undertaking to retain the information in confidence.

A person signing a document will be sent:

1. an email to their nominated email account advising that the document is ready for signing. Upon clicking the 'Click to Sign' button, they will then be sent
2. an SMS text to their mobile, containing a '*Passcode*' to enter into the email.

Following this 2 factor authentication process, which links the identity of the signatory to their signature, the signatory will be able to proceed to electronically sign the document.

D. Signatory Capacity

This section applies if a signatory is not signing the document in their personal capacity. ADLS has amended the signing panels in our WebForm documents (as below) which allow the lawyer setting up the document to select the capacity in which the signatory is signing the document – director, trustee, authorised signatory or attorney. Where the signing panel is not available on a WebForm document, or a third party document is being used, ADLS recommends that the lawyer setting up the document canvas the issue of signatory capacity with their client and other parties who will be signing the document.

SIGNED by:

_____
Director / Trustee / Authorised Signatory / Attorney*
Delete the options that do not apply
If no option is deleted, the signatory is signing in their personal capacity

D1. Company as signatory

Companies may sign contracts in accordance with section 180 of the Companies Act 1993. Whichever signing case is relevant (two directors / the sole director plus witness /if authorised, 1 authorised person or director plus witness / 1 attorney plus witness) the signatory will always be a natural person not the company.

The natural person is not signing indicating that he/she intends to be bound by the document but that the entity on whose behalf the person is signing intends to be bound.

It is therefore important that:

- the execution clause typed in the document being signed names the party who is being bound by the document; and
- the signature of the person signing is supported by the appropriate signing capacity, selected by the document owner.

D2. Verification of identity of signatory in another capacity

The information contained in sections B and C above also apply to a natural person who is signing as a corporate officer, trustee, authorised signatory or as an attorney.

Note that in the case of the attorney, a Certificate of Non-Revocation (Form reference 4098WFP) should also be provided and signed by the attorney.

E. Witness details

The identity of the witness will likely not be known at the time digital signing is set up by the lawyer.

Accordingly, the witness details will be left to be completed by the person whose signature is to be witnessed. These details are required to be included at, or prior to, the time of signing by the signatory.

The witness details include the full name, occupation and address of the witness plus an email address and a mobile phone number to enable the witness to electronically access the document for witnessing.

The witness should be asked to attend the signing with his or her mobile phone and should be able to view the signatory digitally sign on the signatory's computer or an adequate device such as a laptop, tablet or smart phone.

As the witness will be physically present when the signatory digitally signs the document, it is expected that the time stamp for the witness will indicate that the witness digitally signed the document shortly after the signatory.

There may be circumstances in which there is a delay. For example, the witness may not have an adequate device and may need to go to another location to log on to another computer, or the witness may be called away before they can complete their part. If there is a time delay of, say, greater than 20 minutes between signatory and witness, it is recommended that you consider phoning the witness and recording the explanation for the delay and retaining this note on your client's file.

F. Sequential Signing

The ADLS Digital Signing Process allows the lawyer setting up the document for signing to select the sequence in which the various signatories will digitally sign the document.

If another lawyer is acting for another party, the lawyer may wish to contact the lawyer to agree the signing sequence for the parties.

G. Reviewer

The reviewer function enables the person setting up the signing to designate a Reviewer (presumably the party's lawyer) for each Signatory. The document to be signed is forwarded to the Reviewer who will review the document and then release the document for digital signing to the client. This process automatically enables sequential signing.

H. Date Stamper

Normally the person setting up the document for signing will also act as the Date Stamper but they can nominate another person to perform the function. Once all signing, by both signatories and witnesses, is complete the Date Stamper will be notified to add the date of execution to the document in the designated field. Where the date of execution is not also the effective date, a clause should be added to the agreement which sets out the effective date of the contract as distinct from the execution date.

I. Sealing and distribution of completed document

Section 228(1)(c) and (d) of the Contract and Commercial Law Act 2017 requires that any alteration to the electronic signature or to the information contained in the document must be detectable.

The ADLS Digital Signing Service, involves the generation of a Digital Certificate that records when each party and/or witness signs the document, and seals the document. The PDF document can be verified by clicking on the Digital Certificate at any time in the future and any tampering of the document after the Digital Certificate is generated will be detectable. The Digital Certificate becomes part of the document and is included in each copy made of the PDF document.

PDF copies of the document signed by all parties with the Digital Certificate may then be distributed to all parties.

J. Readability

> ***222. Legal requirement that information be in writing***
>
> *A legal requirement that information be in writing is met by information that is in electronic form if the information is readily accessible so as to be usable for subsequent reference.*

Section 222 of the Contract and Commercial Law Act 2017 requires that the document remains able to be read in the future.

All ADLS Digital Signing Service documents, once signed, are retained in PDF (portable document format) that complies with universally accepted specifications. The security features assigned to a PDF document with imbedded PKI digital certificate technology provide an acceptable level of surety that this information is readily accessible and usable for subsequent reference.

K. Counterparts - Document partly electronically and partly wet signed

Provided that a counterparts clause is included in the agreement and provided all parties consent to the form of signatures; a wet signed document and an electronically signed document can together comprise the counterpart signing in the same way that counterpart documents are currently signed and exchanged in the paper environment.

This means that the PDF document provided to the party electronically signing, is a scanned pdf of the prior wet signed document, which has been uploaded into WebForms and submitted for electronic signing. This eliminates the need for multiple counterpart documents - one signed by each party.

L. Counterparts / Certified documents

A benefit of the ADLS Digital Signing Service is that the ultimate control of the signing process is within the hands of the lawyer who has set up the document to be signed.

For example, if time is of the essence and you cannot wait for both parties to sign sequentially, or one party overseas wishes to sign digitally first and the local party wishes to sign in front of their lawyer the parties can agree upon an alternative to the above method of digital and paper counterparts.

In the paper environment, counterparts are by their nature multiple copies of the same document.

The same can occur in the digital environment with even greater security.

The lawyer receiving the completed documents can put them together in one scanned PDF with an additional page to which is added a digital certification. This means that the lawyer adds a statement that the document is a true and correct copy of the documents signed by both parties and then the lawyer adds his or her electronic signature to the certification page.

As indicated in section I above, the Digital Certificate is embedded with the signature in the document. In this way, the PDF including both counterpart copies (wet signed and electronically signed) is certified and sealed for future reference.

If the circumstances require, this method could be used by lawyers to ensure a paper document that has been wet signed by all parties is retained in a tamper proof electronic form.

ADLS Digital Signing Service – Protocol Checklists

ADLS suggests that a Checklist be completed and retained on the client file.

Checklist 1 - Lawyer/Client

This protocol is intended to apply to electronic signing when a lawyer prepares a document for signing by a client or clients represented only by the lawyer.

A. Consent:

Clients should be advised in advance of the option to sign a document electronically and asked for their consent. The lawyer must check that each party to the documents including the parties relying upon the document has consented to the document being in electronic form and electronically signed by the relevant parties. Both the parties relying on the document and the parties intending to be bound by it need to provide consent. Consent may be:

(a) express consent

If the circumstances require – obtain a written acknowledgment from the client. If a client is asked to sign and return a client engagement letter, ADLS suggests including the acknowledgement of the consent in that letter.

(b) oral consent

If electronic signing is discussed with the client and consent is given orally, note this on the checklist with a date, time and place of the conversation.

(c) continuing consent

Consent may be implied from past conduct. Circumstances may imply consent – for example where the client is overseas and asks for the document to be sent for signing. If the document is sent with the option to sign electronically, the act of accessing the document for signing can be taken as consent.

B. Verification of identity

Determine if the nature of the transaction requires limited or high level verification of identity.

In each case, note the level of evidence of identity (EOI) or verification of identity required on the checklist and attach to the checklist any copies of EOI obtained.

C. Link information

If not already obtained, collect the full name, email address and mobile number of each signing party, reviewer, date stamper; and, if available, each witness. Note this information on the checklist.

D. Signatory Capacity

If a party is signing as a director, trustee, authorised signatory or under a power of attorney, and this is known before the documents are prepared for signing; ensure the relevant information is included in the signing panel of the document to indicate the role of the signatories.

Note on the checklist the name of the signatory as well as their capacity and on whose behalf they will be signing.

Upload document for signing

This may be done using a finalised WebForms document or by uploading a third party PDF document to WebForms. Follow the ADLS Digital Signing Service User Guide instructions.

Checklist 2 - Lawyer/Lawyer

A. Consent:

For your own client, follow the Lawyer/Client process outlined above.

For the client of the other lawyer, you need to seek consent of the other lawyer and his/her client(s) for electronic signing confirming the client(s):

(i) accepts electronic signing by your client; and

(ii) agrees to electronically sign document.

If the other lawyer's client(s) intend to sign electronically:

(i) determine who establishes the client as a user;

(ii) determine order of signing;

(iii) determine whether the other lawyer wishes to review the document in the digital signing process before releasing it to their client for signing; and

(iv) obtain evidence/ verification of identity (if required) that other parties are who they say they are.

D. Signatory Capacity

Confirm the signatory capacity of other signatories.

Checklist 3 - Lawyer/self-represented third party

A. Consent:

For your own client follow the Lawyer/Client process outlined above.

For the self-represented third party seek consent to electronic signing and confirm the self-represented third party:

(i) accepts electronic signing by your client; and

(ii) agrees to electronically sign document.

Best practice would require express written consent from the other party. This could be by way of email confirmation.

B. Verification of identity

Determine the level of evidence and verification of identity required.

Best practice would require when interacting with a self-represented third party that at least a minimum level of verification is required in all cases unless your client is relying on the document and consents to limited third party

verification of identity. Obtain acceptance of a lower standard of verification of identity, in writing, from your client and attach this to the checklist.

C. Linking information

If not already obtained, collect the full name, email address and mobile number of each signing party, and if available, each witness. Note this information on the checklist.

D. Signatory Capacity

Confirm the signatory capacity of other signatories.

ADLS Digital Signing Service – Checklist 1 – Lawyer/ Client

A. Consent	**Written obtained (dated and attached)**	**Oral obtained (dated)**	**Implied by conduct (specify)**	**Wet Sign**
(name)				
(name)				
(name)				
(name)				

B. Verification of identity	**Held**	**Passport ***	**Drivers Licence ***	**Real Me assertion**
(name)				
(name)				
(name)				

C. Link information	**Signing party, Date stamper OR Reviewer capacity**	**Email**	**Mobile**
(name)			
(name)			
(name)			
(name)			

Link information – witnesses	**Email**	**Mobile**	**Address**	**Occupation**
(name)				
(name)				
(name)				
(name)				

D. Signatory capacity ****Name of signatory and capacity of signatory – director, trustee, authorised signatory or attorney**	**On whose behalf they are signing – name of company, trust or donor**

*** If this is a New Zealand Passport or drivers licence, consider getting documentary verification**

**** this should correspond to the name of a person identified above**

ADLS Digital Signing Service – Checklist 2 – Lawyer/Lawyer

A. Consent of other parties (via other lawyer)	**Confirmed**	**Digitally Sign**	**Wet Sign**
(name)			
(name)			
(name)			
(name)			

B. Verification of identity (confirmed by other lawyer)	**Held**	**Passport ***	**Drivers Licence ***	**Real Me assertion**
(name)				
(name)				
(name)				

C. Link information	**Signing party, Date stamper OR Reviewer capacity**	**Email**	**Mobile**
(name)			
(name)			
(name)			
(name)			

Link information – witnesses	**Email**	**Mobile**	**Address**	**Occupation**
(name)				
(name)				
(name)				
(name)				

D. Signatory capacity ****Name of signatory and capacity of signatory – director, trustee, authorised signatory or attorney**	**On whose behalf they are signing – name of company, trust or donor**

*** If this is a New Zealand Passport or drivers licence, consider getting documentary verification**

**** this should correspond to the name of a person identified above**

ADLS Digital Signing Service – Checklist 3 – Lawyer/Self-represented third party

A. Consent of third party	**Written obtained**	**Oral given dated**	**Implied by conduct (specify**	**Wet Sign**
(name)				
(name)				
(name)				
(name)				
B. Verification of identity of self-represented third party	**Held**	**Passport ***	**Drivers Licence ***	**Real Me assertion**
(name)				
(name)				
(name)				

C. Link information of self-represented third party	**Signing party, Date stamper OR Reviewer capacity**	**Email**	**Mobile**
(name)			
(name)			
(name)			
(name)			

Link information – witness to self-represented third party	**Email**	**Mobile**	**Address**	**Occupation**
(name)				
(name)				
(name)				
(name)				

D. Signatory capacity ****Name of signatory and capacity of signatory – director, trustee, authorised signatory or attorney**	**On whose behalf they are signing – name of company, trust or donor**

*** If this is a New Zealand Passport or drivers licence, consider getting documentary verification**

**** this should correspond to the name of a person identified above**