Document Verification Using Acrobat / Acrobat Reader

RAFFCOMM TECHNOLOGIE SDN BHD
Company No. 201001015771 (1000449-W)

Licensed Certification Authority
License No: LPBP-4/2021 (1)

Level 32, Sunway Putra Tower
100, Jalan Putra, 50350 Kuala Lumpur

Tel: +6 03 4040 0195
Email: hello@rafftech.my
Website: https://www.rafftech.my

What is a digital signature?

Digital signatures are a secure and efficient way to electronically sign and authenticate documents, ensuring their authenticity and integrity. By using digital signatures, you can sign documents quickly and easily, and be confident that they can't be tampered with or forged.

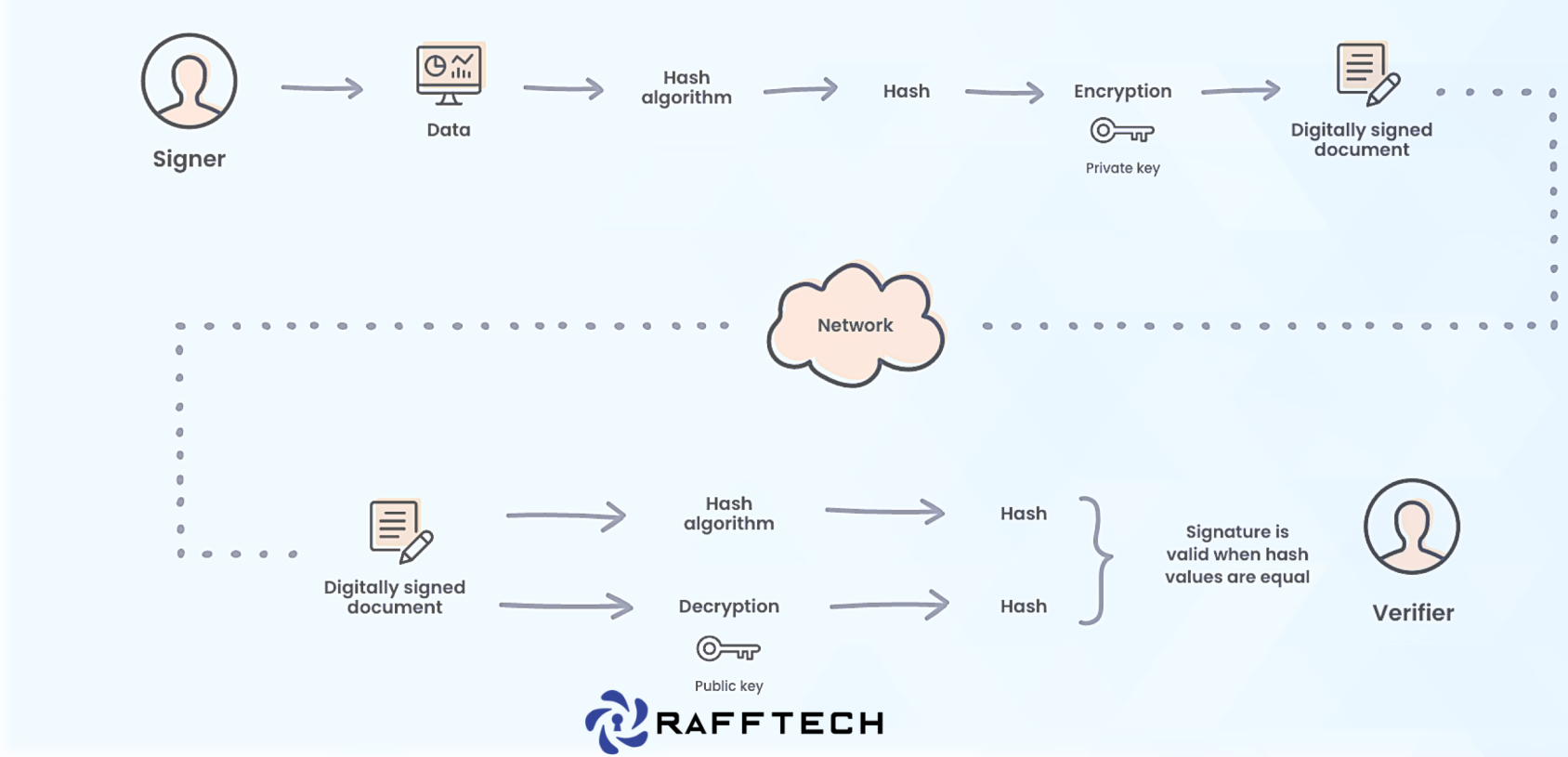


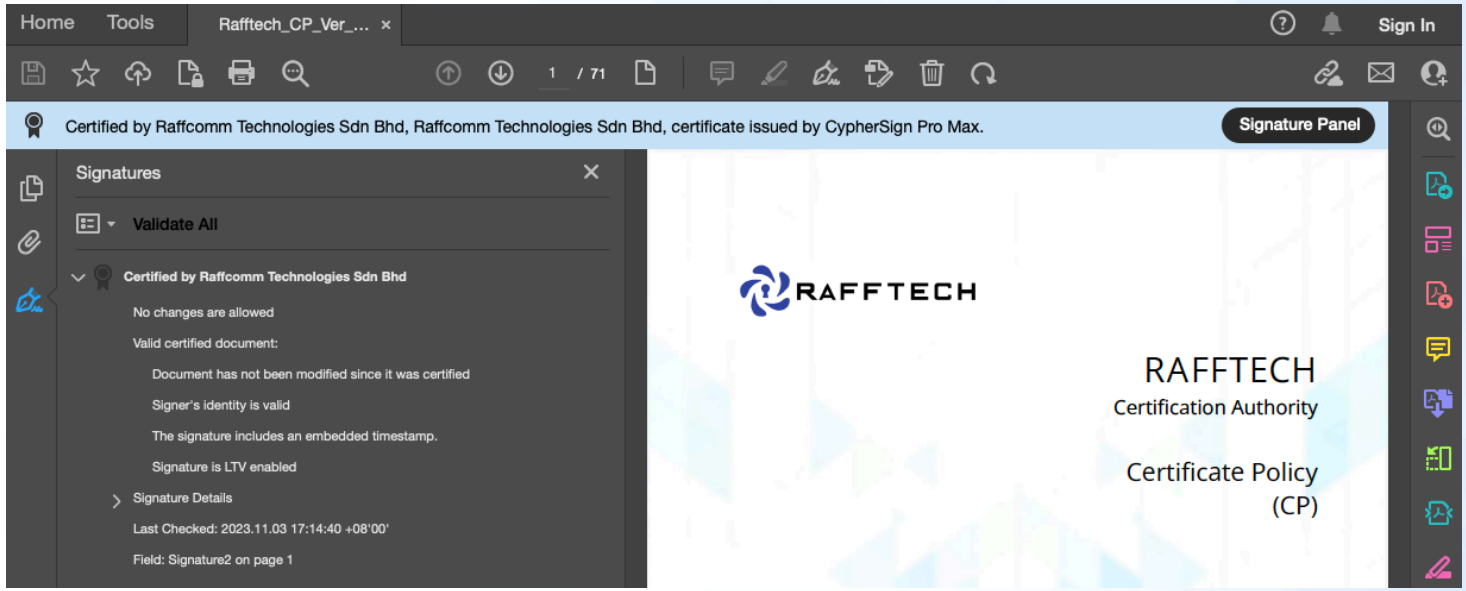
Diagram from GetAccept - How do digital signatures work? https://www.getaccept.com/blog/digital-signature

Why validate a digital signature?

When you receive a signed document, you may want to validate its signatures to verify the signer and the signed content. Validation may occur automatically depending on how you've configured your Acrobat or Acrobat Reader. Signature validity is determined by checking the authenticity of the signature's digital ID certificate status and document integrity.

To verify authenticity, the validator checks if the signer's certificate or its parent certificates are trusted. The signing certificate's validity is also checked based on the user's Acrobat or Acrobat Reader settings.

To verify document integrity, the validator checks if the signed content was altered after signing. If changes were made, the verification ensures that they were allowed by the signer.



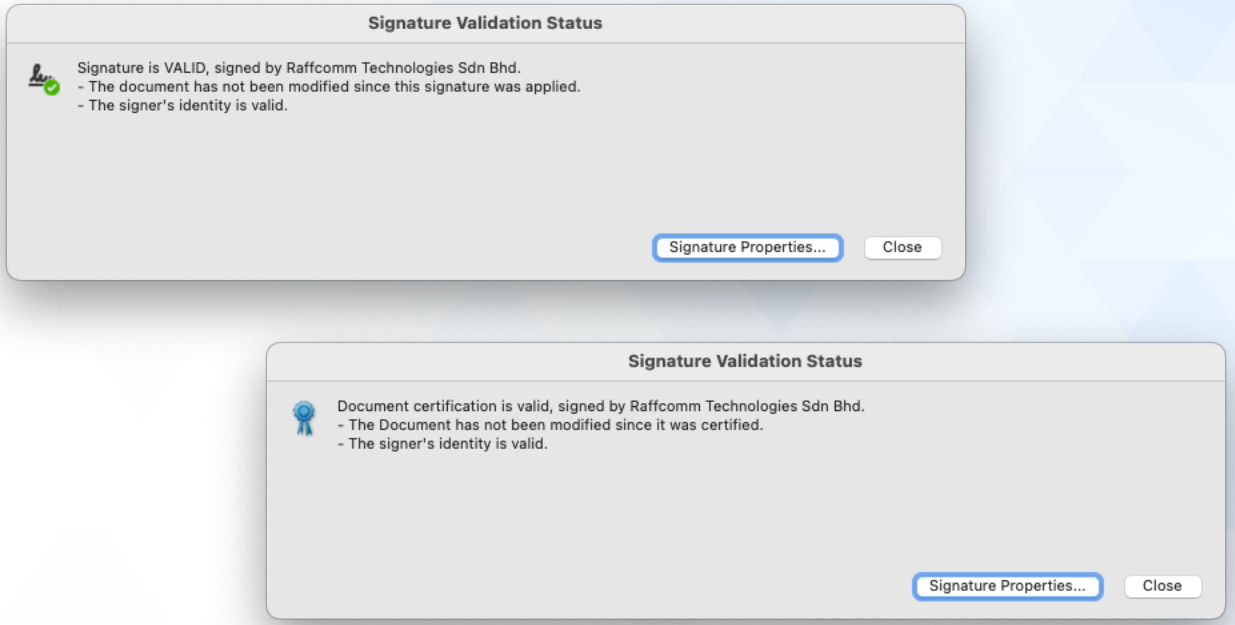
Reference: Validating digital signatures https://helpx.adobe.com/acrobat/using/validating-digital-signatures.html

How to validate a digital signature?

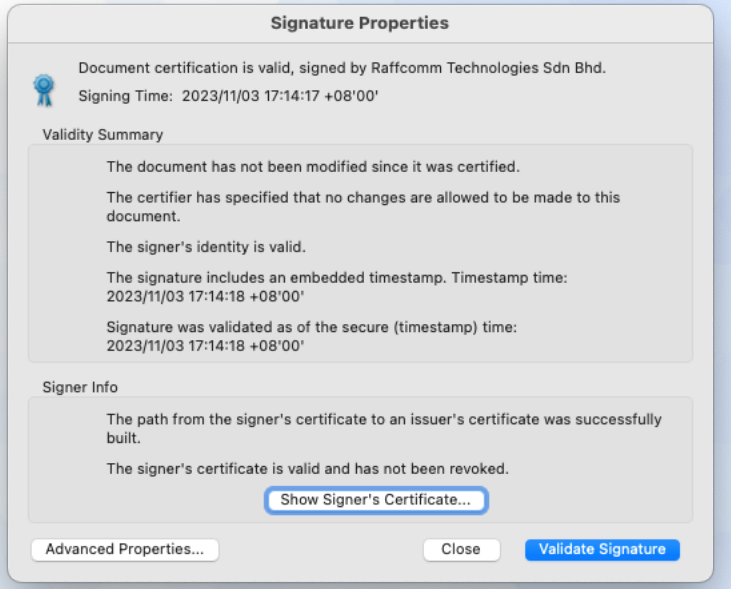
If the signature status is unknown or unverified, manually validate it to identify the issue and find a potential solution. In case the signature status is invalid, you must contact the signer to resolve the issue.

You can assess the validity of a digital signature and timestamp by checking the signature properties.

1. Open the PDF containing the signature and then select the signature.
   The Signature Validation Status dialog box describes the validity of the signature.



2. For more information about the Signature and Timestamp, select **Signature Properties**.



3 In the *Signature Properties* dialog box, review the Validity Summary that may display one of the following messages:

- **Signature date/time are from the clock on the signer's computer**: The time is based on the local time on the signer's computer.
- **Signature is time-stamped**: The signer used a Timestamp Server and your settings indicate that you have a trust relationship with that timestamp server.
- **Signature is time-stamped but the timestamp couldn't be verified**: Timestamp verification requires obtaining the timestamp server's certificate to your list of trusted identities. Check with your system administrator.
- **Signature is time-stamped but the timestamp has expired**: Acrobat validates a timestamp based on the current time. This message is displayed if the timestamp signer's certificate expires before the current time. To accept an expired timestamp, go to the hamburger menu (Windows) or the Acrobat menu (macOS) > **Preferences** > **Signatures** > Verification: **More**... and then in the *Signature Verification Preferences* dialog box, select **Use expired timestamps**. It displays an alert message when validating signatures with expired timestamps.

4 For details about the signer's certificate, such as trust settings or legal restrictions of the signature, select **Show Signer's Certificate** in the *Signature Properties* dialog box.

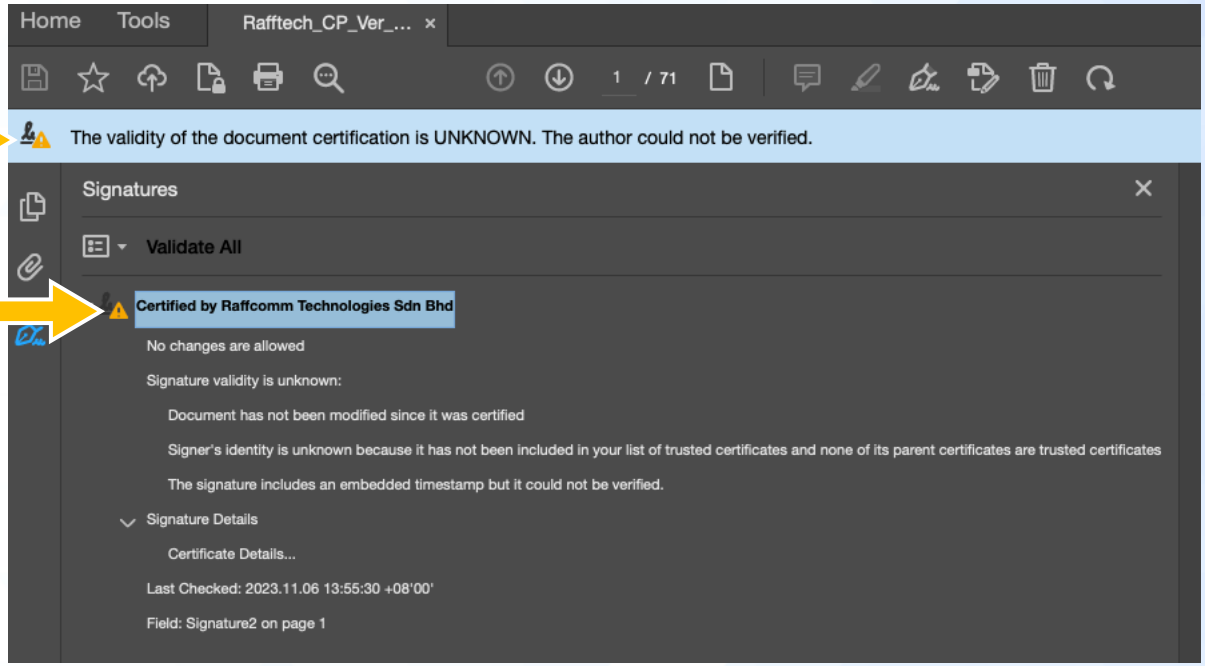
If the document was modified after it was signed, check the signed version of the document and compare it to the current version.

Reference: Validating digital signatures https://helpx.adobe.com/acrobat/using/validating-digital-signatures.html

Set RAFFTECH's Root CA certificate to Trusted Certificates

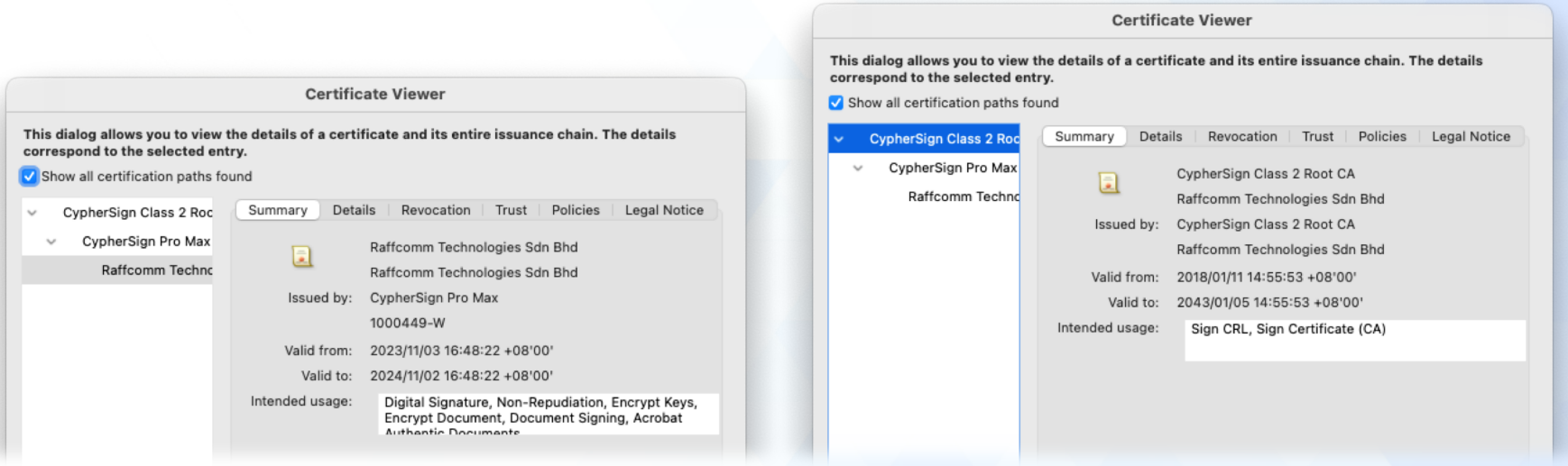
In Acrobat or Acrobat Reader, the signature of a certified or signed document is valid if you and the signer have a trust relationship. The trust level of the certificate indicates the actions for which you trust the signer.

If RAFFTECH's Root CA has not been trusted yet, this message will be displayed.

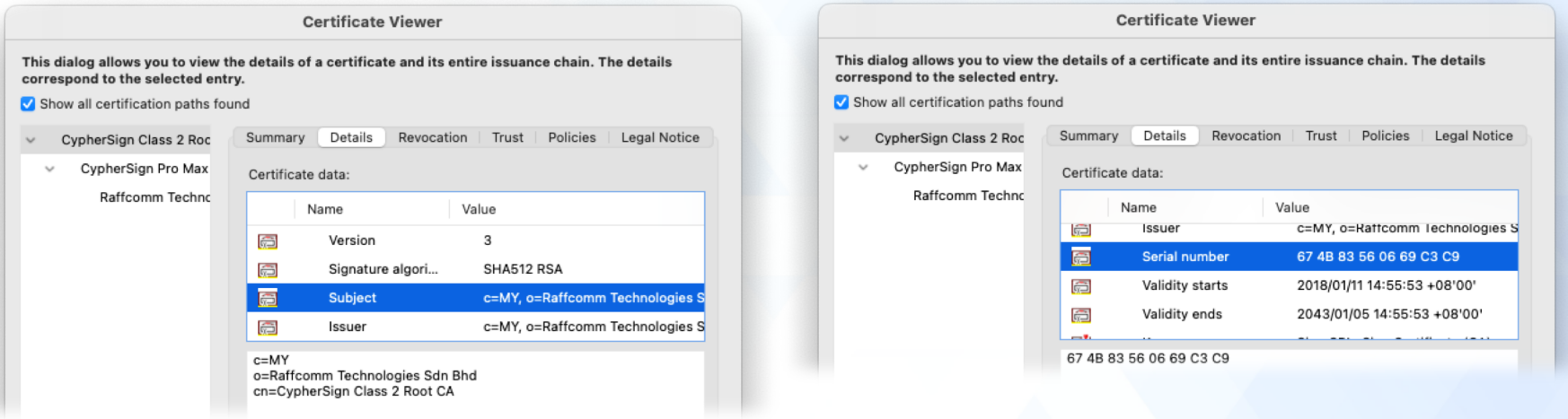


5 Show details about the signer's certificate by selecting **Show Signer's Certificate** in the *Signature Properties* dialog box to open the *Certificate Viewer* dialog box.

6 In the *Certificate Viewer* dialog box, review the signer's certificate and its parent certificates.



7 Select the signer's parent (Root CA) certificate, then navigate to the **Details** tab. Review the certificate's **Subject** and the **Serial Number** are cross-checked with the following details of RAFFTECH's Root CA certificates below.



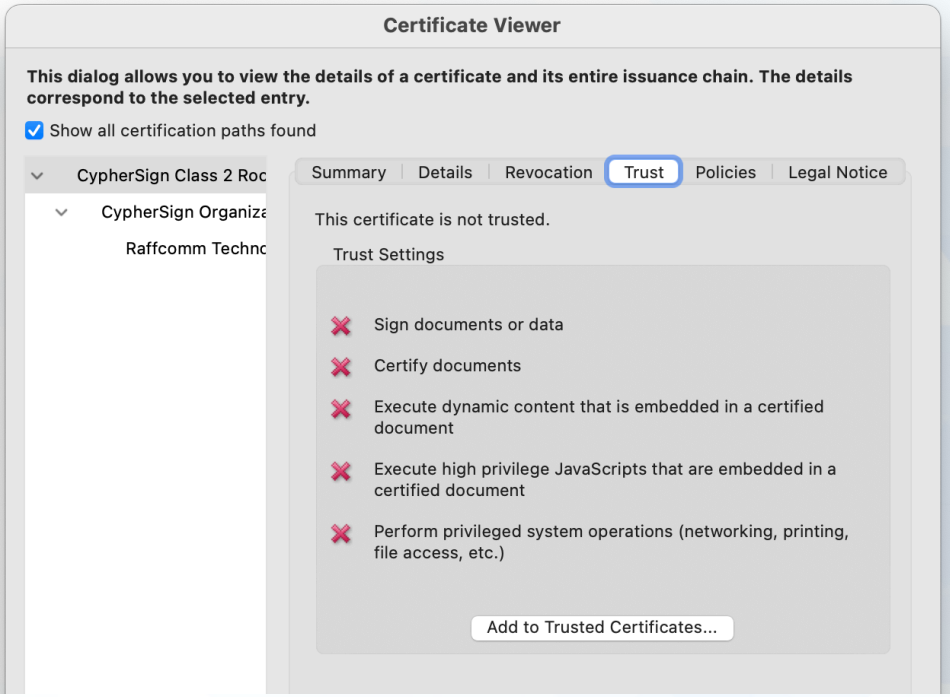
RAFFTECH's Root CA Certificates

Subject Distinguish Name (DN)	
Common Name (CN)	**CypherSign Class 2 Root CA**
Organization (O)	Raffcomm Technologies Sdn Bhd
Country (C)	MY
Certificate Serial Number (hex)	67 4B 83 56 06 69 C3 C9
Signature Algorithm	SHA-512 with RSA Encryption
Not Valid Before	Thursday, 11 January 2018 at 2:55:53 PM Malaysia Time
Not Valid After	Monday, 5 January 2043 at 2:55:53 PM Malaysia Time
Public Key Algorithm	RSA Encryption
Public Key Size	4,096 bits
Fingerprints SHA-256	4F 95 60 B4 E8 F1 53 61 CA F7 04 E8 60 57 63 0E AC FF E8 83 B9 C0 C8 82 37 F7 63 CA 02 0A 3A C6
Fingerprints SHA-1	B4 8E CE 60 CF DB 52 B9 CD E9 E0 C5 BF 62 87 9D 9B A1 2B 1D

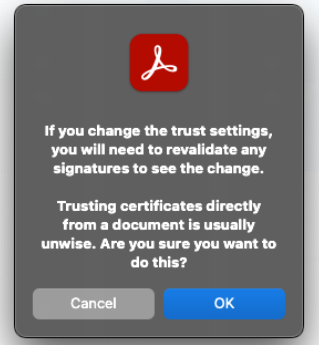
Subject Distinguish Name (DN)	
Common Name (CN)	**RAFFTECH Class 2 RSA Root CA**
Organization (O)	Raffcomm Technologies Sdn Bhd
Country (C)	MY
Certificate Serial Number (hex)	6E 52 3C 1D 06 54 4A B0
Signature Algorithm	SHA-512 with RSA Encryption
Not Valid Before	Wednesday, 10 March 2021 at 11:02:58 AM Malaysia Time
Not Valid After	Sunday, 4 March 2046 at 11:02:58 AM Malaysia Time
Public Key Algorithm	RSA Encryption
Public Key Size	4,096 bits
Fingerprints SHA-256	0E FE 53 67 7F EF 63 1A 2A 2F 8B 6F B1 B6 21 86 1B F5 73 52 EB 85 70 26 FE A9 B9 9E 7C 92 52 4D
Fingerprints SHA-1	E5 68 1E F9 FD 8C 93 9C 13 37 F9 12 08 6B C0 86 55 FD 2B 97

Subject Distinguish Name (DN)	
Common Name (CN)	**RAFFTECH Class 2 ECC Root CA**
Organization (O)	Raffcomm Technologies Sdn Bhd
Country (C)	MY
Certificate Serial Number (hex)	60 5B AF 78 12 EA 11 4B
Signature Algorithm	ECDSA Signature with SHA-384
Not Valid Before	Wednesday, 10 March 2021 at 11:16:19 AM Malaysia Time
Not Valid After	Sunday, 4 March 2046 at 11:16:19 AM Malaysia Time
Public Key Algorithm	Elliptic Curve Public Key
Public Key Size	384 bits
Fingerprints SHA-256	6E D7 3C 5F 47 DC 10 6E 83 8B 97 F8 FA 61 1A 11 E0 71 5A E4 08 CD B3 3F 7C 52 85 D7 F2 1B 12 43
Fingerprints SHA-1	A7 5A FD BC 9B 09 AB 27 EB 12 E2 11 C2 3E 6A B0 0D 6E 28 D7

8 If the values for the certificate's **Subject** and the **Serial Number** are matched with the one of the Root CA in the list above, you can continue to trust the Root CA certificate by navigating to the Trust tab.



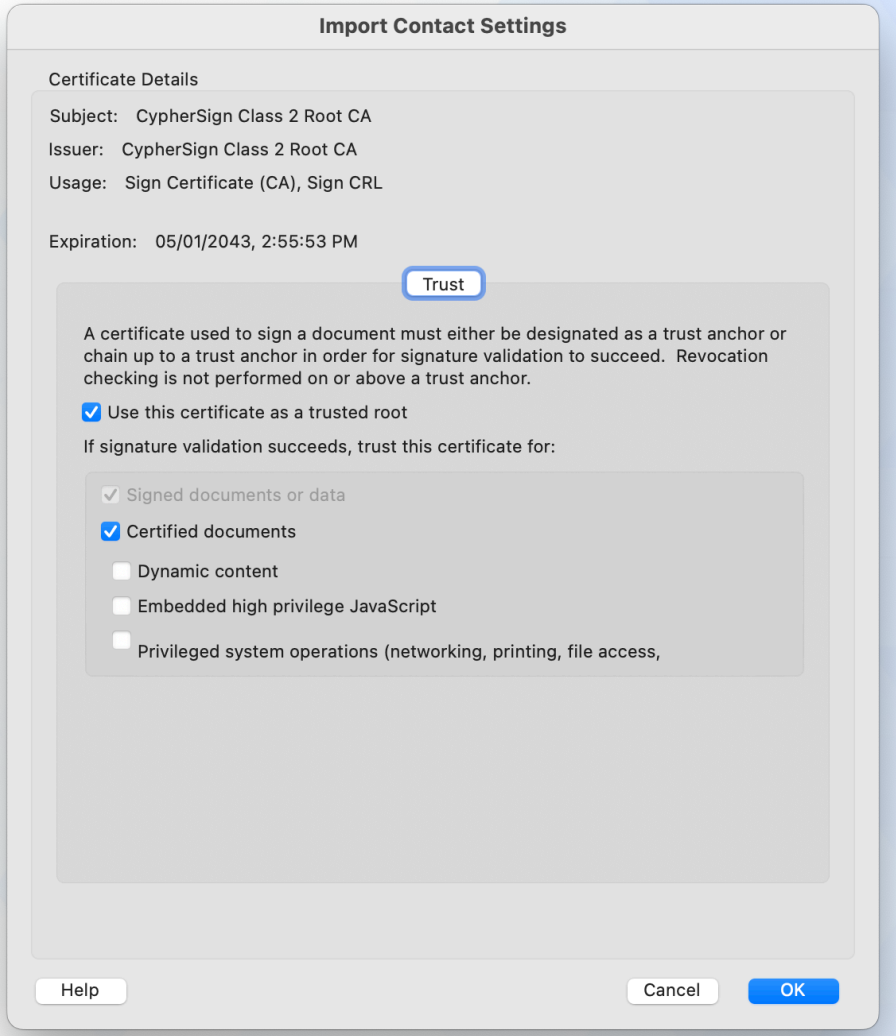
9 Select **Add to Trusted Certificates**… in the *Certificate Viewer* dialog box to proceed to trust RAFFTECH's Root CA certificate. The application will prompt a notice, then select **OK**.



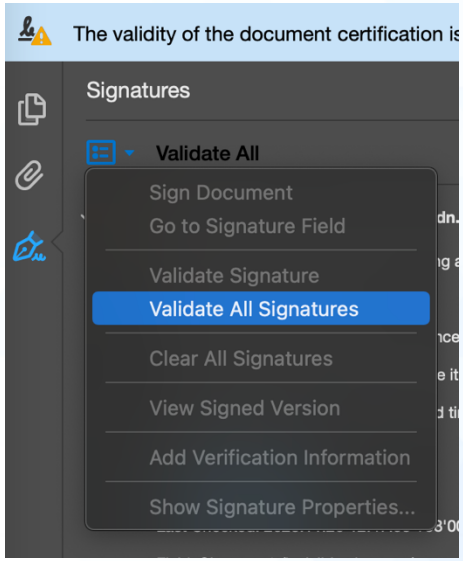
10 In the *Import Contact Setting* dialog box, review Certificate Details and check the following checkbox:

- ☑ Use this certificate as a trusted root
- ☑ Certified documents

Select OK to continue.



11 Do signature validation by clicking the **Validate All** or **Validate All Signatures** from the drop-down menu.



Any Question?

Feel free to contact us via the following channels:

Email: hello@rafftech.my
Website: www.rafftech.my