Law Society of Scotland

SMARTCARD QES
VERIFYING SIGNATURES – Adobe PDF

This guide will take you through how to view and verify/validate signatures on documents you have received. You do not need a Smartcard to verify the signature applied with one, but you need to be connected to the internet. The most common types of document used within the profession are Microsoft Word (DOC) and Adobe Acrobat (PDF), which is why we are concentrating on these.

For clarity, the version used in this guide is Adobe PDFMaker 10.0 for Windows. The QES, and the process of verifying one, is compatible with all Adobe versions, though. Even if you use a different version of either software, you will be able to use either of the following instructions. The icons might look differently, but the process is mostly the same.

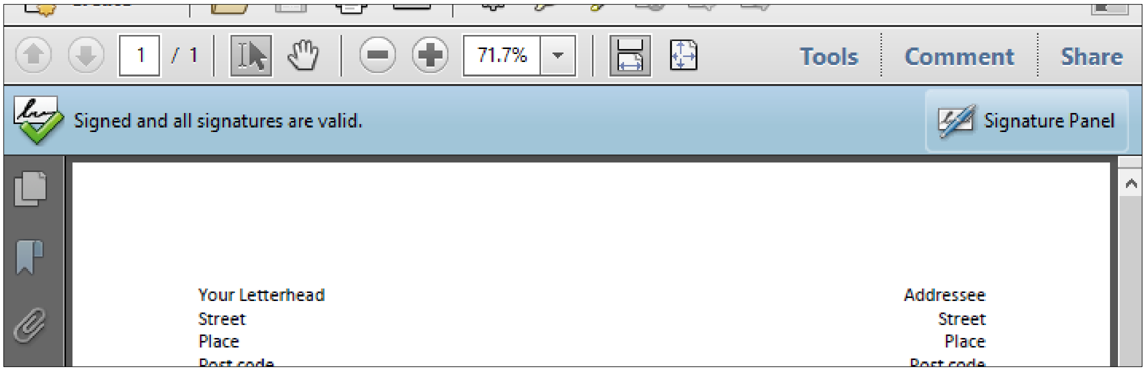
Regardless of what word processing software or edition is used: You need to interrogate the digital signature itself, NOT the visual representation that may or may not be visible on the document. That means, validating or confirming a digital signature is only possible on the computer, not with a print-out of the document.

Visual Check

NB: If you have never validated a signature in a PDF document before and you come across one that says right on top "At least one signature has problems," please go first to **Trusting the Signature**. Nothing is wrong with the signature; it simply means your Adobe version has not been set up yet.

1. "Signed…"

Adobe makes it really easy to conduct preliminary checks on the signature in a document you received - it says so right on top of the PDF:



Signed and all signatures are valid.

Your Letterhead
Street
Place
Post code

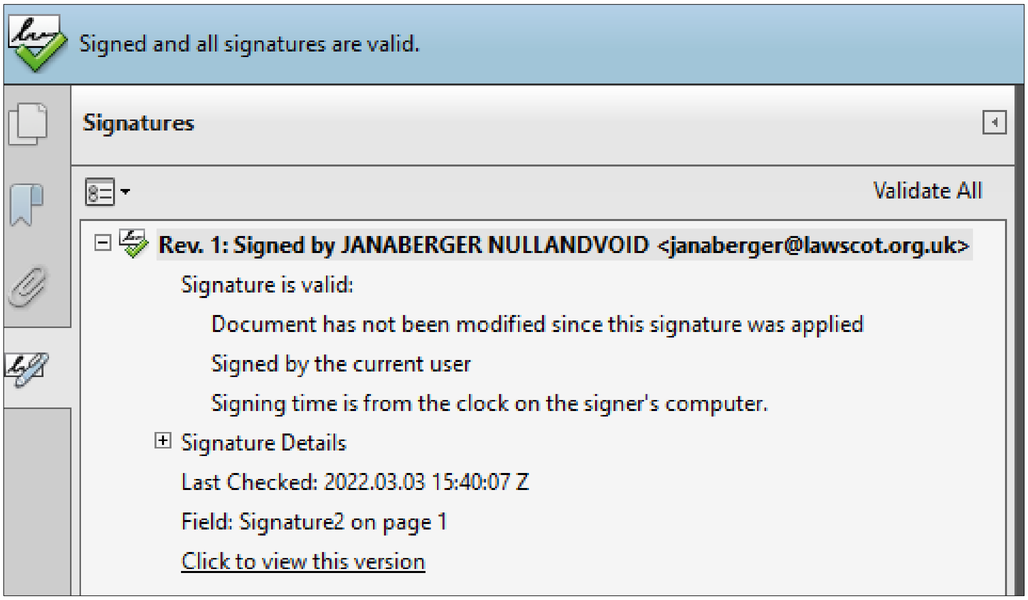
Addressee
Street
Place
Post code

Interrogating the Signature

However, it doesn't give much information about the signatory and the signature itself. For that, you can check in two different places. There are several ways to confirm the validity of the signature and the identity of the signatory.

1. Signature Panel

The **Signature Panel** in a signed PDF document lets you see useful information.



Signed and all signatures are valid.

Rev. 1: Signed by JANABERGER NULLANDVOID <janaberger@lawscot.org.uk>

Signature is valid:

Document has not been modified since this signature was applied

Signed by the current user

Signing time is from the clock on the signer's computer.

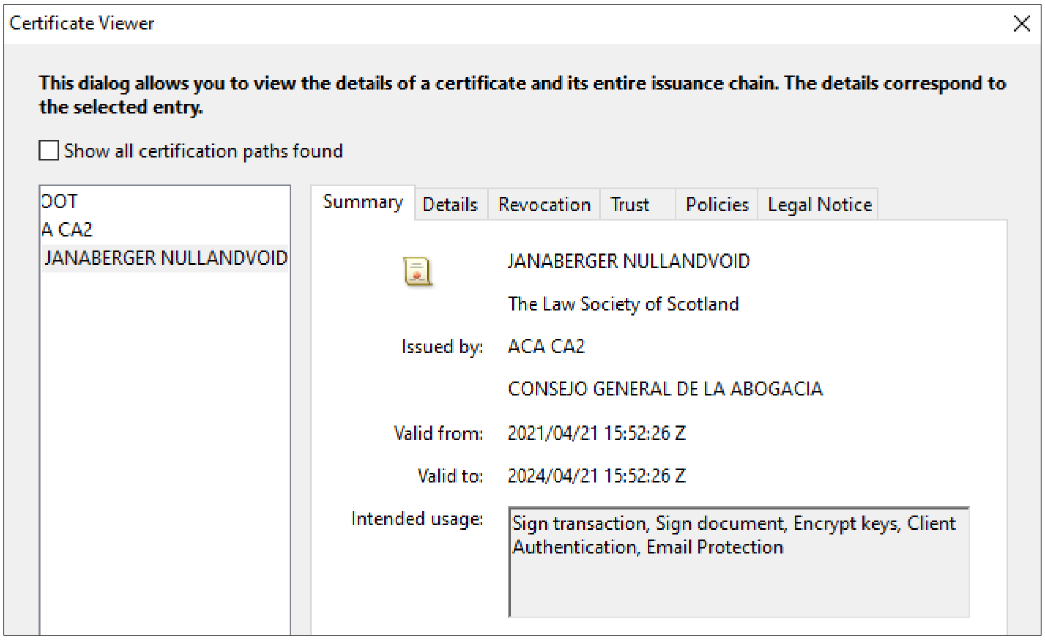
Signature Details

Last Checked: 2022.03.03 15:40:07 Z

Field: Signature2 on page 1

Click to view this version

If you want to be thorough, go to **Signature Details** and here to **Certificate Details…** to check on the underlying information:



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

OOT
A CA2
JANABERGER NULLANDVOID

JANABERGER NULLANDVOID

The Law Society of Scotland

Issued by: ACA CA2

CONSEJO GENERAL DE LA ABOGACIA

Valid from: 2021/04/21 15:52:26 Z

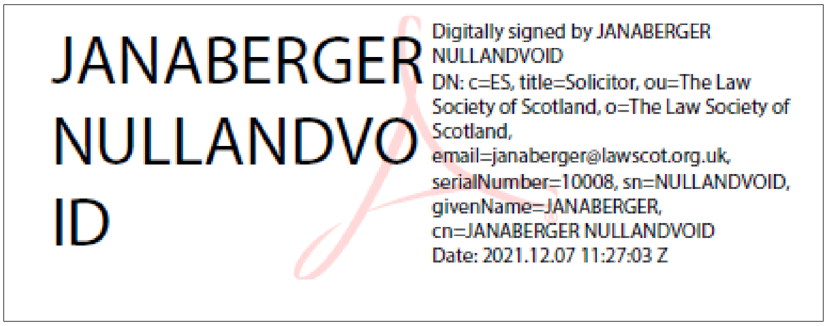
Valid to: 2024/04/21 15:52:26 Z

Intended usage: Sign transaction, Sign document, Encrypt keys, Client Authentication, Email Protection

Important to note here are two lines: one, the name of the signatory and the fact that it says "Law Society of Scotland" underneath, and two, that the certificate was issued by ACA. Since only qualified solicitors, registered with the LSS, and in possession of a valid practicing certificate can obtain a Smartcard with a digital signature, this proves the signatory's identity as a qualified solicitor. ACA is the Spanish Bar Association, the Certification Authority. QES need to include the CA in their underlying certificate.

2. Signature Line

That is the graphic representation of the signature at the bottom of the document.



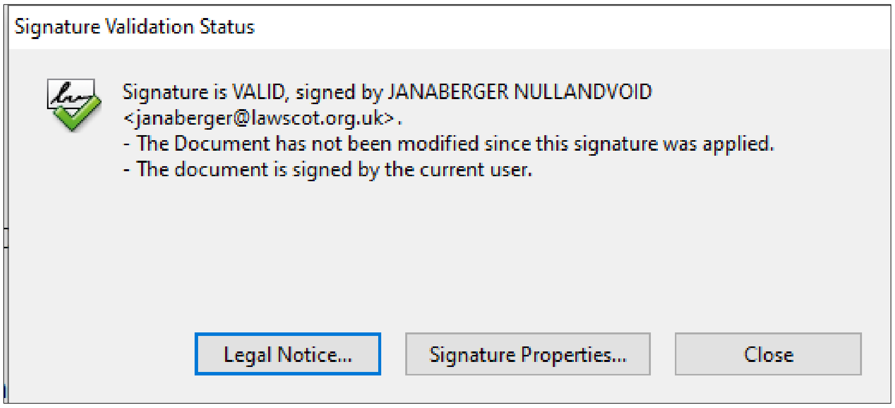
JANABERGER NULLANDVO ID

Digitally signed by JANABERGER NULLANDVOID
DN: c=ES, title=Solicitor, ou=The Law Society of Scotland, o=The Law Society of Scotland, email=janaberger@lawscot.org.uk, serialNumber=10008, sn=NULLANDVOID, givenName=JANABERGER, cn=JANABERGER NULLANDVOID
Date: 2021.12.07 11:27:03 Z

As mentioned earlier, the digital signature is embedded in the bit & bytes of the document; just having that the rectangle there will not provide proof that the document was properly signed with a QES.

Click the on the name of the signatory and it will give you several levels of validity checks:

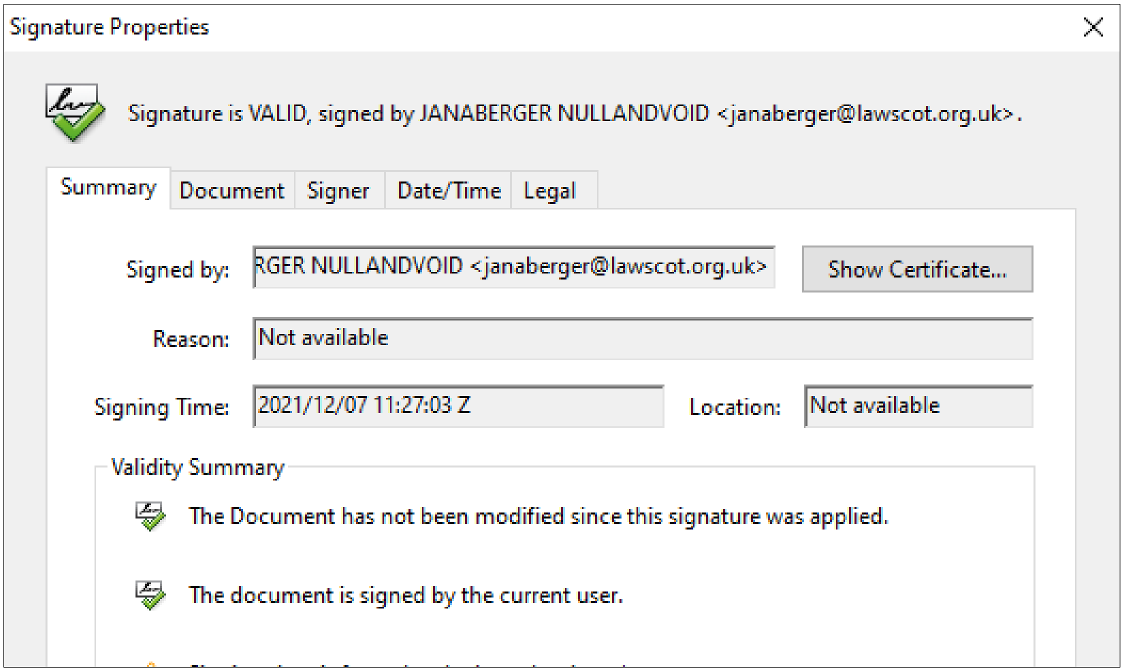
General Status:



Signature Validation Status

Signature is VALID, signed by JANABERGER NULLANDVOID <janaberger@lawscot.org.uk>.
- The Document has not been modified since this signature was applied.
- The document is signed by the current user.

Signature Properties:
Clicking on the above button will open up a window that lets you thoroughly interrogate the signature in front of you:



Signature is VALID, signed by JANABERGER NULLANDVOID <janaberger@lawscot.org.uk>.

Signed by: RGER NULLANDVOID <janaberger@lawscot.org.uk>

Reason: Not available

Signing Time: 2021/12/07 11:27:03 Z

Location: Not available

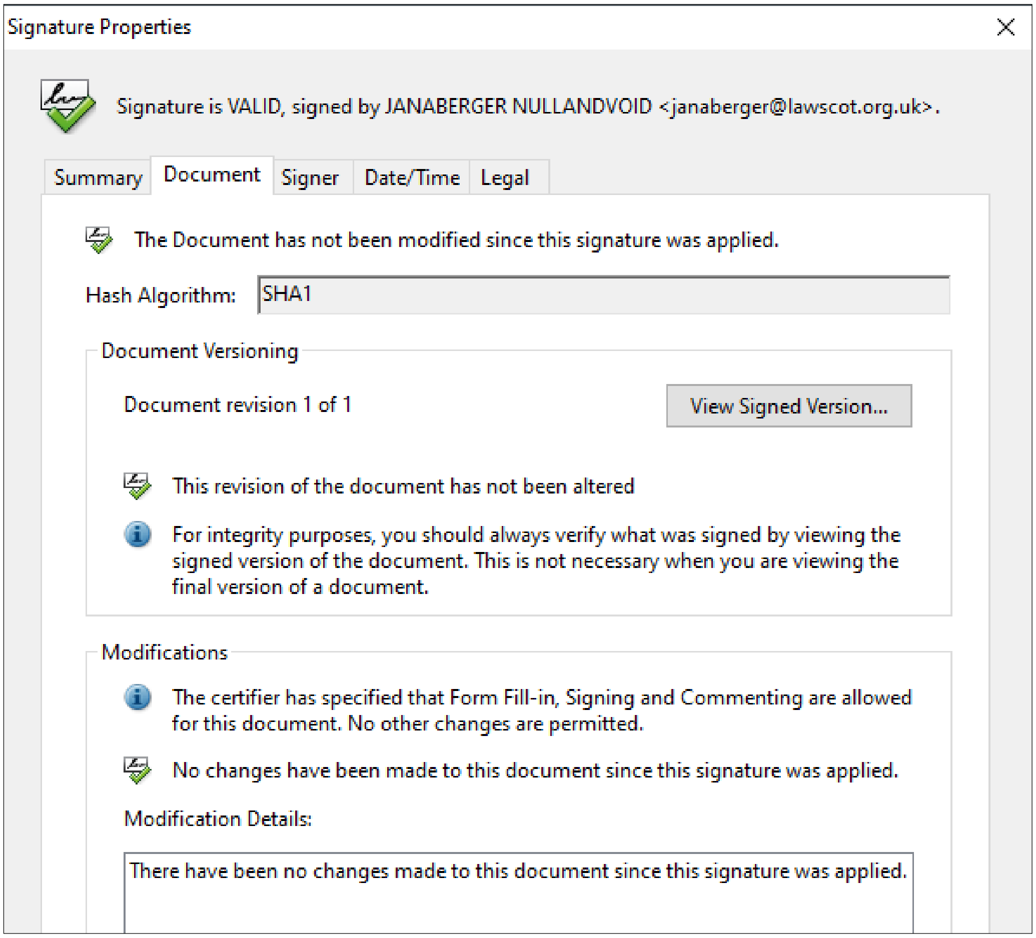
Validity Summary

The Document has not been modified since this signature was applied.

The document is signed by the current user.

Most important here are the tabs labelled **Document** and **Signer**.

Document will further confirm the integrity of the document in question:



Signature is VALID, signed by JANABERGER NULLANDVOID <janaberger@lawscot.org.uk>.

The Document has not been modified since this signature was applied.

Hash Algorithm: SHA1

Document Versioning

Document revision 1 of 1

This revision of the document has not been altered

For integrity purposes, you should always verify what was signed by viewing the signed version of the document. This is not necessary when you are viewing the final version of a document.

Modifications

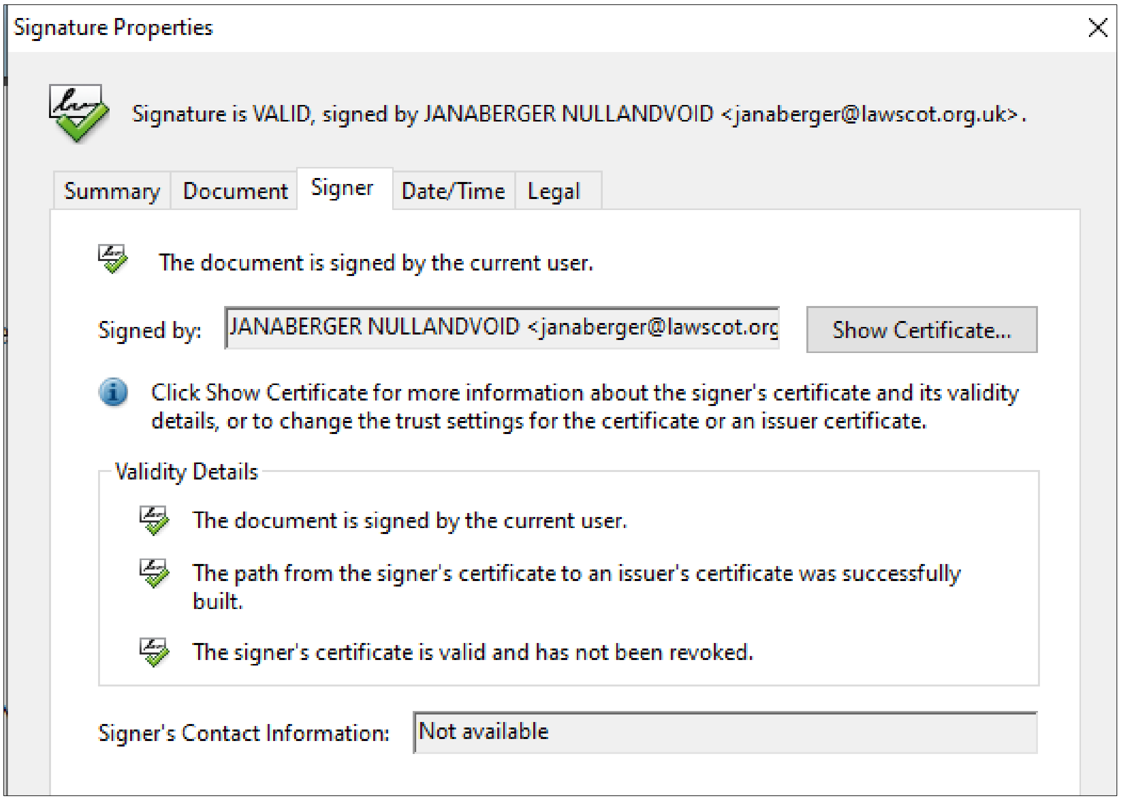
The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.

No changes have been made to this document since this signature was applied.

Modification Details:

There have been no changes made to this document since this signature was applied.

Signer will confirm the signatory:



Signature Properties

Signature is VALID, signed by JANABERGER NULLANDVOID <janaberger@lawscot.org.uk>.

The document is signed by the current user.

Signed by: JANABERGER NULLANDVOID <janaberger@lawscot.org

Click Show Certificate for more information about the signer's certificate and its validity details, or to change the trust settings for the certificate or an issuer certificate.

Validity Details

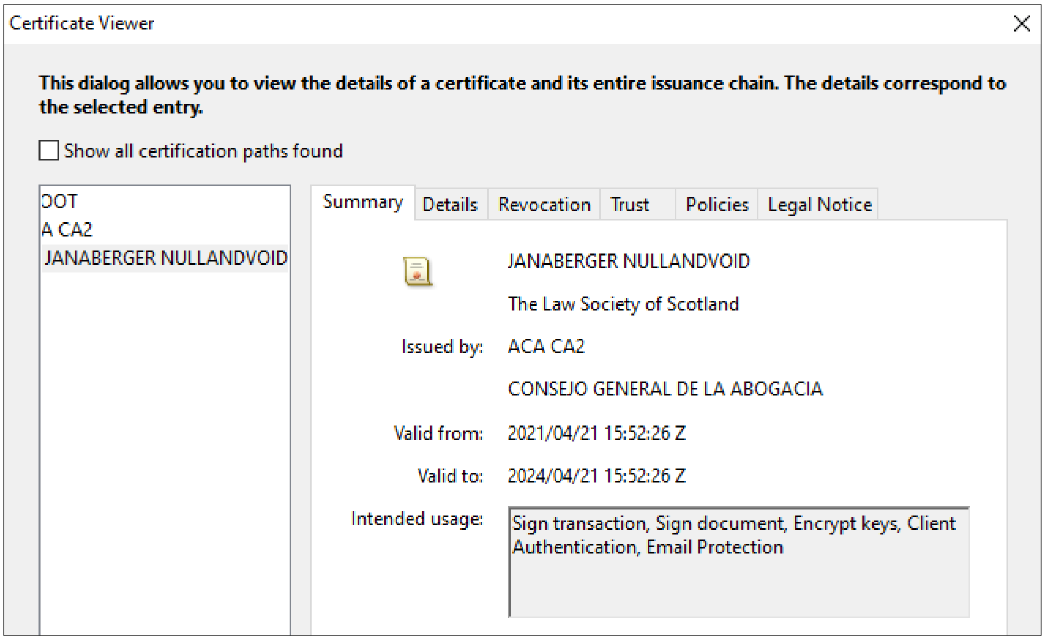
The document is signed by the current user.

The path from the signer's certificate to an issuer's certificate was successfully built.

The signer's certificate is valid and has not been revoked.

Signer's Contact Information: Not available

Going one step further, you can click **Show Certificate** to ensure it is valid and was issued by ACA, the Certification Authority for the LSS Smartcard signatures:



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

OOT
A CA2
JANABERGER NULLANDVOID

JANABERGER NULLANDVOID

The Law Society of Scotland

Issued by: ACA CA2

CONSEJO GENERAL DE LA ABOGACIA

Valid from: 2021/04/21 15:52:26 Z

Valid to: 2024/04/21 15:52:26 Z

Intended usage: Sign transaction, Sign document, Encrypt keys, Client Authentication, Email Protection

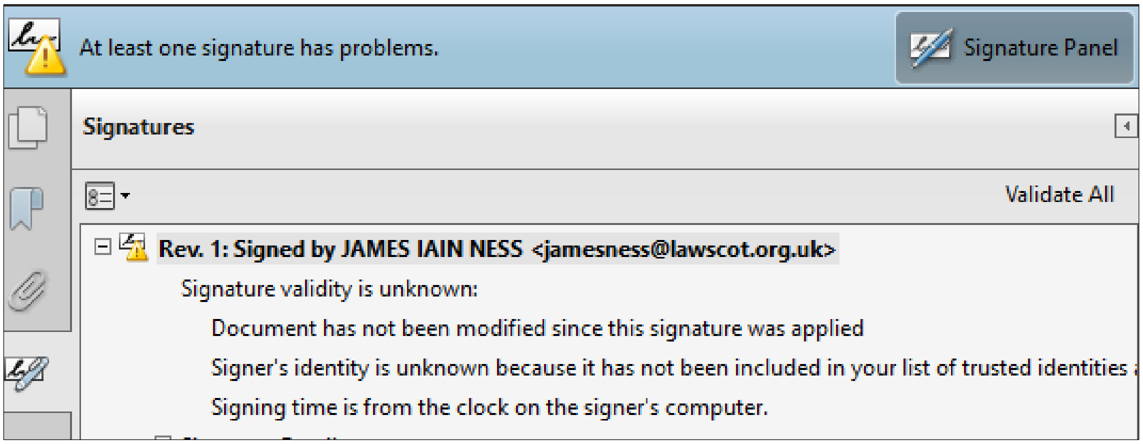
Trusting the Signature

In order to apply a signature, the so-called root certificate needs to be installed. With Microsoft Windows, that is done in the "Windows Certificate Store." Once there, it is used for applying signatures as well as validating them. Every other signature with the same root certificate is subsequently recognised as belonging to the same root. It is validated by the system automatically when you receive a document signed with such a signature. You can still do your own checks as to the identity of the signatory and the quality of the signature itself.
Adobe, on the other hand, does not quite work this way. Here, root certificates are collected in the "Trusted Identity List" that gets updated automatically in regular intervals. Your Adobe version then checks against that list to determine what's what in a signed document.

However, not every IT system allows all updates, or they do not filter through to every computer. And although ACA, the Spanish Bar Association and Certification Authority supplying the root certificate for the LSS Smartcard QES, is on the "Trusted Identities" list, it is not always recognised as trusted root. Which means, signing a PDF is easy, but you as the recipient might not see a valid a signature because your own Adobe list is incomplete.

"At least one signature has problems" is the error message indicating missing trusted roots.

If you click on the **Signature Panel** next to it and then open the signature in question, the PDF will tell you that it cannot verify the signature:



At least one signature has problems.

Rev. 1: Signed by JAMES IAIN NESS <jamesness@lawscot.org.uk>

Signature validity is unknown:

Document has not been modified since this signature was applied

Signer's identity is unknown because it has not been included in your list of trusted identities

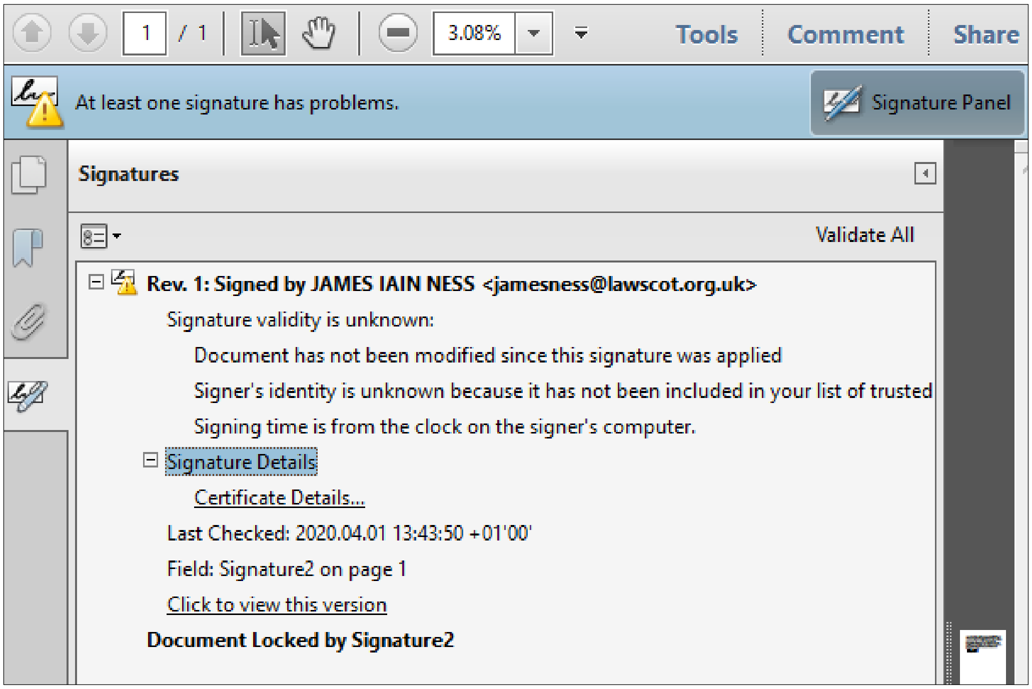
Signing time is from the clock on the signer's computer.

There are two ways around that problem. One is to independently import the ACA root certificate manually into the allowed certificate provider list, the "Trusted Identities." However, that requires a deep dive into your Adobe set-up, which is why it is usually done by the IT department. If you want to have a look, the following Adobe sites offer advice and help: Managing Certificates, and Manage Trusted Identities.

The other way would be to trust the root certificate of the signature itself. This way, similar to Microsoft Word, all subsequently received signatures with the same root are automatically trusted as well. This needs to be done on the recipient's side and requires a few clicks with the mouse:

1. Open the Signature Panel

Inside the panel, double-click the signature in question and from here go to **Signature Details** and then **Certificate Details…**



At least one signature has problems.

Rev. 1: Signed by JAMES IAIN NESS <jamesness@lawscot.org.uk>

Signature validity is unknown:

Document has not been modified since this signature was applied

Signer's identity is unknown because it has not been included in your list of trusted

Signing time is from the clock on the signer's computer.

Signature Details

Certificate Details...

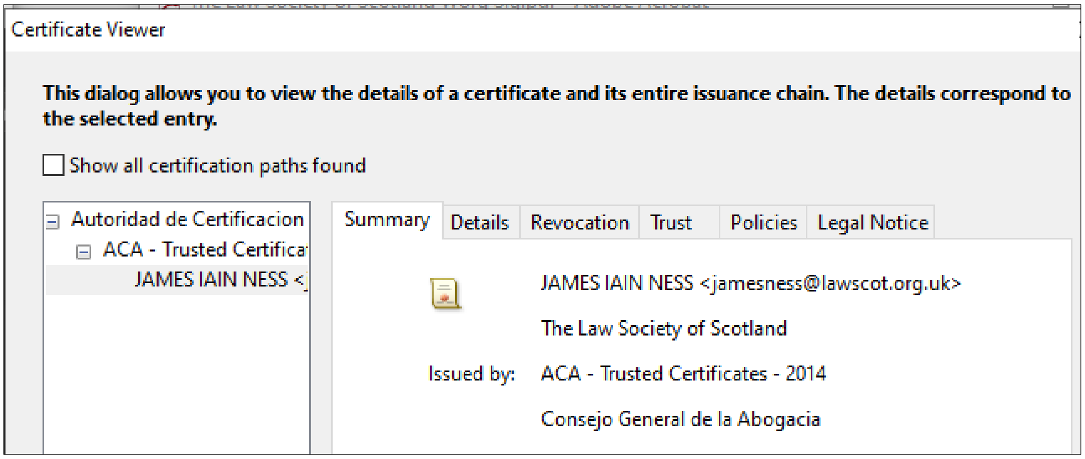
Last Checked: 2020.04.01 13:43:50 +01'00'

Field: Signature2 on page 1

Click to view this version

Document Locked by Signature2

The **Certificate Details…** panel provides information about the signature in question: The name of the signatory, who issued the underlying certificate, how long it is valid.



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

Autoridad de Certificacion
ACA - Trusted Certifica
JAMES IAIN NESS <

JAMES IAIN NESS <jamesness@lawscot.org.uk>

The Law Society of Scotland

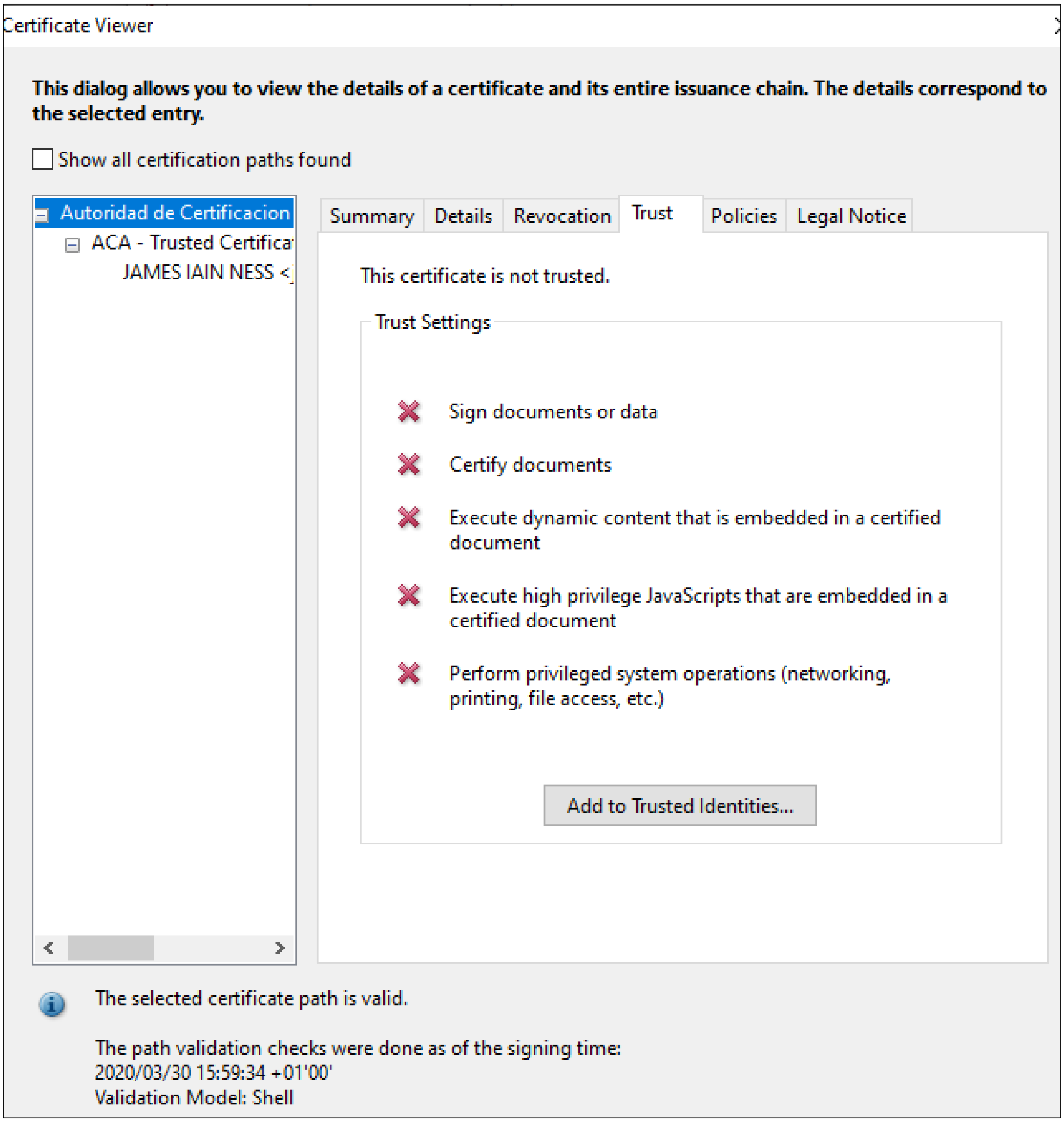
Issued by: ACA - Trusted Certificates - 2014

Consejo General de la Abogacia

You can also see what's called an "issuance chain" on the left-hand side. The signature you are looking at is based on an underlying certificate issued by ACA. That in itself is based on a root certificate - the top entry in that list. This is the one that needs to be trusted in your Adobe version on your computer. Once done, every other signature based on the same root, i.e. every other Smartcard QES, will also be trusted in your system.

2. Trusting the root certificate

Go to the tab labelled **Trust**.



Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

□ Show all certification paths found

This certificate is not trusted.

Trust Settings

✗ Sign documents or data

✗ Certify documents

✗ Execute dynamic content that is embedded in a certified document

✗ Execute high privilege JavaScripts that are embedded in a certified document

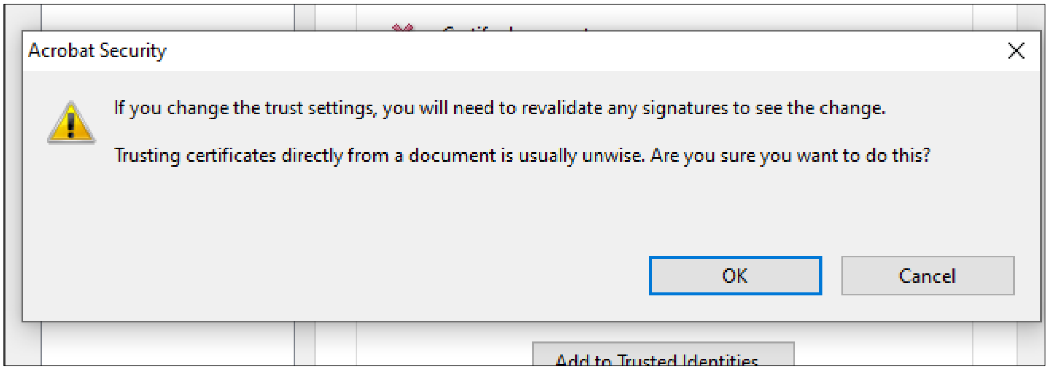
✗ Perform privileged system operations (networking, printing, file access, etc.)

The selected certificate path is valid.

The path validation checks were done as of the signing time:
2020/03/30 15:59:34 +01'00'
Validation Model: Shell

Please make sure you highlight (one mouse-click) the top entry in the left-hand side window. This is the root certificate that needs to be added to the “Trusted Identities” in Adobe. In contrast, should you e.g. highlight only the last entry on that list (i.e. the signatory), your system would only trust this particular signatory/signature, and no-one else. Any other PDF document from anyone else, even when signed with the Smartcard QES, would not be trusted and you would get the original error message again and again. You need to enable the root certificate - the top entry.

Click the button **Add to Trusted Identities**. Adobe will put up a warning:

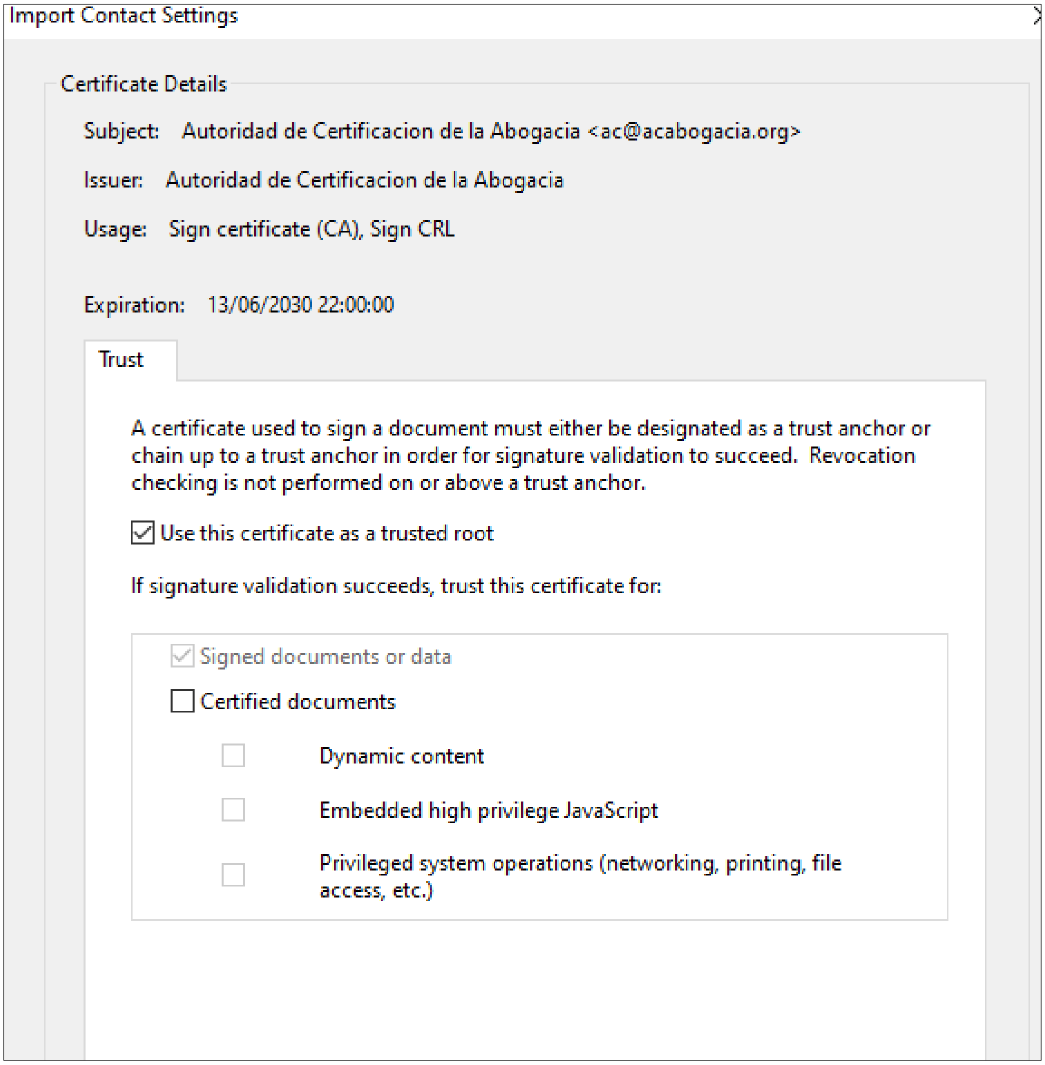


If you change the trust settings, you will need to revalidate any signatures to see the change.

Trusting certificates directly from a document is usually unwise. Are you sure you want to do this?

This is supposed to happen. It is a safety message to prevent users/recipients from trusting signatures from just anyone & anywhere without thinking about it. However, in this case you are trusting the ACA, i.e. the Spanish Bar Association and Certification Authority for the Smartcard signatures. It's perfectly alright - click **OK**.

The following window shows you the specifics of that root certificate (issuer, expiration date) and lets you specify to "Use this certificate as a trusted root" - please do.



Subject: Autoridad de Certificacion de la Abogacia <ac@acabogacia.org>

Issuer: Autoridad de Certificacion de la Abogacia

Usage: Sign certificate (CA), Sign CRL

Expiration: 13/06/2030 22:00:00

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

☑ Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

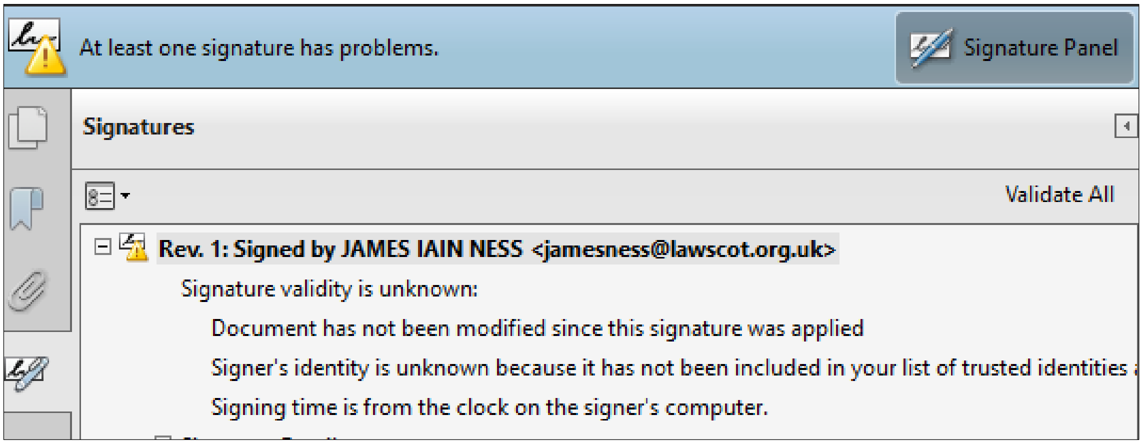
- ☑ Signed documents or data
- □ Certified documents
  - □ Dynamic content
  - □ Embedded high privilege JavaScript
  - □ Privileged system operations (networking, printing, file access, etc.)

Click **OK**.

This window will disappear, and the **Trust** tab appear again, without any changes. That is normal, just click **OK** again.

3. Revalidating

As the warning said, you will need to revalidate the signatures in your document to see any changes. “Revalidating” in this context simply means re-checking. By adding the root certificate to your “Trusted Identities,” you changed a setting in Adobe and it needs to check/”validate” against this new parameter. You do that by clicking **Validate All** in the **Signature Panel**:



At least one signature has problems.

Rev. 1: Signed by JAMES IAIN NESS <jamesness@lawscot.org.uk>

Signature validity is unknown:

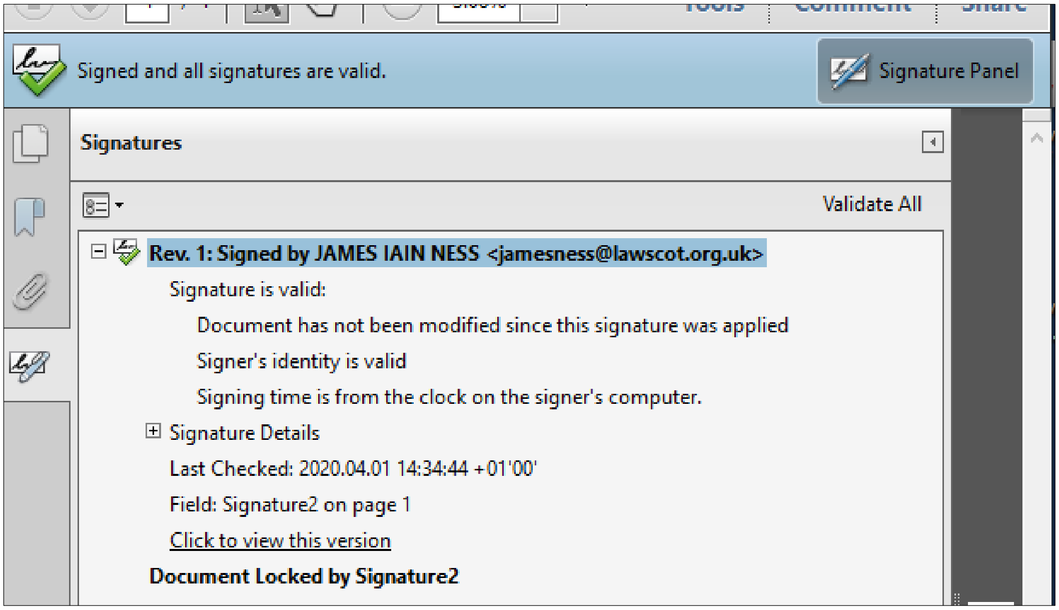
Document has not been modified since this signature was applied

Signer's identity is unknown because it has not been included in your list of trusted identities

Signing time is from the clock on the signer's computer.

Adobe will ask you if you really want to do that - it might take some time in large documents - and will then inform you that the check is complete.

You can see the change immediately:



Signed and all signatures are valid.

Rev. 1: Signed by JAMES IAIN NESS <jamesness@lawscot.org.uk>

Signature is valid:

Document has not been modified since this signature was applied

Signer's identity is valid

Signing time is from the clock on the signer's computer.

Signature Details

Last Checked: 2020.04.01 14:34:44 +01'00'

Field: Signature2 on page 1

Click to view this version

Document Locked by Signature2

From now on, all other Smartcard signatures applied to pdf documents will be checked against the ACA certificate you just added.

Declining a Signature

If the **Certificate Details** and the **issuance chain** do not say "ACA" as the issuing agency, then that signature in front of you is not a QES issued by the Law Society. You will need to conduct your own checks as to the validity of the signature and the identity of the signatory.

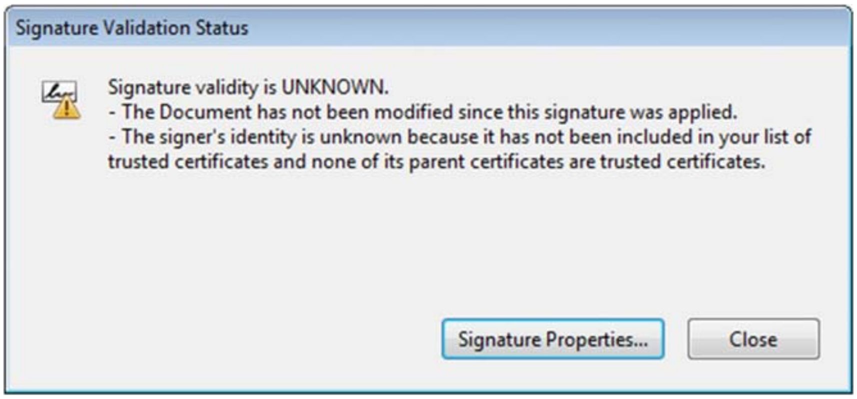
Older versions of Adobe

As mentioned earlier, older editions of Adobe software might have different looking windows and pop-ups. Below you find a selection of screenshots from previous versions of the guide to validating a signature in PDF documents.

Please remember, when confirming the validity of a digital signature, you need to interrogate the digital signature itself, NOT the visual representation that may or may not be visible on the document. That means, validating a digital signature is only possible on the computer, not with a print-out of the document.

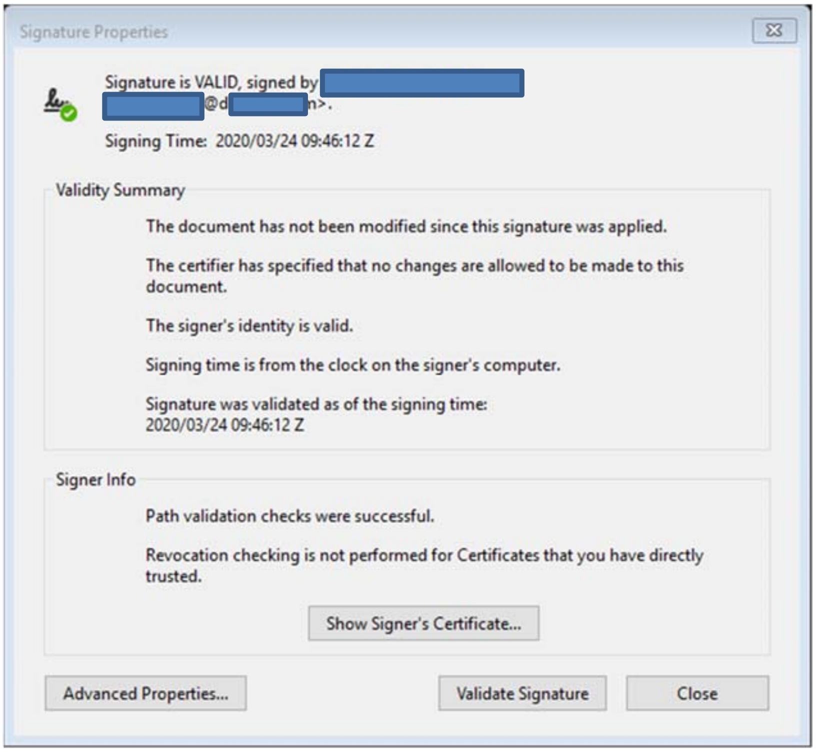
Signature Line

Clicking on the name of the signatory visible at the bottom of the document will give you a high-level overview.
(Ignore the "unknown validity," this is just an example.)



Signature validity is UNKNOWN.
- The Document has not been modified since this signature was applied.
- The signer's identity is unknown because it has not been included in your list of trusted certificates and none of its parent certificates are trusted certificates.

By selecting **Signature Properties**, more information will be available.



Signature is VALID, signed by [redacted] [redacted]@d[redacted]n>.

Signing Time: 2020/03/24 09:46:12 Z

Validity Summary

The document has not been modified since this signature was applied.

The certifier has specified that no changes are allowed to be made to this document.

The signer's identity is valid.

Signing time is from the clock on the signer's computer.

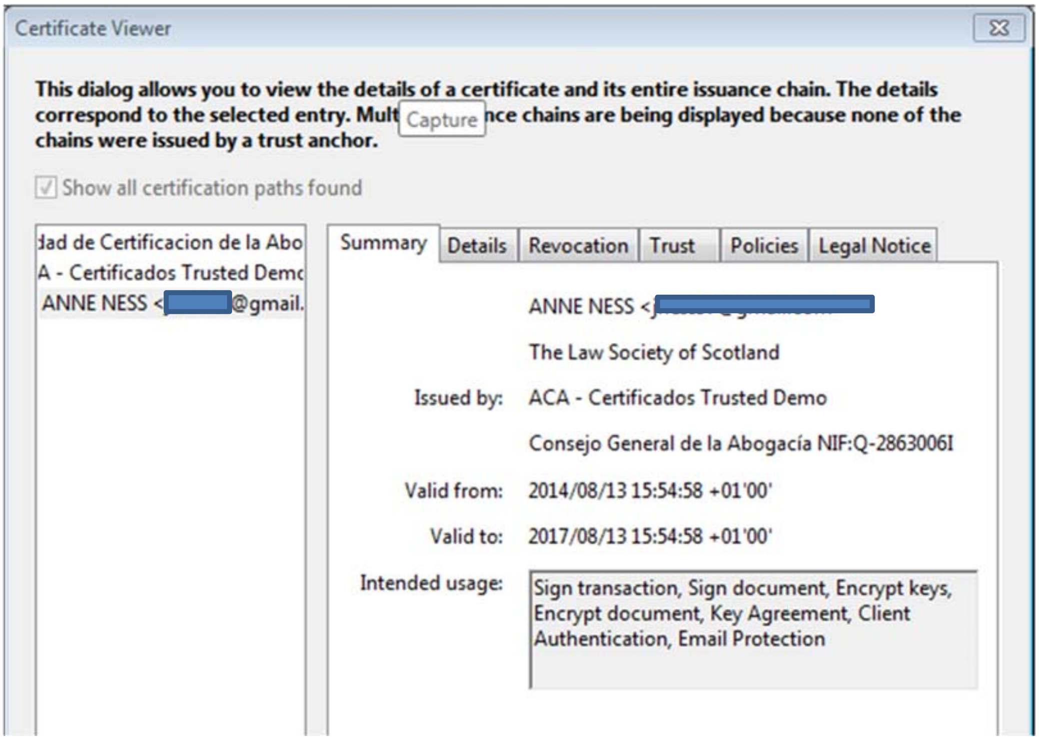
Signature was validated as of the signing time:
2020/03/24 09:46:12 Z

Signer Info

Path validation checks were successful.

Revocation checking is not performed for Certificates that you have directly trusted.

By clicking **Show Signer's Certificate…** you will see information identical to the one in later versions of Adobe:



This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry. Mult nce chains are being displayed because none of the chains were issued by a trust anchor.

☑ Show all certification paths found

dad de Certificacion de la Abo
A - Certificados Trusted Demo
ANNE NESS <[redacted]@gmail.

	ANNE NESS <[redacted]
	The Law Society of Scotland
Issued by:	ACA - Certificados Trusted Demo
	Consejo General de la Abogacía NIF:Q-2863006I
Valid from:	2014/08/13 15:54:58 +01'00'
Valid to:	2017/08/13 15:54:58 +01'00'
Intended usage:	Sign transaction, Sign document, Encrypt keys, Encrypt document, Key Agreement, Client Authentication, Email Protection

As before, important to note here are two lines: one, the name of the signatory and the fact that it says "Law Society of Scotland" underneath, and two, that the certificate was issued by ACA.