Luna SA and IBM Tivoli Access Manager for e-business

Integration Guide

SafeNet. THE DATA PROTECTION COMPANY

Preface

Part Number: PN007-009524-001 (Rev D, 07/2013)

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

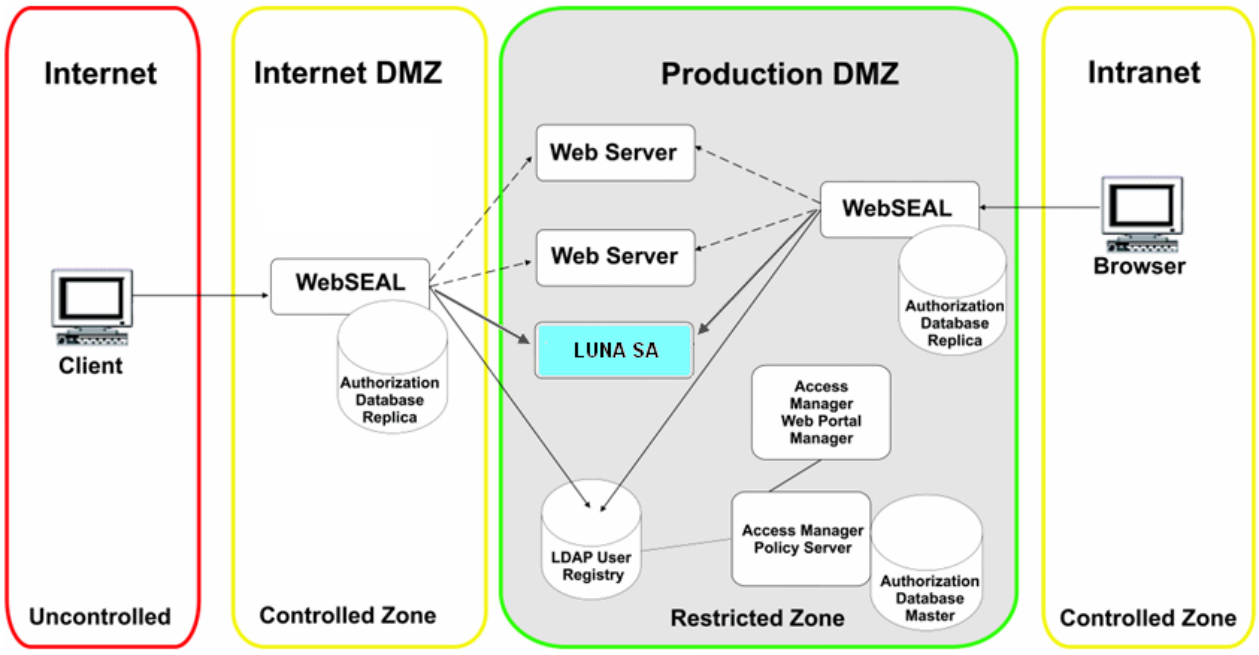
Table of Contents

Chapter 1
Introduction

This document covers the necessary information to install, configure and integrate IBM® Tivoli® Access Manager with SafeNet Luna SA Hardware Security Module (HSM).

The Luna SA hardware security module integrates with the IBM Tivoli Access Manager to deliver enhanced performance by off-loading SSL connections from the Tivoli Access Manager Web server to the Luna SA HSM. In addition, the Luna SA module provides added security by protecting the Tivoli Access Manager's SSL identity private key in a FIPS 140-2 hardware security module.

An example deployment for Luna SA with IBM Tivoli Access Manager is shown below:



Scope

3rd Party Application Details

- IBM Tivoli Access Manager for e-business for AIX V6.1
- IBM Tivoli Access Manager for e-business for Linux V6.1
- IBM Tivoli Access Manager for e-business for Solaris SPARC
- IBM Tivoli Access Manager for e-business for Windows Server 2003
- IBM Tivoli Access Manager for e-business for Linux V6.1.1

Supported Platforms

The integration between the SafeNet Luna SA and the IBM TAM for e-business has been tested for the following Combinations:

Operating System	SafeNet Luna SA Version	IBM Tivoli Access Manager Version
AIX 5.3 (64-bit)	4.3.2*	6.1
Solaris 10 SPARC	4.4.1	6.1
Solaris 9 SPARC	4.4.1 (32-bit)	6.1
RHEL 5 (32-bit)	4.4.1	6.1
Windows 2003 Server (32-bit)	4.4.1	6.1
RHEL 5 32-bit (running on VMWare ESXi)	5.0*	6.1
RHEL 6 32-bit	5.2.1	6.1.1

✍ * For AIX v5.3 and RHEL 5 32-bit (on VMWare ESXi), we have tested Tivoli Access Manager v6.1 with Luna SA v4.3.2 and Luna SA v5.0 respectively.

HSMs and Firmware Version

- K5 HSM f/w 4.6.1
- K5 HSM f/w 4.6.8
- K6 HSM f/w 6.0.8
- K6 HSM f/w 6.10.1

Library and Driver Support

- PKCS#11 v2.01 dynamic library

Distributions

- Luna SA 1U Appliance s/w v4.3.2
- Luna SA 1U Appliance s/w v4.4.1
- Luna SA 1U Appliance s/w v5.0
- Luna SA 1U Appliance s/w v5.2
- Luna SA Client s/w v4.3.2 (64-bit)
- Luna SA Client s/w v4.4.1 (32-bit)
- Luna SA Client s/w v4.4.1 (64-bit)
- Luna SA Client s/w v5.0 (32-bit)
- Luna Client s/w v5.2.1 (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 AIX, RHEL, Windows, 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 the IBM Tivoli Access Manager for e-business V6.1. 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 UNIX based systems and C:\Program Files\LunaSA\vtl.exe v for Windows systems.
- 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 Tivoli Access Manager for e-Business setup

For a detailed installation procedure, please refer to the IBM Tivoli Access for e-business v6.1 and v6.1.1 documentation.

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.itame.doc_6.1.1%2Fam611_install06.htm

Chapter 2
Integration IBM Tivoli Access Manager for e-business V6.1 with Luna SA

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

1. Ensure that the file libshim.so(for UNIX) or shim.dll (for Windows) is in the directory:
   UNIX:
   /usr/lunasa/lib

   Windows:
   C:\Program Files\LunaSA

2. Traverse to the directory:
   AIX:
   /usr/opt/ibm/gskta/classes/

   Linux:
   /usr/local/ibm/gsk7/classes/

   Solaris:
   opt/ibm/gsk7/classes

   Windows:
   C:\Program Files\IBM\gsk7\classes

3. Rename **ikmuser.sample** to **ikmuser.properties**.

4. Uncomment and edit the following setting to use the cryptographic shim (libshim):

   UNIX:
   DEFAULT_CRYPTOGRAPHIC_MODULE=/usr/lunasa/lib/libshim.so

   Windows:
   DEFAULT_CRYPTOGRAPHIC_MODULE= C:\\Program Files\\LunaSA\\shim.dll

5. Verify the following in the Luna SA configuration file.

   UNIX: /etc/Chrystoki.conf
   Windows: C:\Program Files\LunaSA\crystoki.ini

   Add the following to the Luna SA configuration (for UNIX /etc/Chrystoki.conf and for Windows C:\Program Files\LunaSA\crystoki.ini) file for Shim support:

   ```
   Misc = {
   ApplicationInstance=HTTP_SERVER;
   AppIdMajor=1;
   AppIdMinor=1;
   }
   ```

   For SA v5.0:

   Add the Shim2 section for Shim support:


```
Chrystoki2 = {
LibUNIX=/usr/lunasa/lib/libshim.so;
}

Shim2 = {
LibUNIX=/usr/lib/libCryptoki2.so;
}
```

Add the following to the existing **Misc** section of the SA v5.0 configuration file:

```
ApplicationInstance=HTTP_SERVER;
AppIdMajor=1;
AppIdMinor=1;
```

Also add the following to the **CardReader** section of the SA v5.0 configuration file:

```
LunaG5Slots=0;
```

6. To enable Cryptoki logging:

Cryptoki with Logging on UNIX

```
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;
}
```

For SA v5.0:

```
Chrystoki2 = {
LibUNIX=/usr/lunasa/lib/libshim.so;
}

CkLog2 = {
LibUNIX=/usr/lib/libCryptoki2.so;
NewFormat=1;
Enabled=1;
Error=/tmp/ErrorLunaSA2.txt;
File=/tmp/LogLunaSA2.txt;
}

 Shim2 = {
 LibUNIX=/usr/lunasa/lib/libcklog2.so;
 }
```

Cryptoki with Logging on Windows

```
[Chrystoki2]
LibNT=C:\Program Files\LunaSA\cklog201.dll
[CkLog2]
Enabled=1
NewFormat=1
File=c:\luna.txt
```

Error=c:\lunaerr.txt
LibNT=c:\program files\lunasa\cryptoki.dll

7. Set the JAVA_HOME environment variable:
   AIX:
   export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java

   Linux:
   export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java

   Windows:
   Set JAVA_HOME= C:\Program Files\IBM\Java50\jre

8. Open **IBM Key Management Utility** to create key database file
   AIX:
   /var/pdweb/www-default/certsgsk7ikm

   Linux:
   /var/pdweb/www-default/certs

   Solaris:
   /opt/IBM/gsk7/bin/gsk7ikm

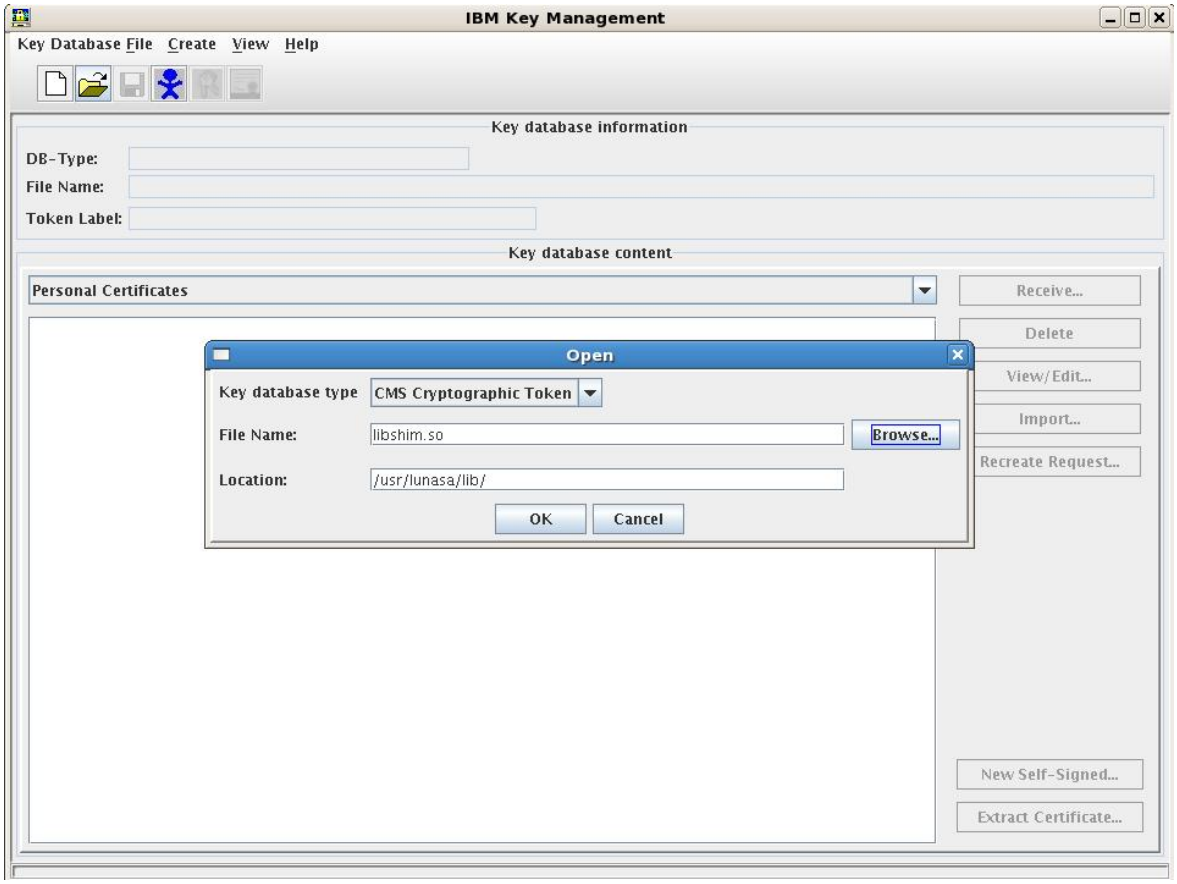
   Windows:
   C:\Program Files\IBM\gsk7\bin\gsk7ikm.exe

   The **Cryptographic Token** menu option appears.

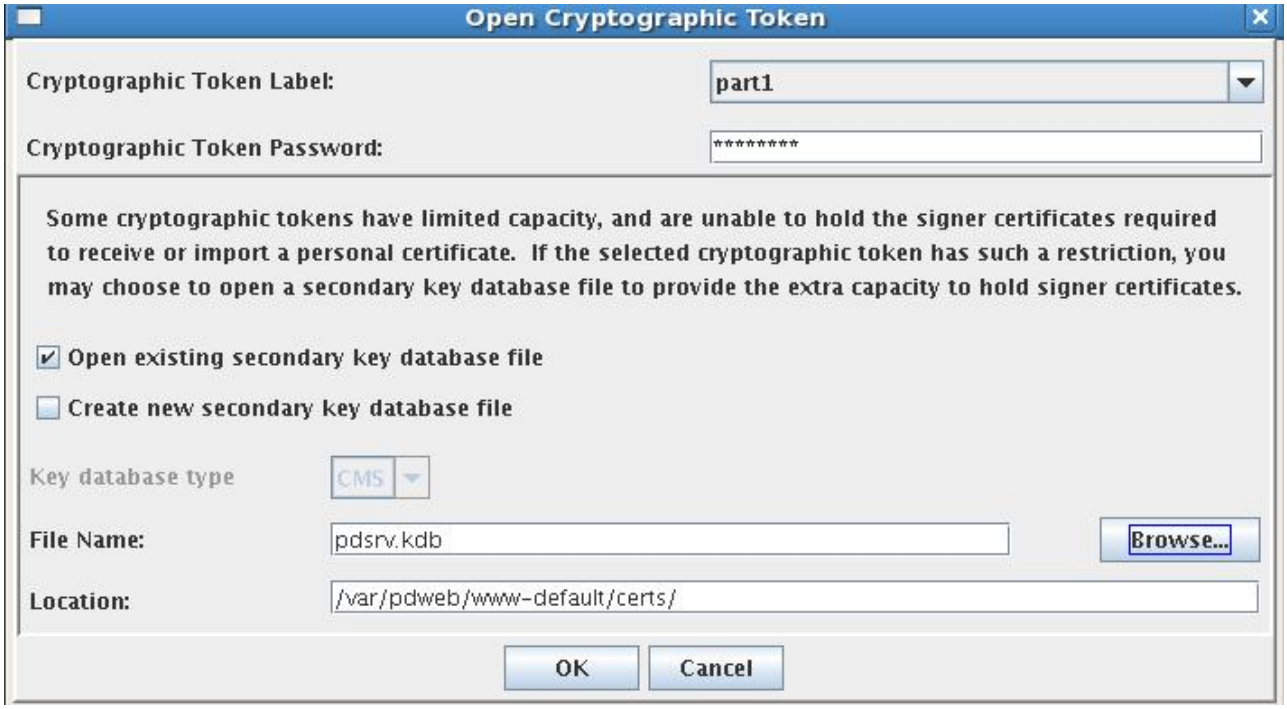
9. Select **Key Database File** and **Open**.
   Specify **KeyDatabase Type** as **CMS Cryptographic Token**,
   File as libshim.so for UNIX and shim.dll for Windows
   Location as /usr/lunasa/lib for UNIX and C:\Program Files\LunaSA for Windows

   Click **OK**.

Note: These snapshots are taken on AIX machine (For user's help), for other platforms same windows will appear.



10. 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 is required to be entered.



11. Check the **Open existing secondary key database file.**

Browse for and select the default WebSEAL key database file.
AIX:
/var/pdweb/www-default/certs/pdsrv.kdb
Linux:
/var/pdweb/www-default/certs/pdsrv.kdb
Solaris:
/opt/pdweb/www/certs/pdsrv.kdb
Windows:
C:\Program Files\Tivoli\PDWeb\www-default\certs\ pdsrv.kdb

Click Ok.

You are prompted for a password to access this file. Enter the default password “pdsrv” and click “OK”.

12. The main iKeyman window returns.

13. Request and store the WebSEAL server certificate.

14. Follow instructions in the IBM Global Security Kit: *Secure Sockets Layer Introduction and iKeyman User's Guide* to request a secure, signed digital certificate for WebSEAL from a Certificate Authority (CA).

15. Follow instructions in the IBM Global Security Kit: *Secure Sockets Layer Introduction and iKeyman User's Guide* to receive the WebSEAL certificate from the CA and store it in a key database. When performing this procedure, select the token device representing the cryptographic hardware as the storage location for the certificate.

16. When it is stored on the token device, the key (certificate) appears (for example) as:
part1: TestTAM. The TestTAM key is stored on the Luna SA hardware and assigned to the token device labeled ″part1″.

17. Configure WebSEAL to use the Luna SA PKCS#11 module.

18. In the WebSEAL configuration file

    UNIX:
    /opt/pdweb/etc/webseald-default.conf

    Windows:
    C:\Program Files\Tivoli\PDWeb\etc\ webseald-default.conf

    Edit the line in the [ssl] stanza that identifies the location of the shared library.
    UNIX:
    [ssl]
    pkcs11-driver-path = /usr/lunasa/lib/libshim.so

    Windows:

pkcs11-driver-path = C:\Program Files\LunaSA\shim.dll

19. In the WebSEAL configuration file, specify the names of the token label and password under the [ssl] stanza:

    [ssl]
    pkcs11-token-label = <token-name>
    pkcs11-token-pwd = <token-secret>

    for example:

    [ssl]
    pkcs11-token-label = part1
    pkcs11-token-pwd = temp123#

20. Modify the WebSEAL server certificate label.
    Configure WebSEAL to use this new hardware-based key rather than the default key in its communications with browser clients. Modify the webseal-cert-keyfilelabel parameter in the [ssl] stanza of the webseald-default.conf configuration file to designate the new key label.

    [ssl]
    webseal-cert-keyfile-label = <token-name>:<key-label>

    for example:

    [ssl]
    webseal-cert-keyfile-label = part1:TestTAM

21. Restart WebSEAL.
    You must restart WebSEAL for all cryptographic hardware configurations to take effect.

Chapter 3
Integration IBM Tivoli Access Manager for e-business V6.1.1 with Luna SA

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

1. Ensure that the file libshim.so(for UNIX) is available after the Luna Client installation in the directory:

   Luna Client v5.2.1:
   /usr/safenet/lunaclient/lib

2. Traverse to the following directory:

   Linux:
   /usr/local/ibm/gsk7/classes

3. Rename **ikmuser.sample** to **ikmuser.properties**.

4. Uncomment and edit the following setting to use the Luna shim library (libshim):

   UNIX:
   DEFAULT_CRYPTOGRAPHIC_MODULE=/usr/safenet/lunaclient/lib/libshim.so

5. Verify the following in the Luna configuration file.

   UNIX:
   /etc/Chrystoki.conf

   Add the following to the Luna configuration file for Shim support:

   ```
   Chrystoki2 = {
     LibUNIX = /usr/safenet/lunaclient/lib/libshim.so;
   }
   Shim2 = {
     LibUNIX = /usr/safenet/lunaclient/lib/libCryptoki2.so;
   }
   ```

   Add the following to the existing **Misc** section of the configuration file:

   ```
   Misc = {
     ApplicationInstance=HTTP_SERVER;
     AppIdMajor=1;
     AppIdMinor=1;
   }
   ```

   Also add the following to the existing **CardReader** section of the configuration file:

   ```
   CardReader = {
     LunaG5Slots=0;
   }
   ```

6. Set the JAVA_HOME environment variable:

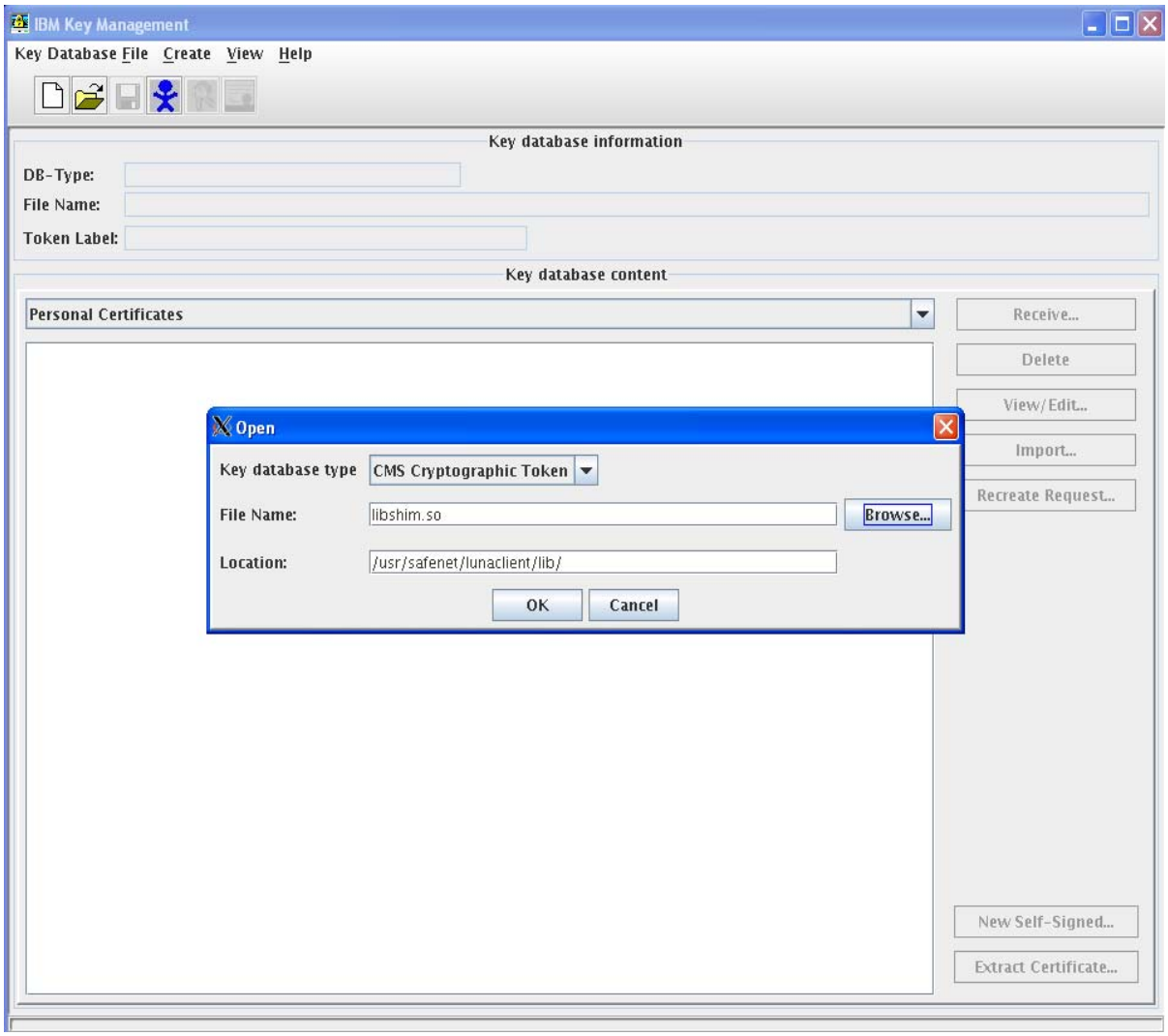
   export JAVA_HOME=/opt/ibm/java2-i386-50/jre

7. Open **IBM Key Management Utility** to create key database file

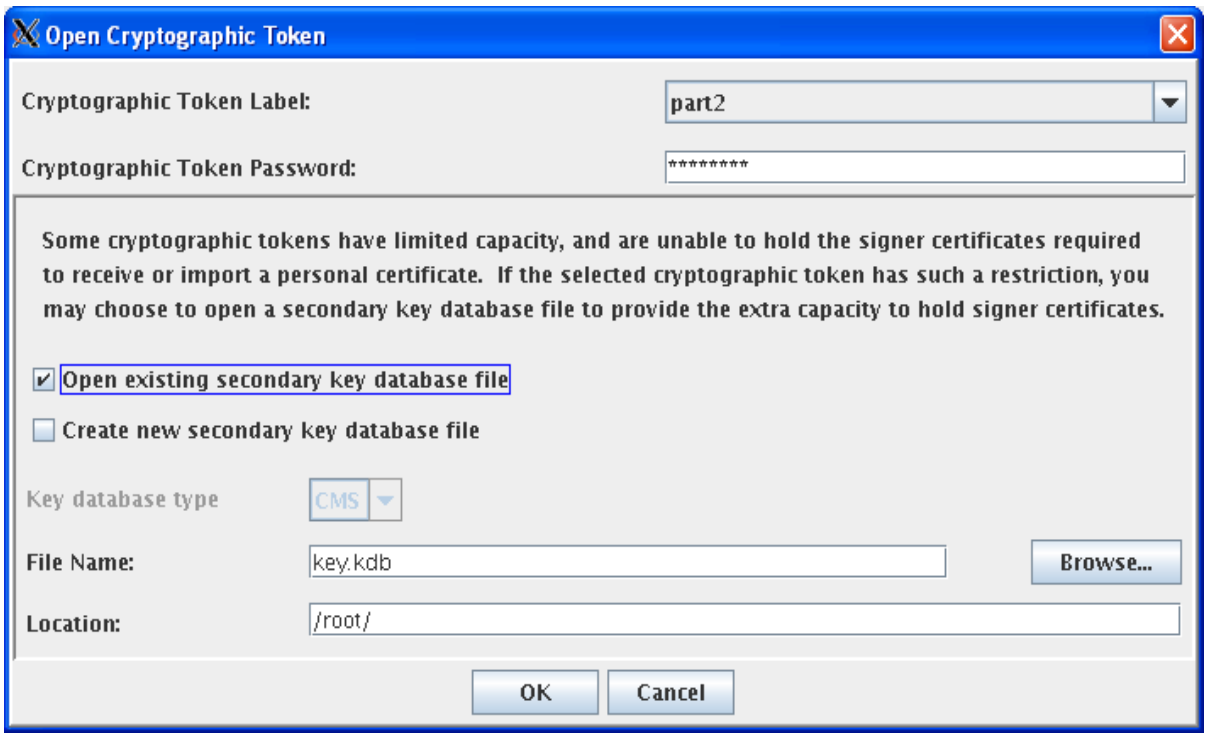
   Linux:
   /usr/local/ibm/gsk7/bin/gsk7ikm

   The **Cryptographic Token** menu option appears.

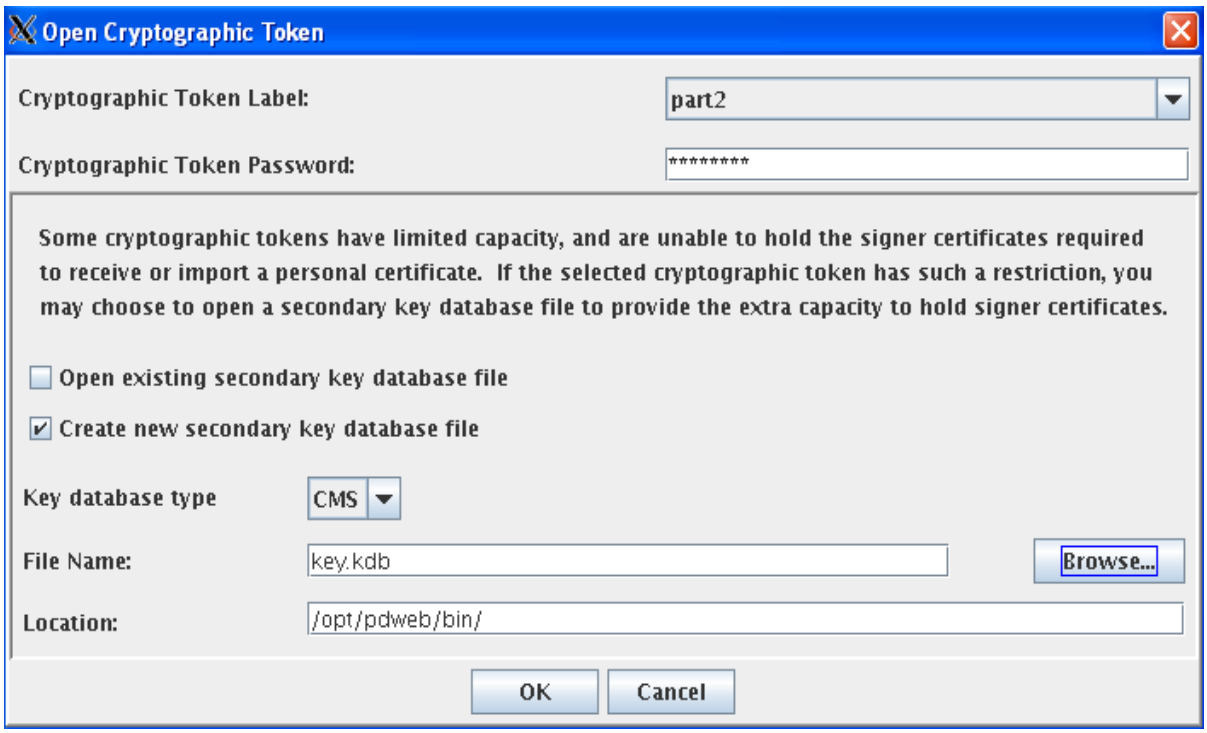
8. Select **Key Database File** and **Open**. Specify **Key Database Type** as **CMS Cryptographic Token**, File Name as **libshim.so** and Location as **/usr/safenet/lunaclient/lib/**. Click **OK**.



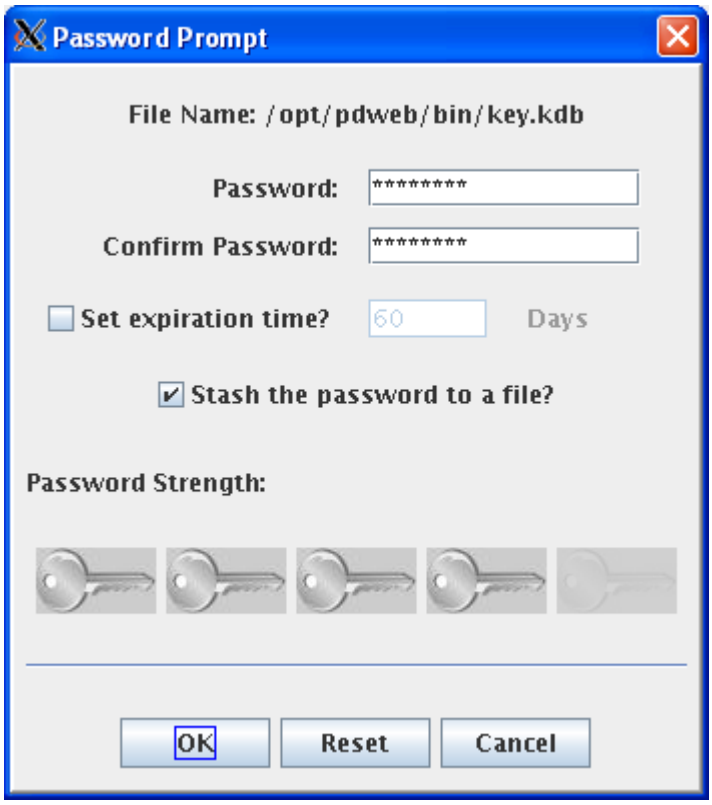
9. The Open Cryptographic Token window appears; where **Cryptographic Token Label** represents the Partition in which objects will be created. Specify the Luna SA Partition password for **Cryptographic Token Password**. You should check on PED device if password/Key is required to be entered.



10. Check the **Create new secondary key database file** to create the CMS Key Database **key.kdb**, **Browse** and select the **Location** and click **OK**.



11. You are prompted to create a password to access this file. In addition, check **Stash the password to a file**. Click **OK** to return to the main window.



12. For key database content, select **Personal Certificate Requests**, and click **New**.

13. Enter the **Key Label** and other details in **Create New Certificate Request**, and click **OK**.

14. Send the certificate request to any Certificate Authority (CA), and obtain the signed certificate and CA root certificate.

15. For key database content, select **Signer Certificates**. Click **Add** to add the Signer Certificate for the Trust which is downloaded from certificate Authority to iKeyman, navigate to **CA root certificate**, and click **OK**.

16. For key database content, select **Personal Certificates**. Click **Receive** to receive the signed certificate (Server Certificate) that protects the WebSEAL in SSL mode with Token Authentication, navigate to signed certificate, and click **OK**.

    IBM Key Management window shows the token name with the certificate label (<TokenName>:<CertificateLabel>).

Follow instructions in the IBM Global Security Kit: *Secure Sockets Layer Introduction and iKeyman User's Guide* to request a secure, signed digital certificate for WebSEAL from a Certificate Authority (CA).

Configuring WebSEAL to use the Luna PKCS #11 library

1. Open the WebSEAL configuration file. The default location is

   UNIX:
   /opt/pdweb/etc/webseald-default.conf

2. Locate [ssl] section and edit the line in the [ssl] stanza that identifies the location of the shared library.

   pkcs11-driver-path = /usr/safenet/lunaclient/lib/libshim.so

3. In the WebSEAL configuration file, specify the names of the token label and password under the [ssl] stanza:

   pkcs11-token-label = <token-name>
   pkcs11-token-pwd = <token-secret>

   For example:

   pkcs11-token-label = part2
   pkcs11-token-pwd = userpin2

4. Modify the WebSEAL server certificate keyfile, password and label. Configure WebSEAL to use this new hardware-based key rather than the default key in its communications with browser clients. Modify the following parameters in the [ssl] stanza of the webseald-default.conf configuration file to designate the new server certificate.

   webseal-cert-keyfile-label

   webseal-cert-keyfile-stash

   webseal-cert-keyfile-label

   For example:

   webseal-cert-keyfile = /opt/pdweb/bin/key.kdb

   webseal-cert-keyfile-stash = /opt/pdweb/bin/key.sth

   webseal-cert-keyfile-label = part2:WebSeal

5. Restart the WebSEAL server to make all of the cryptographic hardware configurations take effect:

   /opt/pdweb/bin/pdweb_start restart

6. Open the web browser, and entre the following:

   https://<ServerName or IP Address>:443

7. Check the certificate when it is displayed.

8. To view the page enters the WebSEAL Administrator ID and Password.

Chapter 4
Troubleshooting

Problem 1:
Webseal 6.1 installation fails with incorrect keyfile password.
Problem summary:
When configuring WebSEAL with SSL for LDAP enabled, SSL validation to LDAP fails in Solaris 10 and WebSEAL config fails.

Local fix
Creating the symbolic link /opt/IBM/ldap/V6.0 ->/opt/IBM/ldap/V6.1

Problem conclusion
The fix for this APAR is expected to be contained in the following maintenance delivery vehicle:
| fix pack | 6.1.0-TIV-AWS-FP0004

END OF DOCUMENT

