

LAW SOCIETY OF SOTLAND - SMARTCARD

Verifying a Digital Signature in Electronic Documents - Adobe

This guide will take you through how to view and 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.

Since different firms use different editions of word processing software, the following steps are duplicated - one version for Word 2010 & Office 365, and one for Adobe PDF. Even if you use a different version of either software, you will be able to use either of the following instructions. (The buttons might look different, but the functionality will be the same.)

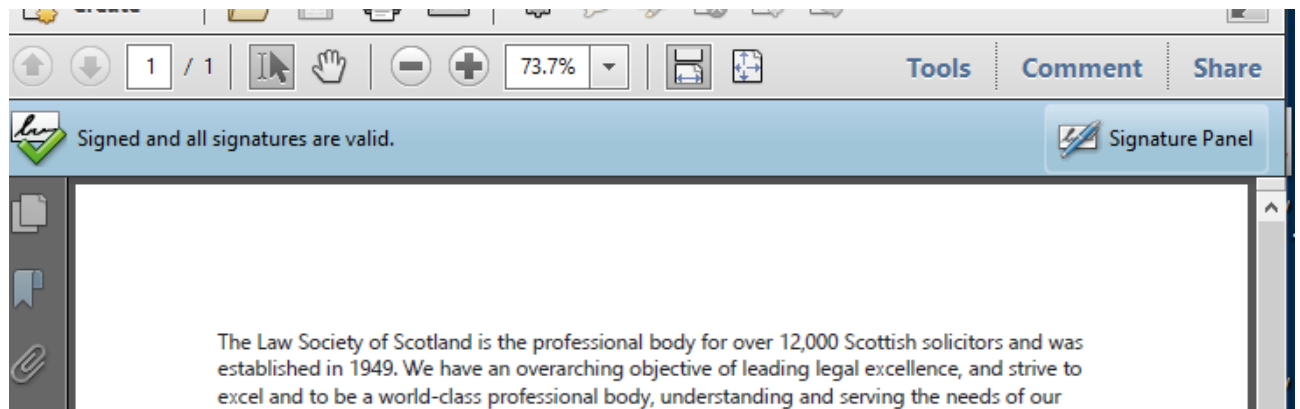
Regardless of what word processing software or edition is used: You need to interrogate the digital signature itself, NOT the visual representation that may or may not be visible on the document. That means, validating or confirming a digital signature is only possible on the computer, not with a print-out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

Digital Signature Verification – Adobe PDF

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 **STEP 3 - Trusting the Signature** and **STEP 4 - Revalidating**. Nothing is wrong with the signature, it simply means your Adobe version has not been set up yet.

STEP 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:



However, it doesn't give much information about the signatory and the signature itself. For that, you can check in two different places.

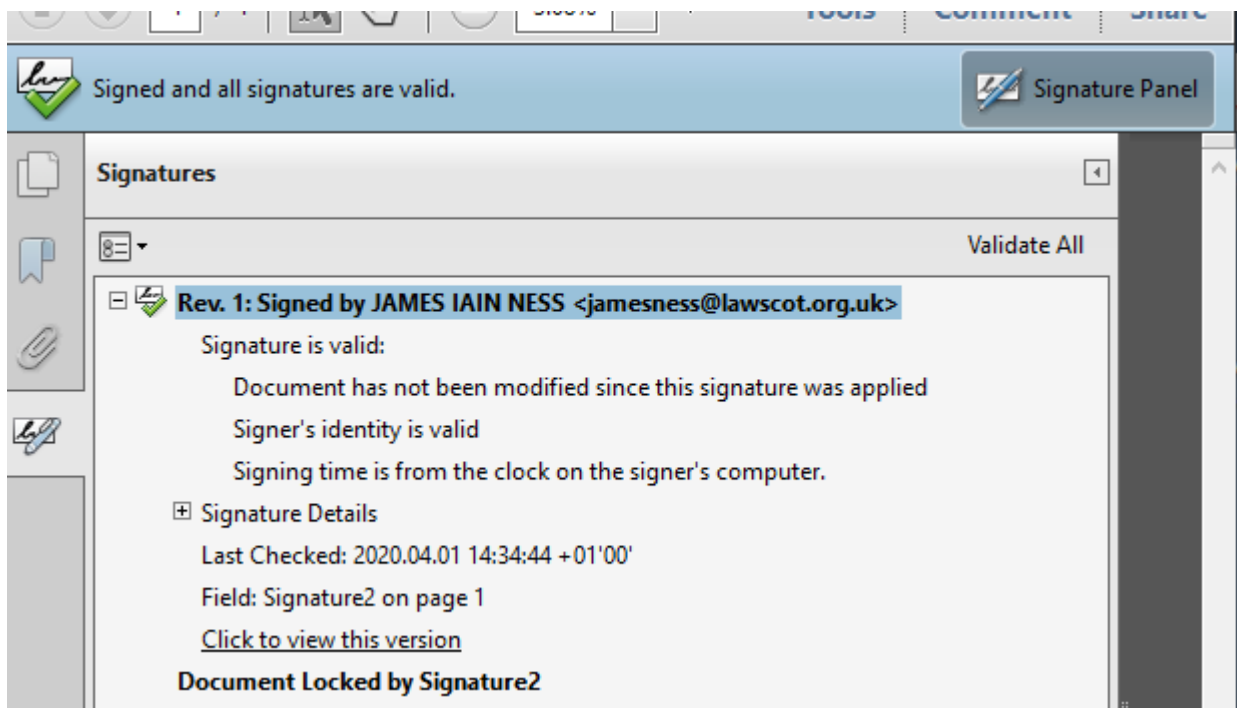
STEP 2 - Interrogating the signature

There are several ways to confirm the validity of the signature and the identity of the signatory.

NB: Different versions of Adobe Acrobat or Reader will have different looking windows and pop-ups. However, the name of the panels and the information contained therein will be the same. See at the end of this guide for screenshots from older versions of the software.

1) Signature Panel

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



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

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

dad de Certificación de la Abo
A - Trusted Certificates - 2014
JAMES IAIN NESS <jamesness@

Summary Details Revocation Trust Policies Legal Notice



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

The Law Society of Scotland

Issued by: ACA - Trusted Certificates - 2014

Consejo General de la Abogacia

Valid from: 2017/05/09 11:23:44 +01'00'

Valid to: 2020/05/09 11:23:44 +01'00'

Intended usage: Sign transaction, Sign document, Encrypt keys, Encrypt document, Key Agreement, 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.

2) Signature Line

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

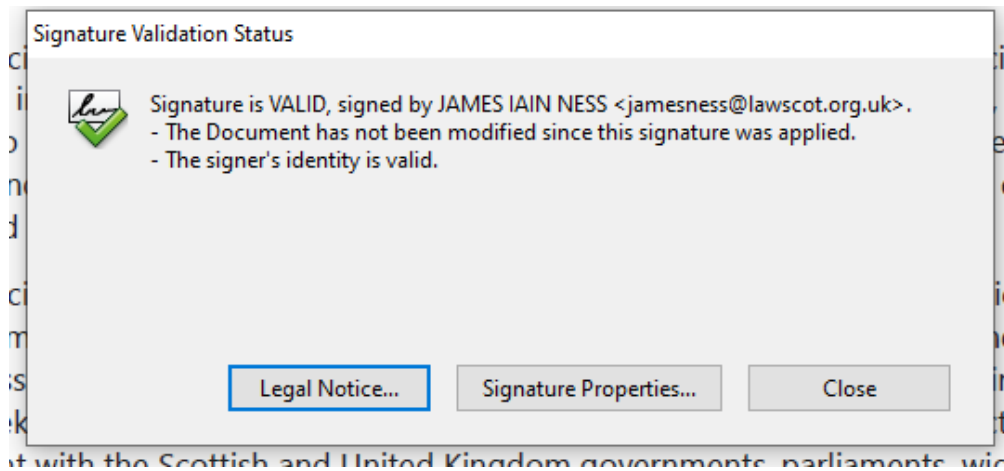
legal profession working in the interests of the
law. We seek to influence the creation of a firm
engagement with the Scottish and United Kingdom
stakeholders and our membership.

**JAMES
IAIN NESS** Digitally signed by
JAMES IAIN NESS
Date: 2020.03.30
15:59:34 +01'00'

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.

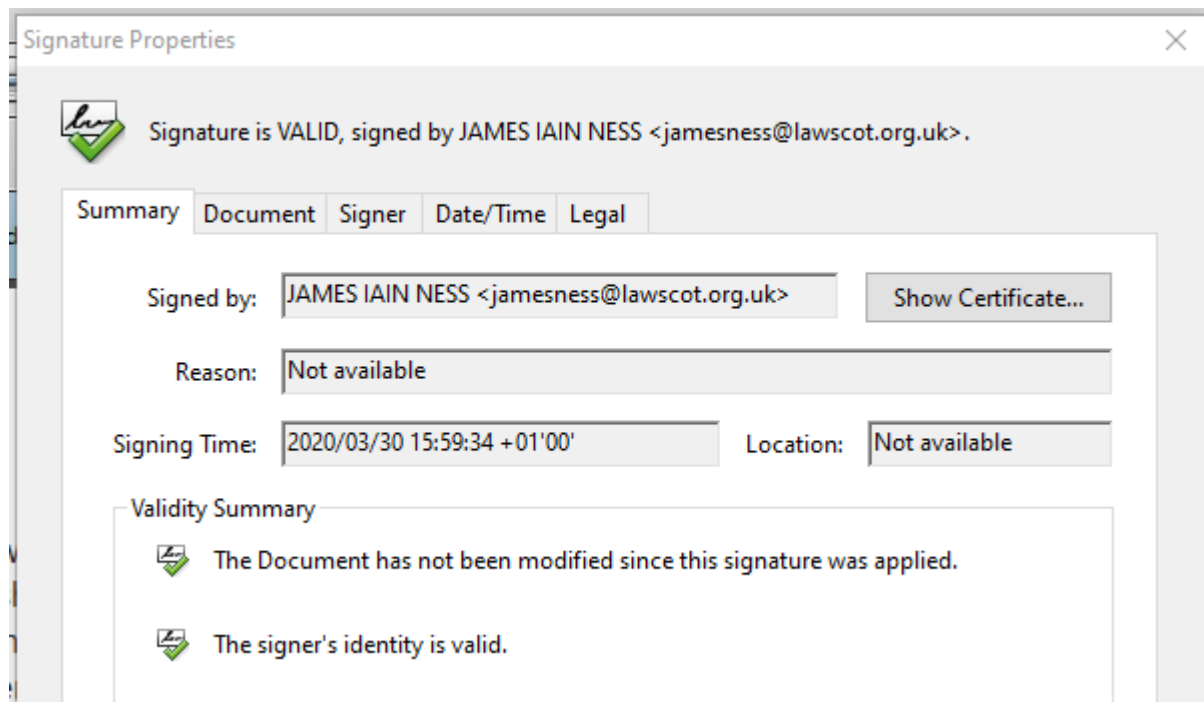
Click the on the name of the signatory and it will give you several levels of validity checks:

General Status:



Signature Properties:

Clicking on the above button will open up a window that let's you thoroughly interrogate the signature in front of you:



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

Summary Document Signer Date/Time Legal

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

Hash Algorithm: SHA256

Document Versioning

Document revision 1 of 1

[View Signed Version...](#)

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 no changes are allowed to be made to this document.

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.



[Compute Modifications List](#)

Signer will confirm the signatory:

 Signature is VALID, signed by JAMES IAIN NESS <jamesness@lawscot.org.uk>.

Summary Document **Signer** Date/Time Legal

 The signer's identity is valid.

Signed by:

 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 signer's certificate has been issued by a certificate authority that you have trusted to issue certificates for the purpose of signing.
-  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.

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

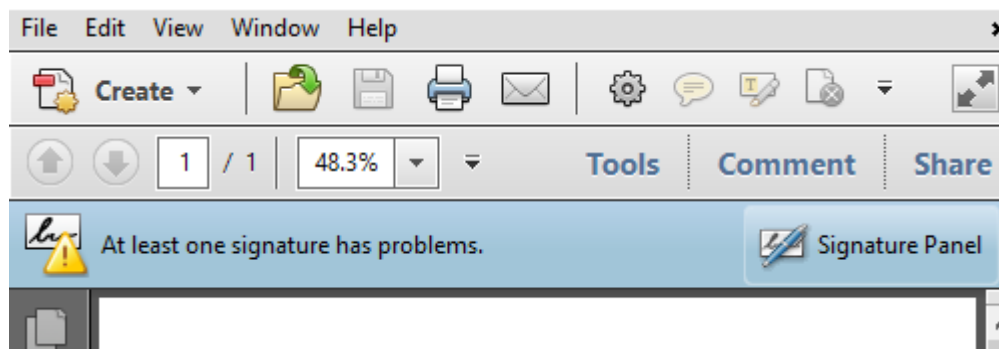
dad de Certificacion de la Abo A - Trusted Certificates - 2014 JAMES IAIN NESS <jamesness@	Summary	Details	Revocation	Trust	Policies	Legal Notice
	 JAMES IAIN NESS <jamesness@lawscot.org.uk> The Law Society of Scotland Issued by: ACA - Trusted Certificates - 2014 Consejo General de la Abogacia Valid from: 2017/05/09 11:23:44 +01'00' Valid to: 2020/05/09 11:23:44 +01'00' Intended usage: Sign transaction, Sign document, Encrypt keys, Encrypt document, Key Agreement, Client Authentication, Email Protection					

STEP 3 - Trusting the Signature

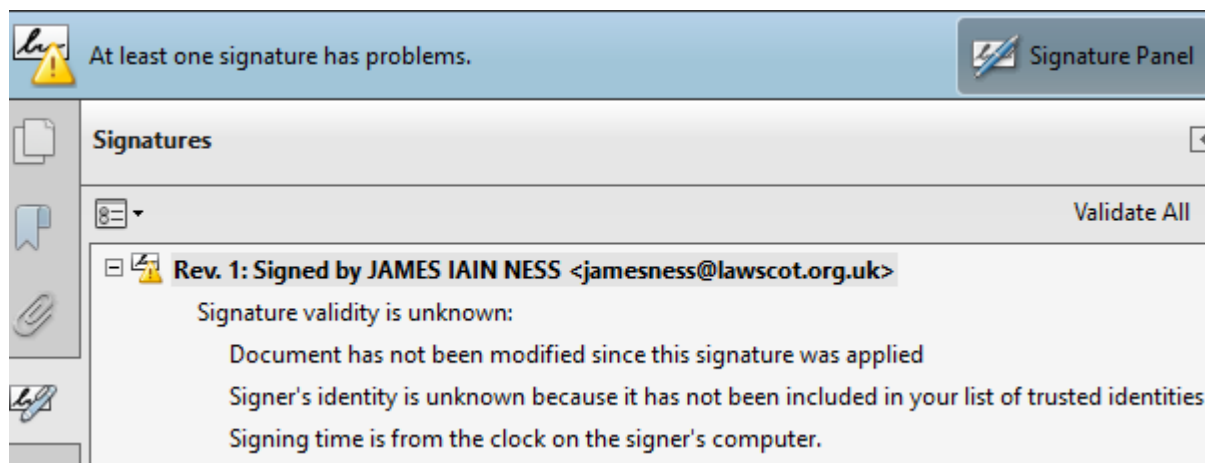
In order to apply a signature, the so-called root certificate needs to be installed. With Microsoft Windows, that is done in the “Windows Certificate Store.” Once there, it is used for applying signatures as well as validating them. Every other signature with the same root certificate is subsequently 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 signature, 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. Instead, when opening the document, you would see this message:



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:

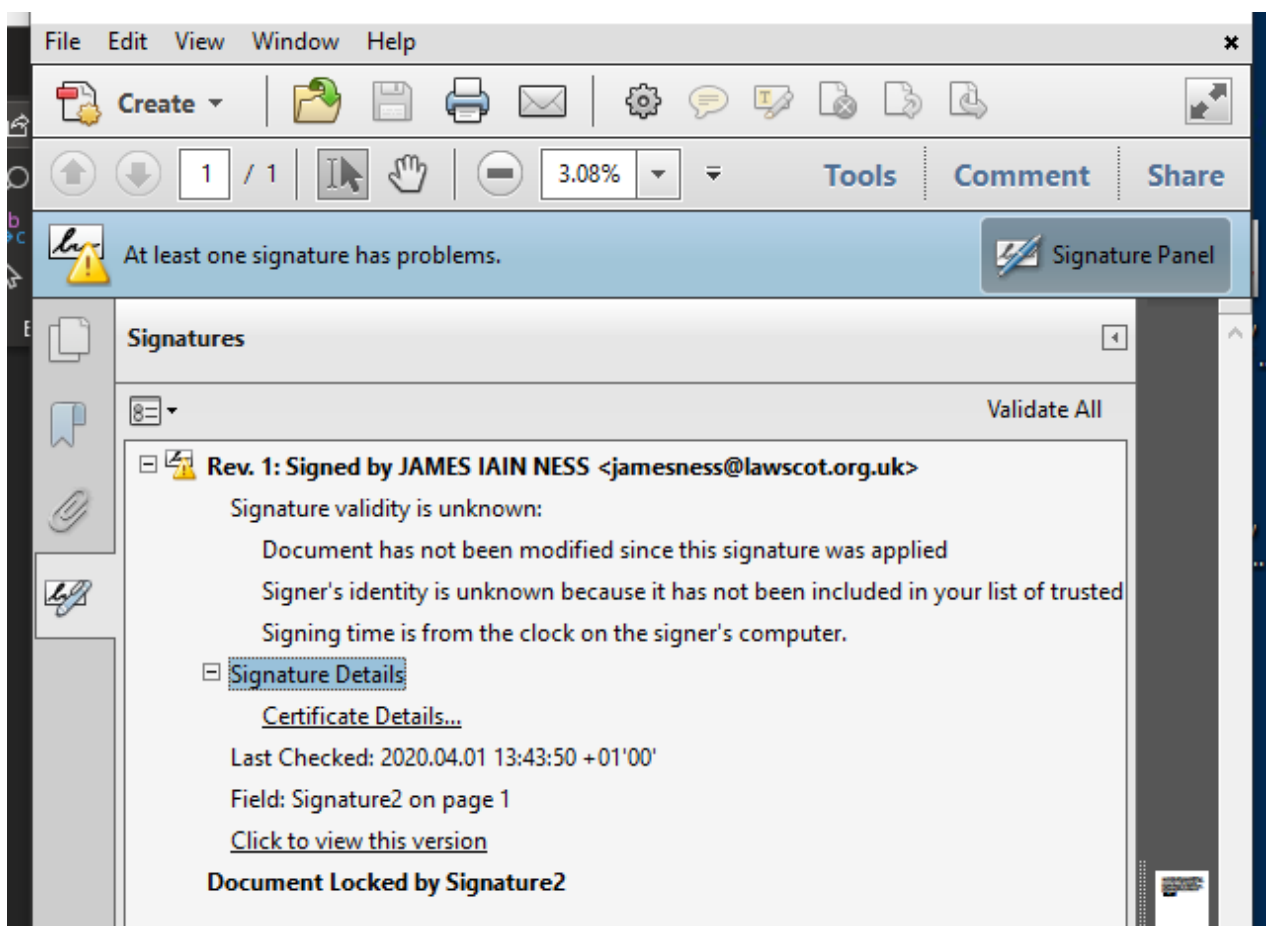


There are two ways around that problem. One is to independently import the ACA root certificate manually into the allowed certificate provider list, the “Trusted Identities.” However, that requires a deep dive into your Adobe set-up, which is why it is usually done by the IT department. If you want to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

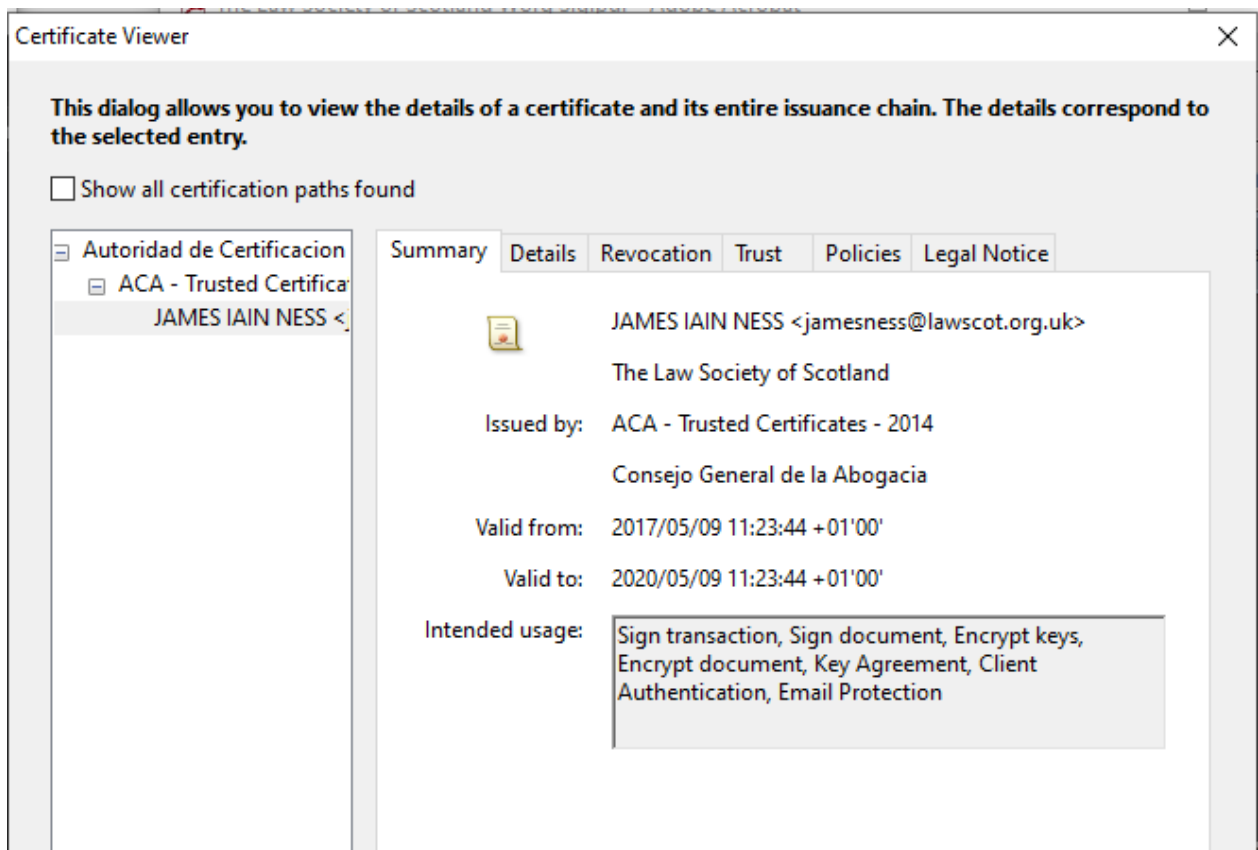
The other way would be to trust the root certificate of the signature itself. This way, similar to Microsoft Word, all subsequently received signatures with the same root are automatically trusted as well. This needs to be done on the recipient’s side and requires a few clicks with the mouse:

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...**



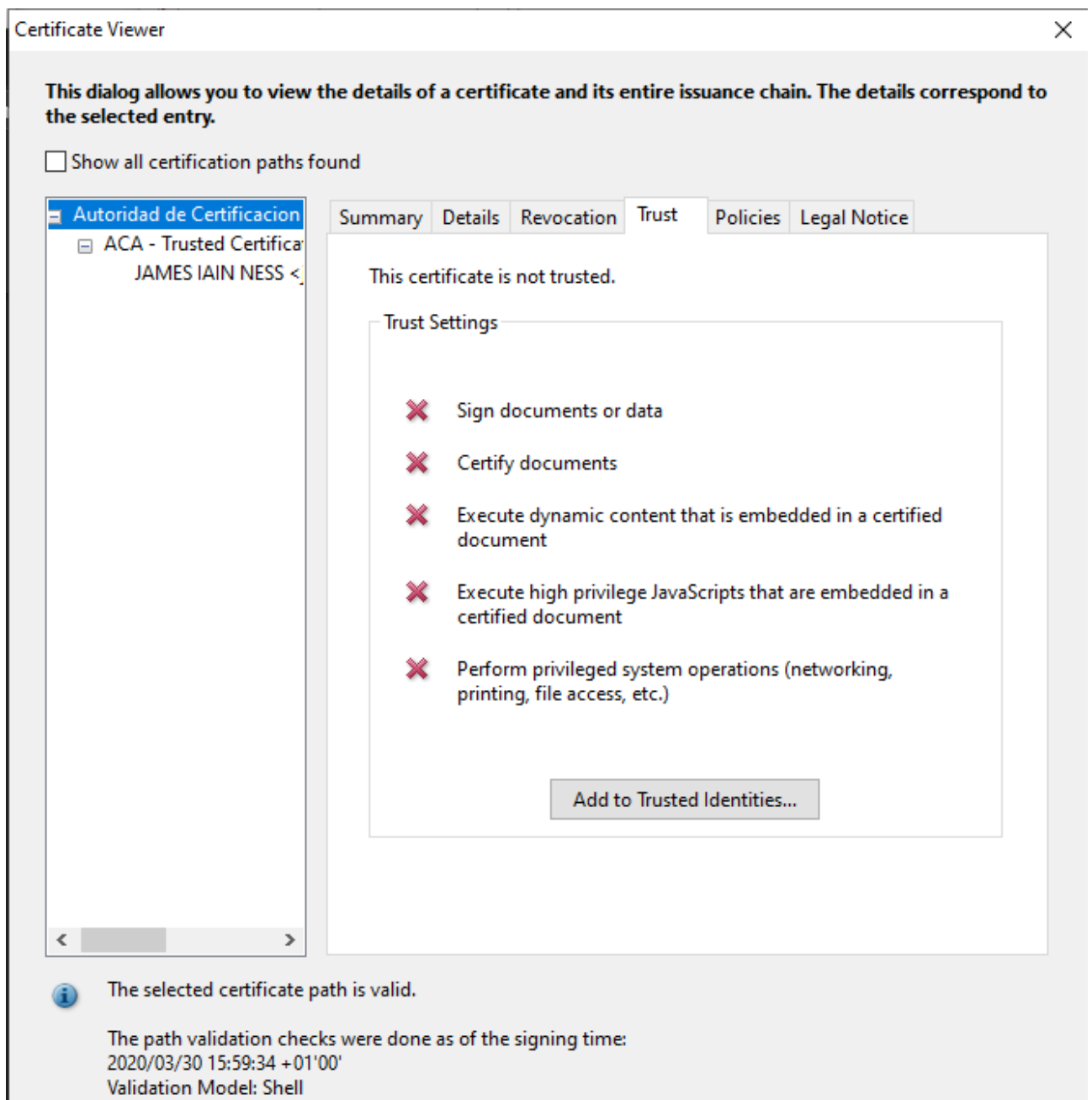
The **Certificate Details...** panel will give you all kinds of information about the signature in question: The name of the signatory, who issued the underlying certificate, how long it is valid.



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. 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 signature, will also be trusted in your system.

2) Trusting the root certificate

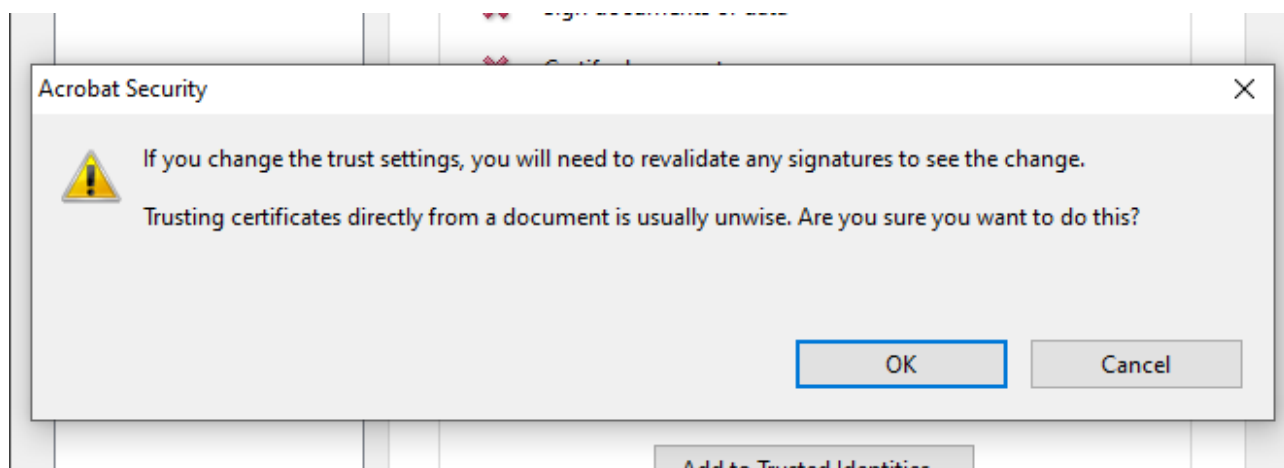
Go to the tab labelled **Trust**.



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 other pdf document from anyone else, even when signed with the Smartcard signature, 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**.

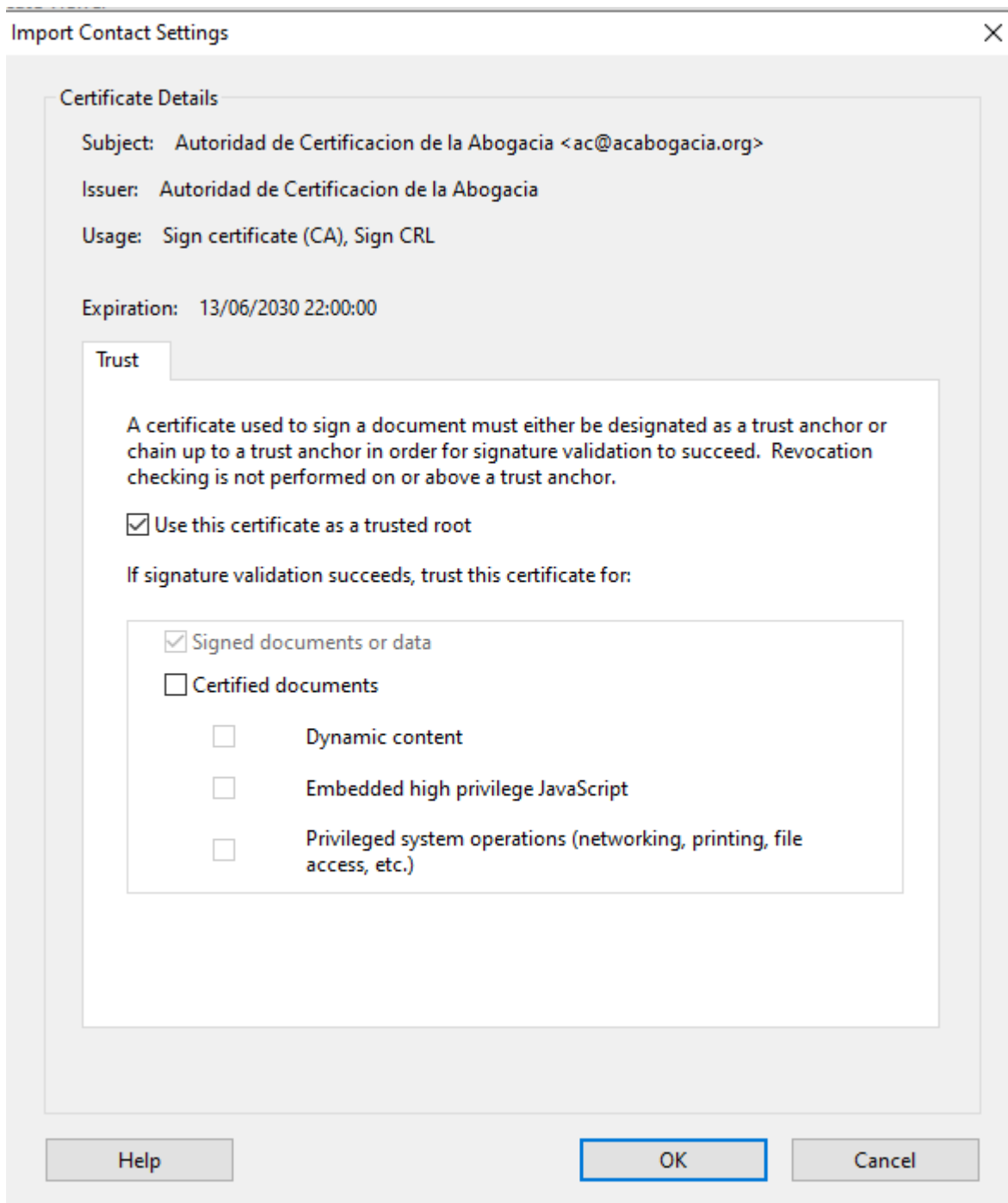
Adobe will put up a warning:



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.

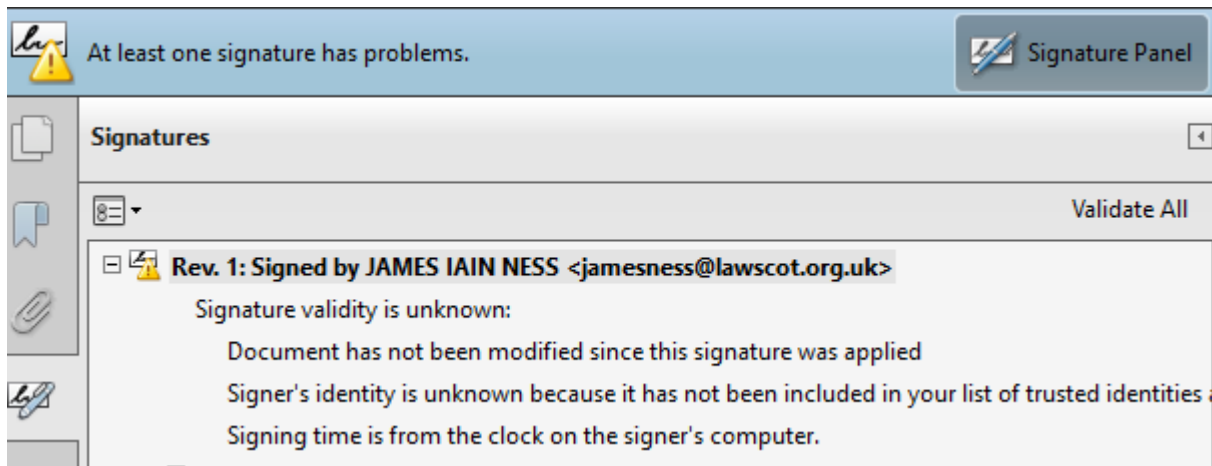
Click **OK**.



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

STEP 4 - 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**:



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:



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

OLDER VERSIONS OF ADOBE ACROBAT AND READER

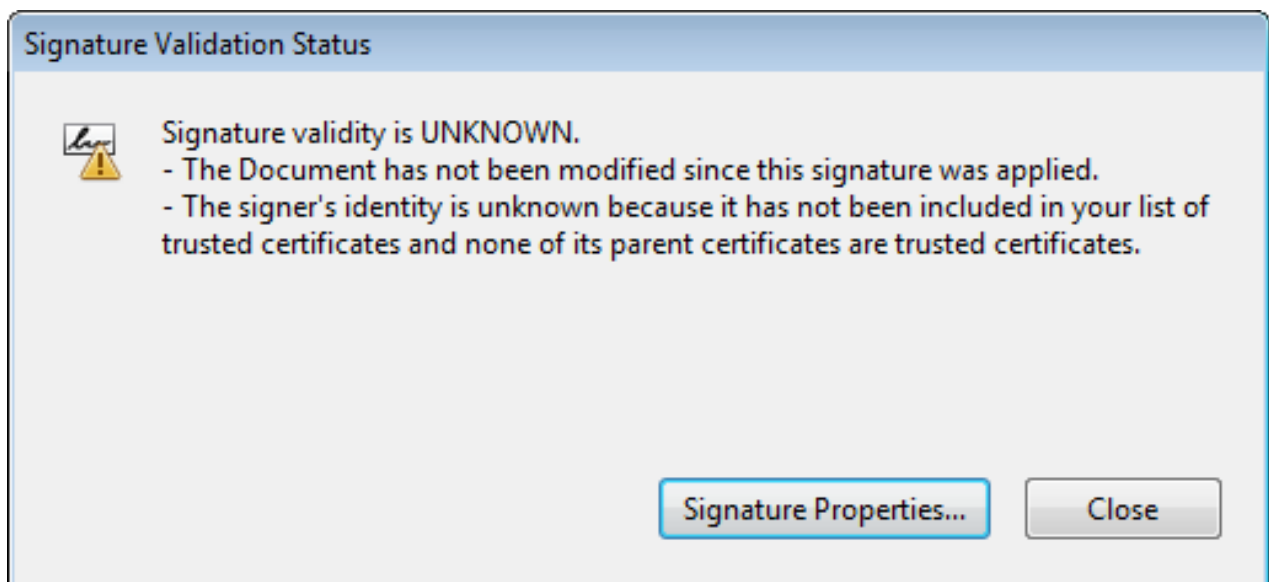
As mentioned earlier, older editions of Adobe software might have different looking windows and pop-ups. Below you find a selection of screenshots from previous versions of the guide to validating a signature in pdf documents.

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.

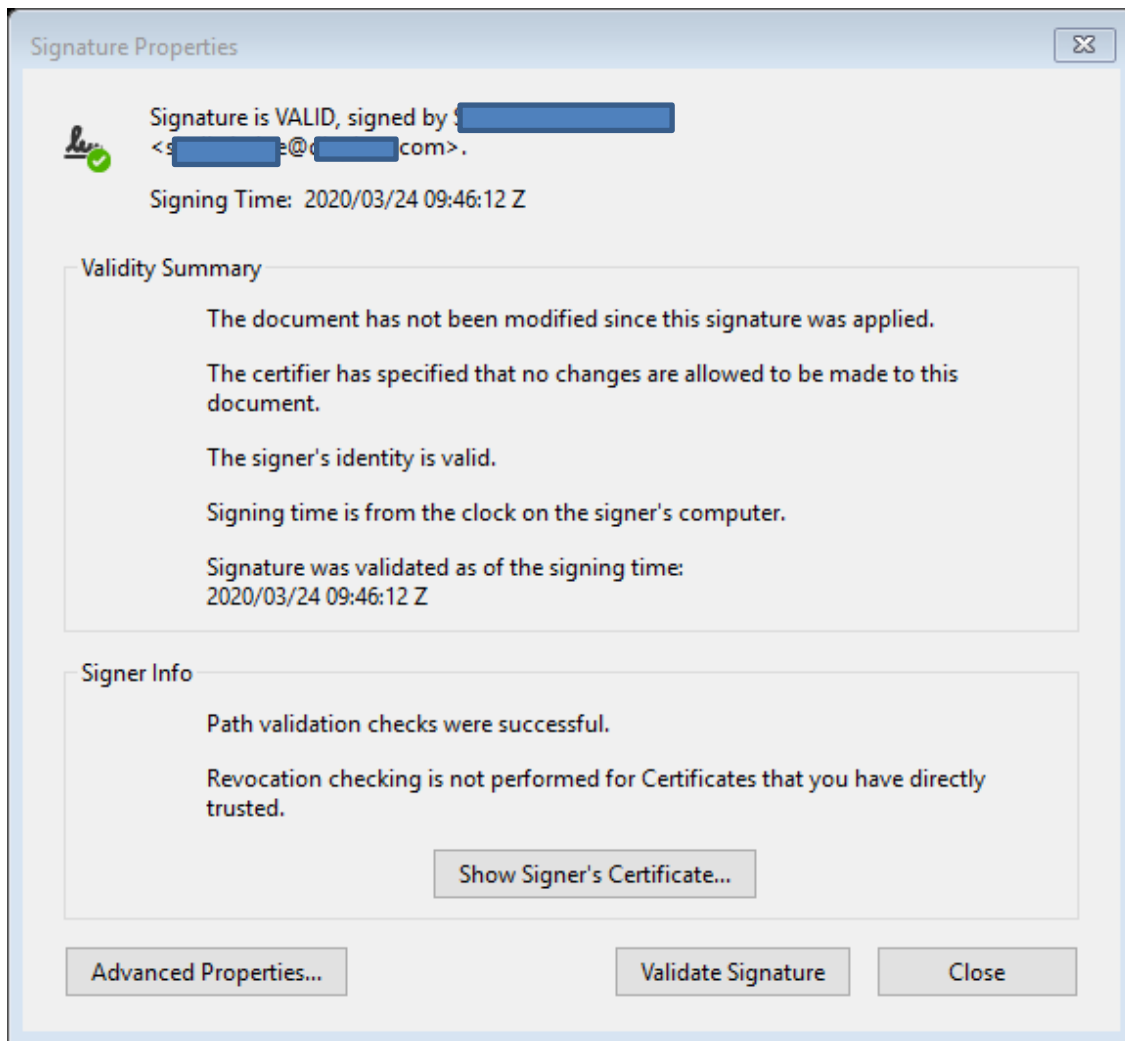
Signature Line

Clicking on the name of the signatory visible at the bottom of the document will give you a high-level overview.

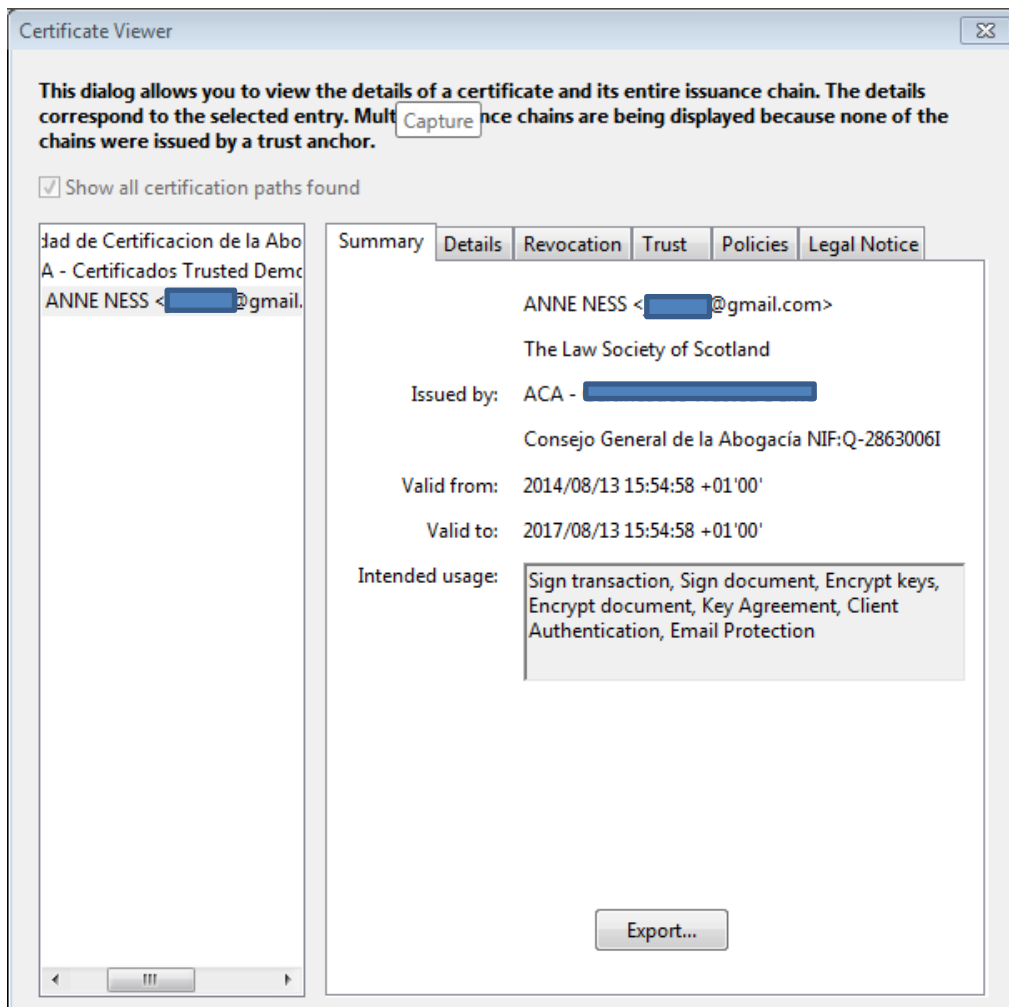
(Ignore the “unknown validity,” this is just an example.)



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



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



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.