Luna SA and IBM HTTP Server/IBM WebSphere Application Server

Integration Guide
Preface

© 2012 SafeNet, Inc. All rights reserved.

Part Number: 007-012077-001 (Rev B, 06/2012)

All intellectual property is protected by copyright. IBM HTTP Server is trademark or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

SafeNet, Inc.

4690 Millennium Drive
Belcamp, Maryland  21017
USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, please contact your supplier or SafeNet support.

SafeNet support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Technical Support Contact Information:
Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com

© SafeNet Inc.
# Table of Contents

**Preface** ............................................................................................................................................................. i

**Chapter 1 Introduction** ........................................................................................................................................ 5  
| Luna SA Setup ................................................................. | 6 |
| IBM HTTP 7.0 & IBM Web Sphere Application Server 7.0 Setup ................................................................. | 6 |

**Chapter 2 Integration with Luna SA** ........................................................................................................ 7  
| Solaris 10 SPARC (64-bit) .......................................................................................................................... | 7 |
Chapter 1
Introduction

This document covers the necessary information to install, configure and integrate IBM® HTTP Server & IBM WebSphere Application Server with SafeNet Luna SA Hardware Security Module (HSM).

IBM WebSphere Application Server is a software platform for deploying Enterprise Java™ Based Applications utilizing IBM HTTP Server. We provide Key Management security for Certificates and certificate-based authentication, including import of trusted CA certificates from software based keystores to hardware based keystores, generation of self signed certificates and personal certificate requests via the IBM Key Management Utility. In addition, the IBM HTTP Server can be configured to use our HSM for SSL connectivity. IBM WebSphere Application Server utilizes the following APIs: PKCS #11, JCA/JCE and their own JSSE implementation that makes calls to the PKCS #11 library.

The Luna SA solutions for IBM WebSphere Application Server provides secure key management and accelerated signing for private keys associated with the IBM WebSphere Application Server as well as secure SSL Acceleration. SSL acceleration is accomplished by IBM WebSphere Application Server through JSSE (Java Secure Sockets Extension) Provider.

Scope

3rd Party Application Details

- IBM HTTP Server V7.0.(32-bit) for Solaris 10 SPARC 64-bit
- IBM WebSphere Application Server V7.0 (32-bit) for Solaris 10 SPARC 64-bit

Supported Platforms

The following platforms are supported for Luna SA v4.4.1 & v4.5-12:

- Solaris 10 SPARC (64-bit)

HSMs and Firmware Version

- K5 HSM f/w 4.8.1

Library and Driver Support

- PKCS#11 v2.01 dynamic library

Distributions

- Luna SA Client s/w v4.4.1 (32-bit)
- Luna SA Client s/w v4.5 (32-bit)
Prerequisites

Luna SA Setup

Please refer to the Luna SA documentation for installation steps and details regarding to configure and setup the box on Solaris systems. Before you get started ensure the following:

- Luna SA appliance a secure admin password
- Luna SA a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your "Client" system.
- Created a partition on the HSM, remember the partition password that will be later used by IBM HTTP Server. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is "/usr/lunasa/bin/vtl verify" for Solaris.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

IBM HTTP 7.0 & IBM Web Sphere Application Server 7.0 Setup

IBM HTTP Server V7.0 & IBM Web Sphere Application Server 7.0 must be installed on the target machine to carry on with the integration process. For a detailed installation procedure, please refer to the HTTP Server and Web Sphere Application Server documentation.

You need to install the following patches-

On IBM HTTP Server version 7.0:

- IHS70 FP21 (32bit) (7.0.0-WS-IHS-SolarisSparc-FP0000021.pak) patch using UpdateInstaller on Solaris 10 SPARC (64-bit).

On IBM Web Sphere Application Server 7.0

- IBM Web Sphere Application Server70 FP21 (32 bit) (7.0.0-WS-WAS-SolarisSparc-FP0000021.pak) patch using UpdateInstaller on Solaris 10 SPARC (64-bit).
Chapter 2
Integration with Luna SA

Solaris 10 SPARC (64-bit)

Integrating IBM HTTP Server V7.0 with Luna SA

To configure IBM Key Management Utility to recognize the Luna SA cryptographic device:

1. Ensure that the file `libCryptoki2.so` is in the directory:
   `/usr/lunasa/lib`

2. Traverse to the directory:
   `/opt/IBM/HTTPServer/gsk7/classes`

3. Rename `ikmuser.sample` to `ikmuser.properties`.

4. Uncomment and edit the following setting to use the cryptographic lib:
   `DEFAULT_CRYPTOGRAPHIC_MODULE=/usr/lunasa/lib/libCryptoki2.so`

5. Verify the following in the `Chrystoki.conf` under `/etc`.

   **Cryptoki with Logging**
   
   ```
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libcklog2.so;
   }
   
   Cklog2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   NewFormat=1;
   Enabled=1;
   Error=/tmp/ErrorLunaSA2.txt;
   File=/tmp/LogLunaSA2.txt;
   }
   
   OR
   
   **Cryptoki without Logging**
   
   Chrystoki2 = {
   LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
   }
   ```

6. Set the `JAVA_HOME` environment variable:
   `/opt/IBM/HTTPServer/java`

7. Stop and start the HTTP Server.
   `/opt/IBM/HTTPServer/bin/apachectl stop`
   `/opt/IBM/HTTPServer/bin/apachectl start`

8. Modify the `java.security` file located in directory:
/opt/IBM/HTTPServer/java/jre/lib/security

to include the following:

security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
security.provider.2=sun.security.provider.Sun
#security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.jsse.IBMJSSEProvider
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
#security.provider.10=com.ibm.crypto.pkcs11.provider.IBMPKCS11

Create configuration file luna.cfg. The required entries in *luna.cfg* are:

```
name = LUNA
library = /usr/lunasa/lib/ libCryptoki2.so
description = Luna config
tokenLabel = <partition name>
```

9. Open IBM Key Management Utility:
   Traverse to directory /opt/IBM/HTTPServer/bin/
   Execute ./ikeyman.

10. Select Key Database File and Open. Specify Key Database Type as PKCS11Config. Click OK.
11. The Open Cryptographic Token window appears; where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the **Luna SA Partition password** for **Cryptographic Token Password**. You should check on PED device if password/Key are required to be entered.

![IBM Key Management](image)

12. Check the **Create new secondary key database file** to create the CMS Key Database *key.kdb*. You are prompted to create a password to access this file. In addition, check **Stash the password to a file**.
13. The IBM Key Management window appears. Select **Signer Certificates** from the drop down in **Key Database Content** block. Select one of the Signer certificates (except for the "... - Persona Not Validated" certificates) and click **Extract**.

14. When the **Extract Certificate to a File** dialog appears, make the filename unique such that you can later recall the name of the certificate, and select **Binary DER data**, and click **OK**. Repeat for each certificate in the list, (except for the "... - Persona Not Validated" certificates).

15. Next, import each .Der Certificate to the HSM, by selecting the certificate in the list, clicking **Add** and selecting **Binary DER Data**. Click **OK**, which opens a label dialog, and enter the label. Repeat for each certificate.

16. Signer Certificates appear as:
   `<token label>;<certificate label>`
17. For example, if the token label is "HTTP Server" and the certificate label is "Verisign Class 3 Primary Certification Authority" then you will see the "Signer Certificate" as: HTTP Server:Verisign Class 3 Primary Certification Authority. As an example, it is also shown in above figure (highlighted one).

18. Click Create - New Self Signed Certificate.... Specify the mandatory settings for Key Label and Organization. Click OK. RSA Public and Private Keys as well as Self Signed Certificate now exist on the Luna SA Partition. Self Signed Certificate will also appear in the form <token label>:<key label>.

19. Select Personal Certificate Request and click New....
20. Give the appropriate details as required (as shown above) and the name of the file (*.arm) in which the certificate request will be stored.

21. Generate the CA signed certificate from a CA with this request. (By visiting to CA website and pasting the request where required). Save the generated certificate also in .arm format.

22. Add the root certificate to the HSM.

23. Select **Signer Certificates** and click **Add**.

24. Select **Data Type** as **Binary DER data**.

25. Enter the **Certificate file name** and click **OK**.

26. The root certificate now exists on Luna SA partition.
27. Select **Personal Certificates** and click **Receive**.

28. Select **Data type** as **Base64-encoded ASCII data**.

29. Enter the **Certificate file name** and click **OK**.
RSA Public and Private Keys as well as Self Signed Certificate and CA certified certificate now exist on the Luna SA Partition.

To enable SSL Security:

1. Open the shell and change to directory `/usr/IBM/HTTPServer/bin`.
2. To Save the Luna SA Partition Password using the SSLStash Utility, type the following at shell:
   
a. `./sslstash –c /opt/IBM/HTTPServer/conf/ssl.passwd crypto "partition password"`
3. To enable SSL Security, you must modify and add settings to the file:
   
a. `/opt/IBM/HTTPServer/conf/httpd.conf`
4. Add or uncomment the appropriate lines throughout the file, as explained in the associated online documentation (http://httpd.apache.org/docs/2.0/). In the VIRTUAL HOST section, add or uncomment the line as shown in given example:

  ```
   LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
   Listen localhost:443
   <VirtualHost localhost:443>
   SSLEnable
   KeyFile /usr/IBM/HTTPServer/bin/key.kdb
   SSLServerCert <partition name>:<key label>
   SSLClientAuth None
   ```
SSLPKCSDriver /usr/lunasa/lib/libshim.so
SSLStashfile /usr/IBM/HTTPServer/conf/ssl.passwd

5. Stop and start the HTTP Server.

Open a Browser and type the following as a web address: https://<machinename>. You should receive a message similar to the following:

Click Yes. The Welcome to the HTTP Server web page appears.
Integrating IBM WebSphere Application Server V7.0 with Luna SA

Once you have installed IBM WebSphere Application Server, you must complete the following POST Installation instructions:

1. Modify the java.security file located in directory:

   ```
   /opt/IBM/Websphere/AppServer/java/jre/lib/security
   ```

   to include the following:

   ```
   security.provider.1=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.2=sun.security.provider.Sun
   security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.4=com.ibm.jsse.IBMJSSEProvider
   security_provider.5=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.6=com.ibm.security.cert.IBMCertPath
   security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl /usr/lunasa/luna.cfg
   security.provider.8=com.ibm.security.cmskeystore.CMSProvider
   security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   security.provider.10=com.ibm.crypto.pkcs11.provider.IBMPKCS11
   ```

   Create configuration file luna.cfg. The required entries in luna.cfg are:

   ```
   name = LUNA
   library = /usr/lunasa/lib/ libCryptoki2.so
   description = Luna config
   tokenLabel = <partition name>
   ```

2. Restart IBM Websphere Application Server.

Configuring a hardware cryptographic keystore

Complete the following steps in the administrative console:

1. Click Security > SSL certificate and Key management > Key stores and certificates.

2. Click New. Type a name to identify the keystore. This name is used to enable hardware cryptography in the Web services security configuration.

3. Type the path for the hardware device-specific configuration file (luna.cfg).

   ```
   /usr/lunasa/luna.cfg
   ```

4. Type a password if the token login is required. Select the type as Cryptographic Token Device (PKCS11).

5. Select Read only, Click OK and Save.
6. Click **Security > SSL Certificate** and **Key Management > SSL Configurations > Node Default SSLSettings**. Select **Keystore name** as new created keystore and click **Get Certificate Aliases**.

7. **Default server certificate alias** and **Default client certificate alias** drop down box will list all the certificates present on hardware. Select any one certificate. Press **OK** and **Save**.

8. Click **Security > SSL certificate** and **Key management > Manage endpoint security configurations > Inbound | Outbound > SSL_configuration_name**. Select SSL configuration as **NodeDefaultSSLSettings** and click **Update certificate alias list**. **Certificate alias in keystore** drop down box will list all the certificates present on the hardware. Select a certificate. Press **OK** and **Save**.
9. Use RetrieveSigners Utility to add server certificate to the ClientDefaulttrust store from CellDefaulttruststore. The utility is located under:

/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/retrieveSigners.sh

10. Logout and restart server. The following page is displayed before the Logging page:
View the Certificate and check. It should be same as that selected in step 8 and 9. If yes, press Yes to continue.