

Adobe[®] Acrobat[®] DC with Entrust Time Stamp Server[™]

nShield[®] HSM Integration Guide

© 2024 Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction
1.1. Product configurations
1.2. Requirements
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
2.7. Check how many time-stamps have been issued
3. Additional resources and related products
3.1. nShield Solo
3.2. Time Stamping Option Pack
3.3. Entrust digital security solutions
3.4. nShield product documentation 11

Chapter 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 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	Adobe Acrobat	nShield TSS	Security	Firmware
System	DC version	version	World	
Windows Server 2019	Pro	8.0	12.81.2	12.72.1



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



Throughout this guide, the term HSM refers to the nShield Solo XC.

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.



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

Chapter 2. Procedures

2.1. Check the status of TSS and the Security World

To check the status of TSS and the Security World:

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. If you
do not have all green lights after creating a new certificate, then try restarting
the DSE200 service.

TSA Management		TSA Operational Status					
Operational Status Certification Status	TSA Name	Clock	Audit	Time- stamping	ТАС		
 Configuration 				Stamping			
Certificate Management	10-4	A	<u> </u>	<u> </u>			
Server Management	[Deraut]						
Logging							
Card Set Management		Detai	s	Cert Info	TAC Info		
User Management							

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

TSA Management Operational Status Cortification Status Confluenzation Status Confluenzation Certificate Management O Server Management O Logging	Application Version Application Dicense		
O Card Set Management O User Management • Help • About • Log out	Module #1: enquiry reply flags enquiry reply level serial number mode version	none Six 1461-6601-0725 operational 17.00.2	^

- 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.

TSA Management • Operational Status • Cortification Status • Confliguration O cortificate Management O server Management O Logging	Application Version Application License	
Card Set Management		
User Management	nfkminfo output:	^
• Help	generation 2	
About	state 0x1fa70000 Initialised Usable Recovery PINRecovery !ExistingClient	
Log out	RTC NVRAM FTO 'AlwaysUseStrongPrimes !DisablePKCS1Padding !PpStrengthCheck ! AuditLogging SEEDebugForAll n modules 1	
	hkmso 96dc220decda39d383a5f81754002a61c1558ac1 hkm 65b821caa6c936b42910cd40b768214827c914ef (type Rijndae1) hkmwk 1d572201be53bec69530fd8f3f3a6c6a395bf0 hkre 48f365a759c6900b5731588bde1894ec3e210aa0	~

 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.

즈 Ad	lobe Ac	robat Pro DC							
File 🚺	dit V	iew Window Help							
Ho	5	Undo	Ctrl+Z						
	Ċ	Redo	Shift+Ctrl+Z						
F			Ctrl+X	PDI	E 🔼 Crasta PDE	Combine Filer	🗐 Organiza Pagor		See All Tools
4	E	Copy	Ctrl+C	10	r Lo create PDF	Combine rites	U Organize Pages		SEE AIL TOOIS
1		Paste	Ctrl+V						
		Delete							
		Coloret All	Ciel LA		NAME			OPENED	
- 1		Seject All	CIN+A						
		Deselect All	Shift+Ctri+A	1	Welcome			Oct 24	
		Copy File to Clipboard		Ľ.,	PDF				
1		Edjt Text & Images							
1	6	T <u>a</u> ke a Snapshot							
4		Check Spelling	+						
1		Look Up Selected Word							
	Q	Eind	Ctrl+F						
		Advanced Search	Shift+Ctrl+F						
		Manage Tools							
		Preferences	Ctrl+K						
	_								

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

Categories:	Security.
Commenting ^	secunty
Documents	Configure Server Settings
Full Screen	
General	Timestamp Servers More
Page Display	Directory Servers
3D & Multimedia	Adobe Experience Manager - Forms Servers (Document Security)
Accessibility	
Action Wizard	Security Settings
Adobe Online Services	errority errority.
Catalog	Imnort Evnort
Color Management	
Content Editing	Load security settings from a server
Convert To PDF	
Email Accounts	UNL
Forms	Settings must be signed by: Aller Castlerate
Identity	Allow Any Certificate V Browse
Internet	Check every: Week Month
JavaScript	Update Now
Language	O 2 Weeks O 3 Months ⊘Ask before updating
Measuring (2D)	
Measuring (SD)	Adobe Experience Manager Document Security
Multimedia (legaci)	
Multimedia Trust (legacy)	Clear remembered account information
Reading	
Reviewing	
Search	
Security	
Security (Enhanced)	
Signatures	
Spelling	

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

🔒 Server Settings						
Directory Servers	📲 New	📝 Edit	≒ Import	À Export	🔕 Remove	😭 Clear
Time Stamp Servers Adobe Experience Man	ivame		URL			

- 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.

🔒 Server Settings						
Directory Servers	省 New	📝 Edit	≒ Import	🚧 Export	📀 Remove	📄 Set Default
Time Stamp Servers	Name		URL	<u>^</u>		
Adobe Experience Man	Adobe Docs	s Signer	http://	/TSS/HttpTsp		

- 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.

🔒 Server Settings						
Directory Servers	📲 New	📝 Edit	🦱 Import	혀 Export	📀 Remove	😭 Clear
Time Stamp Servers	Name		URL	^		
Adobe Experience Man	Adobe Docs	: Signer	http://1	/TSS/HttpTsp		

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**.

	Digital Signatures	
ocuments ^	Counting the Association	
ull Screen	Creation of Appearance	
eneral	Control ontions for signature creation	
age Display	 Set the appearance of signatures within a document 	More
0 & Multimedia		
ccessibility	Verification	
ction Wizard		
dobe Online Services	 Control how and when signatures are verified 	More
atalog		
olor Management		
ontent Editing	Identities & Trusted Certificates	
onvert From PDF		
onvert To PDF	 Create and manage identities for signing 	More
mail Accounts	 Manage credentials used to trust documents 	
orms		
lentity	Document Timestamping	
ternet		
waScript	 Configure timestamp server settings 	More
anguage		
leasuring (2D)		
leasuring (3D)		
leasuring (Geo)		
lultimedia (legacy)		
lultimedia Trust (legacy)		
eading		
eviewing		
earch		
ecurity		
ecurity (Enhanced)		
anatures		

- 2. In the Identities & trusted Certificates box select More.
- 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.

🔒 Di	gital ID and Trusted Certific	ate Settings					
\sim	Digital IDs	📩 Add ID 🛛 🥒 Us	age Options 👻 🛐	Certificate Details	≓ Export	Refresh	🕲 Remove ID
	Roaming ID Accour	Name	Issuer	Expires			
	D: 1 UD 51	Users, Administrator	ADCS	2021.10.14 15:	37:58 Z		
	Digital ID Files	TSS Admin <tssadmin@email< td=""><td>.net> TSS Admin <tssadmir< td=""><td>n@email.ne 2024.11.11 16:</td><td>:38:34 Z</td><th></th><td></td></tssadmir<></td></tssadmin@email<>	.net> TSS Admin <tssadmir< td=""><td>n@email.ne 2024.11.11 16:</td><td>:38:34 Z</td><th></th><td></td></tssadmir<>	n@email.ne 2024.11.11 16:	:38:34 Z		
	Windows Digital IDs						
	PKCS#11 Modules a						
	Trusted Certificates						

2.4. Import certificates into Adobe Acrobat DC

To import certificates into Adobe Acrobat DC:

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

🔐 Digital ID and Trusted Certificate Settings						
~	Digital IDs	🥖 Edit Trust	ҁ Import	产 Export	💇 Certificate Details	🔕 Remove
	Roaming ID Accour	Name	Certi	ficate Issuer	Expires	
		Adobe Root CA	Adol	be Root CA	2023.01.09 00:07:23 Z	
	Digital ID Files	Adobe Root CA G2	Adol	be Root CA G2	2046.11.28 23:59:59 Z	
	Windows Digital IDs	AdobeTSA.test	Adol	beSub.test	2020.11.15 11:39:00 Z	
	PKCS#11 Modules a					
	Trusted Certificates					

- 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**.

Name	Er	nail	Remove
🖾 AdobeSub.test	test		Browse
			_
			Search
tificates his list displays the	certificates associated	with the currently selected conta	act.
tificates This list displays the Subject	certificates associated	with the currently selected conta	act. Details
tificates This list displays the Subject	certificates associated	with the currently selected conta Expires	act. Details Trust

- 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.

🔒 Digital ID and Trusted Certificate Settings						
\sim	Digital IDs	🥖 Edit Trust 🛛 ล Ir	nport <i> i</i> Export	🝸 Certificate Details	🔕 Remove	
	Roaming ID Accour	Name	Certificate Issuer	Expires		
	Digital ID Files	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		
	Windows Digital IDs	AdobeRootCA.test	AdobeRootCA.test	2020.11.15 11:39:00 Z		
		AdobeSub.test	AdobeRootCA.test	2020.11.15 11:39:00 Z		
	PKCS#11 Modules a	AdobeTSA.test	AdobeSub.test	2020.11.15 11:39:00 Z		
	Trusted Certificates					

2.5. Configure the certificates

To configure the certificates:

 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.

🚞 D	igital ID and Trusted Certifi	ate Settings				
~	Digital IDs	🥖 Edit Trust	측 Impo	rt <i> i</i> Export	🖹 Certificate Details	🔕 Remove
	Roaming ID Accour	Name	۱ I	Certificate Issuer	Expires	
	Digital ID Files	Adobe Root CA	1	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	
	Windows Digital IDs	AdobeRootCA.test		AdobeRootCA.test	2020.11.15 11:39:00 Z	
		AdobeSub.test	1	AdobeRootCA.test	2020.11.15 11:39:00 Z	
	PKCS#11 Modules a	AdobeTSA.test	,	AdobeSubitest	2020.11.15 11:39:00 Z	
	Trusted Certificates					

- 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.



- 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**.



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**.

Certit	licates	🖧 Digitally Sign	🖹 Time Stamp 🤣 Validate Al Signatures 🔹 Certify (Visible Signature) 🦉 Certify (Invisible Signature)	Close
¢				^ <i>b</i> a
П				to.
P			ENTRUST	
			accompa a noncura nazioni	
			Adobe Acrobot	
			Utrag your mouse, rick and dags to dave the rear where you would like the granter to appear to expose the second the desired area, you will be taken to the met frage of the significant process.	
4			Tim	

- 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.



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.



Chapter 3. Additional resources and related products

- 3.1. nShield Solo
- 3.2. Time Stamping Option Pack
- 3.3. Entrust digital security solutions
- 3.4. nShield product documentation