

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

nShield[®] HSM Integration Guide

08 Sep 2021

© 2022 Entrust Corporation. All rights reserved.

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

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



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+ 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:

 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 Management		TSA Opera	tional Stat	us	
Operational Status Certification Status Configuration	TSA Name	Clock	Audit	Time- stamping	TAC
Certificate Management Server Management	[Default]	0	0	0	0
 Logging Card Set Management User Management 		Detail	s	Cert Info	TAC Info

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

TSA Management • Operational Status • Certification Status • Confliguration Certificate Management O Server Management O Logging	Application Version Application Dicense	
O Card Set Management O User Management Help Apout Log out	Module #1: enquiry reply flags enquiry reply level serial number mode Version speed index	nome 51x 1461-6681-0F25 0peretional 12:00.2 552

- 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.

TSA Management Operational Status Certification Status Configuration Certificate Management Server Management Logging	Application Version Application License	
 Card Set Management User Management 	nfkminfo output: Norld	^
• Help • About • Log out	generation 2 state Oxifa70000 Initialised Usable Recovery PINRecovery !ExistingClient RTC NVRAM FTO !AlwaysUseStrongFrimes !DisablePKCSIFadding !PpStrengthCheck ! AuditLogging SEEDebugForAll n_modules 1	
	hkmso 96dc3220decda39d383a5f81754002461c1558ac1 hkm 65b821caa6c936b42910cd40b76a214827c914ef (type Rijndael) hkmsk 14572201be533bcb98100fd6873fac6ca395bf0 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.

入 Ac	lobe Ac	robat Pro DC							
File	Edit Vi	iew Window Help		_					
Ho	5	Undo	Ctrl+Z						
	Ċ	Redo	Shift+Ctrl+Z						
1		Cu <u>t</u>	Ctrl+X	PDF	🔥 Create PDF	👫 Combine Files	📒 Organize Pages		See All Tools
4	E	<u>C</u> opy	Ctrl+C		-0	•			
	Ê	Paste	Ctrl+∀						
		Delete							
		Select All	Ctrl+A		NAME			OPENED	
]		D <u>e</u> select All	Shift+Ctrl+A	5	Welcome			Oct 24	
		Copy File to Clip <u>b</u> oard			PDF			0000	
1		Edit Text & Images							
1	0	Take a Snapshot							
1		Check Spelling	÷						
4		Look Up Selected Word	d						
	Q	Eind	Ctrl+F						
		Advanced Search	Shift+Ctrl+F						
		<u>M</u> anage Tools							
- F		Preferences	Ctrl+K						

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

ategories:		
Commenting 🔥	Security	
ocuments	Configure Server Settings	
ull Screen		1.
ieneral	Timestamp Servers More	
age Display	Directory Servers	
D & Multimedia	Adobe Experience Manager - Forms Servers (Document Security)	
ccessibility		
ction Wizard	Security Settings	
dobe Online Services		
atalog	Import Export	
olor Management	in portan	
ontent Editing onvert From PDF	Load security settings from a server	
onvert From PDF onvert To PDF		
nvert To PUF	URL:	
nali Accounts orms		
entity	Settings must be signed by: Allow Any Certificate 🗸 Browse	
itemet		
vaScript	Check every: O Week O Month Update Now	
inguage	2 Weeks 3 Months ☑ Ask before updating	
leasuring (2D)		
leasuring (3D)	Adobe Experience Manager Document Security	
leasuring (Geo)	Adobe Experience Manager Document Security	
lultimedia (legacy)	Clear remembered account information	
lultimedia Trust (legacy)	Clear remembered account information	
eading		
eviewing		
earch		
ecurity		
carity (Enhanced)		
gnatures		
pelling racker		
racker v		

- 4. In the **Configure Server Settings** pane, select **More**.
- 5. 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	ivarrie		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	📲 New	📝 Edit	≒ Import	≓ Export	📀 Remove	📄 Set Default
Time Stamp Servers	Name		URL	^		
Adobe Experience Man	Adobe Docs	Signer	http://100101	/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	省 New	📝 Edit	ҁ Import	<i> i</i> Export	🔕 Remove	😭 Clear
Time Stamp Servers	Name		URL	^		
Adobe Experience Man	👷 Adobe Docs	Signer	http://	/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**.

Documents A	Digital Signatures	
Full Screen	Creation & Appearance	
General		
Page Display	Control options for signature creation	More
-3	 Set the appearance of signatures within a document 	
D & Multimedia		
Accessibility	Verification	
Action Wizard		
Adobe Online Services	 Control how and when signatures are verified 	More
Catalog		
Color Management		
Content Editing	Identities & Trusted Certificates	
Convert From PDF		
Convert To PDF	 Create and manage identities for signing 	More
mail Accounts	 Manage credentials used to trust documents 	
orms		
dentity	Document Timestamping	
nternet		
avaScript	 Configure timestamp server settings 	More
anguage		
Measuring (2D)		
Measuring (3D)		
Measuring (Geo)		
vlultimedia (legacy)		
Aultimedia Trust (legacy)		
Reading		
leviewing		
earch		
ecurity		
Security (Enhanced)		
šignatures 🗸 🗸		

- 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.

🔒 Digital ID and Trusted Certifi	ate Settings
 Digital IDs 	撞 Add ID 🥖
Roaming ID Accour	Name
Digital ID Files	Users, Administrator
Windows Digital IDs	
PKCS#11 Modules a	
Trusted Certificates	

- 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 dropdown lists to select the key algorithm and the digital ID usage, then select **Finish**.
- 6. Confirm that the new ID appears in the list.

6	Digital ID and Trusted Certifi	cate Settings				
\sim	Digital IDs	1 🛃 🕹 🕹 🕺 🕹 🕺 🕹 🕹	ge Options 👻 🎦 Certifica	te Details 🛛 🌈 Export	🔁 Refresh	🕲 Remove ID
	Roaming ID Accour	Name	Issuer	Expires		
	01.01.00.00	Users, Administrator	ADCS	2021.10.14 15:37:58 Z		
	Digital ID Files	TSS Admin <tssadmin@email.ne< td=""><td>t> TSS Admin <tssadmin@email.ne< td=""><td>2024.11.11 16:38:34 Z</td><td></td><td></td></tssadmin@email.ne<></td></tssadmin@email.ne<>	t> TSS Admin <tssadmin@email.ne< td=""><td>2024.11.11 16:38:34 Z</td><td></td><td></td></tssadmin@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 Certifi	ate Settings		1		
\sim	Digital IDs	🥖 Edit Trust	ҁ Import	产 Export	🝸 Certificate Details	🔕 Remove
	Roaming ID Accour	Name	Cert	ficate Issuer	Expires	
	District D Dist	Adobe Root CA	Ado	be Root CA	2023.01.09 00:07:23 Z	
	Digital ID Files Adobe Root CA G2		Ado	be Root CA G2	2046.11.28 23:59:59 Z	
	Windows Digital IDs	AdobeTSA.test	Ado	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**.

ntacts Name 🖾 AdobeSub.test		Email	Remove
AdobeRootCA.	.test		<u>B</u> rowse <u>S</u> earch
tificates This list displays the	e certificates associat	ed with the currently selecte	:d contact.

- 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 IDs	🥖 Edit Trust	🐂 Impoi	't 🧀 Export	🝸 Certificate Details	📀 Remove
Roaming ID Accour	Name	C	ertificate Issuer	Expires	
	Adobe Root CA	A	dobe Root CA	2023.01.09 00:07:23 Z	
Digital ID Files	Adobe Root CA G2	A	dobe Root CA G2	2046.11.28 23:59:59 Z	
Windows Digital IDs	AdobeRootCA.test	A	dobeRootCA.test	2020.11.15 11:39:00 Z	
·····	AdobeSub.test	A	dobeRootCA.test	2020.11.15 11:39:00 Z	
PKCS#11 Modules a	AdobeTSA.test	A	dobeSub.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	cate Settings				
\sim	Digital IDs	🥖 Edit Trust	🦱 Imp	ort , 🔶 Export	🝸 Certificate Details	🔕 Remove
	Roaming ID Accour	Name		Certificate Issuer	Expires	
		Adobe Root CA		Adobe Root CA	2023.01.09 00:07:23 Z	
	Digital ID Files	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. 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.

Certificate Viewer								\times
This dialog allows you to view the selected entry. Show all certification paths f		tails of	a certifi	cate and its o	entire is:	suance c	hain. The details correspond t	to
AdobeRootCA.test	Sum	mary	Details	Revocation	Trust	Policie	es Legal Notice	
		rust obf Trust S This certi	tained fr ettings – certifica	om manually te is set as a t	importe	ed trusted	d certificates list. Source of d identity. result being that this h this certificate are	
		«	Sign d	ocuments or	data			
		×	Certify	documents				
		×	Execut docum		intent th	at is emb	edded in a certified	
		×		e high privile d document	ge JavaS	cripts tha	at are embedded in a	
		×		m privileged : :ess, etc.)	system o	peration	s (networking, printing,	

- 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 X			^	Find your tools here
	E- 🗓 🕞 🖫				1 Create PDF
O	V 1 Introduction		ENTRUST		Edit PDF
	configurations 1.2 Requirements		SECURING A WORLD IN MOTION		Export PDF
	1.3 This guide				💬 Comment
	□ 1.4 More information ∨ □ 2 Procedures				Crganize Pages
	2.1 Check the status of TSS and the Security				📇 Enhance Scans
	World 2.2 Configure Adobe				D Protect
	Acrobat DC to use TSS 2.3 Set up a digital ID				🔏 Fill & Sign
	2.4 Import certificates into Adobe Acrobat DC				Prepare Form
	 2.5 Configure the certificates 		Time Stamp Server™		Compare Files
	2.6 Sign and time-stamp a PDF	1	nShield [®] HSM Integration Guide for Adobe Acrobat DC		Certificates
	document				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.



- 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.

TSA Management		TSA Time-Stamps Issued				
Operational Status Configuration	TSA Name	Since Startup	Under Current TAC			
Clock Management Time Stamps Issued	[Default]					
 Server Management Logging 		Details				
User Management						