Symantec[™] Managed PKI[®]

Integrating Adobe CDS Organization Certificates with Adobe[®] LiveCycle[®] Enterprise Suite and Adobe[®] Reader[®]



Symantec[™] Managed PKI[®] Integrating Adobe CDS Organization Certificates with Adobe[®] LiveCycle[®] Enterprise Suite and Adobe[®] Reader[®]

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated November 13, 2013

Legal Notice

ii

Copyright © 2013 Symantec Corporation. All rights reserved

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign, VeriSign Trust, and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. Other names may be trademarks of their respective owners. The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec[®] product.

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

http://www.symauth.com/support/index.html

Contents

Chapter 1	Integrating Adobe CDS Organization Certificates with Adobe [®] LiveCycle [®] Enterprise Suite and Adobe [®] Reader [®]	1
	Partner Information	1
	How the Adobe CDS Organization Certificate Works	2
	Integration Workflow	3
	Prerequisites	5
	Generate CSR on HSM	5
	PKI Manager approval	7
Chapter 2	Configuring Partner Products	9
	Setting Up Adobe LiveCycle Enterprise Suite	9
	Configuring TrustManager on Adobe LiveCycle Enterprise Suite	9
	Configuring Adobe LiveCycle Workbench for Signing Process	11
	Setting Up Adobe Reader	15
	Configuring HSM module on the Adobe Reader	15
	Digitally Signing Documents using Adobe Reader	16

iv Contents

Chapter

Integrating Adobe CDS Organization Certificates with Adobe[®] LiveCycle[®] Enterprise Suite and Adobe[®] Reader[®]

The enterprise workplace has moved beyond the walls of the organization into a global, mobile environment. To maintain productivity, your end users need to access company resources using a mobile platform. However, you need to be able to trust the end users accessing your systems, and the mobile devices they use, whether you provide their devices or they bring their own.

Symantec's Managed PKI digital certificates can provide that trust without the burden of user names, passwords, or additional hardware tokens. Managed PKI is scalable from several to thousands of devices, providing an in-the-cloud solution for quick deployment and easy management. It also incorporates features from Symantec's other leading security products.

Symantec's digital certificates for Certified Document Services (CDS) Organization allow you to include digital signatures that let you sign PDF files. By digitally signing a pdf, you apply your unique digital mark to the document and also confirm the document has not been altered in transit.

This document describes how to configure CDS Organization certificate with Adobe® LiveCycle® and Adobe® Reader[®] to digitally authenticate Adobe[®] PDF documents.

Partner Information

These procedures have been tested on the following platforms:

Table 1-1Pa	artner Information
Partner Name	Adobe®
Product Name and Version	Adobe® LiveCycle® Enterprise Suite 4, Adobe® Reader® XI

How the Adobe CDS Organization Certificate Works

The following diagram describes how Managed PKI certificates support CDS Organization certificate and integrates with Adobe Reader for digital authentication.



Figure 1-1 Adobe CDS Certificate integration with Adobe Reader

- 1 Organization A digitally signs an Adobe PDF document using Organization A's private key.
- **2** Organization B or User B of Organization B receives the document and authenticates it using Organization A's public key.

Integration Workflow

The following diagram describes the general steps required to set up a Symantec Managed PKI account and integrate Managed PKI certificates with Adobe LiveCycle and Adobe Reader.



Figure 1-2 Managed PKI Integration Workflow

Task 1. Set up your Managed PKI 8.9 account

Contact your Symantec Sales representative to set up your Managed PKI account. Your representative will provide you with the necessary information to begin defining your account and certificate profile.

You will need to complete and return the following documents. As needed, your Symantec representative will assist you in obtaining and completing these forms.

- Master Service Agreement
- Issuing Authority Naming Application (also known as the CA Naming Document)
- Symantec Services Order Form
- Purchase Order, credit card, or reference number

You will need to obtain your initial Managed PKI administrator ID, which is your credential to access your Managed PKI account. Your Symantec representative will assist you with obtaining your Managed PKI administrator ID. You will use your Managed PKI administrator ID to log into PKI Manager, configure your Managed PKI account, and obtain your RA certificate. For more information on configuring Managed PKI, refer to PKI Manager and its online help.

Task 2. Create a certificate profile

Managed PKI uses a certificate profile to define the certificates issued. Certificate issued by Adobe CDS Organization enables digital authentication of PDF documents.

Complete the following steps to create your Managed PKI Adobe CDS Organization certificate profile:

- 1 Log on to Managed PKI's PKI Manager using your administrator certificate. You will be prompted for your PKI Client PIN.
- 2 On PKI Manager, click **Manage certificate profiles** or select **Manage certificate profiles** from the Tasks menu on the bottom navigation bar.

antec" PKI Manager	<mark>⊘</mark> Symantec.	Lo	gged in as: 📾	switt@ycpmail.
Account activity Lat update: Col 17. 2015 05 AM Refere All Recent activity There is no recent activity for this function	Aters Symatter Managed PIO is plassed to announce that version 0.5 is now LIVE. This version includes significant solvances in a number of key areas: administrators now have the ability to detex certificate porties and revice multiplic certificates at order time. Web services have been enhanced, and third-party integrational solvances in a number of key areas: administrators now available for download through the PIO Marger Resources page. Additionally, managed PIO 3 enables organizations to perform foglat single with a recent care to available on the Resources page. For more information on the these and other security updates available in this release, refer to Managed PIO V&S Release notes available on the Resources page.	Account status You need to set a you can issue ce users. Set up your acco Next senice re	up a few ite rtificates to unt newal: Oct 17	ims before i your
	There is no data to display for this account.			
		Seat usage Seat pool	Total used	Total purchased
	User and vertificates Manage cards Manage collicates	User	0	1000
	Manage subtriced pointer Manage subtriced user lists Recording	Device	0	100
	View recent reports Schedule a report	server	0	100
	View andot trail Your account Manage account and sub-	Adobee CDS Organization	0	100
	accontra Manage administrators Manage RA Manage RV Enderprise dateways Get an RA cestificate Get a signing authority certificate	Secure Email Gatewa Buy more seats	0	100

Figure 1-3 Manage Certificate Profile

- **3** Click **Add Certificate profiles** from the top of the resulting Manage certificate profiles page. The Create profile page appears.
- 4 Select whether these certificates will be issued in Test mode or Production Mode, and click **Continue**. The Create profile page appears.
- 5 Select **Adobe**[®] **CDS Organization** as the certificate template and click **Continue**. The Customize certificate options page appears.
- 6 In the Customize certificate options, enter a certificate profile name.

📕 Manage Certificate profiles 🛛 🤅	Add Certificate profiles 🛛 💿 Manage custom scripts	
O Certificate profiles O Certificate profiles No results found.	Create profile: Select template Customize options Customize services Customize certificate options Review and change the template options for this profile. Certificate friendly name: Adobe Organization Image: Certificate options Image: Certificate options Primary certificate options Image: Certificate options Image: Certificate options Certificate options Image: Certificate options Image: Certificate options Certificate authority: Image: Certificate options Image: Certificate options Certificate store: Image: Certificate store: Image: Certificate store: Image: Certificate store: Not applicable Image: the rest for weasy t is for your users to manage their certificates. Image: term of the certificates. Image: term of the certificates. Producable Image: term of the certificates. Image: term of the certificates. Image: term of the certificates.	1
	Advanced options Back Cancel Preview Save	

Figure 1-4 Adobe CDS Organization Certificate options

- 7 Click Advanced options to view certificate options and define any additional attributes you may need.
- 8 Click Save.

On the confirmation page, you can view the attribute used for the seat ID, a mandatory attribute that authenticates the user for third-party configurations or during enrollment process. This is typically the user's email address.

You can also customize the profile further, such as adding custom scripts, and customizing languages or email notifications on this page.

Prerequisites

- The Adobe CDS end-user certificate must be stored on a Hardware Security Module (HSM).
- Your administrator must configure the HSM to be partitioned. The Luna SA client must be installed and configured on the partitioned HSM.

Generate CSR on HSM

You must generate Certificate Signing Request (CSR) on Hardware Security Module (HSM) before enrolling for certificates. The certificate along with its private key is stored in HSM.

- 1 Open the command prompt.
- 2 Go to the Luna SA client install directory on your system. For example, C:\Program Files <x86>\LunaSA.
- **3** Enter the following commands to generate the CSR on the HSM.

 Generate key pair - Use the certificate management utility of Luna SA Client to generate public and private key pair.

```
cmu generatekeypair -modulusbits=2048 -publicexponent=65537 -sign=T -verify=T -
labelpublic="<public_key_label>" -labelprivate="<private_key_label>"
```

Enter the password for the token slot to generate the key pair.

• Generate CSR - After the key pair is generated, you can generate the CSR.

```
cmu requestcertificate -c="<two_letter_country_code>" -o="<organization_name>" -
cn="<common_name>" -s="<state>" -l="<city/locality>" -publichandle=<public_handle>
-privatehandle=<private handle> -outputfile=""
```

- 4 After you generate the CSR, log in to PKI Manager.
- 5 Click the Certificate Service URL that is displayed on the confirmation of profile creation page.



Figure 1-5 PKI Certificate Service URL

6 Enter the required details and paste the CSR that was generated on the HSM.

Symantec. PKI CERT	IFICATE SERVICE	English 🔻
Enroll: Enrollment informati	ion Next steps	
Verify your informa	ition	
Verify that the information asso	ciated with your certificate is correct, and complete any required fields.	
* Required information		
Common name	RTR	
Organization Unit	ADOBE(r)-CDS	
Company	RTR	
* Country]
* DN Qualifier		1
* Email		
Comments		•
Paste CSR Upload CS	BR	
* Paste CSR below: 😮		
If you have any questions, cont	act your certificate administrator	
apachertr@yopmail.com	-	
By clicking Continue, Laccept t	he terms and conditions.	

Figure 1-6 Paste CSR

7 Click **Continue**. The request is submitted for approval.

PKI Manager approval

- 1 Log on to Managed PKI's PKI Manager using your administrator certificate.
- 2 Click Manage Users or select Managed Users from the Tasks menu on the bottom navigation bar.
- **3** Select the pending approval request for Adobe Certificate.
- 4 Click Manage this request.
- 5 Select Approved and click Save.
- 6 Certificate is issued and sent to the registered email ID.
- 7 Copy the certificate and root in separate files and save them as a .p7b extension.
- 8 After the certificate is saved, import the certificate into the HSM by using the certificate management utility of Luna SA by entering the following command:

```
cmu import -inputFile="<filepath_and_filename_of_cert>" -label="<certificate_label>"
```

- 8 Integrating Adobe CDS Organization Certificates with Adobe® LiveCycle® Enterprise Suite and Adobe® Reader® PKI Manager approval
 - **9** Verify the imported certificate on the Luna SA by entering the following list command:

cmu list

The certificate is installed on the HSM. You must configure Adobe LiveCycle Enterprise Suite to use this as a credential to sign the PDF.



Configuring Partner Products

This chapter discusses how to configure Adobe LiveCycle and Adobe Reader using Managed PKI certificates and sign PDF documents using it.

Setting Up Adobe LiveCycle Enterprise Suite

Adobe LiveCycle can be used to manage the signing process as part of any existing or ongoing workflow in the organization where centralized generation or signing of document content is required and can be easily managed on the server.

Configuring TrustManager on Adobe LiveCycle Enterprise Suite

The following are the steps to configure Adobe LiveCycle Enterprise Suite 4 Server:

1 Log on to the Adobe LiveCycle Administration Console portal using the credentials provided during installation. The Adobe LiveCycle ES4 Home page is displayed.





- 2 Click Settings and select Trust Store Management. The True Store Management page is displayed.
- 3 Click HSM Credentials, then click Add. The Add HSM Credential page is displayed.

10 Configuring Partner Products Setting Up Adobe LiveCycle Enterprise Suite

LC ADOBE* LIVECYCLE* ES4	Welcome administrator
	🟠 Home 🛱 Services 📰 Settings 🔚 Health Monitor 🌗 About 😭 Logout
Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential	
Add HSM Credential	Cancel
Enter an Alias(Credential Identifier) and the location of the PKCS11 Library of the HSM Device. The PKCS11 Library path should be same Profile Name:	ne for all servers in the LiveCycle cluster.
*PKCS11 Library:	
Offline Profile Creation:	
Test HSM Connectivity Next	

Figure 2-2 Add HSM Credential page

- 4 Enter the profile name and provide the path for cryptoki.dll of LUNA SA client in the PKCS11 Library field.
- **5** Click **Test HSM Connectivity** to test if HSM is reachable. An acknowledgment message is displayed as confirmation.

The Test HSM Connectivity button is disabled if you select the Offline Profile Creation check box.

6 Click **Next**. Select the token name, slot ID, and slot list index and enter the token pin for the slot and click **Next**.

Settings * Tout Store Mensament * HSM Credentials* Add HSM Credential HSM Credential Ject the Token Name or Stot List Index or Stot Id for the desired stot to use and provide the stor's password.	Home 🛱 Services	E Settings	Ess Health Monitor	(1) About 👫 Logo
Sattings > Toust Store Management > HSM Credentials > Add HSM Credential HSM Credential alect the Token Name or Slot List Index or Slot Id for the desired slot to use and provide the slot's password.				Cancel
HSM Credential alect the Token Name or Slot List Index or Slot Id for the desired slot to use and provide the slot's password.				Cancel
elect the Token Name or Slot List Index or Slot Id for the desired slot to use and provide the slot's password.				
en Name:				
um 🔹				
i let:				
¥				
List Index:				
v				
i Pin:				

Figure 2-3 Add HSM Credential token details

The HSM connection is established and the available certificates/keys installed on HSM slot are displayed.

7 Select the credential that you want to use while signing the document.

LC ADOBE' LIVECYCLE' ES4	Welcome administrator
	🏠 Home 🔚 Services 🔚 Settings 🔚 Health Monitor 🕕 About 🕀 Logout
Home > Settings > Trust Store Management > HSM Credentials> Add HSM Credential	
Add HSM Credential	Cancel
Q Select Credential by selecting the Subject Name in the List.	
*Credentials: C-US, EMAILADDRESS-testl @yapmail.com, 0U-TESTorg. 0 ▼	
Back Save	

Figure 2-4 Add HSM Credential selection

8 Click Save. The HSM Credential page is displayed.

	.54		🟠 Home 🛱 Se	rvices \Xi Settings 🕞 Health Monitor 🕕 About 🔇	🗟 Logou
Home > Settings > Trust Store Ma	anagement > HSM Credentials				7 Helr
HSM Credentials				Reset All HSM Conne	ections
Į Manage HSM Credential	Is				
📺 Delete 📔 🗋 Add 🛛	Check Status				
Name 🔺	Туре	Slot Info	Slot Type	Status	
ADOBECERT	Other	0	SlotIndex		
ADOBECERT1	Other	0	Slot Index		

Figure 2-5 Manage HSM Credential

Configuring Adobe LiveCycle Workbench for Signing Process

You must establish a connection with a server (JBoss, WebSphere, WebLogic) while you work on Adobe LiveCycle Workbench. Your administrator must configure your user account and the server so that you can use LiveCycle Workbench. For more information on LiveCycle Workbench, refer to *Adobe documentation*.

Process represents the business processes that you are automating using LiveCycle. Processes are services that run on the LiveCycle server. The following are the steps to create a process:

- 1 Log on to Adobe LiveCycle Workbench ES4.
- 2 Click **File** \rightarrow **New** \rightarrow **Process** to create an empty process.

Manage Record and Playback Image Record and Playback Open File Process Upgrade ES Artifacts Image Record and Playback Archive Migration Tool Image Record and Playback Get Application Image Record and Playback Image Record and Playback Image Record and Playback Save Ctrl+S Save Ctrl+Shift+S Save All Ctrl+Shift+S Print Ctrl+P Image Record and Playback Image Record and Playback	Manage Record and Playback Image Record and Playback Open File Process Upgrade ES Artifacts Image Record and Playback Archive Migration Tool Image Record and Playback Get Application Image Record and Playback Save As Image Record and Playback Save All Ctrl+Shift+S Print Ctrl+Shift+S Logout Image Record and Playback Exit Image Record and Playback		New	×		Application	
Open File Process Upgrade ES Artifacts Form Archive Migration Tool Guide Get Application Guide Import Data Model Save Ctrl+S Save As Ctrl+Shift+S Print Ctrl+P Vulde WSDL Service Reference Vulde WSDL Service Reference Uogout Other	Open File Image: Process Upgrade ES Artifacts Form Archive Migration Tool Guide Get Application Guide Import Data Model Save Ctrl+S Save As Ctrl+Shift+S Print Ctrl+Shift+S Print Ctrl+N Exit Other	D	Manage Record and Playback		fix.	Application Version	
Upgrade ES Artifacts Archive Migration Tool Get Application Import Save Save Save As Save All Print Ctrl+Shift+S Print Ctrl+P Uogout Ctrl+N	Upgrade ES Artifacts Archive Migration Tool Get Application Import Save Save Ctrl+S Save As Save All Ctrl+Shift+S Print Logout Exit		Onen File		280	Process	
Archive Migration Tool Import Get Application Import Save Ctrl+Shift+S Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+P	Archive Migration Tool Import Get Application Import Save Ctrl+S Save As Event Type Save As User List Save All Ctrl+P Print Ctrl+P Logout Import Exit Other		Upgrade ES Artifacts			Form	
Get Application Import Import Kassembly Descriptor Save Ctrl+S Save As Ctrl+Shift+S Print Ctrl+P Import Ctrl+P	Get Application Import Import Save Save Ctrl+S Save As Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N Exit Other		Archive Migration Tool			Guide	
Import Assembly Descriptor Save Ctrl+S Save As Event Type Save As User List Print Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N	Import Assembly Descriptor Save Ctrl+S Save As Ctrl+Shift+S Print Ctrl+Shift+S Logout Ctrl+N Exit Other	.	Get Application		Ť	Data Model	
Save Ctrl+S Save As Ctrl+Shift+S Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N	Save Ctrl+S Save As Ctrl+Shift+S Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N Exit Ctrl+N		Import			Assembly Descriptor	
Save As Image: Component Reference Save All Ctrl+Shift+S Print Ctrl+P Image: Component Reference WSDL Service Reference Image: Ctrl+P Image: Ctrl+P	Save As Save As Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N Exit Ctrl+N		Save	Ctrl+S	0	Event Type	
Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+P Logout Ctrl+N	Save All Ctrl+Shift+S Print Ctrl+P Logout Ctrl+N Exit Other		Save As			Component Reference	
Print Ctrl+P WSDL Service Reference Logout Ctrl+N	Print Ctrl+P WSDL Service Reference Logout Ctrl+N Exit	C	Save All Ctrl+S	hift+S		XML Schema	
Logout Ctrl+N	Logout Ctrl+N Exit	8	Print	Ctrl + P		WSDL Service Reference	
	Exit	X	Logout			Other	Ctrl+N
Exit			Exit		1		

Figure 2-6 New Process

3 Enter a name and description for the process. Enter or select the path to the process location within the application hierarchy and click **Finish**.

🗠 Adobe LiveCycle Workbench ES4		LC New Process	
File Edit Window Help 😨 📰 🛃 💕 🔝 🕋 🗶 🛷 🕶 😭 📴 Process Design		New Process Enter a name, description and location for the process.	
Applications 23 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다		Name: DigitalSigning Description: (optional) Digital Signing for Adobe PDF documents	
		Location Enter or select the parent folder:	
		/MyApplication/10/Test MyApplication MyApplication Test MyApplication2	
-	${\mathcal X}$ Variables Name	(Back Next > Einish Cancel)	- irpose
		🚚 jboss[administi	rator]

Figure 2-7 New process

- 4 Select Activity Picker from the activity toolbar by dragging and dropping in Default start point.
- 5 Select Digital Signatures and select Sign Signature Field and click OK.
- 6 Enter the path for the pdf document in the Input PDF field.
- 7 Select the credential for signing that was created in "Configuring TrustManager on Adobe LiveCycle Enterprise Suite" on page 9. After the input document is provided, the signature fields are populated.
- 8 Select the signature field for signing.
- 9 Complete the required process and click **Save** icon.

C Adobe LiveCurle Workbench FS4			_		- 8 -
Eile Edit Window Help					
% 🔲 🖌 🗎 🛍 ≍ 🔗 ▾					
Pa Process Design					
🔚 Applications 🔝 Process Properties 🛛 👘 🗖	1	*DigitalSigning 🖾			- 0
sign Operation			Ð.		-
() A com.adobe.livecycle.signatures.client.types.C					
Name activity0					
Description		point activity			
Category Digital Signatures		u u u u u u u u u u u u u u u u u u u			=
Service Name SignatureService					
Service Operation Sign Signature Field					۲
Route Evaluation					
▼ Common 😣					
*Input PDF literal value 👻 😑	Ī				
URI = Test/pdf_signing_v1.pdf, C 🥥	Ē	NINS .			
*Signing Credential literal value 👻					Ĩ
Use SPI 📃					
Alias MYPROFILE -					
SPI Name	•	III.			•
Certificate	x	Variables 🕱 🔀 Validation Report		+ 🥖 =	
SPI Properties	N	ame Data Type Purpose	Input	Output	Requir
*Signature Field Name literal value 👻					
· · ·					

Figure 2-8 Process Design

10 After the process is complete, go to the **Applications** view and select **Deploy** to deploy the application on the server for further usage.

Adobe LiveCycle Workbencl	h ES4										
Edit Window Help											
🗑 🔄 🛃 💼 💼 🗶	1 -										
Process Design											
Applications 🐹 🗉 Proce	ess Propertie	es 📃 🗖 📴 Digita	Signing 😪								- 1
A A	at at 1										
🔲 🖓 🖓 🌍 [
MyApplication	a										
▲ (⇒ Test	New		+								
📆 DigitalSigr	🚈 Impor	t	1			-					
RewProce	式 Denlo	v	star	rt							
pdf_signir	🖬 Under	, alov	it		(
MvApplication2	Create	LiveCycle Archive				activity0					
▲ 😥 MyApplication2/:	cie oreate	- encoyere national									
RewProcess1	Paste		Ctrl+V								
Pdf_signing_v	💢 Delete		Delete								۲
76 Pdf_signing_v	🖨 Check	Out									1
1	🍃 Check	In									
	Sunch	ropiza									
	A Revert										
	-										4
	E Prope	rties									ľ
		4									•
		X Variat	oles 23 🐼 Valio	dation Re	nort					4 🧷 .	
		pe vana	and of an	acconne	-poit		La constante				
		Name					Data Type	Purpose	Input	Output	Requir
									1		1 1
							🚽 j	boss[administrator]			

Figure 2-9Application Deploy

11 Select the files that need to be checked-in and click **OK**. The selected files are deployed.

elect assets to be checked in.		
) Check in all files		
) Check in selected files		
Reason	File	
This folder should be checked in	/iboss/MyApplication/1.0/Test	
This file should be checked in	/jboss/MyApplication/1.0/Test/DigitalSigning.process	
This file should be checked in	/jboss/MyApplication/1.0/Test/NewProcess1.process	
This file should be checked in	/jboss/MyApplication/1.0/Test/Pdf_signing_v3.pdf	
This file should be checked in	/jboss/MyApplication/1.0/Test/pdf_signing_v1.pdf	
escription		

Figure 2-10 Check in files

Setting Up Adobe Reader

Adobe Reader allows you to sign a PDF document based on digital certificates to attest the authenticity and integrity of data exchanged.

Configuring HSM module on the Adobe Reader

Complete the following steps to set up a digital certificate on Adobe Reader XI.

- 1 Open Adobe Reader XI.
- 2 Choose Edit \rightarrow Preferences.
- 3 Click **Signatures** from the Preferences dialog box.
- 4 Click More on the Identities & Trusted Certificates under Digital Signature.

	Digital Signatures	
Commenting Documents	Creation & Appearance	
Full Screen General Page Display	 Control options for signature creation Set the appearance of signatures within a document 	More
3D & Multimedia	Verification	
Accessibility Adobe Online Services Email Accounts	Control how and when signatures are verified	More
Forms	Identities & Trusted Certificates	
Identity Internet JavaScript Language	Create and manage identities for signing Manage credentials used to trust documents	More
Measuring (2D) Measuring (3D)	Document Timestamping	
Measuring (Geo) Multimedia (legacy)	Configure timestamp server settings	More
Reading		
Reviewing		
Search		
Security Security (Enhanced)		
Security (Ennanced)		
Spelling		
Tracker		
Trust Manager		
Units		
Updater		

Figure 2-11 Preferences dialog box for Adobe Reader XI

- 5 Click PKCS#11 Modules and Tokens under Digital IDs.
- 6 Click Attach Module to attach a PKCS#11 module (HSM).
- 7 Browse and select the cryptoki.dll of the LUNA SA client. The attached modules are opened.
- 8 View the list of credentials imported for the module or import from Reader to the module. You can click the partition name to view the details.
- 9 Select one of the listed IDs for signing or click Add ID to choose the certificate from your credential.
- 10 Click Usage Options and select the certificate that you received from Managed PKI and click Use for Signing.
- 11 Click OK.

Digitally Signing Documents using Adobe Reader

To digitally sign a PDF document using Adobe Reader XI, follow these steps:

- 1 Open the PDF document you want to sign.
- 2 Choose **View** \rightarrow **Sign**.
- 3 Select I Need to Sign on the Sign panel.



Figure 2-12 Digital Signing

- 4 Click Add Text if you require to add information such as company name, title, date, to name a few.
- 5 Click **Place Signature**, then click **Drag New Signature Rectangle** to place the signature anywhere in the PDF. Alternatively, you can click on **Sign Here** text box to place the signature.
- 6 Select the appropriate signature from the **Sign As** field. If you have not configured a default digital signature, Adobe Reader will use the most recently configured digital signature.



Figure 2-13 Sign Document

You can click **Info** to view the details of a certificate and its entire issuance chain.

7 Click **Sign**. The Adobe Reader will save the document with a different name.