



Configuring LiveCycle Rights Management ES for Certificate-based Authentication

This document provides a walk-through to configure LiveCycle Rights Management ES to enable Smartcard/Certificate-based authentication from client Acrobat/Reader. The walk-through includes sample files to assist you in understanding the steps required.

This document also contains the detailed step-by-step procedures required to create and sign your own certificates using OpenSSL.

APPLIES TO

LiveCycle Rights Management ES

Getting Started with the sample

The section provides detailed steps to walk you through the configuration steps necessary to use certificate-based authentication with LiveCycle Rights Management ES. See the detailed procedures to create and sign your own certificates using OpenSSL, see [“Creating and Signing documents using your own certificates and OpenSSL” on page 4](#).

The sample files are attached to this document. Select the the attachment and click the Save button in Acrobat to save the attachment.

CONTENTS

Configuring LiveCycle Rights Management ES for Certificate-based Authentication.....	1
Getting Started with the sample	1
Creating and Signing documents using your own certificates and OpenSSL	4

WORLDCORPCAROOT.cer

- A sample Issuer Certificate (also known as a CA or Root Certificate).

PaulSmith.p12

- A sample End-user Certificate signed by the CA above.

Note: The instructions in this document assume the use of the sample root and end-user certificates attached.

Overview of steps:

- Importing the sample Issuer Certificate into Trust Store Management. See [page 2](#).
- Adding the corresponding Certificate Mapping under User Management. See [page 2](#).
- Creating the corresponding principal, Paul Smith, in User Management. See [page 3](#).
- Installing the sample Issuer and End-user certificates on client machine. See [page 3](#).
- Ensuring that the certificate authentication is present under AuthSchemes and AuthProviders in User Management configuration. See [page 3](#).
- Verifying configuration. See [page 3](#).

► Importing the sample Issuer Certificate into Trust Store Management:

1. Log in to LiveCycle ES Administrator user interface as administrator.
2. Navigate to **Settings>Trust Store Management>Certificates** and click **Import**.
3. Select all check boxes, enter `WORLDCORPCAROOT` for Alias field, and browse and choose the file `WORLDCORPCAROOT.cer` for Certificate field.
4. Click OK.

► Adding the corresponding Certificate Mapping under User Management:

1. Log in to LiveCycle ES Administrator user interface as administrator.
2. Navigate to **Settings>User Management>Configuration>Certificate Mapping**, and click **New Certificate Mapping**.
3. Make the following selections:

Form Field	Value
For Issuer	WORLDCORPCAROOT
map Certificate's	E (e-mail)
To User's	Primary e-mail
for Domain	DefaultDom

4. Click OK.

► Creating the corresponding principal, Paul Smith, in User Management:

1. Create a user, Paul Smith, using **User Management > Users and Groups administrator** user interface.
2. Ensure that Paul Smith's e-mail ID is `paulsmith@worldcorp.com`, and that the e-mail ID belongs to `DefaultDom` domain.
3. Assign Paul Smith a minimum role of LiveCycle Rights Management End User.

► **Installing the sample Issuer and End-user certificates on client machine:**

1. Install the sample Issuer Certificate, WORLDCORPCAROOT.cer, and sample Paul Smith's certificate, PaulSmith.p12, on the client machine. To log in, double-click the corresponding files on the client machine and choose defaults on all the dialogs.

Alternatively, in Internet Explorer, you can navigate to **Tools->Internet Options->Content (tab)->Certificates**, and import the certificates.

► **Verifying the certificate authentication in User Management:**

LiveCycle ES enables Certificate Authentication as one of the Authentication Schemes by default. Use these steps to verify your configuration.

1. Navigate to **User Management > Configuration > Import and export configuration files** to export the User Management configuration file, config.xml.
2. Open config.xml file and verify the following:

Under "AuthSchemes" node:

```
<node name="CertificateAuth">
  <map>
    <entry key="order" value="3" />
    <entry key="name" value="edc.server.auth.scheme.certificate" />
  </map>
</node>
```

If this code does not exist, copy it into the config.xml file.

Note: If you want to enforce only Certificate Authentication on the client; remove the UsernamePwd and Kerberos nodes from the config.xml file and import it back to User Management.

Under the "AuthProviders" node:

```
<node name="AdobeDefaultCertificate">
  <map>
    <entry key="configured" value="true"/>
    <entry key="visibleInUI" value="false"/>
    <entry key="enabled" value="true"/>
    <entry key="allowMultipleConfigs" value="false"/>
    <entry key="className"
value="com.adobe.idp.um.provider.authentication.CertificateAuthProviderIm
pl"/>
    <entry key="order" value="5"/>
  </map>
</node>
```

If this code does not exist, copy it into the config.xml file.

► **Verifying the configuration:**

1. Log into LiveCycle Rights Management ES server from Adobe Acrobat or Adobe Reader.
2. Verify that the "Choose Authentication type" dialog displays the Smartcard/Certificated-based authentication option. Ensure Paul Smith's certificate displays in the list of available certificates.

Creating and Signing documents using your own certificates and OpenSSL

This section provides detailed step-by-step procedures to help you create and sign your own certificates using OpenSSL.

OpenSSL is used in creating, signing, and exporting of certificates. These instructions use Microsoft Windows XP.

Overview of steps:

- Installing and preparing OpenSSL. See [page 4](#).
- Creating the root certificate. See [page 4](#).
- Creating an Issuer Certificate (also known as CA or Certifying Authority or Root Certificate). See [page 5](#).
- Importing this Issuer Certificate into Trust Store Management. See [page 5](#).
- Creating an End-user Certificate and signing it using the Issuer Certificate. See [page 5](#).
- Adding the corresponding Certificate Mapping in User Management. See [page 5](#).
- Creating the corresponding principal, Paul Smith, in User Management. See [page 6](#).
- Ensuring that the certificate authentication is present under AuthSchemes and AuthProviders in User Management configuration. See [page 6](#).
- Installing the sample Issuer and End-user certificates on client machine. See [page 6](#).
- Verifying configuration. See [page 6](#).

► Installing and preparing OpenSSL:

1. Install OpenSSL, accepting the defaults. These instructions assume OpenSSL is installed in c:\OpenSSL.
2. Create a working directory. In this step we use C:\certificates as our working directory.
3. Set up the directory structure required by OpenSSL:

```
C:\certificates>md demoCA
C:\certificates>md demoCA\newcerts
```
4. Set up the files required by OpenSSL:
 - Create a file called index.txt, an empty (zero-byte) text file under the folder C:\certificates\demoCA\.
 - Create the serial number file named "serial" under the folder C:\certificates\demoCA\. Create this plain ASCII file containing the string "01" on the first line, followed by a newline.

► Creating Root Certificate (CA):

1. Create private key, CA.key, for our CA:

```
C:\certificates>openssl.exe genrsa -des3 -out CA.key 1024
```

Enter pass phrase when prompted.

2. Create Root Certificate, the following is an example key:

```
C:\certificates>openssl.exe req -new -x509 -days 1001 -key CA.key -out  
WORLDCORPCAROOT.cer -subj "/C=US/ST=California/L=San Jose/O=World  
Corp./OU=Marketing/CN=World Corp. Cert Auth"
```

Enter pass phrase when prompted.

► **Importing this Issuer Certificate into Trust Store Management:**

1. Log in to LiveCycle ES Administrator user interface as administrator.
2. Navigate to **Settings > Trust Store Management > Certificates** and click **Import**.
3. Select all check boxes, enter certificate name (this example uses "WORLDCORPCAROOT") for Alias field, and browse and choose the file certificate file (this example uses, WORLDCORPCAROOT.cer) for Certificate field.
4. Click OK.

► **Creating an End-user certificate and sign it using the Issuer Certificate:**

1. Create private key. The following code uses Paul Smith (Paul.key) as the end user:

```
C:\certificates>openssl.exe genrsa -des3 -out Paul.key 1024
```

Enter pass phrase when prompted.

2. Create a Certificate Signing Request (CSR). The following code assumes that the signing request is "Paul.csr":

```
C:\certificates>openssl.exe req -new -key Paul.key -out Paul.csr -subj  
"/C=US/ST=California/L=San Jose/O=World Corp./OU=Marketing/CN=Paul  
Smith/emailAddress=paulsmith@worldcorp.com"
```

Enter pass phrase when prompted.

3. Sign the certificate request to obtain the certificate. The following code uses the certificate "PaulSmith.cer":

```
C:\certificates>openssl.exe ca -policy policy_anything -cert  
WORLDCORPCAROOT.cer -in Paul.csr -keyfile CA.key -days 360 -out  
PaulSmith.cer -key "123456"
```

Enter 'y' when prompted.

4. Export the certificate as PKCS12 format:

```
C:\certificates>openssl.exe pkcs12 -export -out PaulSmith.p12 -inkey  
Paul.key -in PaulSmith.cer
```

Enter pass phrase when prompted for the key.

Enter or the Export password when prompted

► **Adding corresponding Certificate Mapping under User Management:**

1. Log in to LiveCycle ES Administrator user interface as administrator.
2. Navigate to **Settings > User Management > Configuration > Certificate Mapping**, and click **New Certificate Mapping**.

3. Enter the following details:

Form Field	Value
For Issuer	<i>your value</i>
map Certificate's	E (e-mail)
to User's	Primary e-mail
for Domain	DefaultDom

4. Click OK.

► **Creating the corresponding principal in User Management:**

1. Create a user (this example uses "Paul Smith", using **User Management->Users and Groups** Administrator user interface.
2. Ensure that the correct email id is set and that it belongs to DefaultDom domain.
3. Assign this e-mail ID a minimum role of LiveCycle Rights Management End User.

► **Verifying the certificate authentication in User Management:**

LiveCycle ES enables Certificate Authentication as one of the Authentication Schemes by default. Use these steps to verify your configuration.

1. Navigate to **User Management > Configuration > Import and export configuration files** to export the User Management configuration file, config.xml.
2. Open config.xml file and verify the following:

Under "AuthSchemes" node:

```
<node name="CertificateAuth">
  <map>
    <entry key="order" value="3" />
    <entry key="name" value="edc.server.auth.scheme.certificate" />
  </map>
</node>
```

If this code does not exist, copy the above text into the config.xml file.

Note: If you want to enforce only Certificate Authentication on the client; remove the UsernamePwd and Kerberos nodes from the config.xml file and import it back to User Management.

Under the "AuthProviders" node:

```
<node name="AdobeDefaultCertificate">
  <map>
    <entry key="configured" value="true"/>
    <entry key="visibleInUI" value="false"/>
    <entry key="enabled" value="true"/>
    <entry key="allowMultipleConfigs" value="false"/>
  </map>
</node>
```

```
<entry key="className"
value="com.adobe.idp.um.provider.authentication.CertificateAuthProviderIm
pl"/>
  <entry key="order" value="5"/>
</map>
</node>
```

If this code does not exist, copy the above text into the config.xml file.

► **Verifying the configuration:**

1. Log into LiveCycle Rights Management ES server from Adobe Acrobat or Adobe Reader.
2. Verify that the "Choose Authentication type" dialog displays the Smartcard/Certificated-based authentication option. Ensure the certificate for the user created displays in the list of available certificates.



Adobe

Adobe Systems Incorporated

345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, Reader, Flash, Flex, and Adobe LiveCycle are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and other countries. Java is a registered trademark of Sun Microsystems, Inc. Documentum is a registered trademark of EMC Corporation. FileNet is a registered trademark of FileNet Corporation, an IBM company. Microsoft and Active Directory are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

© 2009 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

January 2009