



LunaSA/PCI/CA4 and IAIK PKCS#11Wrapper

Integration Guide

Preface

© 2010 SafeNet, Inc. All rights reserved.

Part Number: 007-011101-001(Rev A, 02/2010)

All intellectual property is protected by copyright. IAIK registered trademarks of Stiftung Secure Information and Communication Technologies SIC. 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

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

| | |
|---|----------|
| Preface | i |
| Chapter 1 Introduction | 5 |
| Luna SA Setup:..... | 6 |
| Luna PCI Setup:..... | 6 |
| Luna PCM Setup: | 6 |
| Chapter 2 IAIK PKCS#11 Implementation with Luna SA / Luna PCI / Luna CA4 | 7 |
| References | 9 |

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1

Introduction

This document covers the necessary information to install, configure and integrate IAIK Pkcs#11 Provider with SafeNet Luna SA v 4.4.1 / Luna PCI v3.0 / Luna CAv2.4 Hardware Security Module (HSM) into Java™ applications.

IAIK PKCS#11 Provider provides a simple `java.security.keyStore` view of these tokens and makes cryptographic operations of these devices accessible via the JCA/JCE framework. For the application, it is just like working with pure software crypto and file key stores. The library accesses the hardware tokens via the PKCS#11 API, also known as Cryptoki. Hence, it can work with any product which supports PKCS#11.

The IAIK JCE Provider for PKCS#11 provides cryptographic functionality, including hash functions, message authentication codes, symmetric, asymmetric, stream encryption, block encryption, key and certificate management. It makes most of the functionality of the PKCS#11 standard accessible to Java™ applications through the JCE API from SUN.

This enables developers to use cryptographic hardware within their Java™ applications. Applications which are already based on a pure software implementation of the JCE API can use cryptographic hardware with little or no change of their existing applications.

All cryptographic tokens with PKCS#11 version 2.x compliant drivers can be used; this includes cryptographic smart cards and USB tokens as well as hardware security modules (HSMs). In particular, we tested with product SafeNet Luna SA 4.4.1 / Luna PCI v3.0 / Luna CAv2.4

Scope

3rd Party Application Details

- SUN Java™ Application

Supported Platforms

The following platforms are supported for Luna SA 1U v4.4.1, Luna PCI v3.0, Luna CAv2.4

- RHEL 5.3 X86_64
- Solaris 10 SPARC

HSMs and Firmware Version

- K5 HSM f/w 4.6.8(LunaSA)
- K5 HSM f/w 4.6.1(Luna PCI)
- G4 Base f/w 4.6.8(Luna CA4)

Library and Driver Support

- PKCS#11 v2.01 dynamic library
- IAIK PKCS#11 Provider

Distributions

- Luna SA 1U Appliance s/w v4.4.1
- Luna SA Client s/w v4.4.1
- Luna PCI Client s/w v3.0
- Luna PCM Client s/w v2.4

Prerequisites:

Luna SA Setup:

Please refer to the **Luna SA** documentation for installation steps and details regarding to configure and setup the box on UNIX 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 that will be later used by the IAIK demo or SafeNet demo programs. 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".
- 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).

Luna PCI Setup:

Please refer to the **Luna PCI** documentation for installation steps and details regarding configuring and setting up the box on UNIX systems. Before you get started ensure the following:

- Initialize the HSM on the Luna PCI appliance
- Create a partition on the HSM that will be later used by the IAIK demo or SafeNet demo programs..
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Luna PCM Setup:

Please refer to the **Luna PCM** documentation for installation steps and details regarding configuring and setting up the box on UNIX systems. Before you get started ensure the following:

- Initialize the HSM on the Luna CA4 token.
- Create a partition on the HSM that will be later used by the IAIK demo or SafeNet demo programs..
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

Chapter 2

IAIK PKCS#11 Implementation with Luna SA / Luna PCI / Luna CA4

To run the demo programs provided by IAIK PKCS#11 provider with SafeNet Luna SA / Luna PCI / Luna CA4 library:

Install the IAIK PKCS # 11 Provider

1. Include the jar files `iaikPkcs11Provider.jar`, `iaikPkcs11Wrapper.jar` and `iaik_jce.jar` in your class path or put them in the `jre/lib/ext` directory of your Java runtime (use the signed versions [lib-signed directory] of `iaikPkcs11Provider.jar` and `iaik_jce.jar` for JDK 1.4 and higher or if you use JCE 1.2.1 [e.g. IBM JDK 1.3]).
2. Put the shared library `libpkcs11wrapper.so` for UNIX, in any directory of your system's library search path or VM library path. You can set the VM library path using the `java.library.path` system property (e.g. using the VM command line argument `-Djava.library.path=/home/IAIK_Tools/IAIK_conversion/`)

Alternatively, you can specify the absolute path to the library in your properties file with the key `PKCS11_WRAPPER_PATH`, eg. `PKCS11_WRAPPER_PATH = /home/IAIK_Tools/IAIK_conversion/ libpkcs11wrapper.so`.

Configure the Provider with SafeNet Luna SA / Luna PCI HSM

1. Create a properties file called `iaik/pkcs/pkcs11/provider/IAIKPkcs11.properties` which contains the configuration for your provider (e.g. SafeNet Luna SA HSM). This properties file must contain at least one property entry with the key `PKCS11_NATIVE_MODULE`.

Its value must be the PKCS#11 module of the crypto hardware; e.g. `PKCS11_NATIVE_MODULE = libCryptoki2_64.so`

You may need to specify the PKCS#11 module with full path name, if it is not in your system's search path. The name of the PKCS#11 module may vary depending on your crypto hardware. Other entries are optional.

2. Put the configuration file somewhere in the class path taking the subdirectory structure into account (same as for class files). You may also include this configuration file in any jar file which is in your class path.

Test the Provider Configuration

Try to run an application that makes a simple test with the provider. Here we have tested SafeNet Luna SA/PCI/CA4 HSM with the demo programs provided by IAIK PKCS#11 provider.

<http://jce.iaik.tugraz.at/sic/Products/Core-Crypto-Toolkits/PKCS-11-Provider/demos>

You may try some of the included demos; e.g. `demo.pkcs.pkcs11.provider.RSASigningDemo0` in the demo directory.

The demo directory contains several samples that show how to use this library. The demos read their PKCS#11 module configuration from properties files. These properties files reside under the resources directory of the respective demo directory. If you do not launch the demos with the included shell files in the

test subdirectory, you must ensure that the resources directory is included in the CLASSPATH. Otherwise, the demo will throw an exception saying something like `iaik.pkcs.pkcs11.provider.IAIKPkcs11Exception: Required PKCS11_NATIVE_MODULE property has not been configured; e.g. check if properties files are in the CLASSPATH.`

In addition, you should not forget to edit the `resources/iaik/pkcs/pkcs11/provider/IAIKPkcs11.properties` file and enable the appropriate `PKCS11_NATIVE_MODULE` entry for your PKCS#11 module, in our case it is `libCryptoki2_64.so`.

These are some crypto operations that we have tested using IAIK PKCS #11 Provider with SafeNet Luna SA v4.4 (PKI Bundle), Luna PCI v3.0 (KE Mode), Luna CA4 v 2.4.

SafeNet provides some demo programs for testing of the following functionality with IAIK pkcs#11 provider.

1. Symmetric Key Generation
2. RSA Key Pair Generation
3. Wrapping of RSA Private Key from the symmetric key

 Luna CA4 does not support wrapping private keys off the token.

4. Decrypting/unwrapping the wrapped key from the symmetric Key
5. Sign/Verify using RSA key pair
6. Encryption and Decryption using Secret Key
7. Multi-slot support for multiple partitions on a Luna SA or multiple Luna PCM or PCI tokens.
8. Client authorization for SSL

The Safenet demo programs are available at Customer connection center (<http://c3.safenet-inc.com>). Look for "Sample programs for IAIK provider".

To test Client authorization for SSL use demo programs provided by IAIK.

<http://jce.iaik.tugraz.at/sic/Products/Core-Crypto-Toolkits/PKCS-11-Provider/demos>

Run SafeNet demo programs:

Use Readme.txt file for safenet demo details.

1. These demo programs are tested on java version "1.6.0_18-ea" with RHEL 5.3 X86-64 and Solaris 10 SPARC with SafeNet Luna SA 4.4.1 with PKI bundle, Luna PCI v3.0 (KE Mode), Luna CA4 v2.4.
2. Include the jar files `iaik_javax_crypto.jar`, `iaik_jce.jar`, `iaik_jce_full.jar`, `iaikPkcs11Provider.jar` `iaikPkcs11Wrapper.jar` in your class path.
3. Put the shared library `libpkcs11wrapper.so` for UNIX, in any directory of your system's library search path or VM library path.
4. Please note that these demos use dynamic provider registration. So don't need to update `IAIKPkcs11.properties` file.
5. Run the SafeNet demos

E.g.: Encryption and decryption using Triple – DES algorithm on Luna SA HSM

```
# javac -classpath
./iaik_javax_crypto.jar:./iaik_jce.jar:./iaik_jce_full.jar:./iaikPkcs11Provider.jar:./iaikPkcs11Wrapper.jar
:./IAIKPkcs11.properties: enc_dec_3des.java

# java -Djava.library.path=/home/IAIK_Tools/IAIK_conversion/ -cp
./iaik_javax_crypto.jar:./iaik_jce.jar:./iaik_jce_full.jar:./iaikPkcs11Provider.jar:./iaikPkcs11Wrapper.jar
:./IAIKPkcs11.properties: enc_dec_3des
```

References

1. Details about demos in IAIK demo directory
<http://jce.iaik.tugraz.at/sic/Products/Core-Crypto-Toolkits/PKCS-11-Provider/demos>
2. Download center for IAIK provider jars
<http://jce.iaik.tugraz.at/sic/Download>
3. SafeNet general purpose HSMs, Network attached
http://www.safenet-inc.com/Products/Data_Protection/Hardware_Security_Modules/General_Purpose_HSMs_Network_Attached.aspx