Intertek eSignature Customer Reference Document 5.0

Intertek eSignature Customer Reference Document 5.0

Table of Contents

CUSTOMER FREQUENTLY ASKED QUESTIONS

The navigation shown in this document is based on Adobe Acrobat Reader; other versions of Acrobat show data in a different menu.

What is the purpose of eSignature?

eSignature, Intertek's digital signature platform, is used to ensure the long-term integrity of an Intertek document or report. The eSignature solution prevents forged or modified PDF reports by verifying the authenticity of the document and logging any changes after it was signed. Digital signatures allow customers to validate the signature, confirm the time and date stamp, and view the log of modifications made after the document was digitally signed.

An example of the validation message on a signed document could say **"Signed and all signatures are valid"** or **"Certified by NAME (email@intertek.com), Intertek Group plc, certificate issued by Intertek Document Signing Authority"** or **"Certified by Intertek Group plc, (group), certificate issued by QuoVadis Belgium Issuing CA G2"**:

Why could documents signed before September 2016 have a yellow exclamation?

Prior to September 2016 Intertek utilized Comodo as a top-level certificate authority. The result of this was that documents signed using this set of certificates do not automatically verify when using Adobe Acrobat. To validate documents that were signed prior to September 2016, please use the Verifying documents signed before September 2016 section of this document.

VERIFYING INTERTEK-SIGNED DOCUMENTS

Before validating Intertek's eSignature, first ensure that:

- You are using an Adobe-supported and updated version of Adobe Acrobat Reader.
- You have an Internet connection.
- If you are validating a report signed prior to September 2016, you will need to use the Verifying Documents Signed Prior to September 2016 process.

When opening a signed PDF report for the first time, Acrobat Reader should display the message **"Signed and all signatures are valid"** or a variation of **"Certified by Intertek Group plc"** on the top of the document if the

certificate is valid. If the document does not say this, please refer to the section on What steps should be taken if eSignature validation fails.

Note: If your document was signed before September 2016, it may show a yellow exclamation mark with the text "At least one signature has problems." If you see this message, please use the steps for Verifying Documents Signed Prior to September 2016.

Verifying documents signed after September 2016

To verify the digital signature placed by Intertek's eSignature platform:

1. Open the signed document and look for the message that the document is **"Signed and all signatures are valid"** or a variation of **"Certified by Intertek Group plc"**

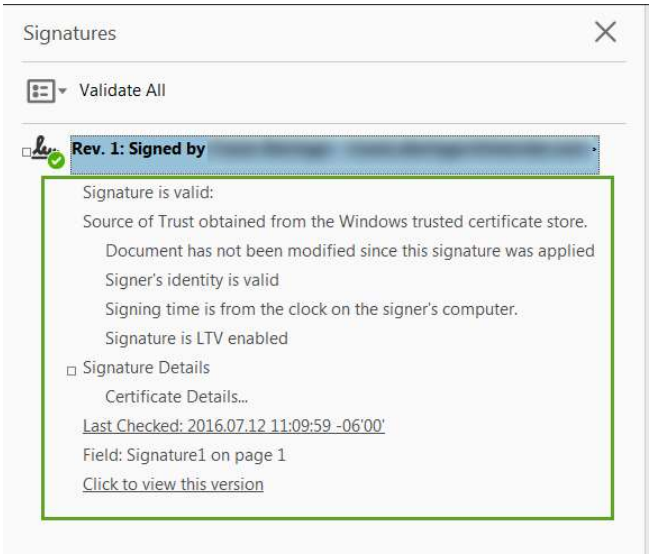
2. Open the signature panel by clicking on the "Signature Panel" button

3. Expand the signature item by double-clicking on it and verify all the appropriate information that is outlined in green below. Verify the certificate details match the details from the Valid Intertek Signing Certificates section.

   This should include the following verifications:

   - Signature is valid.
   - Document has not been modified since this signature was applied.
   - Signer's identity is valid.

- Signature is LTV enabled.



Verifying documents signed before September 2016

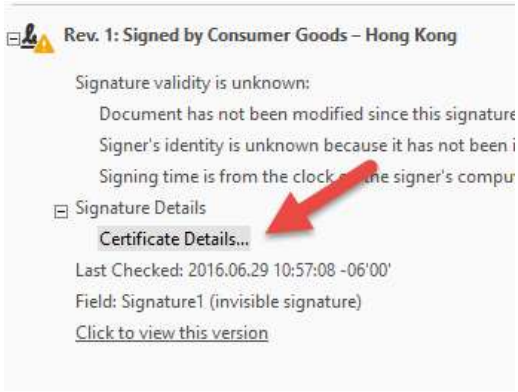
Note: This section only applies to documents signed before September 2016.

If the error says "Signature is valid, but revocation of the signer's identity could not be checked", first ensure that you have an Internet connection, and then follow the steps to check the certificate expiration date.

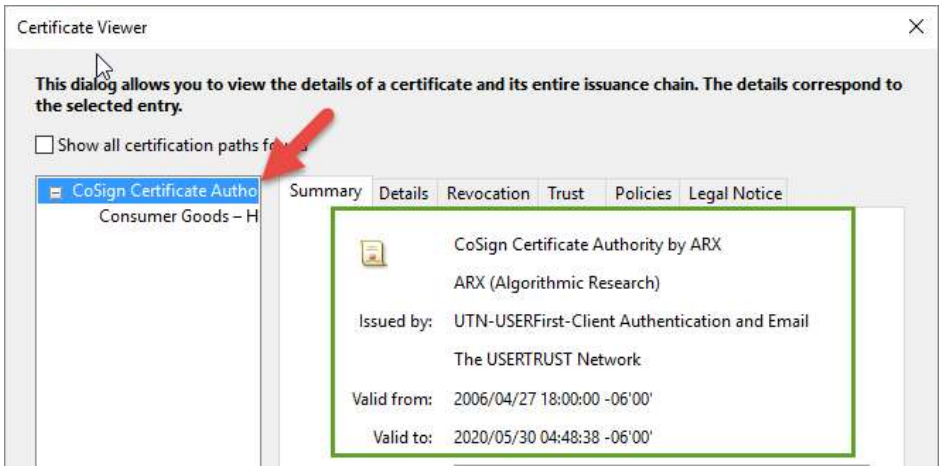
Although this message is received, the signature attached to the document may still be valid for the purpose of authentication and authorization but should be verified. To eliminate this warning and allow the certificate to validate, the following configuration should be done in Adobe Acrobat:

1. Open the signature panel by clicking on the "Signature Panel" button.

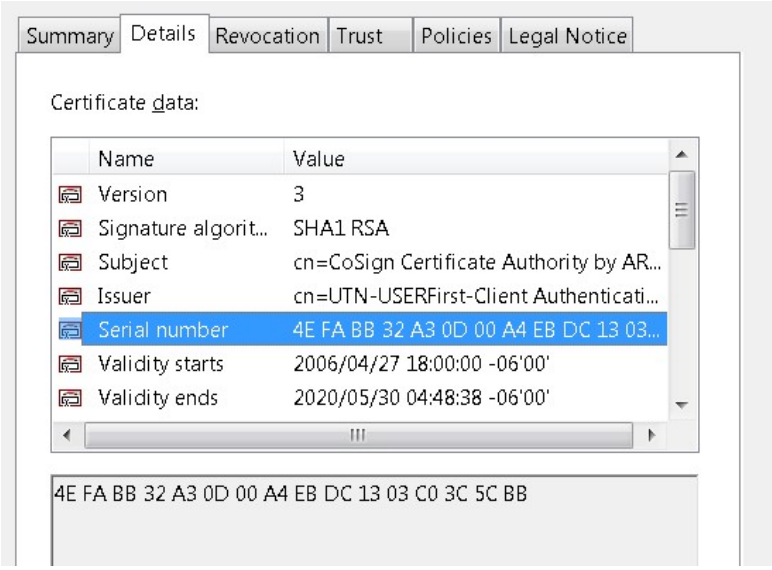
2. Expand the signature properties in the signature panel and click on "Certificate Details…" under the "Signature Details" section.



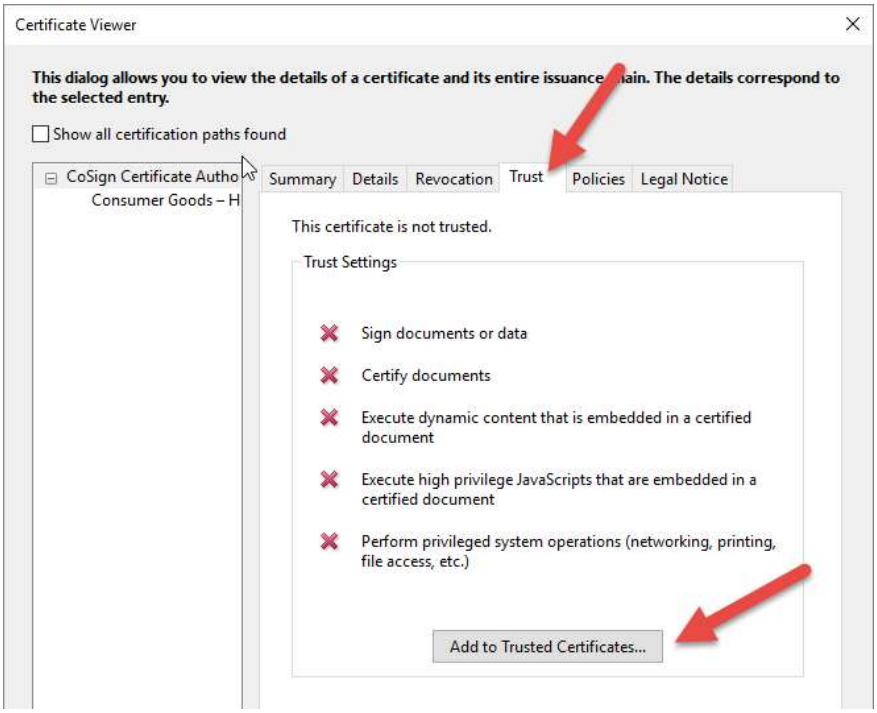
3. With the signature properties open, select the "CoSign Certificate Authority by ARX" certificate in the chain on the left. Once selected you will see the properties of this certificate appear on the right. If you do not see "CoSign Certificate Authority by ARX" and the document was signed prior to September 2016, the document is forged, invalid, or the wrong certificate has been selected. Here are examples of proper Intertek certificates.
   Do NOT continue these steps if the certificate does not say "CoSign Certificate Authority by ARX". If the certificate does not say "CoSign Certificate Authority by ARX" or "Intertek Document Signing Authority", then the document is not a valid signed Intertek document.



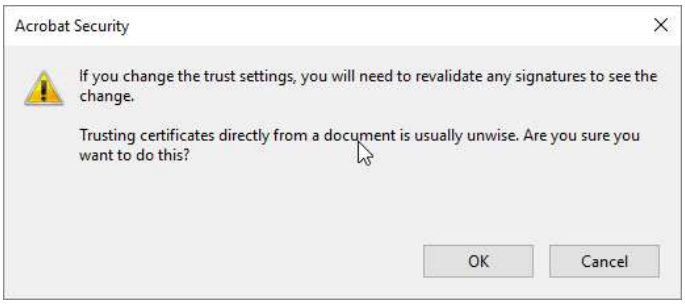
4. Click on the "Details" tab and locate the detail for "Serial Number". Confirm that the serial number on the certificate is: 4E FA BB 32 A3 0D 00 A4 EB DC 13 03 C0 3C 5C BB
   Do NOT continue these steps if the serial number is NOT "4E FA BB 32 A3 0D 00 A4 EB DC 13 03 C0 3C 5C BB".



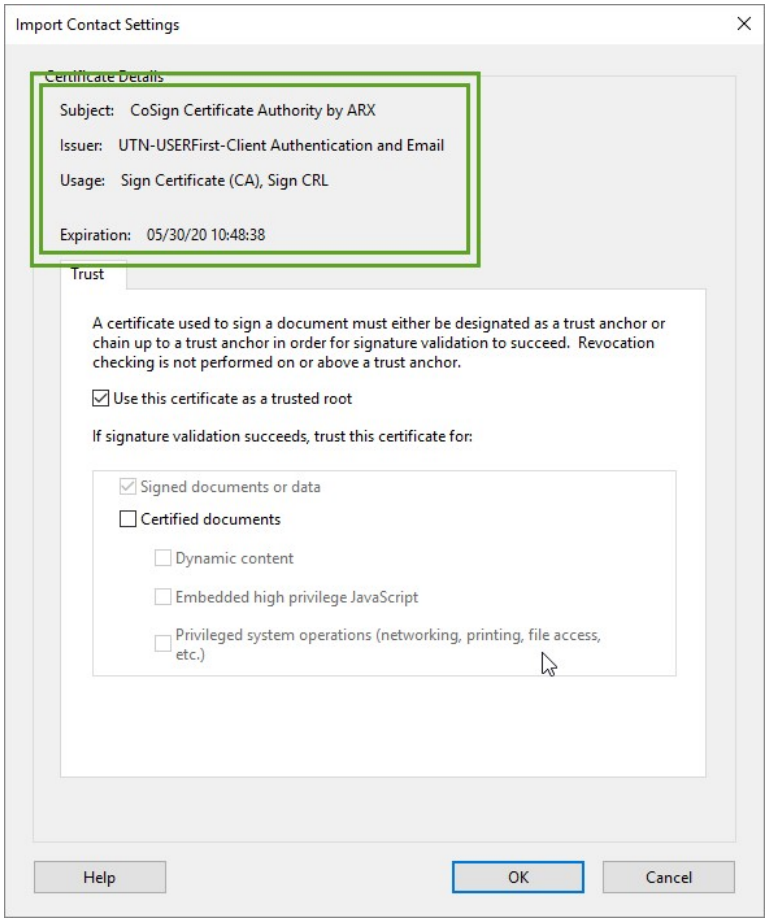
5. If both the name and serial number of the certificate match as described above, click on the “Trust” tab and then click the “Add to Trusted Certificates” button to add the root certificate to your trusted certificate store.



6. After clicking to add the certificate you will be prompted with a warning. If you have properly validated that the certificate that you are importing is “CoSign Certificate Authority by ARX”, please click “OK” to add it to your trusted certificates store.



7. Confirm that the box is checked for “Use this certificate as a trusted root”, and the details outlined in green to make sure that you are importing the proper certificate. If the details match with what is displayed below, click “OK” to finish the process.



8. Re-open the document and you should find that the signature comes up as valid. All other Intertek-signed documents should appear as valid now as well.

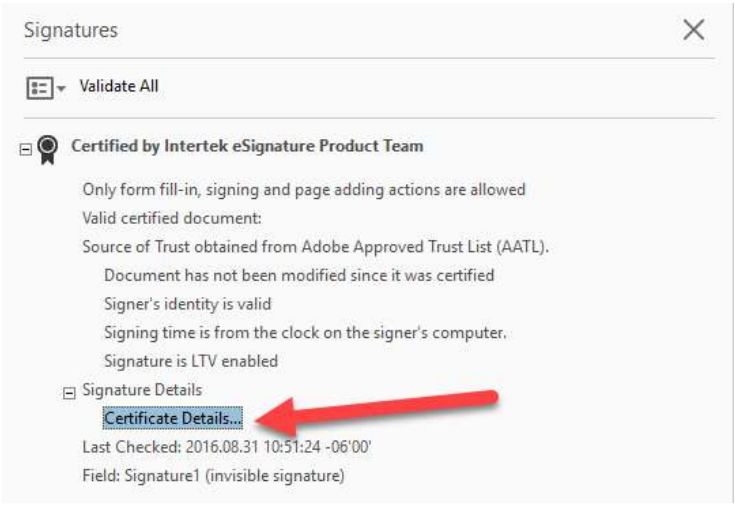
Viewing Certificate Details

Once you have checked that the signature is valid, you should also ensure that the certificate information appears like the information below. An Intertek representative may provide different specifics depending on the region or the type of business.

To get to the certificate details:

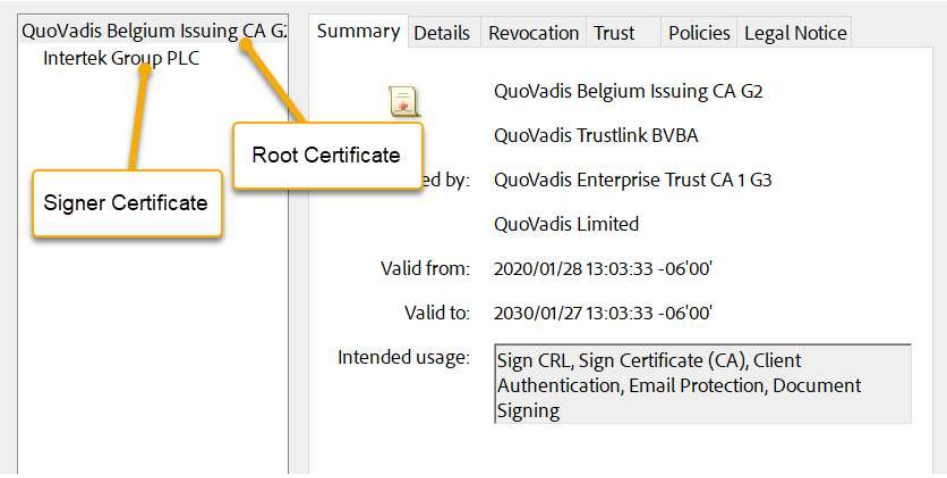
1) Open the signature panel by clicking on the "Signature Panel" button

2) Expand the signature properties in the signature panel and click on "Certificate Details…" under the "Signature Details" section



Valid Intertek Signing Certificates

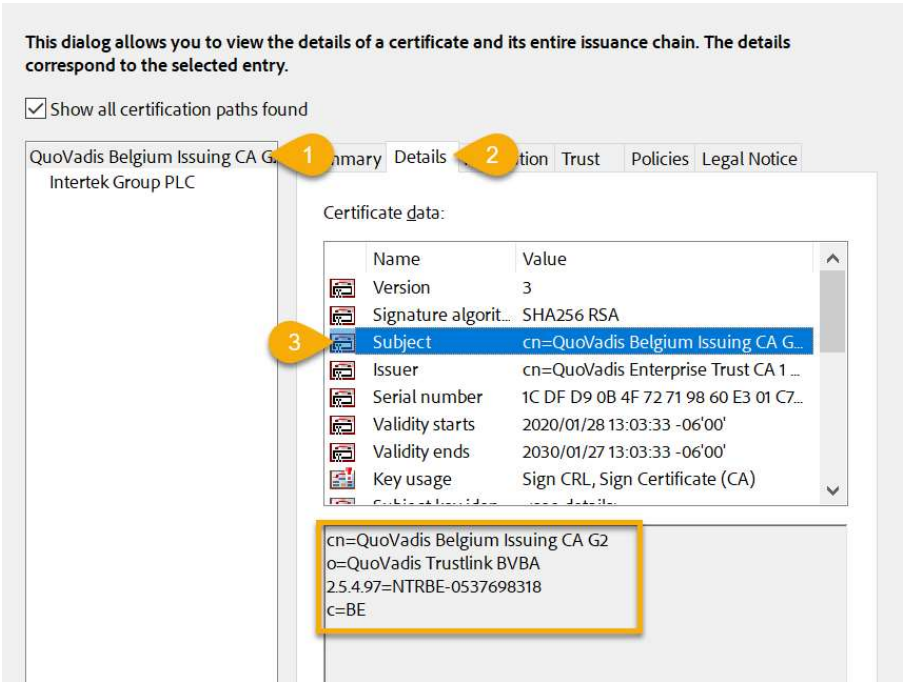
The signing certificate is only a valid Intertek certificate if the root certificate details match what is below and indicate that they are signed by Intertek in the signer's certificate. The root certificate is the certificate in the chain at the top of the certificate chain and the signer's certificate is the last one in the chain. Either can be selected by clicking on it after you have the certificate details open.



Below are the details of the valid Intertek root certificates:

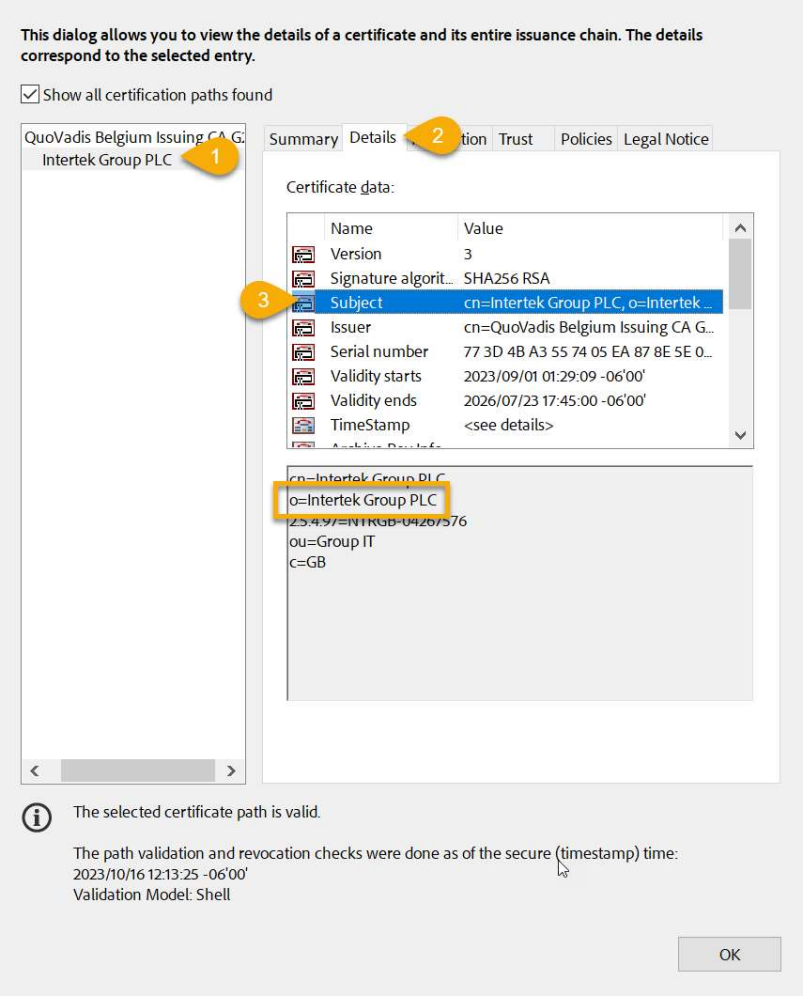
- If the document was signed **after** September 2016, the root certificate will indicate one of the below certificate authorities as the issuer:
  - **Symantec Document Signing RSA Root CA, issued by Symantec Corporation**
  - **GlobalSign CA for AATL - SHA256 - G2, issued by GlobalSign nv-sa**
  - **QuoVadis Belgium Issuing CA G2, issued by QuoVadis Trustlink BVBA**

  You can find this information through the following steps:
  1) Select the root certificate.
  2) Click the “Details” tab.
  3) Click the “Subject” field.
  4) Review the details in the lower section.

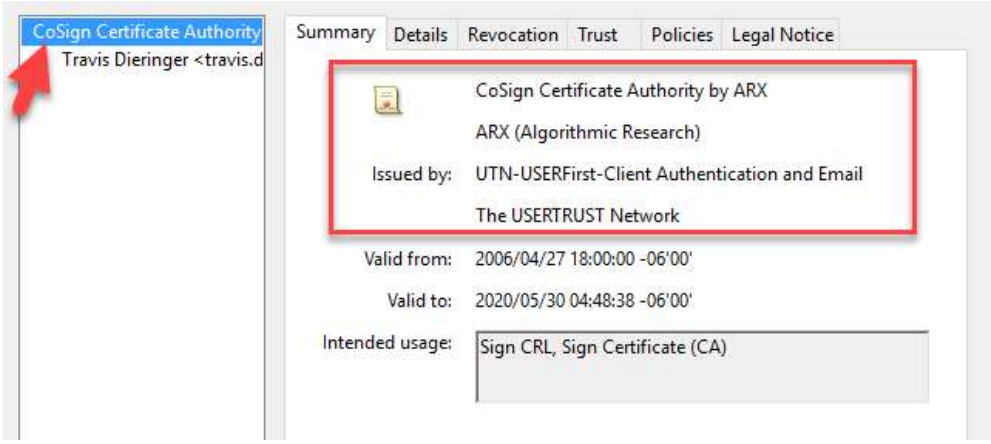


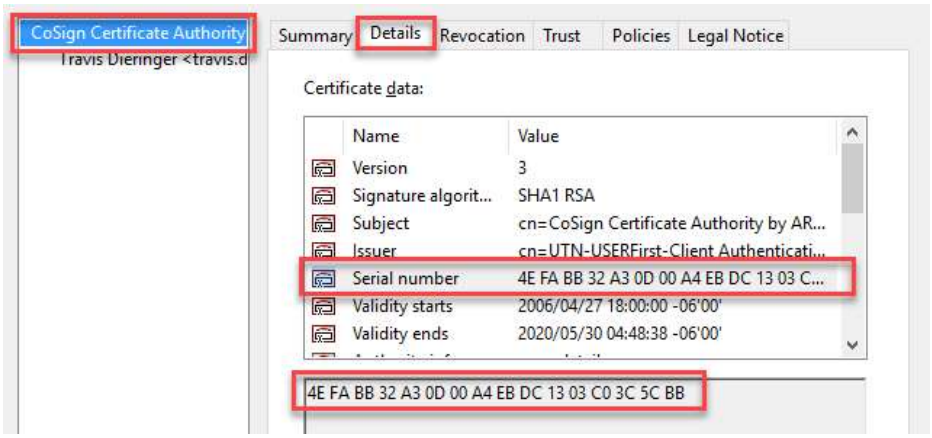
The signer's certificate will indicate the organization of "**Intertek Group plc**"
You can find this information through the following steps:

1) Select the signer's certificate.
2) Click the "Details" tab.
3) Click the "Subject" field.
4) Review the "o=" data in the lower section.



- If the document was signed **before** September 2016, the root certificate will have the following details:
  - Company: CoSign Certificate Authority by ARX | ARX (Algorithmic Research)
  - Issued by: UTN-USERFirst-Client Authentication and Email
  - Serial Number: 4E FA BB 32 A3 0D 00 A4 EB DC 13 03 C0 3C 5C BB





Checking the expiration date of a certificate

Signed documents do not expire even when the signing certificate does. This is because the authorization to sign is embedded at the time of signing, embedding Long Term Validation (LTV) methods into the document. To check the expiration date of a certificate:

1. Open the certificate details as described in the Certificate Details section.
2. Check the "Valid to" section of the certificate details to see the expiration date.

COMMON ISSUES

When validating documents that are Intertek-signed, it is important that you see the following message ensuring that the document is an authentic Intertek document that is unmodified.

- OR -

- OR -

If your document does not show as valid after going through the verification steps listed in this document, you can refer to this list of common issues to try to resolve the problem.

Alert: This file claims compliance with the PDF/A standard and has been opened read-only to prevent modificationb

If your document was signed before September 2016, it may show a yellow exclamation mark with the text **"At least one signature has problems."** If you see this message, please use the steps for Verifying Documents Signed Before September 2016.

Error: At least one signature has problems (documents signed before September 2016)

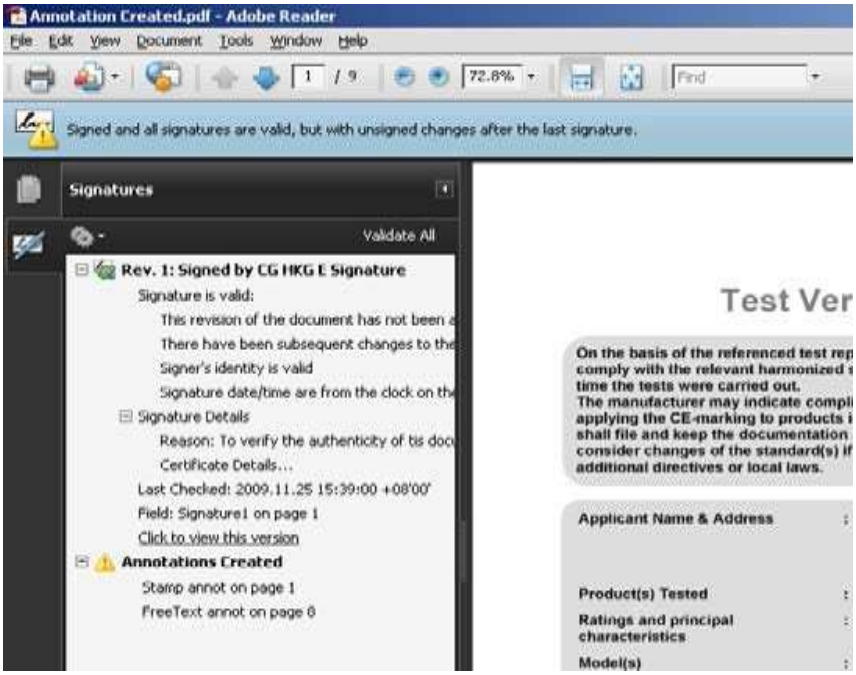
If your document was signed before September 2016, it may show a yellow exclamation mark with the text **"At least one signature has problems."** If you see this message, please use the steps for Verifying Documents Signed Before September 2016.

Error: Signed and all signatures are valid, but with unsigned changes after the last signature

If you see this message, you can easily see what changes have been made to the document since signing.

1. Open the signature panel by clicking on the "Signature Panel" button

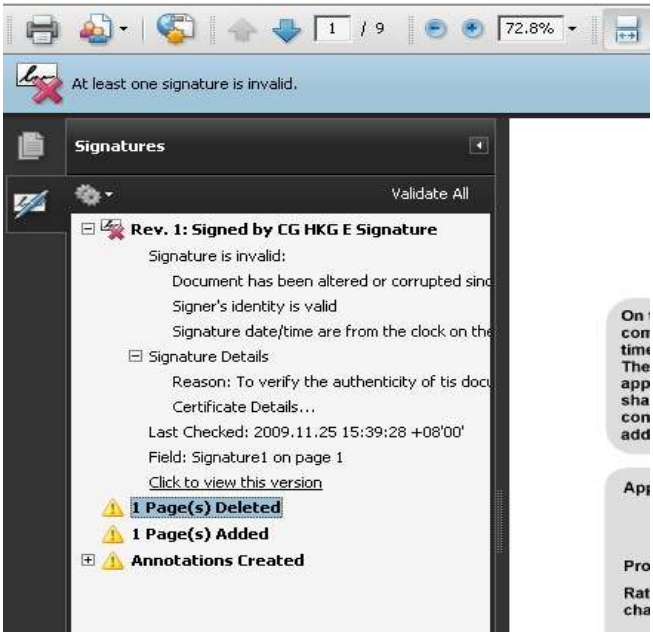
2. In the signature panel, look at the list of items under the “Annotations Created” section to see what changes have been made.



Error: At least one signature is invalid

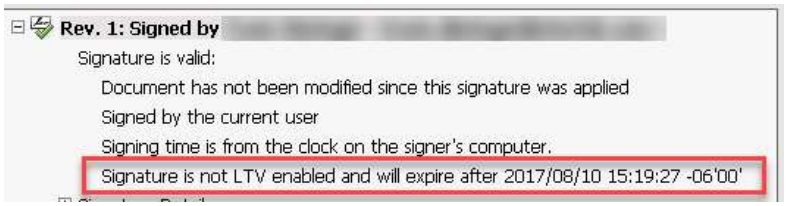
If you see this error message, it could be the result of several issues:

1. The document that you are viewing is a forged or unauthentic Intertek document. Please check the steps as to what to do if the eSignature validation fails.
2. The document has been modified with more than simple annotations. Documents in this state have been invalidated because the content has been modified since signing. This includes page adds, deletes, and text changes. Please check the steps as to what to do if the eSignature validation fails.



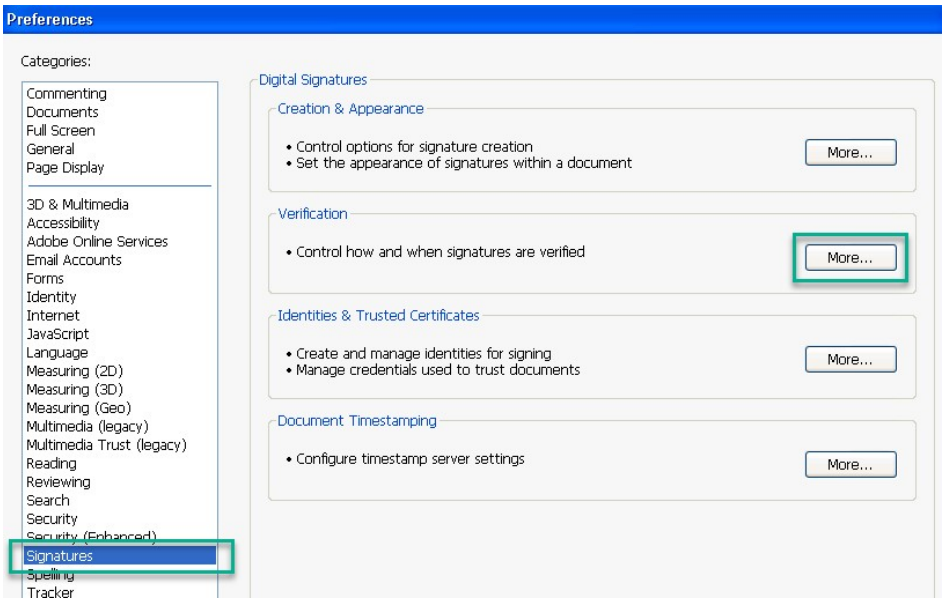
Error: Signature is not LTV enabled and will expire after XXXX/XX/XX (Windows XP/2003)

On Windows XP and Windows 2003, the Adobe Acrobat client does not have a core checking component turned on by default to validate LTV-enabled signatures (Long-Term Validation). When this component is not enabled, documents that have been signed will not show as LTV-enabled and will indicate that the signature will expire on the date of the signer's certificate.

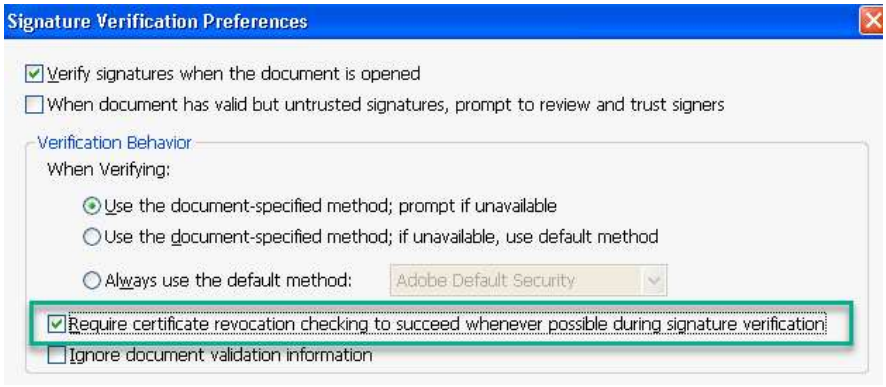


This error message is misleading, as the documents will continue to be valid past the date displayed. To fix this error, please enable the proper certificate verification by doing the following:

1. In Adobe Acrobat, click on the "Edit" menu and then click on "Preferences".
2. In the left-hand pane, click on "Signatures".
3. Click on the "More" button under the "Verification" section.



4. Check the box for “Require certificate revocation checking to succeed whenever possible during signature verification”.



5. Close Acrobat and re-open the document to see the updated verification.

Resetting Adobe Acrobat or Acrobat Reader settings

If you need to reset all settings within Adobe Acrobat or Acrobat Reader, the settings are per-user (individual for each user who logs in). To reset a user’s settings:

1. Log in as the user
2. Close Adobe Acrobat or Acrobat Reader
3. Open the registry by using “regedit.exe”
4. Delete the following keys:
   - HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader
   - HKEY_CURRENT_USER\Software\Adobe\Adobe Acrobat
5. Open Adobe Acrobat or Acrobat Reader

REVISION HISTORY

Version	Author	Reviewed by	Updated	Comments
2.1	Intertek Group IT	Application Support	30-Jul-2014	Corrected index numbering, revised Section 1.6 and references to 1.6; Corrected formatting
2.2	Intertek Group IT	Application Support	01-Aug-2014	Added: 2.2 Document History, Footer and Intertek Logo
2.3	Intertek Group IT	Application Support	18-Aug-2014	Changed document name
2.4	Intertek Group IT	Solutions Architect	06-Jun-2016	Updated section 1.6 regarding Windows XP
3.0	Intertek Group IT	Solutions Architect	29-Jun-2016	Updated to meet the eSignature 8.0 platform
3.2	Intertek Group IT	Solutions Architect	30-Jun-2016	Final review completed for publication
3.8	Intertek Group IT	Solutions Architect	22-Aug-2016	Updated to meet the eSignature 8.01 platform
4.0	Intertek Group IT	Solutions Architect	30-Oct-2018	Updated to new Intertek format
5.0	Intertek Group IT	IT Architect	23-Oct-2023	Updated for 2023 eSignature service