SafeNet Luna SA Application Integration with Adobe– Adobe LiveCycle Document Security 7.0

Requirements

This section describes how to set up Adobe LiveCycle Document Security 7.0 for protection of credentials, used for certifying, signing and verifying PDF documents with the Luna SA appliance. These instructions specify version 7.0 because of 7.0's support for a PKCS *API*.

RedHat Enterprise Linux 3.0 and Microsoft Windows 2003 clients are supported. Therefore, when installing Luna SA for use with Adobe, choose the software in the "/enterprise" or “\windows” directories on the Luna SA Client Software CD.

For release 3.1 of Luna SA, the Adobe integration requires Adobe LiveCycle Document Security 7.0 Release, or later.

These integration notes assume:

- That you are familiar with Adobe LiveCycle Document Security (refer to Adobe-supplied documentation and training)
- That you have installed the Luna SA hardware and software, and performed Luna SA setup procedures (described in the QuickStart Guide or in the Configuration section of this Help).

Briefly, you should have:

- Given the Luna SA appliance a secure admin password
- Given the Luna SA a hostname, suitable for your network
- Set the Luna SA network parameters to work with your network
- Initialized the HSM on the Luna SA appliance
- Created a partition on the HSM
- Created and exchanged certificates between the Luna SA and your "Client" system (registered the Client with the Partition)
- Enabled Partition "Activation" and "AutoActivation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only)
- Configured HA (High Availability) if using multiple HSMs

Preparing Luna SA and Adobe to Work Together

Adobe® LiveCycle Document Security 7.0 utilizes the security features of the SafeNet Luna SA to protect credentials for digitally certifying, signing, and verifying PDF files.

The required Luna SA drivers are provided on the installation CD 'Luna SA Client Software Release 3.1', provided with the Luna SA appliance.

To install credentials on the Luna SA use SafeNet's CMU (Certificate Management Utility), CMU is installed with the Luna SA client software.

Install LunaSA Client Software

Install the Luna SA client software on the machine running LiveCycle Document Security.

Install/Create Credentials on HSM

Install or create credentials on the Luna SA using CMU.

1. Create a certificate request using LunaSA’s CMU:

   cmu gen –slot=1 –modulusBits=2048 –publicExp=65537 –sign=1 –verify=1 –labelPublic=”Public Verify Key” –labelPrivate=”Private Verify Key” –id=101000

2. Determine the key handles for the public and private keys:

   cmu list –slot=1

3. Generate a PKCS #10 request based on the public and private keys:

   cmu requestCert –slot=1

   Fill out the parameters, including the public and private key handles.

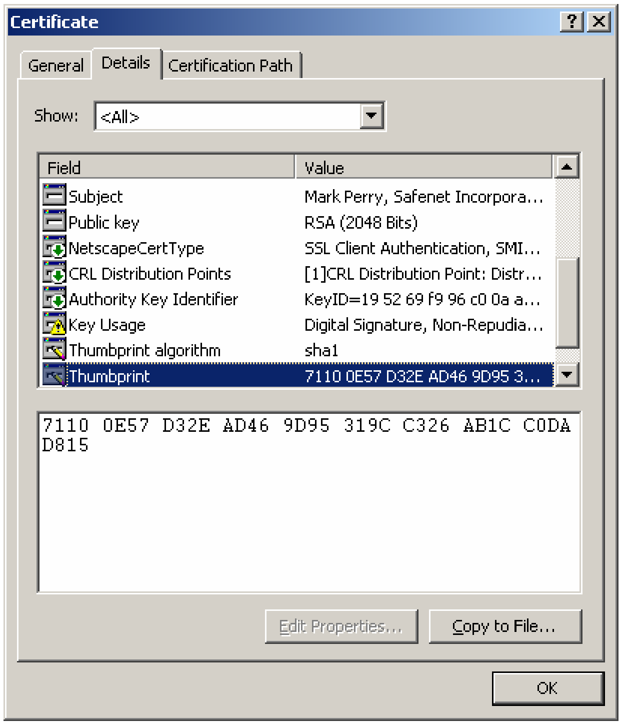
4. Submit the Certificate Signing Request:

   - Open the .req that is created in /usr/lunasa/bin or C:\Program Files\LunaSA and copy the contents
   - Open the “Your CDS Provider Certificate Enrollment” email and click the link from within the email.
   - Specify your email address, PIN/Password and paste the contents of the .req into the “Please paste the certificate signing request CSR for your device below:” field.
   - Agree to the conditions and click submit

5. Retrieve the Certificate Signing Request:

    - Open the response email "Certificate installation email provided by your CDS provider" and copy the certificate information between and including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

- Create a new .txt file and call it "CSR.cer.txt"
- Open the file and paste the certificate information copied from the email
- Save, close and rename file to "CSR.cer."
- Open the file and look at the "thumbprint". This is used as the "sha1" setting for your Trust Manager Module's "trust.xml" file.



Show: <All>

Field	Value
Subject	Mark Perry, Safenet Incorpora...
Public key	RSA (2048 Bits)
NetscapeCertType	SSL Client Authentication, SMI...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Key Identifier	KeyID=19 52 69 f9 96 c0 0a a...
Key Usage	Digital Signature, Non-Repudia...
Thumbprint algorithm	sha1
Thumbprint	7110 0E57 D32E AD46 9D95 3...

```
7110 0E57 D32E AD46 9D95 319C C326 AB1C C0DA
D815
```

6. Convert Certificate to DER format:

    - Double-click on the "CSR.cer"
    - Select "Details" tab and click "Copy to file..."
    - For "Welcome to the Certificate Export Wizard" click "Next"
    - For "Export File Format" select "DER encoded binary X.509(.CER" and click "Next"
    - For "File to Export" click "Browse" and specify a location and filename and click "Save" then "Next"
    - Click "Finish"

7. Import the CSR into the LunaSA appliance:

- Copy the “CSR.cer” to /usr/lunasa/bin or C:\Program Files\LunaSA\
- Import the certificate into the HSM

```
cmu import –slot=1 –inputFile=CSR.cer –label=”ServerCert”
```

```
cmu list –slot=1
```
(To get Certificate Handle on HSM)

- Add an ID to the new Certificate:

```
cmu setAttribute –handle=x –id=101000
```

Where x is the handle of the certificate on the HSM

Configure Trust Manager Module

Configure the LiveCycle Document Security Trust Manager Module by following the instructions in the document “Installation and Configuration Guide” provided with LiveCycle Document Security:

1. To sign, certify or decrypt documents add an <hsmrecord/> entry for each credential to trust.xml.
2. The 'slot' attribute value represents the partition on which the credentials are stored. If your client only has 1 partition assigned to it use slot="1". If you have more than one partition assigned to your client determine the slot number assigned to each partition using the ckdemo utility(option 12 - Token Info), provided with the Luna SA client software.
3. To validate documents signed or certified with the Luna SA add a <cerrecord/> entry for each trusted certificate and a <crl/> entry for each corresponding CRL file to trust.xml. Add the certificates and CRL files to the Trust Manger Module configuration.

   Example entry in trust.xml for a credential installed on the Luna SA:

   Windows:
   ```
   <credentials>
   <hsmrecord alias="HSMIdentity1Cert" slot="1" dllpath="C:\Program
   Files\LunaSA\cryptoki.dll"
   sha1="71100e57d32ead469d95319cc326ab1cc0dad815"/>
   </credentials>
   ```

   Unix:
   ```
   <credentials>
   <hsmrecord alias="HSMIdentity1Cert" slot="1"
   dllpath="/usr/lunasa/lib/libCryptoki2.so"
   sha1="71100e57d32ead469d95319cc326ab1cc0dad815"/>>
   </credentials>
   ```

4. Additional steps for certificates tied to a root authority:

- Obtain the ICA (Intermediate Certification Authority) certificate in DER encoded x.509 format (.cer).
- While configuring the Adobe® LiveCycle Document Security Trust Manager Module, place the ICA certificate in the 'certificates' directory.
- Add an entry to trust.xml for the ICA certificate. There is no need to trust the certificate for specific operations. These steps will ensure that resulting signatures are properly chained to the root authority certificate.

  Example entry in trust.xml for an ICA certificate:

  ```
  <cerrecord cerFile="TestCDS_ICA.cer" TrustedFor=""/>
  ```

For the root authority “Adobe Root CA”, no entry is required for the “trust.xml” because it is built and trusted in the Adobe products such as Adobe Acrobat and Adobe Reader.

SafeNet Overview

SafeNet (NASDAQ: SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.

SafeNet®
The Foundation of Information Security

www.safenet-inc.com

Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** email: ***info@safenet-inc.com***

Phone USA and Canada (800) 533-3958
Phone Other Countries (410) 931-7500
Fax (410) 931-7524
E-mail *info@safenet-inc.com*
Web site *www.safenet-inc.com*

SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The opinions expressed herein are subject to change without notice.

Australia +61 3 9882 8322
Brazil +55 11 4208 7700
Canada +1 613.723.5077
China +86 10 885 19191
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538
Japan +81 45 640 5733
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts)
+1 978.539.4800
U.S. (Minnesota)
+1 952.890.6850
U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)
+1 949.450.7300
U.S. (San Jose, California)
+1 408.452.7651
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers located worldwide.