



# Interoperability of Bloombase StoreSafe and Gemalto SafeNet KeySecure for Data-at-Rest Encryption

April 2016



## Executive Summary

Gemalto SafeNet KeySecure Key Management System is validated by Bloombase InteropLab to run with Bloombase StoreSafe data-at-rest encryption security solution. This document describes the steps carried out to test interoperability of Gemalto SafeNet KeySecure Key Management System with Bloombase StoreSafe software appliance on VMware ESXi. Client host systems on Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Oracle Sun Solaris, IBM AIX and HP-UX are tested with Gemalto SafeNet KeySecure powered Bloombase StoreSafe with NetApp FAS unified storage system as backend storage.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, people and events depicted herein are fictitious and no association with any real company, organization, product, person or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Bloombase.

Bloombase may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Bloombase, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

This document is the property of Bloombase. No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with Bloombase, and neither the document nor any such information may be released without the written consent of Bloombase.

© 2016 Bloombase, Inc.

Bloombase, Keyparc, Spitfire, StoreSafe are either registered trademarks or trademarks of Bloombase, Inc. in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Document No.: BLBS-TN-Bloombase-StoreSafe-Gemalto-SafeNet-KeySecure-Interoperability-USLET-EN-Ro.92

# Table of Contents

<b>Table of Contents</b>	<b>3</b>
<b>Purpose and Scope</b>	<b>5</b>
<b>Assumptions</b>	<b>6</b>
<b>Infrastructure</b>	<b>7</b>
<b>Setup</b>	<b>7</b>
<b>Key Management System</b>	<b>9</b>
<b>Bloombase StoreSafe</b>	<b>9</b>
<b>Storage System</b>	<b>9</b>
<b>Client Hosts</b>	<b>9</b>
<b>Configuration Overview</b>	<b>10</b>
<b>Gemalto SafeNet KeySecure</b>	<b>10</b>
Gemalto SafeNet KeySecure Configurations	11
<b>NetApp FAS Storage</b>	<b>19</b>
<b>Bloombase StoreSafe</b>	<b>21</b>
Network Security, Trust and Authentication Configuration	22
Gemalto SafeNet KeySecure and Bloombase KeyCastle Integration	22
Encryption Key Provisioning	24
Backend Physical Storage Configuration	26
Secure Storage Configuration	27
<b>Conclusion</b>	<b>29</b>
<b>Disclaimer</b>	<b>31</b>
<b>Technical Reference</b>	<b>32</b>

# Purpose and Scope

This document describes the steps necessary to integrate Gemalto SafeNet KeySecure Key Management System with Bloombase StoreSafe to secure sensitive enterprise business data-at-rest managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloombase StoreSafe
- Integrate Bloombase StoreSafe with Gemalto SafeNet KeySecure
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris

# Assumptions

This document describes interoperability testing of Gemalto SafeNet KeySecure with Bloombase StoreSafe. Therefore, it is assumed that the reader is familiar with operation of Gemalto SafeNet KeySecure, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that the reader possesses basic UNIX administration skill-set. The examples provided may require modifications before they could be run in reader's IT environment.

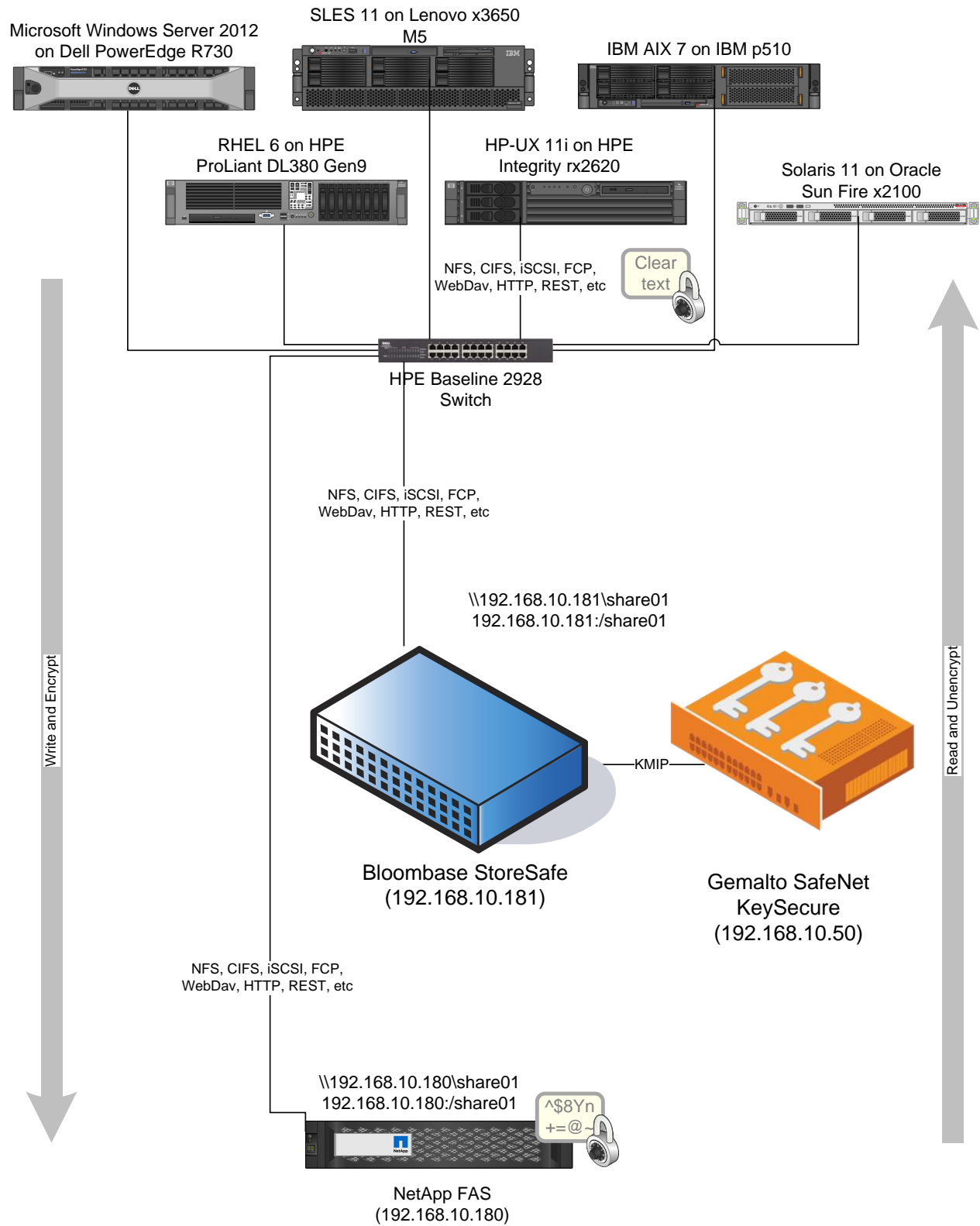
As Gemalto SafeNet KeySecure is a third party hardware option to Bloombase StoreSafe data-at-rest encryption security solution, the reader is recommended to refer to installation and configuration guides of specific model of Gemalto SafeNet KeySecure for the actual use case. We assume the reader has basic knowledge of storage networking and information cryptography. For specific technical product information of Bloombase StoreSafe, please refer to our website at <http://www.bloombase.com> and Bloombase SupPortal <http://supportal.bloombase.com>.

# Infrastructure

## Setup

The validation testing environment is set up as in below diagram:

## Trusted Hosts and Applications



## Storage



## Key Management System

Key Management System	Gemalto SafeNet KeySecure
-----------------------	---------------------------

## Bloombase StoreSafe

<b>Bloombase StoreSafe</b>	Bloombase StoreSafe Software Appliance v3.5 on Bloombase OS 7
<b>Server</b>	VMware Virtual Machine (VM) on VMware ESXi 5.5
<b>Processor</b>	4 x Virtual CPU (vCPU)
<b>Memory</b>	8 GB

## Storage System

Storage System	NetApp FAS Simulator
----------------	----------------------

## Client Hosts

<b>Model</b>	Dell PowerEdge R730	HPE ProLiant DL380 Gen9	Lenovo System x3650 M5	HPE Integrity rx2620	IBM System p5 510	Oracle Sun Fire x2100
<b>Operating System</b>	Microsoft Windows Server 2012	Red Hat Enterprise Linux 6	SUSE Linux Enterprise 11	HP-UX 11i	IBM AIX 7	Oracle Solaris 11

# Configuration Overview

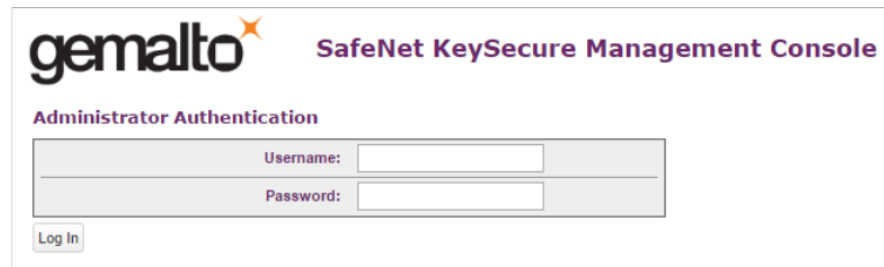
## Gemalto SafeNet KeySecure

Gemalto SafeNet KeySecure is a centralized key management platform, and is available as a hardware appliance or hardened virtual security appliance. By utilizing Gemalto SafeNet KeySecure, organizations benefit from its flexible options for secure and centralized key management – deployed in physical, virtualized infrastructure, and public cloud environments. It includes integration API that supports the industry standards (KMIP 1.1, PKCS #11, JCE, MS-CAPI, ICAP, and .NET) which are used in many application scenarios, e.g., Enterprise PKI application and database encryption. The Gemalto SafeNet KeySecure is available as a hardware appliance or hardened virtual security appliance with a hardware root of trust using SafeNet Network Hardware Security Modules or Amazon CloudHSM service. The key management and cryptographic functionalities provided by Gemalto SafeNet KeySecure are used by Bloombase StoreSafe for encryption protection of data-at-rest for general-purpose use cases.

## Gemalto SafeNet KeySecure Configurations

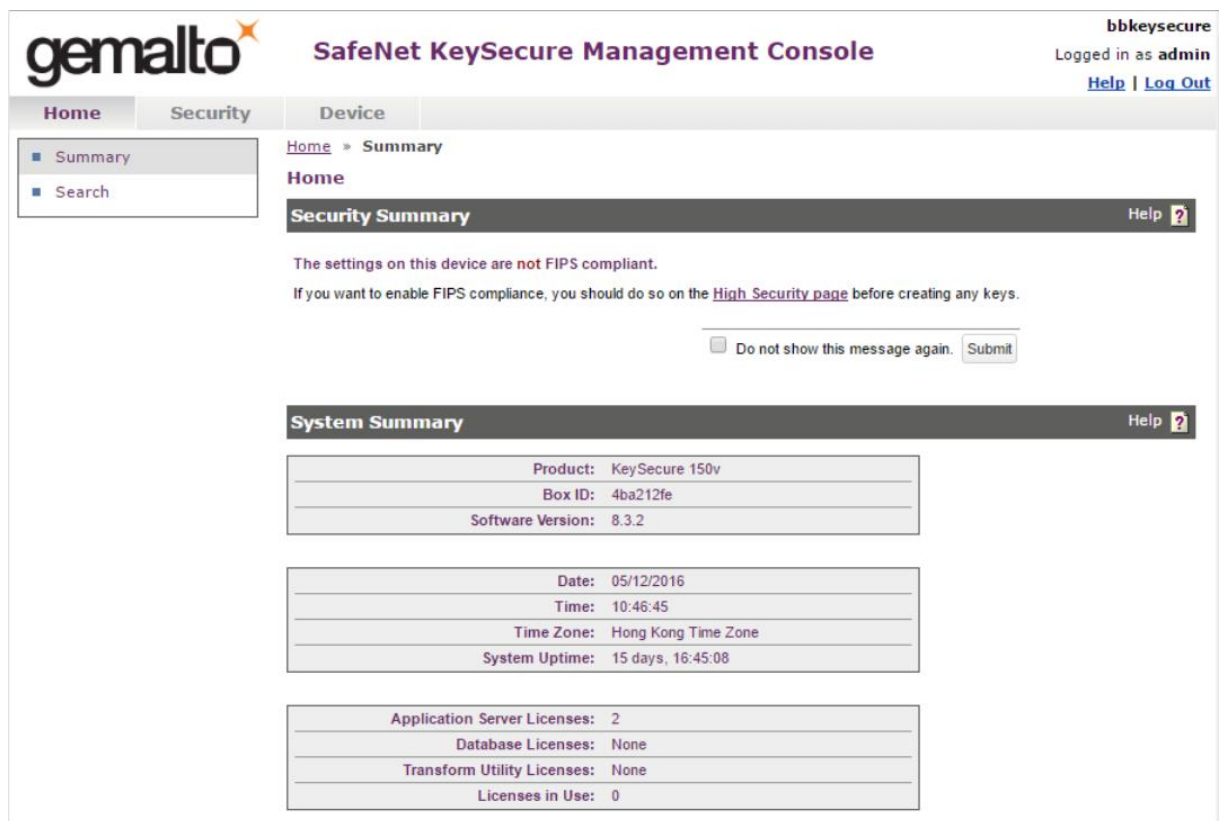
Assume Gemalto SafeNet KeySecure is installed and configured as a network attached appliance with IP address 192.168.10.50.

Gemalto SafeNet KeySecure can be managed remotely via web-based management console.



The screenshot shows the login page of the Gemalto SafeNet KeySecure Management Console. It features the Gemalto logo and the title "SafeNet KeySecure Management Console". Below this is the "Administrator Authentication" section, which contains two input fields: "Username:" and "Password:". A "Log In" button is located below the password field.

Once logged in, basic information of Gemalto SafeNet KeySecure is shown.



The screenshot shows the home page of the Gemalto SafeNet KeySecure Management Console after logging in. The page has a navigation bar with "Home", "Security", and "Device" tabs. The "Home" tab is selected. On the left, there is a sidebar with "Summary" and "Search" options. The main content area displays the "Security Summary" and "System Summary" sections. The "Security Summary" section includes a warning about FIPS compliance and a checkbox to "Do not show this message again." The "System Summary" section displays various system information in a table format.

System Summary	
Product:	KeySecure 150v
Box ID:	4ba212fe
Software Version:	8.3.2
Date:	05/12/2016
Time:	10:46:45
Time Zone:	Hong Kong Time Zone
System Uptime:	15 days, 16:45:08
Application Server Licenses:	2
Database Licenses:	None
Transform Utility Licenses:	None
Licenses in Use:	0

Gemalto SafeNet KeySecure can be configured to support a hardware root of trust using SafeNet Network HSM or the Amazon CloudHSM service to achieve FIPS compliant.

To authenticate the communication between Gemalto SafeNet KeySecure and Bloombase StoreSafe, signed certificates need to be created and stored in the Gemalto SafeNet KeySecure and the Bloombase StoreSafe. In the Gemalto SafeNet KeySecure, this is done as follows.

A Self-signed Local Root CA is first created in “Local CAs” of the Gemalto SafeNet KeySecure under the Security tab.

The screenshot displays the Gemalto SafeNet KeySecure Management Console interface. The top navigation bar includes the Gemalto logo, the title 'SafeNet KeySecure Management Console', and user information 'bbkeysecure Logged in as admin' with links for 'Help' and 'Log Out'. The main navigation tabs are 'Home', 'Security', and 'Device', with 'Security' being the active tab. A left sidebar contains several menu categories: 'Managed Objects' (Keys, Certificates, Certificate Requests, Authorization Policies), 'Users & Groups' (Local Authentication, LDAP), 'Device CAs & SSL Certificates' (SSL Certificates, Trusted CA Lists, Local CAs, Known CAs), and 'Advanced Security' (High Security, SSL, FIPS Status Server). The 'Local CAs' option is selected, leading to the 'Security > Local CAs' page. The page title is 'Certificate and CA Configuration'. Below this is a 'Local Certificate Authority List' table with one entry, 'keysecureca', which is active. Action buttons (Edit, Delete, Download, Properties, Sign Request, Show Signed Certs) are available for this entry. Below the table is the 'Create Local Certificate Authority' form. The form fields include: Certificate Authority Name (keysecureca), Common Name (keysecureca), Organization Name (Safenet), Organizational Unit Name (KeySecure), Locality Name (Sunnyvale), State or Province Name (CA), Country Name (US), Email Address (techpubs@safenet-inc.com), and Key Size (2048). Under 'Certificate Authority Type', the 'Self-signed Root CA' option is selected, with fields for 'CA Certificate Duration (days)' and 'Maximum User Certificate Duration (days)', both set to 3650. The 'Intermediate CA Request' option is unselected. A 'Create' button is at the bottom left of the form.

**gemalto** SafeNet KeySecure Management Console bbkeysecure  
Logged in as **admin**  
[Help](#) | [Log Out](#)

**Home** **Security** **Device**

**Managed Objects**

- Keys
- Certificates
  - Certificate Requests
  - Authorization Policies

**Users & Groups**

- Local Authentication
- LDAP

**Device CAs & SSL Certificates**

- SSL Certificates
- Trusted CA Lists
- Local CAs**
- Known CAs

**Advanced Security**

- High Security
- SSL
- FIPS Status Server

[Security](#) > Local CAs

**Certificate and CA Configuration**

**Local Certificate Authority List** [Help](#) ?

CA Name	CA Information	CA Status
<input checked="" type="radio"/> <a href="#">keysecureca</a>	Common: keysecureca Issuer: Safenet Expires: May 7 09:04:10 2026 GMT	CA Certificate Active

[Edit](#) [Delete](#) [Download](#) [Properties](#) [Sign Request](#) [Show Signed Certs](#)

**Create Local Certificate Authority** [Help](#) ?

**Certificate Authority Name:**

**Common Name:**

**Organization Name:**

**Organizational Unit Name:**

**Locality Name:**

**State or Province Name:**

**Country Name:**

**Email Address:**

**Key Size:**

**Certificate Authority Type:**

☒ Self-signed Root CA

CA Certificate Duration (days):

Maximum User Certificate Duration (days):

☐ Intermediate CA Request

[Create](#)

The newly created Local CA is then added to the “Default” trusted CA lists.

The screenshot displays the Gemalto SafeNet KeySecure Management Console interface. The top navigation bar includes the Gemalto logo, the title "SafeNet KeySecure Management Console", and user information "bbkeysecure" logged in as "admin" with links for "Help" and "Log Out". The main navigation tabs are "Home", "Security", and "Device". The "Security" tab is active, showing a breadcrumb "Security > Trusted CA Lists".

The left sidebar contains several menu sections:

- Managed Objects**: Keys, Certificates, Certificate Requests, Authorization Policies.
- Users & Groups**: Local Authentication, LDAP.
- Device CAs & SSL Certificates**: SSL Certificates, Trusted CA Lists (highlighted), Local CAs, Known CAs.
- Advanced Security**: High Security, SSL, FIPS Status Server.

The main content area is titled "Certificate and CA Configuration" and "Trusted CA List Profile Properties". It features a "Profile Name: Default" field and a "Back" button. Below this is the "Trusted Certificate Authority List" section, which shows "Trusted CAs:" with "Local Certificate Authorities:" listed as "keysecureca" and "CA Certificates:" listed as "[None]". An "Edit" button is located at the bottom of this section.

A signed certificate is created for the Gemalto SafeNet KeySecure. This is done by “Create Certificate Request” under “SSL Certificates”.

The screenshot shows the Gemalto SafeNet KeySecure Management Console interface. The user is logged in as 'admin'. The left sidebar contains navigation menus for 'Managed Objects' (Keys, Certificates, Certificate Requests, Authorization Policies), 'Users & Groups' (Local Authentication, LDAP), 'Device CAs & SSL Certificates' (SSL Certificates, Trusted CA Lists, Local CAs, Known CAs), and 'Advanced Security' (High Security, SSL, FIPS Status Server). The main content area is titled 'Certificate and CA Configuration' and shows a 'Certificate List' with one entry: 'kmpservercert' (Common: kmpservercert, Issuer: Safenet, Expires: May 6 09:08:50 2026 GMT, Purpose: Server, Status: Active). Below the list are buttons for 'Edit', 'Delete', and 'Properties'. The 'Create Certificate Request' form is displayed, with fields for: Certificate Name (kmpservercert), Common Name (kmpservercert), Organization Name (Safenet), Organizational Unit Name (KeySecure), Locality Name (Sunnyvale), State or Province Name (CA), Country Name (US), Email Address (techpubs@safenet-inc.com), and Key Size (2048). A 'Create Certificate Request' button is at the bottom.

Security > SSL Certificates

### Certificate and CA Configuration

#### Certificate Request Information

Certificate Name: keysecurecert	
Key Size: 2048	
Subject:	CN: keysecurecert
	O: Bloombase
	OU: StoreSafe
	L: Sunnyvale
	ST: CA
	C: US
emailAddress: admin@bloombase.com	

-----BEGIN CERTIFICATE REQUEST-----

```
MIIC2DCCACACAwgZIxFAUBGNVBAWTDWt1eXN1Y3V3ZW50cnQxZjAQBGNVBAoT
CUJsb29tYmFzZTESMBAGALUECxmJUS3RvcmlVTWZlMRlWZAYDVQQHEw1TdW5ueXZl
bGUxZCZAJBgNVBAQTAkNBMQswCQYDVQQGEwJVUzEIMCAGCSqGSIb3DQEJARYTYWRt
aW5AYm9vbnV3ZW50cnQxZjAQBGNVBAWTDWt1eXN1Y3V3ZW50cnQxZjAQBGNVBA
AK9H1Ykx1WXTT5mdpDCCOH7u0ouhI8m5cE3VQJ1ATySi26MnTk15+KtNbUTvkaJEn
upZWUIPeynK7+HvMeKyG7V0KG2i+V9NUmUav+j+CgQSBAMSO02emb1vdM81Wp2Fuh
1Gv4pP/j5k6kzZY0ApdWbNM54IbR9h1dcARVXGSDWz1GnM5m/Vk33CDu1aRImRq
oJbY1zK+P/RNSdY3UhHhmy3oxHQDdvCYcHvZrwH8fM6aH/H6FqrdgYHn8/TpzGg
XykeLp10Uom3KLQbkauwQXeeqg3MhAvISE478yfWSeVx6T5WfT/M+qAVyWYNpoa
SsEv69mejhgY6veosFR118ChwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQB2/xQU
AHR5U393I936D7VK9LFRXptGOb/v9nfhwdsA4FiQuaeAA0h1qTcI5a7COqfWVVBHq
v6KR5C5zRoMnSoSbCQ5j7hi5E535Q88S+ReNjMwiDMKjccQTnzEn12N2+bfu6dHj
A97z1LhK9S5K51w6FVCO+8MVRTcHvYcUYN28WOMEAGtHcYARNHcdB3xRKR4/c
UhCNSDTq3X1yMDonaD9MoUjV2q8z1w1Sages3+F4pwiX6e40azVmJbQjYTMgg5GB
LSGDZn+VhNLShB1MLWX1UsNRfWwR/Dd7G2OSK1QeY5dgED9HjI9GLE5b+xlE/C
JFMHG4xm8WhLgdXm
```

-----END CERTIFICATE REQUEST-----

[Download](#) [Install Certificate](#) [Create Self Sign Certificate](#) [Back](#)



And have the signed certificate saved under the Certificate List.

[Security](#) > [SSL Certificates](#)

### Certificate and CA Configuration

#### Certificate Installation

Certificate Name: keysecurecert	
Key Size: 2048	
Subject:	CN: keysecurecert O: Bloombase OU: StoreSafe L: Sunnyvale ST: CA C: US
emailAddress: admin@bloombase.com	
Certificate Response:	
<pre>EG CWC6SAGG+EIBAQQEAWIGQDANBgqhkiG9w0BAQsFAAOCQAQEfC73vXiZVOMHCt xq 2AIDAiKS63dTSjPeN+rSDoMGDEsIo8YEpCzDE/u0EpPQD8KSwqu4fP11CQcURx Cx FN1unWE/XL+zcz076sgju2InVsGxTlbuixzn5/pJf/+oK2akTCrtaHkCWNFnet 0M NZJzu8V1H34kMqs2d3128t2cpgvFicQKBZVGzf8xCeJef0yea9Byt2Sqr+d1T bQ i9vpcxVMhXuPeLz0BNxbADU9cdSeoHPd/kpU76XbRFQ70Br7FKV1zSCBvKEtXS Zu sseYKEhTtFi2Sr6XUyu7B5G0+I664Fps8m8Uw3Gu+8VQcXvp+CvdD8p1kXLi9b qJ dXSU9Q== -----END CERTIFICATE-----</pre>	
Save	Cancel



We can then configure the Gemalto SafeNet KeySecure to enable KMIP with the newly created signed server cert.

The screenshot displays the Gemalto SafeNet KeySecure Management Console interface. The top navigation bar includes the Gemalto logo, the title "SafeNet KeySecure Management Console", and user information "bbkeysecure Logged in as admin" with links for "Help" and "Log Out". The main navigation tabs are "Home", "Security", and "Device". The left sidebar contains three main sections: "Device Configuration" (with sub-items like Key Server, Health Check, Cluster, Date & Time, Network, SNMP, Administrators, SSH Public Key, and Known Hosts), "Logs & Statistics" (with sub-items like Log Configuration, Log Viewer, and Statistics), and "Maintenance" (with sub-items like Backup & Restore, Services, System Information & Upgrade, System Health, and Network Diagnostics). The main content area shows the breadcrumb "Device > Key Server > Key Server" and the title "Cryptographic Key Server Configuration". Below this is the "Cryptographic Key Server Settings" section, which includes a table with columns for Protocol, IP, Port, Use SSL, and Server Certificate. The table shows two rows: one for NAE-XML (IP: [All], Port: 9000, Use SSL: unchecked, Server Certificate: [None]) and one for KMIP (IP: [All], Port: 9002, Use SSL: checked, Server Certificate: kmipservercert). Below the table are "Save" and "Cancel" buttons. The "User Directory Settings" section shows "User Directory: Local" with an "Edit" button. The "User Account Lockout Settings" section shows "Enable Account Lockout" checked, "Number of Failed Authentication Attempts Before Account Lockout" set to 3, and "Account Lockout Duration (sec)" set to 60, with an "Edit" button.

**gemalto** SafeNet KeySecure Management Console bbkeysecure  
Logged in as **admin**  
[Help](#) | [Log Out](#)

Home Security **Device**

**Device Configuration**

- Key Server
- Key Server
- Health Check
- Cluster
- Date & Time
- Network
- SNMP
- Administrators
- SSH Public Key
- Known Hosts

**Logs & Statistics**

- Log Configuration
- Log Viewer
- Statistics

**Maintenance**

- Backup & Restore
- Services
- System Information & Upgrade
- System Health
- Network Diagnostics

Device > Key Server > Key Server

**Cryptographic Key Server Configuration**

**Cryptographic Key Server Settings** [Help](#)

Protocol	IP	Port	Use SSL	Server Certificate
<a href="#">NAE-XML</a>	[All]	9000	<input type="checkbox"/>	[None]
<input checked="" type="radio"/> KMIP	[All]	9002	<input checked="" type="checkbox"/>	kmipservercert

[Save](#) [Cancel](#)

**User Directory Settings** [Help](#)

User Directory: Local

[Edit](#)

**User Account Lockout Settings** [Help](#)

Enable Account Lockout: ☒

Number of Failed Authentication Attempts Before Account Lockout: 3

Account Lockout Duration (sec): 60

[Edit](#)

Edit the authentication settings of the Cryptographic Key Server Settings, “Client Certificate Authentication” to be “Used for SSL session only” and “Trusted CA List Profile” as “Default”.

The screenshot displays the SafeNet KeySecure Management Console interface. The top navigation bar includes the Gemalto logo, the title "SafeNet KeySecure Management Console", and user information "bbkeysecure" logged in as "admin" with links for "Help" and "Log Out". The main navigation menu on the left is divided into three sections: "Device Configuration" (containing Key Server, Health Check, Cluster, Date & Time, Network, SNMP, Administrators, SSH Public Key, and Known Hosts), "Logs & Statistics" (containing Log Configuration, Log Viewer, and Statistics), and "Maintenance" (containing Backup & Restore, Services, System Information & Upgrade, System Health, and Network Diagnostics). The "Device" tab is selected, leading to the "Key Server" configuration page. The breadcrumb trail shows "Device > Key Server > Key Server". The page title is "Cryptographic Key Server Configuration". The "Cryptographic Key Server Properties" section includes fields for Protocol (KMIP), IP ([All]), Port (9002), Use SSL (checked), Server Certificate (keysecurecert), Connection Timeout (sec) (3600), Allow Key and Policy Configuration Operations (checked), and Allow Key Export (checked). Below this is an "Edit" button and a "Back" button. The "Authentication Settings" section includes fields for Password Authentication (Not Used), Client Certificate Authentication (Used for SSL session only), Trusted CA List Profile (Default), Username Field in Client Certificate ([None]), and Require Client Certificate to Contain Source IP (unchecked). An "Edit" button is located below this section.

**gemalto** SafeNet KeySecure Management Console

bbkeysecure  
Logged in as admin  
[Help](#) | [Log Out](#)

Home Security **Device**

**Device Configuration**

- Key Server
- Key Server
- Health Check
- ⊕ Cluster
- Date & Time
- ⊕ Network
- ⊕ SNMP
- ⊕ Administrators
- SSH Public Key
- Known Hosts

**Logs & Statistics**

- ⊕ Log Configuration
- ⊕ Log Viewer
- ⊕ Statistics

**Maintenance**

- ⊕ Backup & Restore
- Services
- System Information & Upgrade
- System Health
- Network Diagnostics

[Device](#) > [Key Server](#) > Key Server

**Cryptographic Key Server Configuration**

**Cryptographic Key Server Properties** [Help](#) ?

Protocol:	KMIP
IP:	[All]
Port:	9002
Use SSL:	<input checked="" type="checkbox"/>
Server Certificate:	keysecurecert
Connection Timeout (sec):	3600
Allow Key and Policy Configuration Operations:	<input checked="" type="checkbox"/>
Allow Key Export:	<input checked="" type="checkbox"/>

[Edit](#) [Back](#)

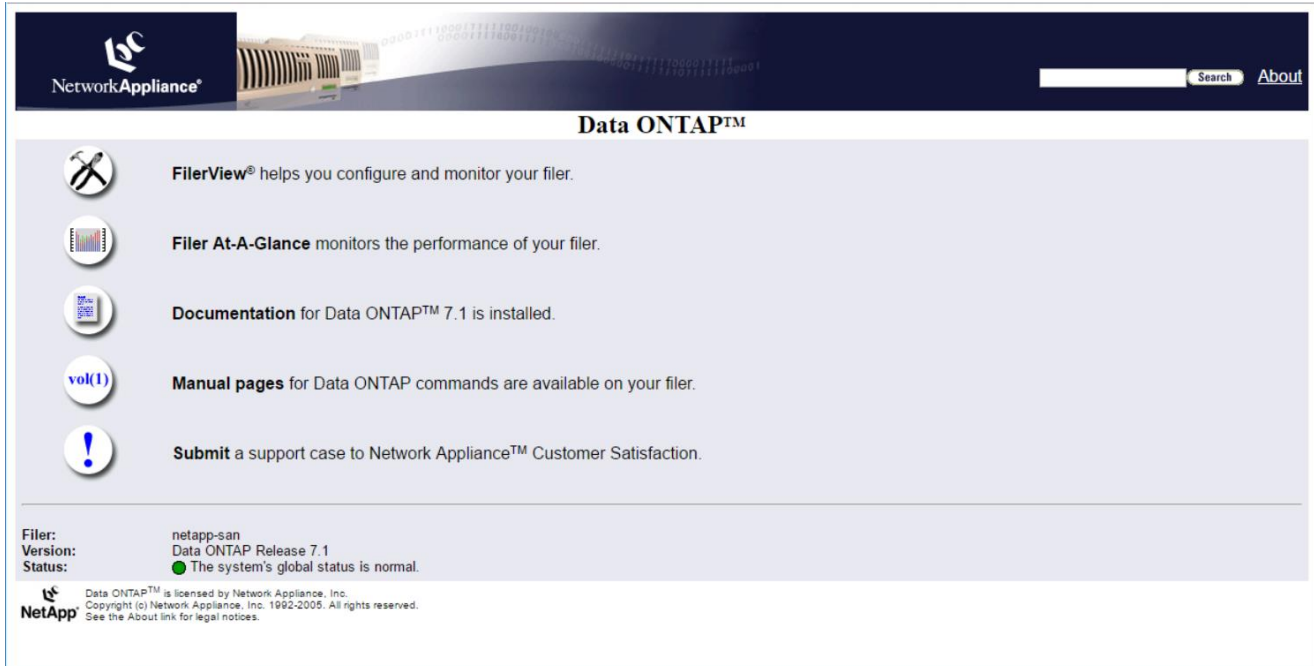
**Authentication Settings** [Help](#) ?

Password Authentication:	Not Used
Client Certificate Authentication:	Used for SSL session only
Trusted CA List Profile:	Default
Username Field in Client Certificate:	[None]
Require Client Certificate to Contain Source IP:	<input type="checkbox"/>

[Edit](#)

# NetApp FAS Storage

NetApp FAS virtual appliance is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.









The screenshot shows the NetApp Data ONTAP web interface. The header includes the Network Appliance logo and a search bar. The main content area is titled "Data ONTAP™" and lists several links: FilerView®, Filer At-A-Glance, Documentation for Data ONTAP™ 7.1, Manual pages, and a link to submit a support case. Below this, the status of the filer is displayed: "netapp-san Data ONTAP Release 7.1" and "The system's global status is normal." The footer contains the NetApp logo and copyright information.

NetworkAppliance®

Search About

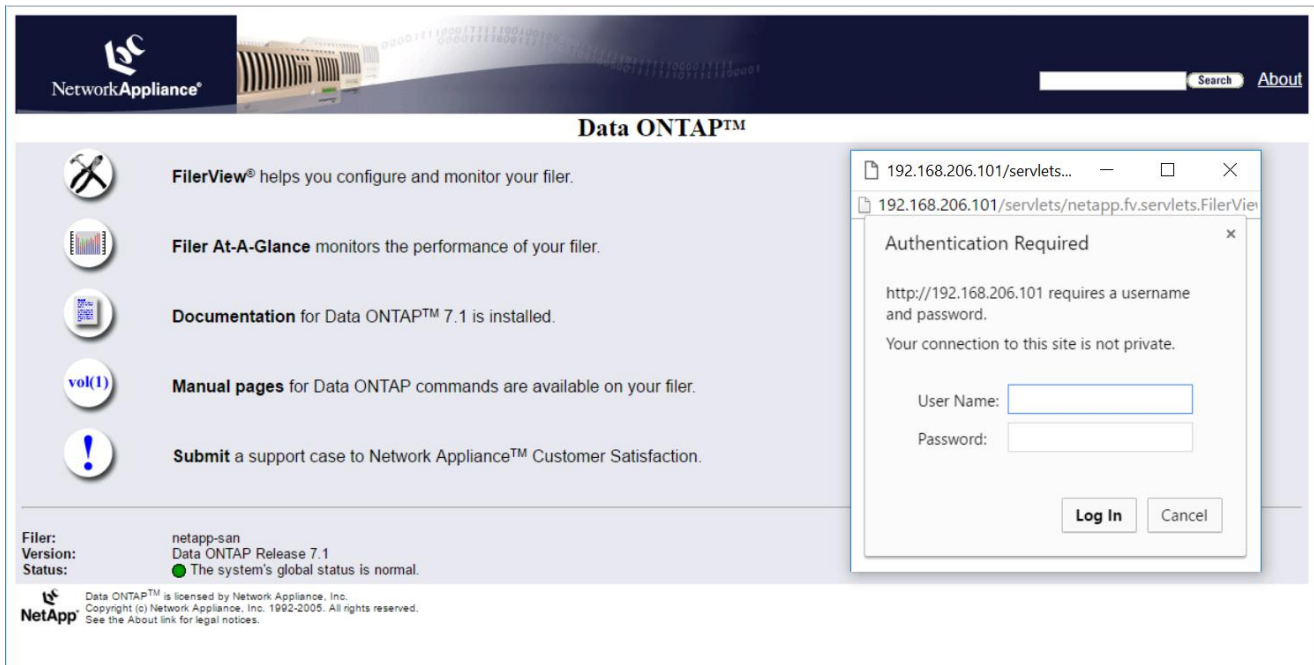
**Data ONTAP™**

-  **FilerView®** helps you configure and monitor your filer.
-  **Filer At-A-Glance** monitors the performance of your filer.
-  **Documentation** for Data ONTAP™ 7.1 is installed.
-  **Manual pages** for Data ONTAP commands are available on your filer.
-  **Submit** a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san  
Version: Data ONTAP Release 7.1  
Status:  The system's global status is normal.

NetApp Data ONTAP™ is licensed by Network Appliance, Inc.  
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.  
See the About link for legal notices.

NetApp FAS is a unified storage system supporting multiple network storage protocols including NFS, CIFS, HTTP, FC, FCoE, iSCSI, etc.









This screenshot is similar to the previous one, but it includes an "Authentication Required" dialog box. The dialog box is titled "192.168.206.101/servlets..." and contains the text: "http://192.168.206.101 requires a username and password. Your connection to this site is not private." It has input fields for "User Name:" and "Password:" and buttons for "Log In" and "Cancel".

NetworkAppliance®

Search About

**Data ONTAP™**

-  **FilerView®** helps you configure and monitor your filer.
-  **Filer At-A-Glance** monitors the performance of your filer.
-  **Documentation** for Data ONTAP™ 7.1 is installed.
-  **Manual pages** for Data ONTAP commands are available on your filer.
-  **Submit** a support case to Network Appliance™ Customer Satisfaction.

Filer: netapp-san  
Version: Data ONTAP Release 7.1  
Status:  The system's global status is normal.

NetApp Data ONTAP™ is licensed by Network Appliance, Inc.  
Copyright (c) Network Appliance, Inc. 1992-2005. All rights reserved.  
See the About link for legal notices.

192.168.206.101/servlets...  
192.168.206.101/servlets/netapp.fv.servlets.FilerView

**Authentication Required**

http://192.168.206.101 requires a username and password.  
Your connection to this site is not private.

User Name:   
Password:

Log In Cancel

CIFS and NFS storage resources are provisioned on NetApp FAS to be used in this testing.

NetAppAppliance®

netapp-san

• Filer

• Volumes

Add

Manage

• Qtrees

• Quotas

• Snapshots

• Aggregates

• Storage

• DFM

• CIFS

• NFS

Add Export

Report

Configure

Manage Exports

• HTTP

• LUNs

• Network

• Security

• Secure Admin

• NDMP

• SNMP

• Real Time Status

• Wizards

FilerView®

[About](#)

Manage Volumes

Volumes → Manage

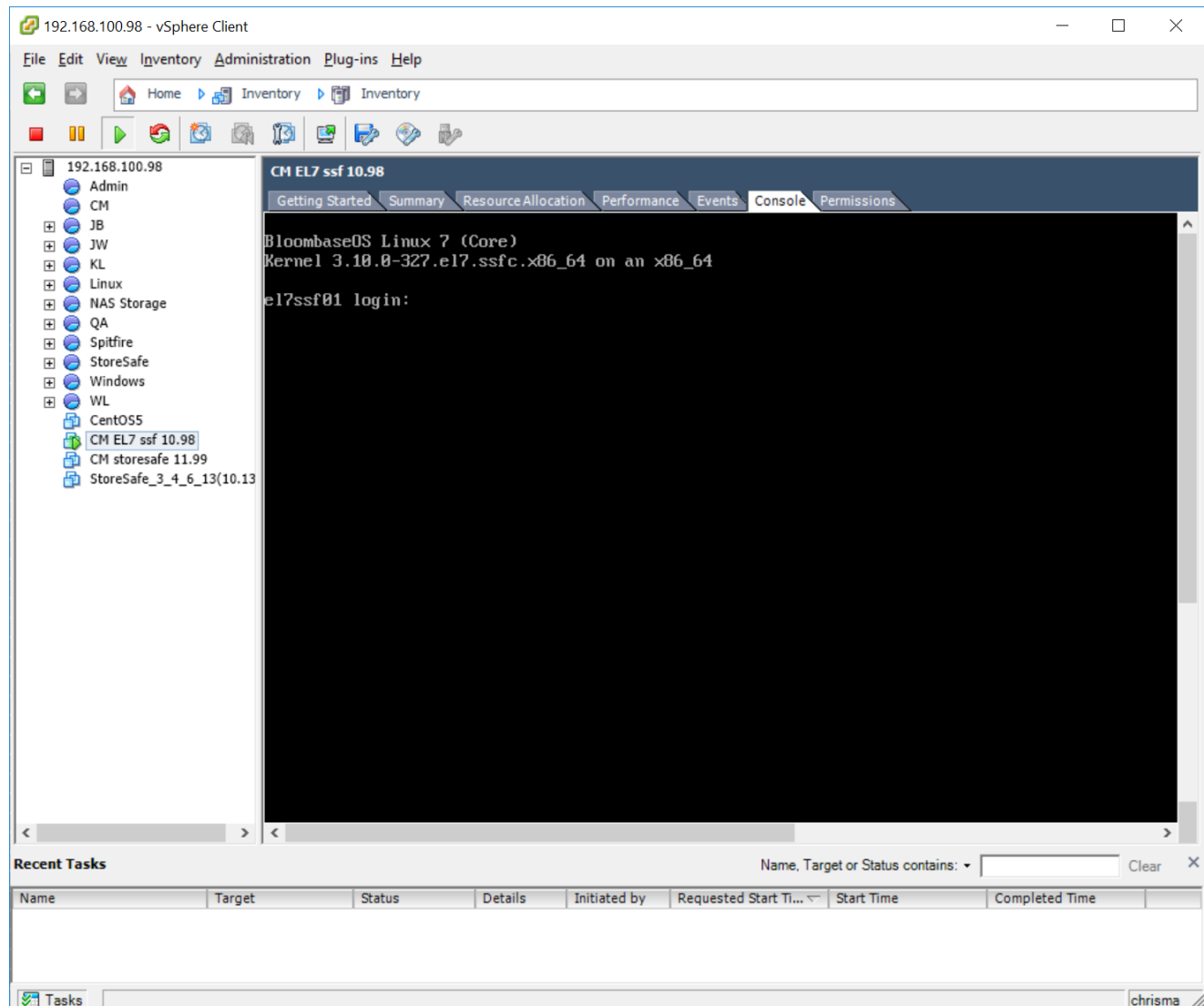
Filter by: All Volumes

Name	Status	Root	Containing Aggregate	Avail	Used	Total	Files	Max Files
<input type="checkbox"/> <a href="#">vol0</a>	online	✓	<a href="#">aggr0</a>	109 MB	57%	255 MB	7.37 k	8.6 k
<a href="#">Select All</a> - <a href="#">Unselect All</a>				<input type="button" value="Online"/>	<input type="button" value="Restrict"/>	<input type="button" value="Offline"/>	<input type="button" value="Destroy"/>	

Volumes: 1-1 of 1

# Bloombase StoreSafe

Bloombase StoreSafe delivers unified data-at-rest encryption security of block storage volumes, files, objects, sequential storage devices, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Gemalto SafeNet KeySecure.



Bloombase StoreSafe software appliance is deployed as a virtual appliance (VA) on VMware ESXi.

## Network Security, Trust and Authentication Configuration

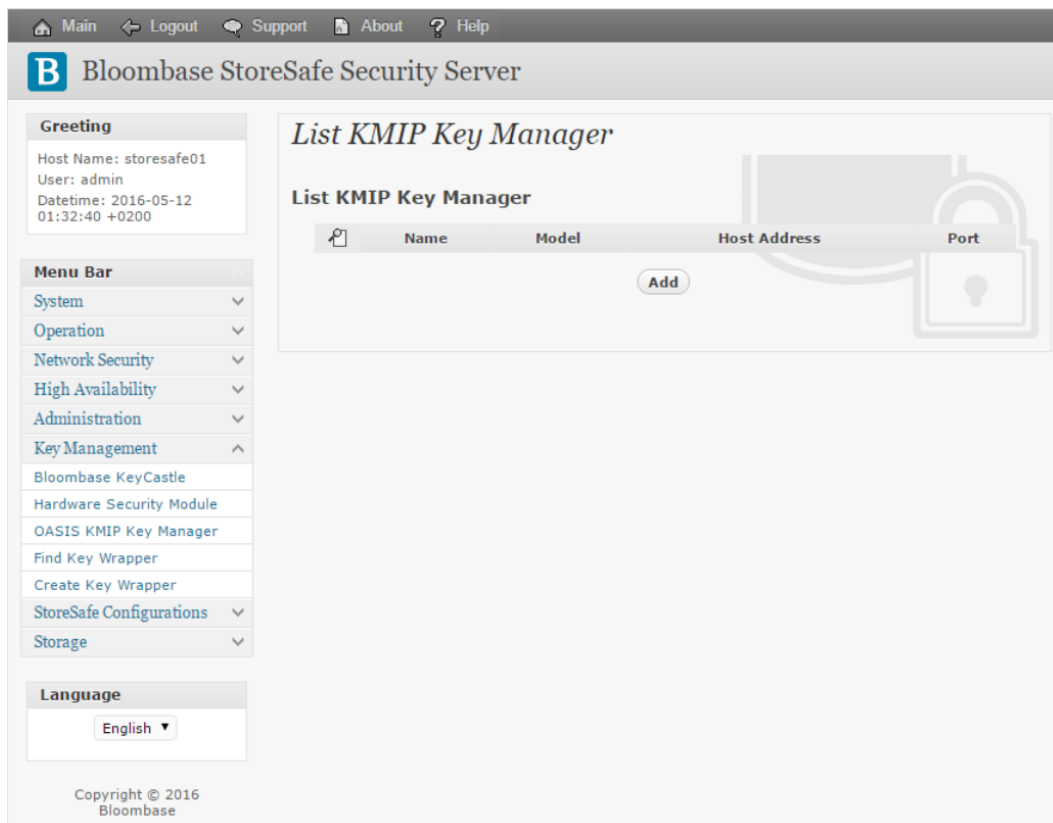
In this interoperability test effort, Bloombase StoreSafe serves as the user of Gemalto SafeNet KeySecure for encryption key access to deliver data at-rest encryption services. Authentication of Bloombase StoreSafe to the Gemalto SafeNet KeySecure is done with signed certificates through SSL communications.

## Gemalto SafeNet KeySecure and Bloombase KeyCastle Integration

Bloombase supports Gemalto SafeNet KeySecure out of the box due to the fact that both support OASIS Key Management Interoperability Protocol (KMIP).

X.509 key pair “CN=bloombaseca, OU=StoreSafe, O=Bloombase, L=Sunnyvale, ST=CA, C=US” is created, signed by the newly created local root CA in the Gemalto SafeNet KeySecure, and assigned as the authentication key pair for Bloombase StoreSafe.

To enable the built-in Bloombase KeyCastle to utilize keys managed in the network attached Gemalto SafeNet KeySecure, the KMIP service configuration at Bloombase web management console has to be set up. This is done by clicking “OASIS KMIP Key Manager” under “Key Management”.



Input a name for the Gemalto SafeNet KeySecure, and select Model as 'SafeNet KeySecure'. Input also the host address and port to access the SafeNet KeySecure, and import the signed X.509 key pair as "Client Keystore", the certificate of the local root CA on Gemalto SafeNet KeySecure as "Trust Certificate".

### Modify KMIP Key Manager

**Modify KMIP Key Manager**

Name

Model

Host Address

Port

Username

Password

Test Results : Success

### Client Keystore

Subject Name CN=StoreSafeCert  
OU=StoreSafe  
O=Bloombase  
L=Sunnyvale  
ST=CA  
C=US

Serial Number 562d

Issuer Name EMAILADDRESS=admin@bloombase.com  
CN=bloombaseca  
OU=StoreSafe  
O=Bloombase  
L=Sunnyvale  
ST=CA  
C=US

Valid Start Date 2016-05-11

Valid End Date 2026-05-09

Client Keystore File  No file selected.

Pin

### Trust Certificate

Subject Name EMAILADDRESS=admin@bloombase.com  
CN=bloombaseca  
OU=StoreSafe  
O=Bloombase  
L=Sunnyvale  
ST=CA  
C=US

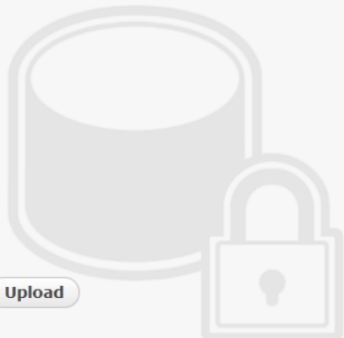
Serial Number 00

Issuer Name EMAILADDRESS=admin@bloombase.com  
CN=bloombaseca  
OU=StoreSafe  
O=Bloombase  
L=Sunnyvale  
ST=CA  
C=US

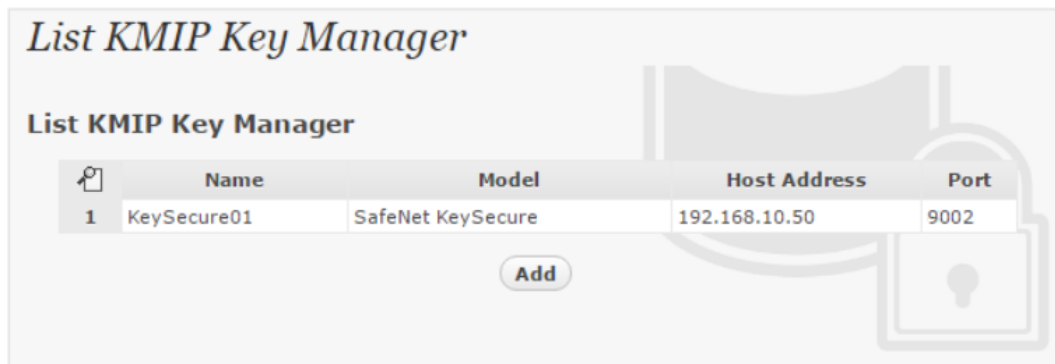
Valid Start Date 2016-05-11

Valid End Date 2026-05-10

Trust Certificate File  No file selected.



Click 'Submit' to commit the configuration. If the certificates are setup properly, "test results" of the KMIP Key Manager would return "Success".



*List KMIP Key Manager*

**List KMIP Key Manager**

	Name	Model	Host Address	Port
1	KeySecure01	SafeNet KeySecure	192.168.10.50	9002

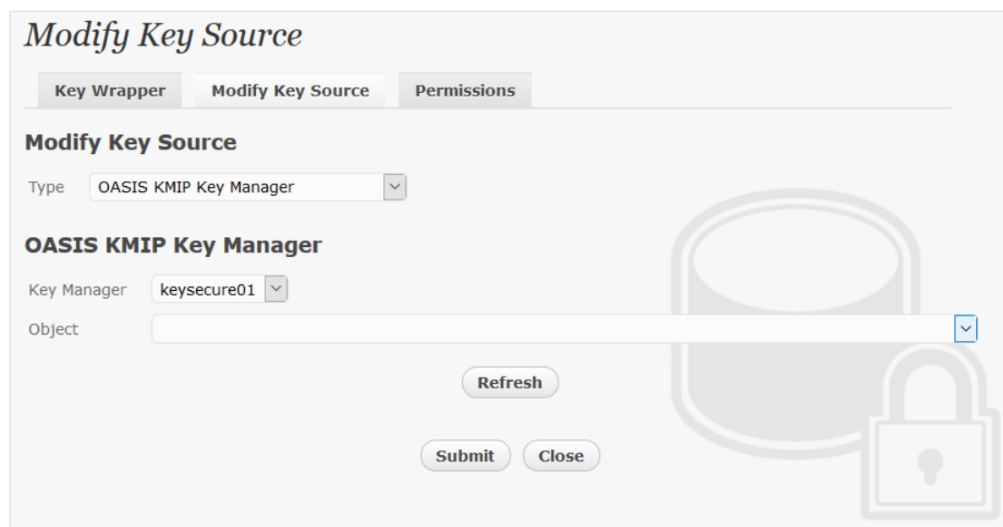
**Add**

## Encryption Key Provisioning

Generate encryption key with name 'key01' in bundled Bloombase KeyCastle key life-cycle management tool.

First configure the key source of the wrapping key as "OASIS KMIP Key Manager" with Gemalto SafeNet KeySecure as the "Key Manager".

If the encryption key is present in the Gemalto SafeNet KeySecure, select it from the dropdown menu of "Object" and click "submit".



*Modify Key Source*

**Key Wrapper** **Modify Key Source** **Permissions**

**Modify Key Source**

Type

**OASIS KMIP Key Manager**

Key Manager

Object

**Refresh**

**Submit** **Close**



Otherwise, in order to generate the key in the attached Gemalto SafeNet KeySecure, leave the “Object” field as empty and turn to the “Key Wrapper” tab to input the name of the key and click ‘Generate’.

**Modify Key Wrapper**

Key Wrapper   Modify Key Source   Permissions

**Modify Key Wrapper**

Name: key01

Type: Symmetric

Active: ☒

KMIP Key Manager: keysecure01

KMIP UUID:

KMIP Key Name:

Key Bit Length: 256

Owner: admin

Last Update Datetime:

Generate

Submit   Close

The key is then generated in the attached Gemalto SafeNet KeySecure.

**Modify Key Wrapper**

Key Wrapper   Modify Key Source   Permissions

**Modify Key Wrapper**

Name: key01

Type: Symmetric

Active: ☒

KMIP Key Manager: keysecure01

KMIP UUID: 487C7F77FD51FC2C791C911E6D96017C39A94EB007A092D9E640301826DF36EF

KMIP Key Name: key01

Key Bit Length: 256

Owner: admin

Last Update Datetime:

Submit   Close

Notice that only symmetric keys are generated and accessed through KMIP Key Managers.

## Backend Physical Storage Configuration

Physical storage namely 'share01' is configured to be secured by Bloombase StoreSafe using encryption.

### Modify Storage Configuration

**Physical Storage****Permissions**

#### Physical Storage Configuration

Name	share01
Description	
Physical Storage Type	Remote
Type	Common Internet File System (CIFS)
Host	192.168.10.180
Share Name	share01
Read Size	
Write Size	
Synchronous	<input type="checkbox"/>
Mount Hard	<input type="checkbox"/>
User	Administrator
Password	
Options	
Owner	admin
Last Update Datetime	2014-02-13 10:07:40 +0800



## Secure Storage Configuration

Virtual storage namely 'share01' of type 'File' is created to virtualize physical storage 'share01' for application transparent encryption protection over network file protocols including CIFS and NFS.

### Modify Virtual Storage

Virtual Storage

Protection

Access Control

Permissions

#### Modify Virtual Storage

Name

share01

Status

☒

Description

Active

☒

Mode

File

Owner

admin

Last Update Datetime

2014-02-13 10:09:11 +0800

#### Settings

Offline Setting

Disabled ▼

#### Physical Storage

Storage

share01 🔑 🔗

Description

Physical Storage Type

Remote

Submit

Delete

Close



Protection type is specified as 'Privacy' and secure the backend EMC VNX storage using AES 256-bit encryption and encryption key 'key01' managed at Gemalto SafeNet KeySecure.

### Modify Virtual Storage Handler

**Virtual Storage** Protection Access Control Permissions

#### Virtual Storage Protection

Protection Type Privacy ▼

#### Encryption Keys

	Key Name	Last Update Datetime
1 <input type="checkbox"/>	key01	2016-05-11 10:09:11 +0800


Add Remove

#### Cryptographic Cipher

Cipher Algorithm AES ▼

Bit Length 256 ▼

Submit Close



CIFS storage protocol relies mainly on user-password authentication for access control. In this test, the Bloombase StoreSafe secure storage resource 'share01' is provisioned for user 'user01' with Microsoft Active Directory integration for user-password authentication and single sign-on.

### Modify Virtual Storage Access Control

**Virtual Storage** Protection **Access Control** Permissions

#### User Access Control

Default ☐ Read ☐ Write

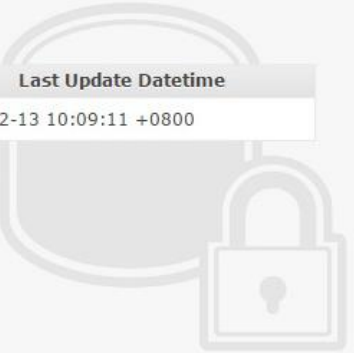
User Repository Microsoft Active Directory (MSAD) ▼

	User	Access Control List	Last Update Datetime
1 <input type="checkbox"/>	<span>user01 ▼</span>	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	2014-02-13 10:09:11 +0800

Add Remove

▼ More Options

Submit Close



# Conclusion

Key management system

- Gemalto SafeNet KeySecure

passed all Bloombase interopLab's interoperability tests with Bloombase StoreSafe

Bloombase Product	Operating System	Hardware Security Module
Bloombase StoreSafe	Microsoft Windows Server	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>
	Red Hat Enterprise Linux (RHEL)	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>
	SUSE Linux Enterprise Server (SLES)	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>
	Oracle Solaris	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>
	IBM AIX	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>
	HP-UX	<ul style="list-style-type: none"><li>• Gemalto SafeNet KeySecure</li></ul>



# Disclaimer

The tests described in this paper were conducted in the Bloomberg InteropLab. Bloomberg has not tested this configuration with all the combinations of hardware and software options available. There may be significant differences in your configuration that will change the procedures necessary to accomplish the objectives outlined in this paper. If you find that any of these procedures do not work in your environment, please contact us immediately.

# Technical Reference

1. Bloombase StoreSafe Technical Specifications, <http://www.bloombase.com/content/8936QA88>
2. Bloombase StoreSafe Hardware Compatibility Matrix, <http://www.bloombase.com/content/e8Gzz281>
3. Gemalto SafeNet KeySecure, <http://www.safenet-inc.com/data-encryption/enterprise-key-management/key-secure/>