Adobe® Acrobat® DC with Entrust Time Stamp Server™

nShield® HSM Integration Guide

08 Sep 2021

Contents

1. Introduction . . . 3

    1.1. Product configurations . . . 3

    1.2. Requirements . . . 4

2. Procedures . . . 5

    2.1. Check the status of TSS and the Security World . . . 5

    2.2. Configure Adobe Acrobat DC to use TSS . . . 6

    2.3. Set up a digital ID . . . 7

    2.4. Import certificates into Adobe Acrobat DC . . . 8

    2.5. Configure the certificates . . . 9

    2.6. Sign and time-stamp a PDF document . . . 10

    2.7. Check how many time-stamps have been issued . . . 11

1. Introduction

Adobe Acrobat DC enables users to create, control, and secure Portable Document Format (PDF) documents. Users can also collectively review and edit documents, and convert documents from other formats to PDF.

The integration of Adobe Acrobat DC with Entrust nShield Time Stamp Server (TSS) performs signing and time-stamping to provide authenticity, integrity and non-repudiation of the document.

TSS is a time-stamp appliance. It uses the industry-standard IETF RFC 3161 protocol to provide time-stamps. TSS also provides a secure auditable trail of time for the purposes of non-repudiation. Adobe Acrobat DC natively supports the RFC 3161 time-stamp service provided by TSS. Time-stamp a PDF document to validate that document's authenticity at the time it was time-stamped.

nShield Hardware Security Modules (HSMs) integrate with Adobe Acrobat DC to enable a customer the ability to identify the publisher of a document and to verify that no one has altered the contents or any other aspect of the original document after it has been signed. Digital signatures, such as those used to sign for example Adobe PDF documents, rely on proven cryptographic techniques and the use of one or more private keys to sign and time-stamp the published software. It is important to maintain the confidentiality of these keys.

The benefits of using an HSM with Adobe Acrobat DC include:

- Protection for the organizational credentials of the software publisher.
- Secure storage of the private key.
- FIPS 140-2 Level 3 validated hardware.
- Provision of a trusted time-stamp to RFC 1631.

The benefits of TSS include:

- Centrally managed and secured time-stamp appliance.
- FIPS secure and audited link to a master time source.

1.1. Product configurations

Entrust has successfully tested the integration between TSS and Adobe Acrobat in the following configurations:

Operating System	Adobe Acrobat DC version	nShield TSS version
Windows Server 2019	Pro	8.0

ℹ This integration requires that the Default TSA be used for Adobe signing and time-stamping functionality.

ℹ Throughout this guide, the term HSM refers to the nShield Solo+ 500.

Other product configurations might work, but not all possible combinations, but have not been tested by Entrust.

1.2. Requirements

Before setting up the time-stamping functionality, ensure that:

- nShield software and hardware are installed and operational - the server URL of TSS will be needed during the integration process.
- Security World has been created and usable.
- The nShield Time Stamp Option Pack™ (TSOP) has been installed and the Default TSA is usable.
- Required certificates have been imported into the trusted Root CA on the local machine:
  - Signing root certificate.
  - If a third party is used to sign TSA certificates, subordinate certificate(s).
- Adobe Acrobat Pro DC has been installed.
- Appropriate Administrator rights are available to edit Adobe Acrobat settings options.

This document assumes that:

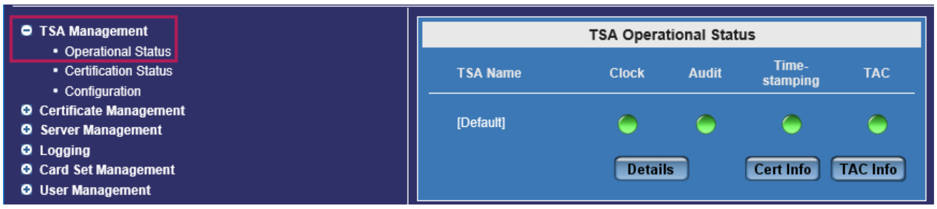
- Familiar with documentation supplied with TSOP and have installed TSS.
- Familiar with Adobe Acrobat DC documentation and have installed Adobe Acrobat DC.

2. Procedures

2.1. Check the status of TSS and the Security World

To check the status of TSS and the Security World:

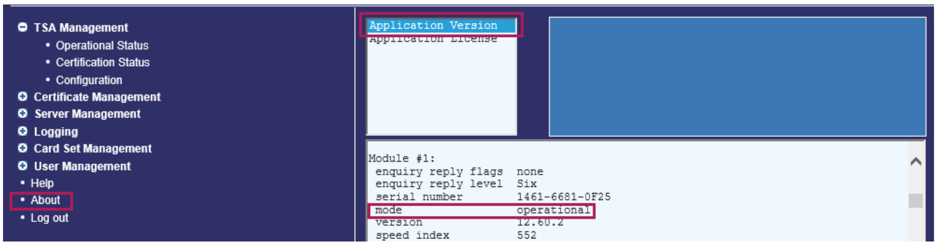
1. Ensure that your TSA is healthy and operational. To do, this, access the **TSA Operational Status** page, and check that the TSA shows all green lights.



TSA Operational Status

TSA Name	Clock	Audit	Time-stamping	TAC
[Default]	●	●	●	●

2. Ensure that the Security World is operational and healthy:



```
Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        1461-6681-0F25
 mode                 operational
 version              12.60.2
 speed index          552
```

   a. On the left, select **About**.

   b. Select **Application Version**.

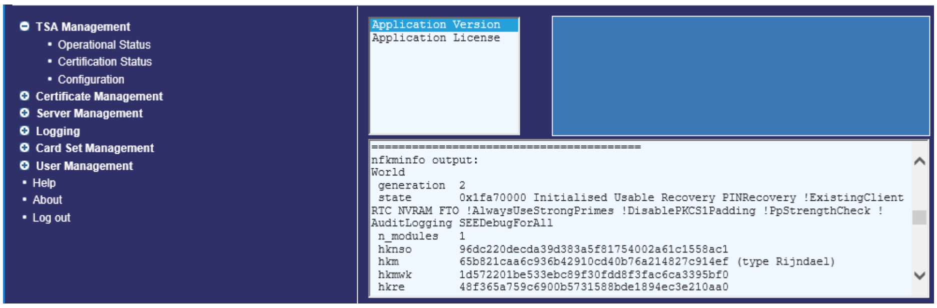
   c. Scroll down to show **Module 1#**.

      The **mode** should show as **operational**.

3. Continue to scroll down to **nfkminfo output: World**.

   The **state** should show as **Initialised** and **Usable**. There should be no exclamation marks (**!**).

   If either properties are preceded by an **!**, ensure that the Security World is available and operational.



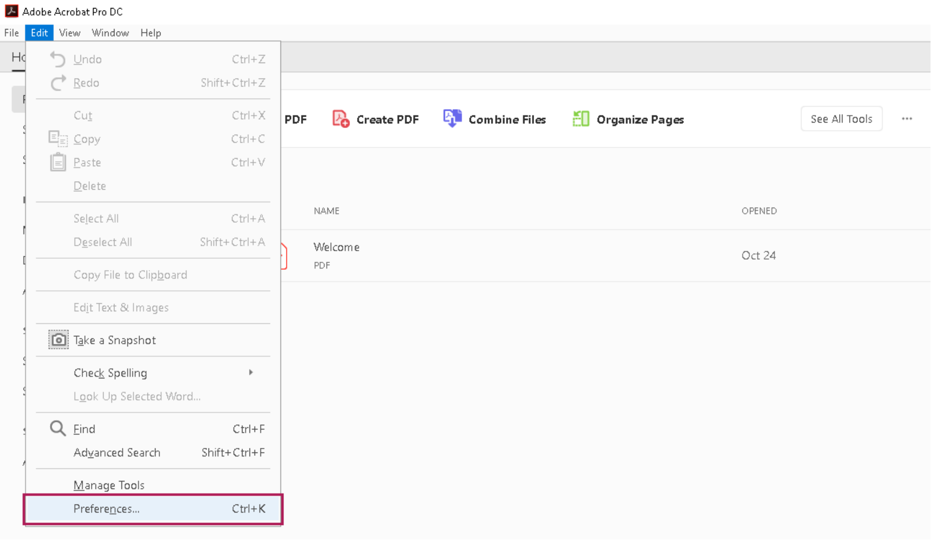
```
=======================================
nfkminfo output:
World
 generation  2
 state       0x1fa70000 Initialised Usable Recovery PINRecovery !ExistingClient
RTC NVRAM FTO !AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck !
AuditLogging SEEDebugForAll
 n_modules   1
 hknso       96dc220decda39d383a5f81754002a61c1558ac1
 hkm         65b821caa6c936b42910cd40b76a214827c914ef (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        48f365a759c6900b5731588bde1894ec3e210aa0
```

4. Continue to scroll down to **hardware status** and ensure that it is reported as **OK**.

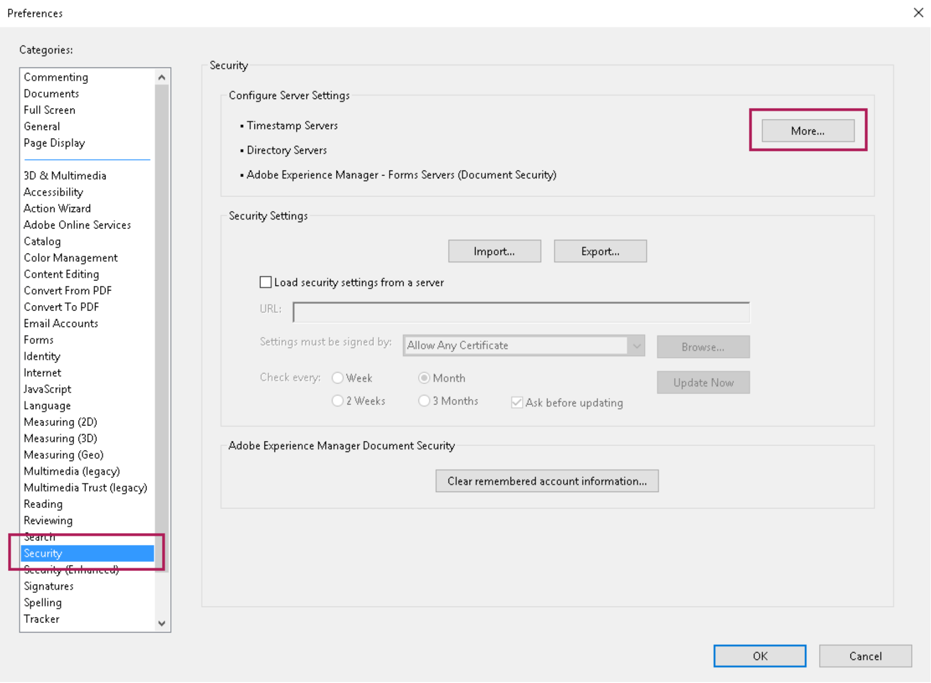
2.2. Configure Adobe Acrobat DC to use TSS

To configure Adobe Acrobat DC to use TSS:

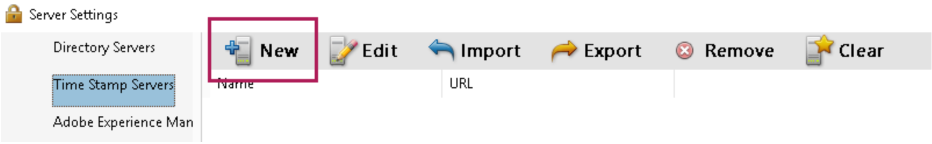
1. In the Windows Start menu, select **Adobe Acrobat DC**.
2. In the **Edit** menu of Adobe Acrobat, select **Preferences**.



3. From the list of categories, select **Security**.

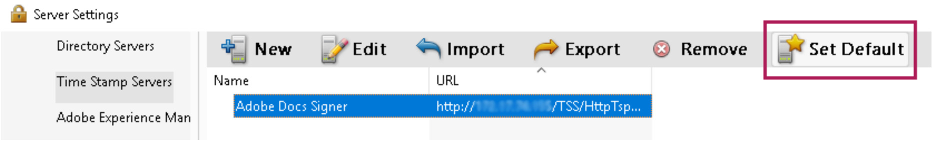


4. In the **Configure Server Settings** pane, select **More**.
5. In the **Server Settings** dialog, from the list of options, select **Time Stamp Servers**.



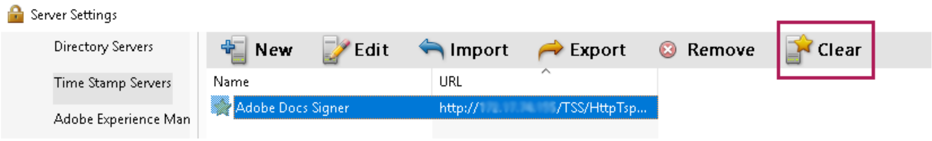
6. In the top ribbon, select **New**.
7. In the **New Time Stamp Server** dialog, enter a name and the server URL of TSS, then select **OK**.

   The server is now added.



8. Select the TSS, and in the top ribbon select **Set Default**.
9. When prompted **Are you sure you want to make this your new default server?**, select **OK**.

   If the default is successfully set, **Set Default** is replaced by **Clear**.

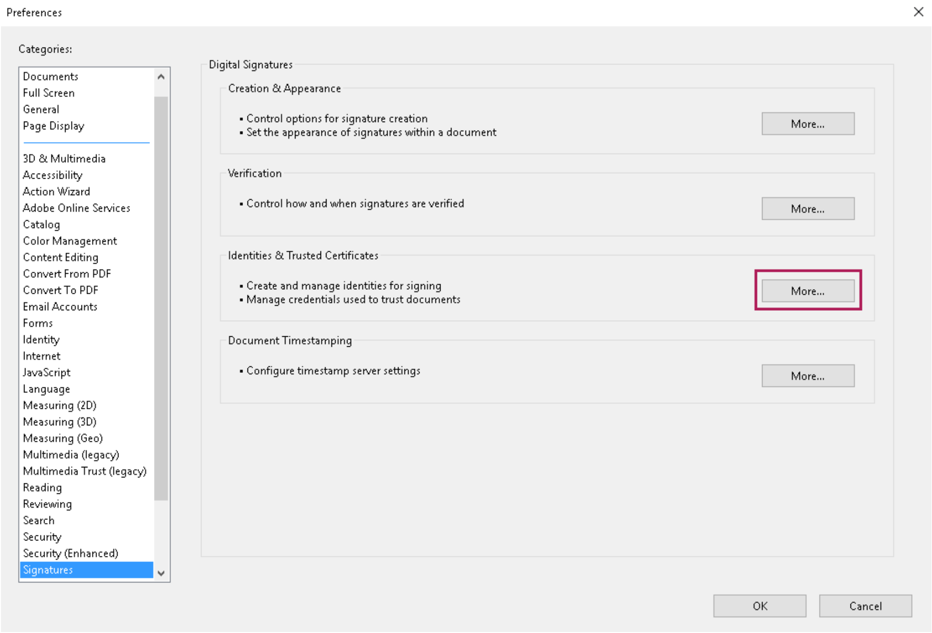


10. Close the **Server Settings** dialog.

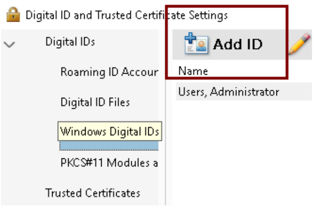
2.3. Set up a digital ID

To set up a digital ID:

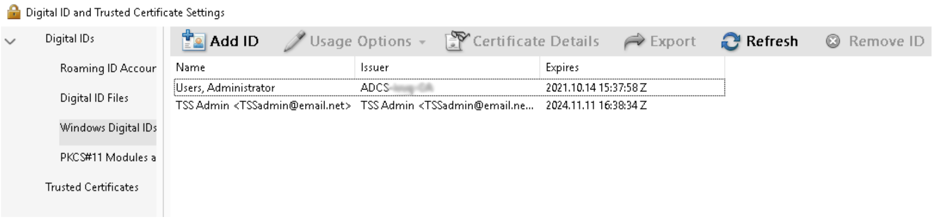
1. Stay in the **Preferences** dialog of Adobe Acrobat DC, and from the list of categories, select **Signatures**.



2. In the **Identities & trusted Certificates** box select **More**.
3. In the **Digital ID and Trusted Certificate Settings** dialog, select **Digital IDs > Windows Digital ID Files**, then select **Add ID**.



4. Select **Add a new self-signed digital ID**, then select **Next**.
5. Fill in the information fields (name, organizational unit, and so on), use the drop-down lists to select the key algorithm and the digital ID usage, then select **Finish**.
6. Confirm that the new ID appears in the list.

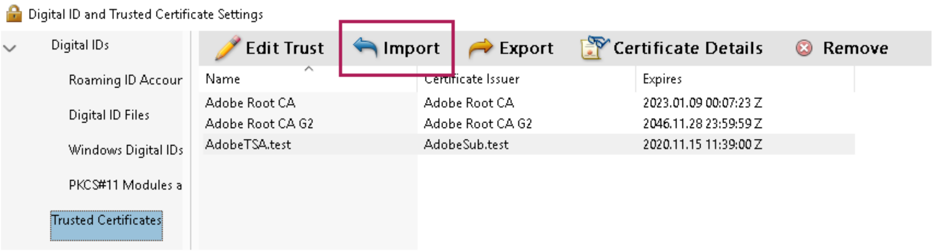


Name	Issuer	Expires
Users, Administrator	ADCS[redacted]	2021.10.14 15:37:58 Z
TSS Admin <TSSadmin@email.net>	TSS Admin <TSSadmin@email.ne...	2024.11.11 16:38:34 Z

2.4. Import certificates into Adobe Acrobat DC

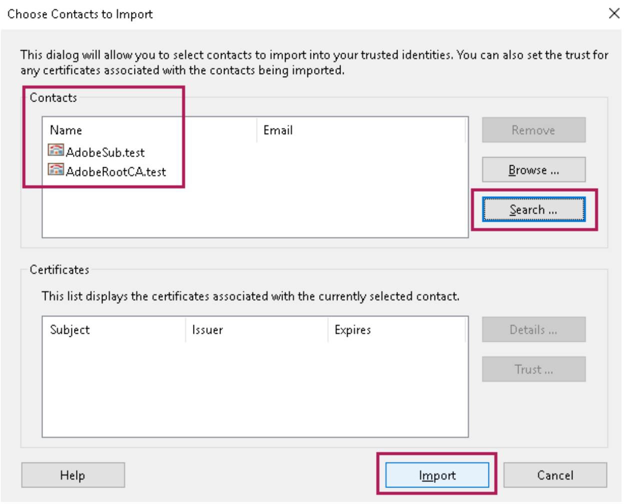
To import certificates into Adobe Acrobat DC:

1. Still in the **Digital ID and Trusted Certificate Settings** dialog, select **Digital IDs > Trusted Certificates**.
2. On the **Trusted Certificates** tab, select **Import**.



Name	Certificate Issuer	Expires
Adobe Root CA	Adobe Root CA	2023.01.09 00:07:23 Z
Adobe Root CA G2	Adobe Root CA G2	2046.11.28 23:59:59 Z
AdobeTSA.test	AdobeSub.test	2020.11.15 11:39:00 Z

3. In the **Choose Contacts to Import** dialog, use **Browse** or **Search** to locate the Root Certificate and any Subordinate Certificates.
4. Double-click the certificates to select. They will appear in the **Contacts**.



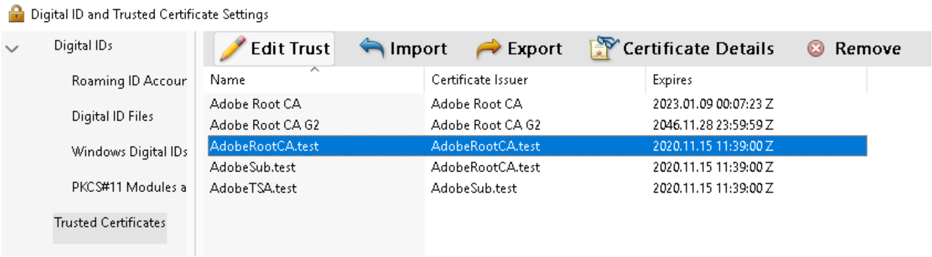
This dialog will allow you to select contacts to import into your trusted identities. You can also set the trust for any certificates associated with the contacts being imported.

Name	Email
AdobeSub.test	
AdobeRootCA.test	

This list displays the certificates associated with the currently selected contact.

Subject	Issuer	Expires

5. To add the certificates, select **Import**, then select **OK** to close the confirmation dialog about the import.
6. Confirm that the imported certificates appear in the list.

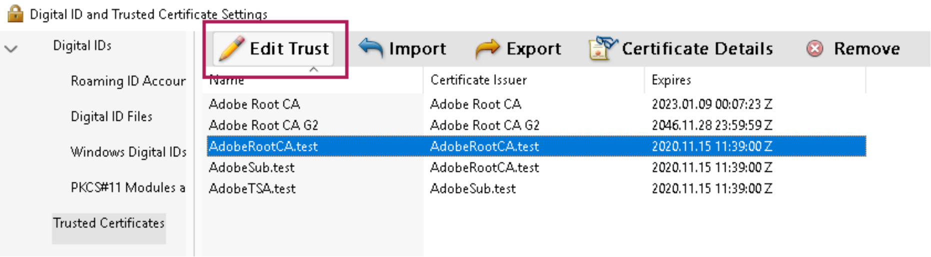


Name	Certificate Issuer	Expires
Adobe Root CA	Adobe Root CA	2023.01.09 00:07:23 Z
Adobe Root CA G2	Adobe Root CA G2	2046.11.28 23:59:59 Z
AdobeRootCA.test	AdobeRootCA.test	2020.11.15 11:39:00 Z
AdobeSub.test	AdobeRootCA.test	2020.11.15 11:39:00 Z
AdobeTSA.test	AdobeSub.test	2020.11.15 11:39:00 Z

2.5. Configure the certificates

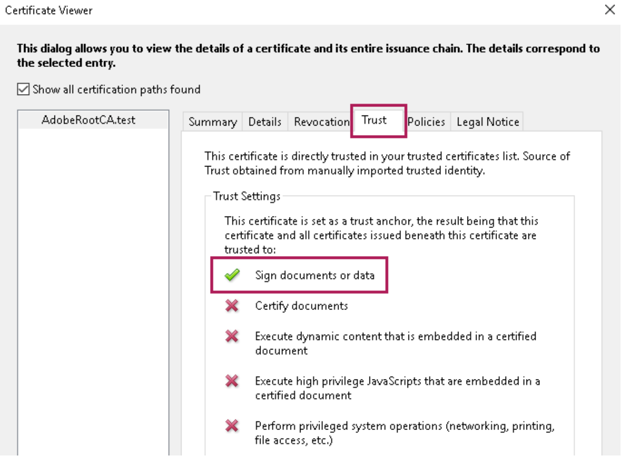
To configure the certificates:

1. Still in the **Digital ID and Trusted CertificateSettings** dialog, select the imported Root CA, then in the ribbon at the top of the window select **Edit Trust**.



Name	Certificate Issuer	Expires
Adobe Root CA	Adobe Root CA	2023.01.09 00:07:23 Z
Adobe Root CA G2	Adobe Root CA G2	2046.11.28 23:59:59 Z
AdobeRootCA.test	AdobeRootCA.test	2020.11.15 11:39:00 Z
AdobeSub.test	AdobeRootCA.test	2020.11.15 11:39:00 Z
AdobeTSA.test	AdobeSub.test	2020.11.15 11:39:00 Z

2. Select **Use this certificate as a trusted root**, then select **OK**.
3. In the ribbon at the top of the window select **Certificate Details**.
4. In the **Certificate Viewer** dialog, switch to the **Trust** tab.



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 directly trusted in your trusted certificates list. Source of Trust obtained from manually imported trusted identity.

This certificate is set as a trust anchor, the result being that this certificate and all certificates issued beneath this certificate are trusted to:

✓ 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

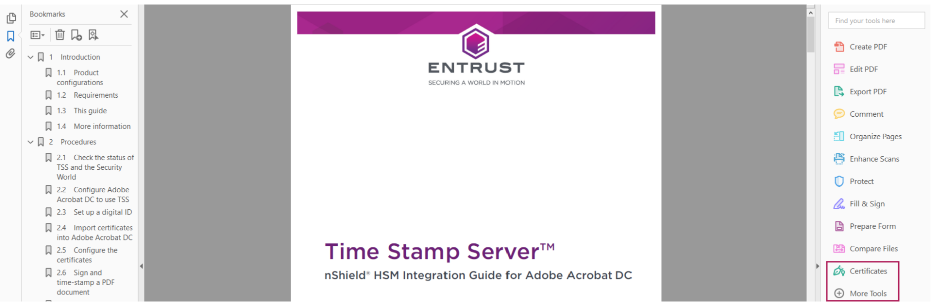
✗ Perform privileged system operations (networking, printing, file access, etc.)

5. Ensure that there is a green check mark next to **Sign documents or data**, then select **OK**.
6. Close the **Digital ID and Trusted Certificates Settings** dialog.
7. To exit the Adobe **Preferences** configuration settings, select **OK**.

2.6. Sign and time-stamp a PDF document

To sign and time-stamp a PDF document:

1. In Adobe Acrobat DC, open the document to sign and time-stamp it digitally.
2. From the ribbon on the right-hand side, select **Certificates**.



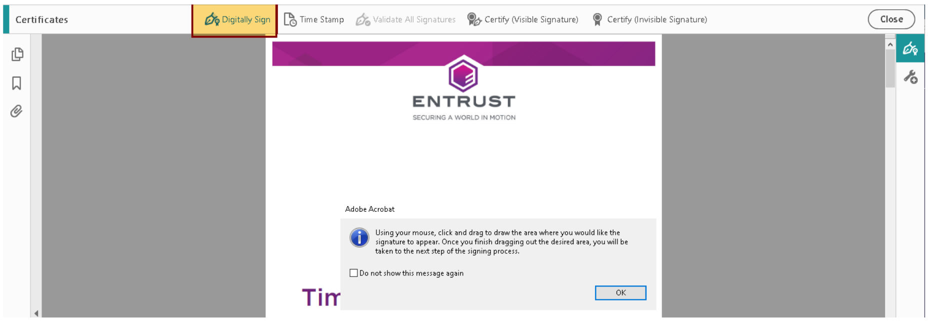
Bookmarks
1 Introduction
1.1 Product configurations
1.2 Requirements
1.3 This guide
1.4 More information
2 Procedures
2.1 Check the status of TSS and the Security World
2.2 Configure Adobe Acrobat DC to use TSS
2.3 Set up a digital ID
2.4 Import certificates into Adobe Acrobat DC
2.5 Configure the certificates
2.6 Sign and time-stamp a PDF document
ENTRUST
SECURING A WORLD IN MOTION
Time Stamp Server™
nShield® HSM Integration Guide for Adobe Acrobat DC
Find your tools here
Create PDF
Edit PDF
Export PDF
Comment
Organize Pages
Enhance Scans
Protect
Fill & Sign
Prepare Form
Compare Files
Certificates
More Tools

If the **Certificates** option is not visible:

a. In the ribbon on the right-hand side, select **More tools**.

b. Under **Forms & Signatures**, select **Add** for the **Certificates** tool.

3. In the **Certificates** toolbar, select **Digitally Sign**.


Certificates
Digitally Sign
Time Stamp
Validate All Signatures
Certify (Visible Signature)
Certify (Invisible Signature)
Close
ENTRUST
SECURING A WORLD IN MOTION
Tim

Adobe Acrobat

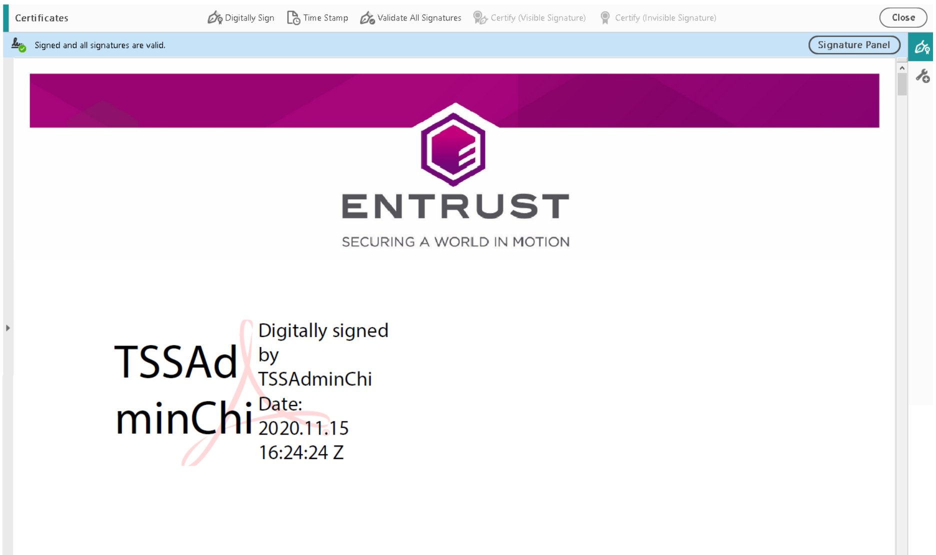
Using your mouse, click and drag to draw the area where you would like the signature to appear. Once you finish dragging out the desired area, you will be taken to the next step of the signing process.

□ Do not show this message again

OK

4. Follow the information in the dialog box to select an area for signature, then select **OK**.
5. Select the Digital ID with which to sign, and select **Continue**.
6. Confirm all details and select **Sign**.
7. Choose a location to save the newly signed document.

   To avoid overwriting the original file, use a different file name for the signed document.



Signed and all signatures are valid.

TSSAdminChi

Digitally signed by TSSAdminChi Date: 2020.11.15 16:24:24 Z

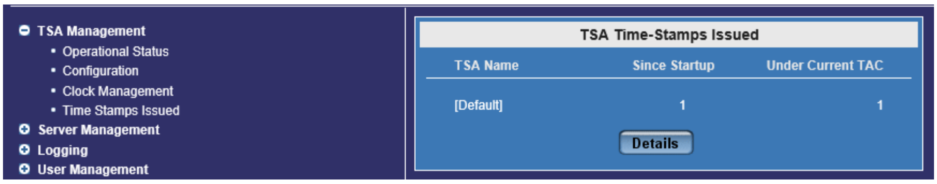
8. To inspect the signature properties, right-click the signature on the PDF page and select **Show Signature Properties**.

2.7. Check how many time-stamps have been issued

To check how many time-stamps have been issued:

1. Log in to TSS as Admin.

2. Under **TSA Management**, select **Time Stamps Issued**.
3. Check for the number of issued time-stamps under the current TAC since TSS was started up.



TSA Time-Stamps Issued

TSA Name	Since Startup	Under Current TAC
[Default]	1	1