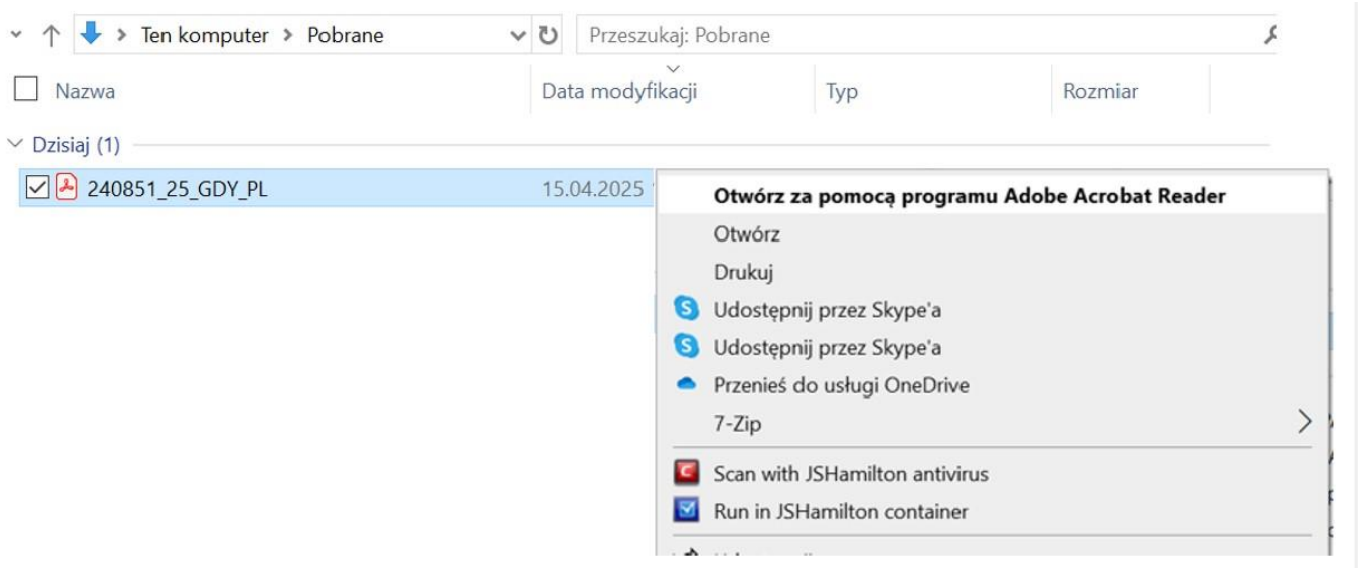
Digital signature verification guide

1. If you do not have Adobe Acrobat Reader installed on your computer, install it (you can download it from the Adobe Acrobat Reader website: https://get.adobe.com/reader).
2. Download the signed PDF with the electronic signature and open it with Adobe Acrobat Reader DC.



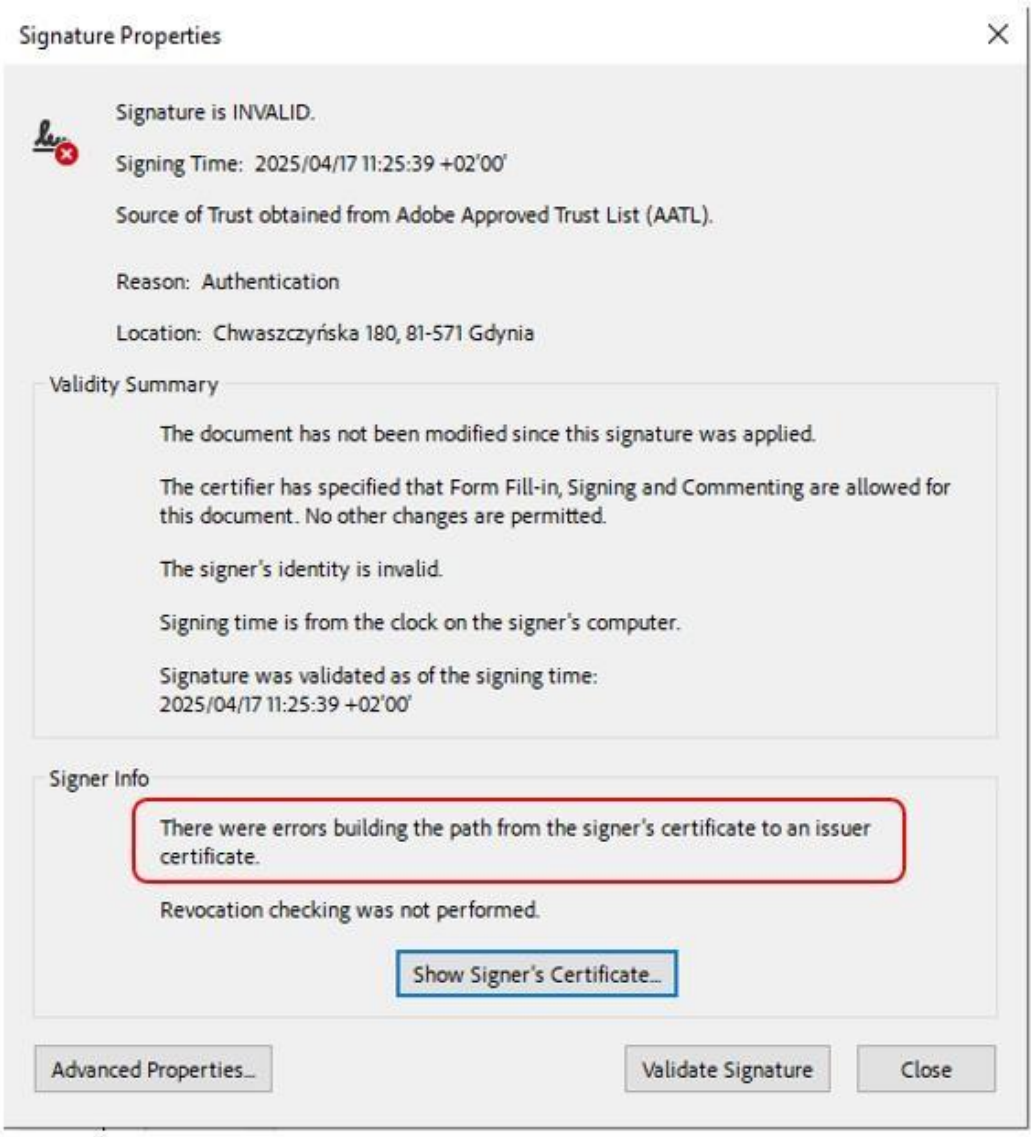
3. If you receive a message that reads **"At least one signature is invalid."** follow the steps below.



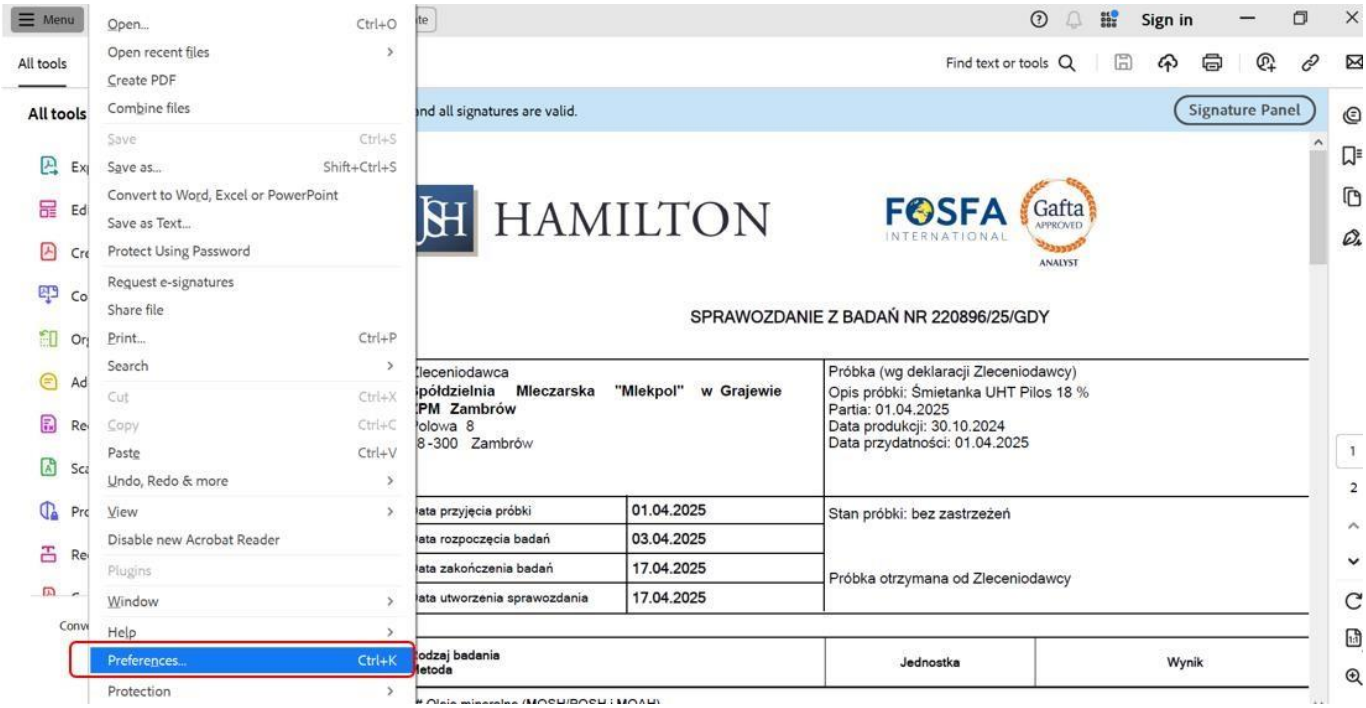
4. To see details of why the signature was found to be invalid click the **"Signature Panel"** and then right-click **"Rev. 1: Signed by Hamilton Poland Sp z.o.o. <info@hamilton.com.pl>** „ and select **"Show Signature Properties...".**



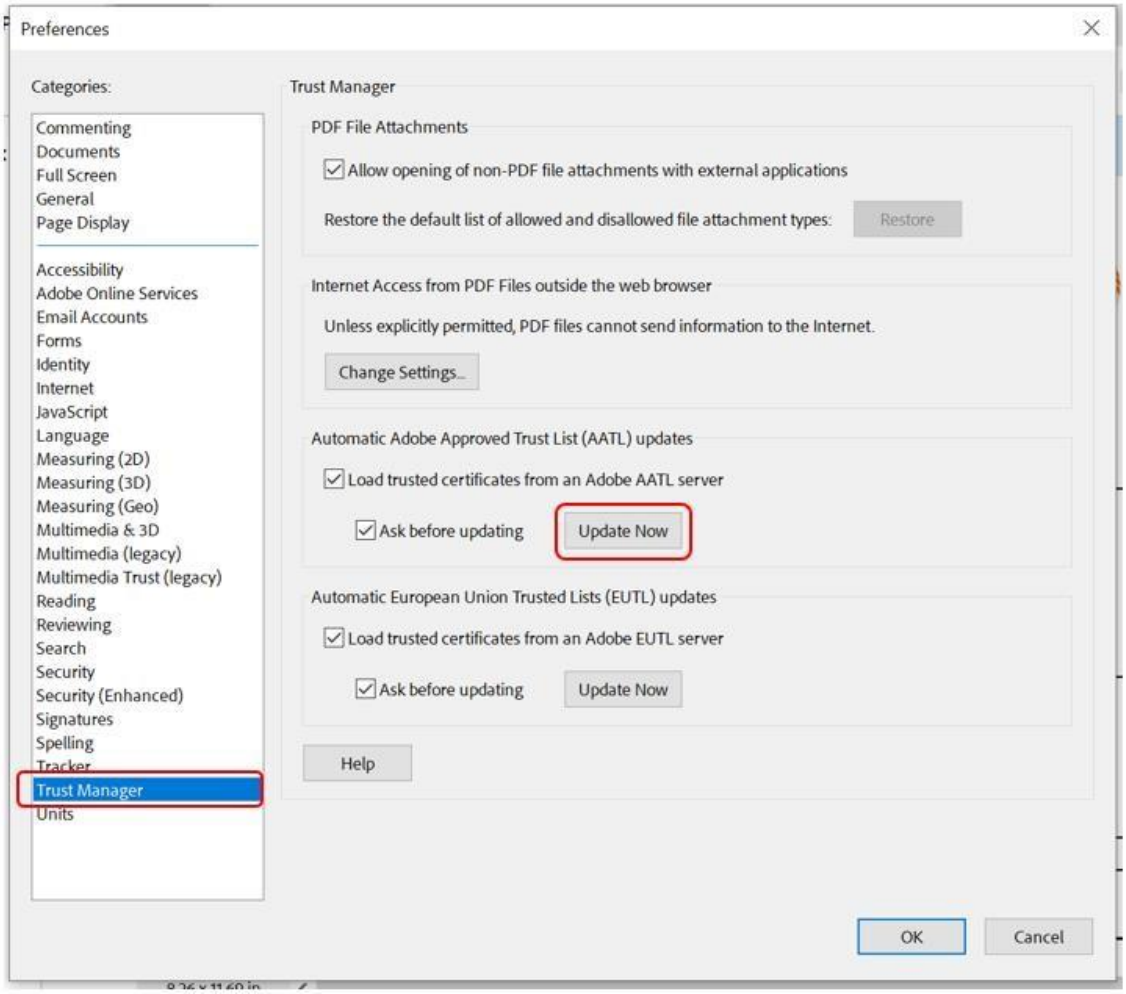
5. The signature properties window will appear. In the Signer Info section, the reason for the error is: **"There were errors building the path from the signer's certificate to an issuer certificate."**



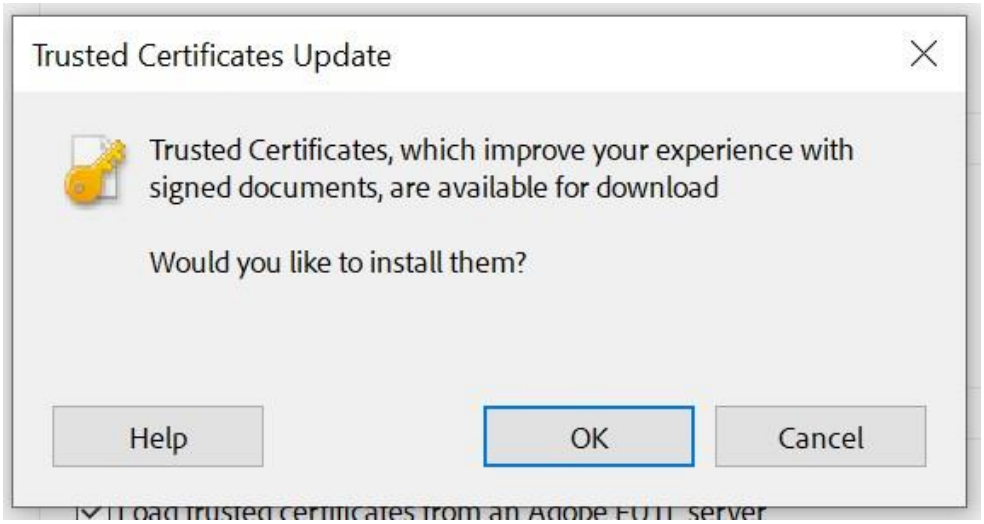
6. A message means that the signature is not compliant with the certificate policy on which it is verified. **In this case, the publisher's certificate is misrepresented in Adobe Acrobat Reader DC.** **Explanation:**
    a. The certificate to which the report is signed is issued by Certum (Certum Digital Identification CA SHA2), which according to the Certification Practice Statement (https://www.certum.pl/pl/wp-content/uploads/2025/03/CCP-DK02-ZK02-Kodeks-Postepowania-Certyfikacyjnego-Niekwalifikowanych-Uslug-Certum_v7.12.pdf) Chapters
        1.3.1.2. Pośrednie urzędy certyfikacji specifies the certification policy identifiers:
        i. 1.2.616.1.113527.2.5.1.6.11
        ii. 1.2.616.1.113527.2.5.1.6.12
        iii. 1.2.616.1.113527.2.5.1.6.13
        iv. 1.2.616.1.113527.2.5.1.6.14
    b. This certificate in Adobe Acrobat Reader DC only has one policy, which is the source of the invalid signature verification.
    c. **Follow the steps below to properly set up the publisher's certificate.**
7. Open the **"Edit"** menu and select **"Preferences..."**



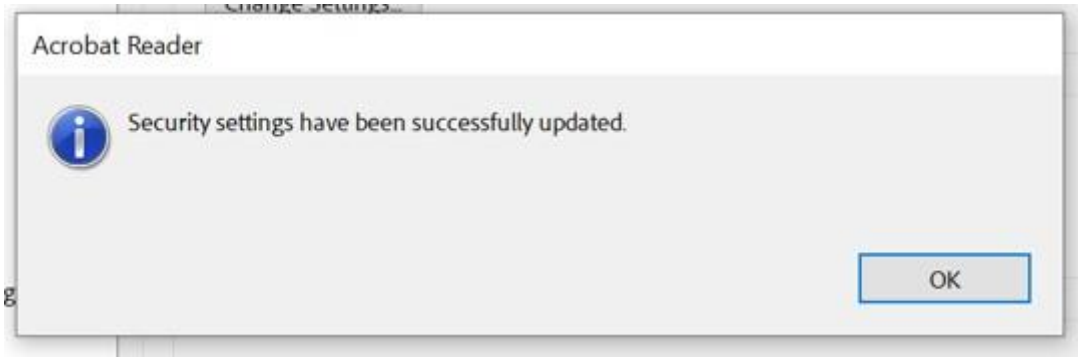
8. In the preferences window that appears, go to **Trust Manager**
    a. In the Automatic Adobe Approved Trust List (AATL) updates section, click **Update Now**



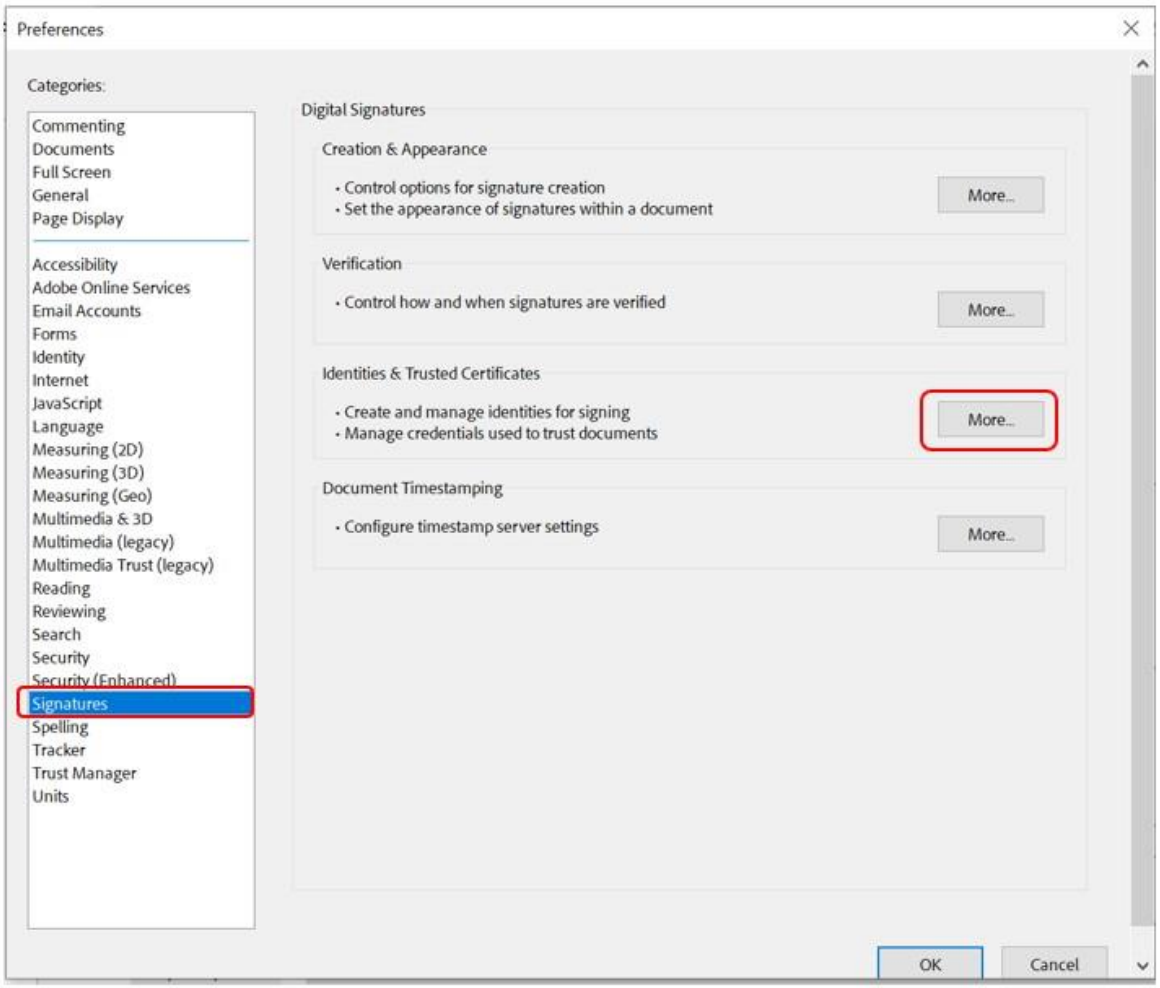
b. Confirm with **OK**



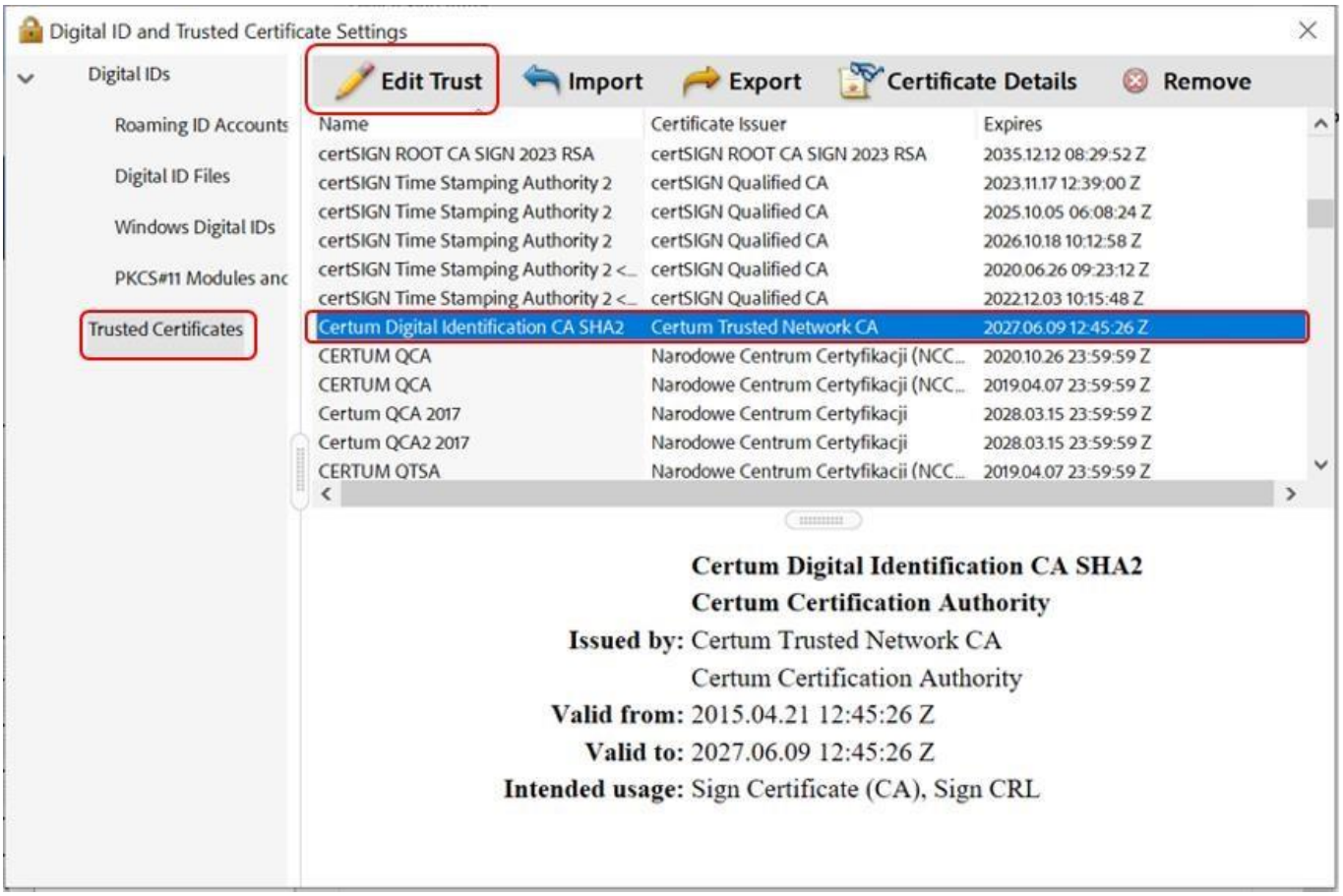
c. After a few moments, you are prompted that the update has completed successfully



9. In the preferences window that appears, go to **Signatures**
   a. In the Identities & Trusted Certificates section, click **More...**

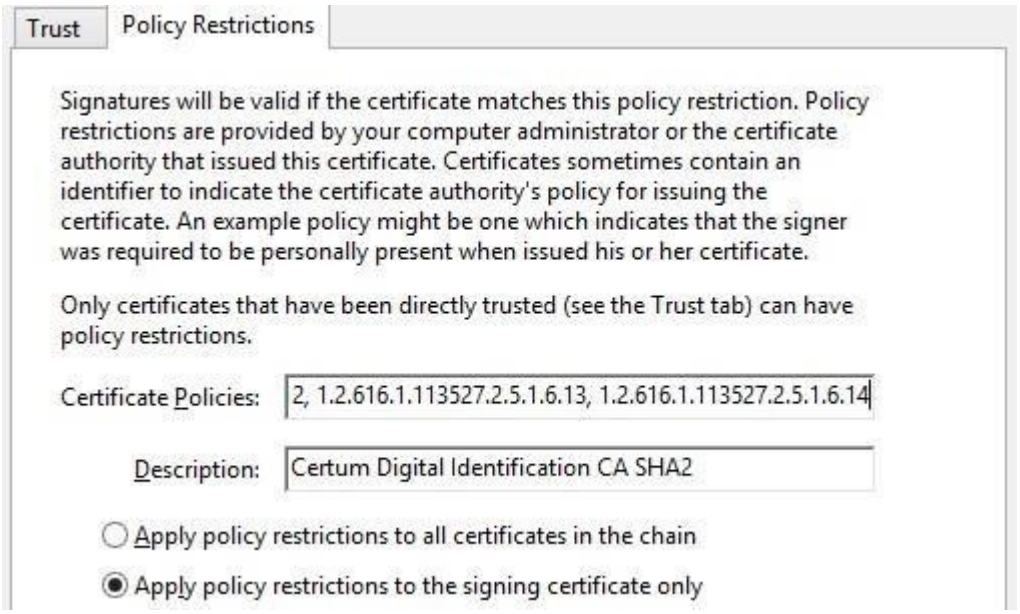


10. In the Digital ID and Trusted Certificate Setting window that appears, go to **Trusted Certificates**, search for **Certum Digital Identification CA SHA2**, and then click **Edit Trust**.



11. In the Edit Certificate Trust window that appears, go to the **Policy Restrictions** tab, and then in the **Certificate Policies** field, type a value and finish editing by clicking OK:

1.2.616.1.113527.2.5.1.6.11, 1.2.616.1.113527.2.5.1.6.12, 1.2.616.1.113527.2.5.1.6.13, 1.2.616.1.113527.2.5.1.6.14



12. Close the window just now to return to the report
13. The program should automatically verify the signature again



14. If verification has not been resumed automatically, click on **"Signature Panel"** and then right-click **" Rev. 1: Signed by Hamilton Poland Sp z.o.o. <info@hamilton.com.pl>** „ and select **"Validate Signature"**.



15. After the verification is complete, the status of the signature is displayed - **signature is VALID**

HAMILTON


Signature Validation Status
Signature is VALID, signed by J.S. Hamilton Poland Sp. z o.o. <info@hamilton.com.pl>.
- The document has not been modified since this signature was applied.
- The signer's identity is valid.
Signature Properties...
Close

HAMILTON