BCHSM Agent 1.1 for the Luna SP

Installation and Operations Guide

Version: BCHSM Agent version 1.1
Release Date: 09/25/2014
Document Revision: 09/23/2014

Topics in this Document

Introduction and Installation of the BCHSM Agent

Introduction

This document describes how to configure Blue Coat's HSM Agent (BCHSM) on a SafeNet Luna SP (v3.0) network-based HSM appliance. With the Agent and accompanying CLI installed, the HSM can interoperate with Blue Coat's SSL Visibility and ProxySG appliances, accepting requests from them to sign certificates for SSL interception.

The SSL Visibility and ProxySG appliances act as a client, exchanging signing requests and responses with the network-attached HSM appliance via this Blue Coat HSM Agent, using a mutually authenticated HTTPS connection. The SSL Visibility and ProxySG appliances send certificate data to the HSM.

With the BCHSM Agent, a user can create new RSA key pairs on the Luna SP and export a CSR for an external CA to sign.

The BCHSM Agent version 1.1 is compatible with SSLV software starting with version 3.8.0-150. The compatible SGOS version will be communicated when the release is available.

Install the Blue Coat HSM Agent

The Blue Coat HSM Agent facilitates resigning operations on the Luna SP appliance. The BCHSM is comprised of two primary components:

- The Blue Coat Web Service

  Related files:
  - hsm.war
- The Blue Coat CLI

  Related files:
  - bcprov-jdk15on-150.jar
  - bcpkix-jdk15on-150.jar
  - key.jar
  - csr.jar
  - delete.jar
  - showcert.jar
  - ListObject.jar

These files are packaged within a .tar file provided by Blue Coat.

To install the components, you will need to copy and then deploy the files included in the Blue Coat HSM Agent package.

Keep in mind, you will need to host the HSM Agent files on a machine capable of copying files via SCP to the Luna SP appliance.

If the Agent doesn't launch or you experience other difficulties using the Luna SP appliance, refer to the Luna SP guides to verify your installation.

Install the Components

Configure the Tomcat Web Server

Configure the Web Service as follows:

1. Create the Tomcat SSL server certificate on the Web server.
   ```
   websvc server cert generateCert
   ```
   Starting the web server generates the self-signed certificate, as well a CSR which can be exported and signed. The CSR can be sent to an external CA that can be imported on the Luna SP if you don't want to use a self-signed certificate.
2. Start the web server.
   ```
   spadmin start webService
   ```
3. Test the Tomcat web server:
   ```
   https://<luna_sp_ipaddress>:8443/
   ```

Import, Install, and Use the Blue Coat Web Service

The Blue Coat Web Service is installed on to the Luna SP appliance to invisibly handle requests from the ProxySG or SSL Visibility appliances.

Copy and install the Blue Coat Web Service

1. Copy the Web Service file to the appliance:
   ```
   scp hsm.war username@luna_sp_ipaddress:
   ```
2. Deploy and start the Web Service:
   ```
   spadmin deploy webapp -autoStart true -file hsm.war -name bc_webapp
   spadmin start webService
   ```
   The .war file will expand and install. No other installation action is required.

Import, Install, and Use the Blue Coat HSM CLI

The Blue Coat CLI comes packaged in seven .jar files alongside two supporting library files. Once installed, the Blue Coat commands will appear within the native HSM CLI.

The Blue Coat HSM CLI - related files are included in the package:

- Bouncy Castle library:
  - bcprov-jdk15on-150.jar
  - bcpkix-jdk15on-150.jar
- key.jar (Generates a key pair)
- csr.jar (Used to view the generated CSR)
- delete.jar (Used to delete a key object)

- showcert.jar (Used to show a certificate corresponding to a key)
- ListObjects.jar (Lists the objects on the HSM)

Copy and install the Bouncy Castle Libraries

1. Copy the library files to the appliance:

```
scp bcprov-jdk15on-150.jar username@luna_sp_ipaddress:
scp bcpkix-jdk15on-150.jar username@luna_sp_ipaddress:
```

2. Deploy the Bouncy Castle Library:

```
spadmin deploy library -name bcmain -file bcprov-jdk15on-150.-
jar -addtocp true
spadmin deploy library -name bcpkcs -file bcpkix-jdk15on-150.-
jar -addtocp true
```

Copy and install the Blue Coat HSM CLI

1. Copy the Blue Coat CLI files to the appliance:

```
scp key.jar username@luna_sp_ipaddress:
scp csr.jar username@luna_sp_ipaddress:
scp delete.jar username@luna_sp_ipaddress:
scp showcert.jar username@luna_sp_ipaddress:
scp ListObjects.jar username@luna_sp_ipaddress:
```

2. Deploy the Blue Coat HSM CLI; each deployment command corresponds to its scp above.

```
spadmin deploy application -name genKey -file key.jar -
startClass GenKey -autoStart false
spadmin deploy application -name showCSR -file csr.jar -
startClass GenCSR -autoStart false
spadmin deploy application -file delete.jar -autoStart false -
startClass DeleteKey -name deleteKey
spadmin deploy application -file showcert.jar -autoStart false
-startClass ShowCert -name showCertificate
spadmin deploy application -file ListObjects.jar -autoStart
false -startClass ListObjects -name listObjects
```

You may need to exit and log in to the appliance after deploying the HSM CLI before moving to the next step.

Verify Installation of the Blue Coat HSM Agent

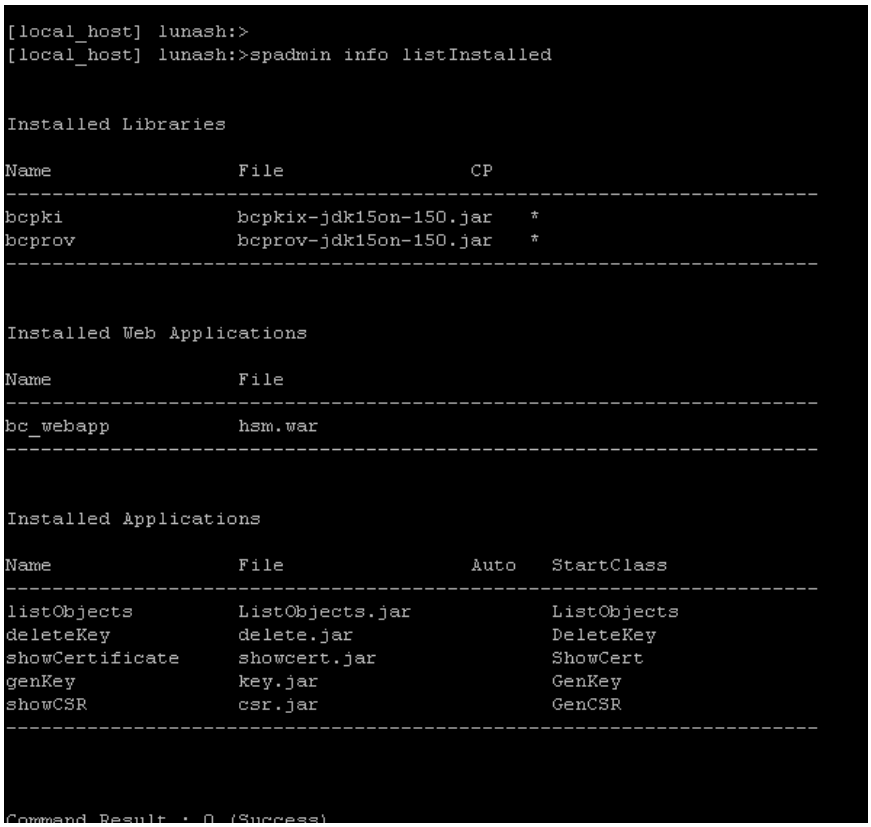
Before you continue with the installation, verify that the Bouncy Castle library, genKey, showCSR, deleteKey, showCertificate and listObjects applications, and the bc_webapp application has been correctly installed.

Verify the installation of the HSM Agent

Enter the following command in the Luna SP CLI:

```
sp /lists the Blue Coat HSM CLI commands
spadmin info listInstalled //Lists all installed components
```

The following is an example of the expected output:



```
[local_host] lunash:>
[local_host] lunash:>spadmin info listInstalled


Installed Libraries

Name                File                CP
------------------------------------------------------------------------
bcpki               bcpkix-jdk15on-150.jar   *
bcprov              bcprov-jdk15on-150.jar   *
------------------------------------------------------------------------


Installed Web Applications

Name                File
------------------------------------------------------------------------
bc_webapp           hsm.war
------------------------------------------------------------------------


Installed Applications

Name                File                Auto   StartClass
------------------------------------------------------------------------
listObjects         ListObjects.jar            ListObjects
deleteKey           delete.jar                 DeleteKey
showCertificate     showcert.jar               ShowCert
genKey              key.jar                    GenKey
showCSR             csr.jar                    GenCSR
------------------------------------------------------------------------



Command Result : 0 (Success)
```

Examples

This section presents BCHSM Agent examples.

Generate a Keypair (Emulated Certificate with Public and Private Keys)

The genKey command is used to create an RSA key pair. The user is expected to provide three input arguments:

- key label
- key size
- X.509 subject name

If you use this command to add a new key pair to the HSM, you must restart the web service (using `spadmin start webService`) in order for the newly created key_alias to be picked up by the Blue Coat web server application

In this example, the appliance has instructed that the data needs to be signed with the key alias/label “sep15.” The command was successfully executed as indicated by the returned result.

```
[local_host] lunash:>
[local_host] lunash:>sp genKey sep15 2048 "C=US,ST=CA,L=Sunnyvale,CN=SelfSigned,O=BC,OU=SG"

Executing Bluecoat's GenKey CLI version: 1.1
Key Pair and selfsigned cert created successfully!
The Self-Signed cert is:

-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIDAeJAMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTESMBAGA1UEBwwJU3Vubnl2YWxlMRMwEQYDVQQDDApTZWxm
U2lnbmVkMQswCQYDVQQKDAJCQzELMAkGA1UECwwCUOcwHhcNMTQwOTE1MTkONzU4
WhcNMTQxMDAzMjAyODI3WjBdMQswCQYDVQQGEwJVUzELMAkGA1UECAwCQOExEjAQ
BgNVBAcMCVN1bm55dmFsZTETMBEGA1UEAwwKU2VsZlNpZ251ZDELMAkGA1UECgwC
QkMxCzAJBgNVBAsMA1NHMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
q5+/R3QPtGSwf5D7iS95YrAYRbkYfWm6FO3fZVcEm/JjNi595TuWaPGqTqqJ2/+U
sYS3tLHuhEbO1SqXr7AoxW6vtoE+qY5acCbJJ+DyFqazjlsQBsVEitYXtmOFLAAB
kRFGzISWFNU7eD6UfPMeaUr/XVfOrW4OiO4ZJJ8zvLO8zddmciKhj1J+ge5Mqst3
Ea988IfpAB4OYiegBSidCwQyxKhgEKQAwT3wn1JWhQKt/XQ4KLCW4WAxDaaHmUjL
H1pLLt8NLqrYINsx2A7s6vu2qr6WnrVt97M9qvFIOu3Oe/4vFse8GIcJ1Fqi3zWF
xQpgcoFqGUnDiiNmgA+BLwIDAQABoOIwQDAPBgNVHRMBAf8EBTADAQH/MBOGA1Ud
DgQWBBTNFForyTwPPYTf6388sod6J1yRcjAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZI
hvcNAQELBQADggEBADxrHBfvOXHFSWyB6RHcgEuY/ZGOgAD12octOxTgCOOMmp1O
ePO3HCHcDKkXkVXnzJrvTFyeQd5z2QuVpVSS58oOxCMRsMMcuP4vOS7OnOYBF6nt
3wyVOTrWnTuBC529RPfQsw1ZxkL1uAa4Ib2SeSOvSEkEGYUny7LxpD7de3YwEw9t
9tilF9+gjLKe8rMxWpiBA4FHmMw11WgIzfjbbJQanoatVKXD/LN4Kv8vuLpTCMkF
SkSIy22OJRiwoPRdLb1oNCxZrURocHR+7ViXkHu6VoYPAIJjAOaMLyOf/r+KQHh8
wNR6qyXMaDNAgfeOHuYzVw5tKFtpjad6yNZ5OOw=
-----END CERTIFICATE-----


Command Result : 0 (Success)
[local_host] lunash:>
```

Blue Coat anticipates you will use the CSR corresponding to this key pair to get your own resigned certificate, and to use that certificate with your Blue Coat appliance.

Process Overview

1. Use the `sp genKey` command to create a key pair.
2. Use the `sp showCSR` command to view the CSR.
3. Sign the CSR, using your Certificate Authority.
4. Create an HSM keyring/key pair on your Blue Coat appliance.
5. Use the HSM test command on your Blue Coat appliance to verify the Luna SP accepts the certificate.

View the Generated CSR

The following example shows the output when viewing the generated CSR:

```
[local_host] lunash:>sp showCSR cs10

Executing Bluecoat's GenCSR CLI version: 1.1
Now generating CSR....
The CSR in PEM format is:


-----BEGIN CERTIFICATE REQUEST-----
MIIC9jCCAd4CAQAwXTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRIwEAYDVQQH
DAlTdW5ueXZhbGUxEzARBgNVBAMMClN1bGZTaWduZWQxCzAJBgNVBAoMAkJDMQsw
CQYDVQQLDAJTRzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAME/sO93
AXipkvoVefPydvCydLDes4bVRZ52O1cHmOXqMSsYi4JiVdYu6+RsWbff7einZFQ/
4mHzYrrd7mk+vsJRVjPp6Yh3NdphZJjUS4Ock4zGQ6v2yYylXMHJCiPX3xej2bMm
16qYyRnaz/2y6y7+vTE5Ov/rfPc3uFi/SBtyEpwyTNnDPH5u7v6eMUBOfsul4N9t
rGyLQ8APgP5/pJJmIyxO3F5Xc+QsCxy9NNMWjeaLnT5fKmHHrZO+x1KPLt1711Vx
L34RZgJVuWkcr9J2XWCRLBXUcTrWzZFr9GPp3nk179siO2EmnPITbFr6SNhNh5y7
H1aMfv1Osv2P/7OCAwEAAaBUMFIGCSqGSIb3DQEJDjFFMEMwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAQYwIAYDVR0OAQH/BBYEFBvvmmBfSyQXOj8RY/Hm
nGj9JZZsMA0GCSqGSIb3DQEBCwUAA4IBAQA+ZbYUiH3lYnKOmQDvUGQouKQxOtMA
QstDNaMFJDyL2EmM1IYeOBqTg+bDxhM8aHphpN93AmFg8hWHRqLFHisqfnldVzUK
R2IL1o5ogEPePb1Avc96xbQH92nlrJe3I4UHP+1DynHs5Pdn7v+gIvujqx5KaePQ
HKgtOoPhH1fX9GOXDz4x91KvOoJKKOEIRHSdhlzz4VdpUI3N1O1fABsI4TdDzAbX
iK47bWSZqmz6WYOH5AO6qUgO6tNMqSYaxud77eQi+YsdpEkTQ+bpDpLZsIRw1SRB
Xs/KAm3EYA9rXBcuk8iCTrhAUFvznVh5SWqgNWWYOjhGqcviIsUhzDHl
-----END CERTIFICATE REQUEST-----


Command Result : 0 (Success)
[local_host] lunash:>
```

Delete a Key Alias

In this example, a key label is deleted.

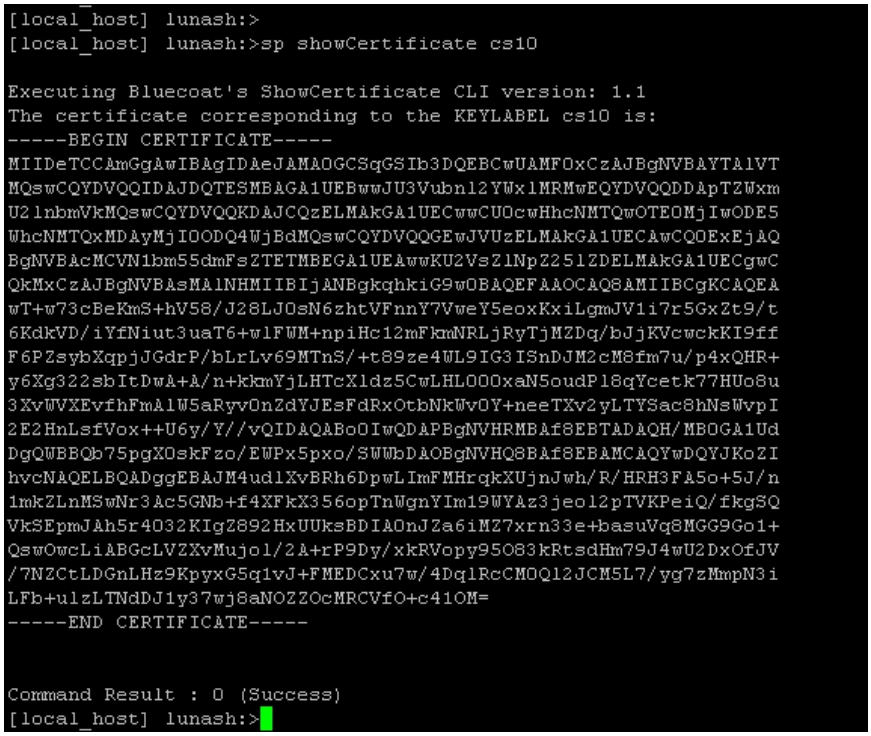
```
[local_host] lunash:>
[local_host] lunash:>sp deleteKey test4

Executing Bluecoat's DeleteKey CLI version: 1.1
Deleted KEYLABEL - test4

Command Result : 0 (Success)
[local_host] lunash:>
```

Show Certificate

View a certificate.



This command only presents certificates which correspond to a key pair created using the Blue Coat `genKey` command.

List Objects

VIew a list of objects in the key store.

```
[local_host] lunash:>sp listObjects

Executing Bluecoat's ListObjects CLI version: 1.1
Luna Keystore Information
Provider - LunaProvider version 5.1
Type     - Luna
Size     - 27 objects
Luna Keystore Contains
        -cs6
        -cs7
        -cs4
        -cs5
        -cs2
        -cs3
        -test
        -cs1
        -cs10
        -newkey
        -newver
        -tomcatCert
        -sepkey
        -cs8
        -cs9
        -test1
        -tomcat
        -tomcat--public
        -cs11
        -sep2k
        -bckey
        -whatever
        -test4
        -test2
        -jul16
        -test3
        -example

Command Result : 0 (Success)
[local_host] lunash:>
```

Limitations

This section documents any known issues or limitations.

Limitations

The current Luna SP shell does not parse white spaces in attribute fields in custom CLI commands. As a result, `genKey` cannot parse white spaces in the subject name. Refer to the Safenet's Luna SP documentation and release notes for updates on this issue.

Known Issues

Blue Coat is not currently aware of any known issues.

Getting Help

To obtain additional information or to provide feedback, please email support@BlueCoat.com or contact the nearest Blue Coat Systems technical support representative.

Visit http://www.bluecoat.com/support/technical-support to download the latest documentation and software, access the knowledge base, or log a support ticket.

Third Party Copyright Notices

Americas:

Blue Coat Systems, Inc.

420 N. Mary Ave.

Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL

3a Route des Arsenaux

1700 Fribourg, Switzerland