



Interoperability of Bloombase StoreSafe and Futurex Vectera HSM for Data-at-Rest Encryption

August 2019



Executive Summary

Futurex Vectera Hardware Security Module (HSM) 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 Futurex Vectera HSM 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 have been tested with Futurex Vectera and Bloombase StoreSafe to secure Microsoft Storage Server on Microsoft Windows Server 2019 as the storage backend.

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 Bloomberg, Inc.

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

© 2019 Bloomberg, Inc.

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

Futurex and Vectera are trademarks of Futurex, LP or its affiliated companies.

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

Document No.: BLBS-TN-Bloomberg-StoreSafe-Futurex-Vectera-HSM-Interoperability-USLET-EN-Ro.92

Table of Contents

Table of Contents	3
Purpose and Scope	5
Assumptions	6
Infrastructure	7
Setup	7
Hardware Security Module	9
Bloombase StoreSafe	9
Storage System	9
Client Hosts	9
Configuration Overview	10
Futurex Vectera	10
Enabling PKCS#11 communication on Futurex Vectera	10
Creating a Key Profile	11
Futurex Vectera Client Setup	12
Microsoft Storage Server on Microsoft Windows Server 2016	14
Bloombase StoreSafe	15
Futurex Vectera and Bloombase KeyCastle Integration	17
Encryption Key Provisioning	18
Backend Physical Storage Configuration	21
Secure Storage Configuration	22
Conclusion	26
Disclaimer	27
Acknowledgement	28
Technical Reference	29

Purpose and Scope

This document describes the steps necessary to integrate Futurex Vectera Hardware Security Module (HSM) with Bloomberg StoreSafe to secure sensitive enterprise business persistent data managed in storage systems. Specifically, we cover the following topics:

- Install and configure Bloomberg StoreSafe
- Integrate Bloomberg StoreSafe with Futurex Vectera
- Interoperability testing on client host systems including Linux, Windows, IBM AIX, HP-UX and Oracle Sun Solaris with Microsoft Storage Server as storage backend

Assumptions

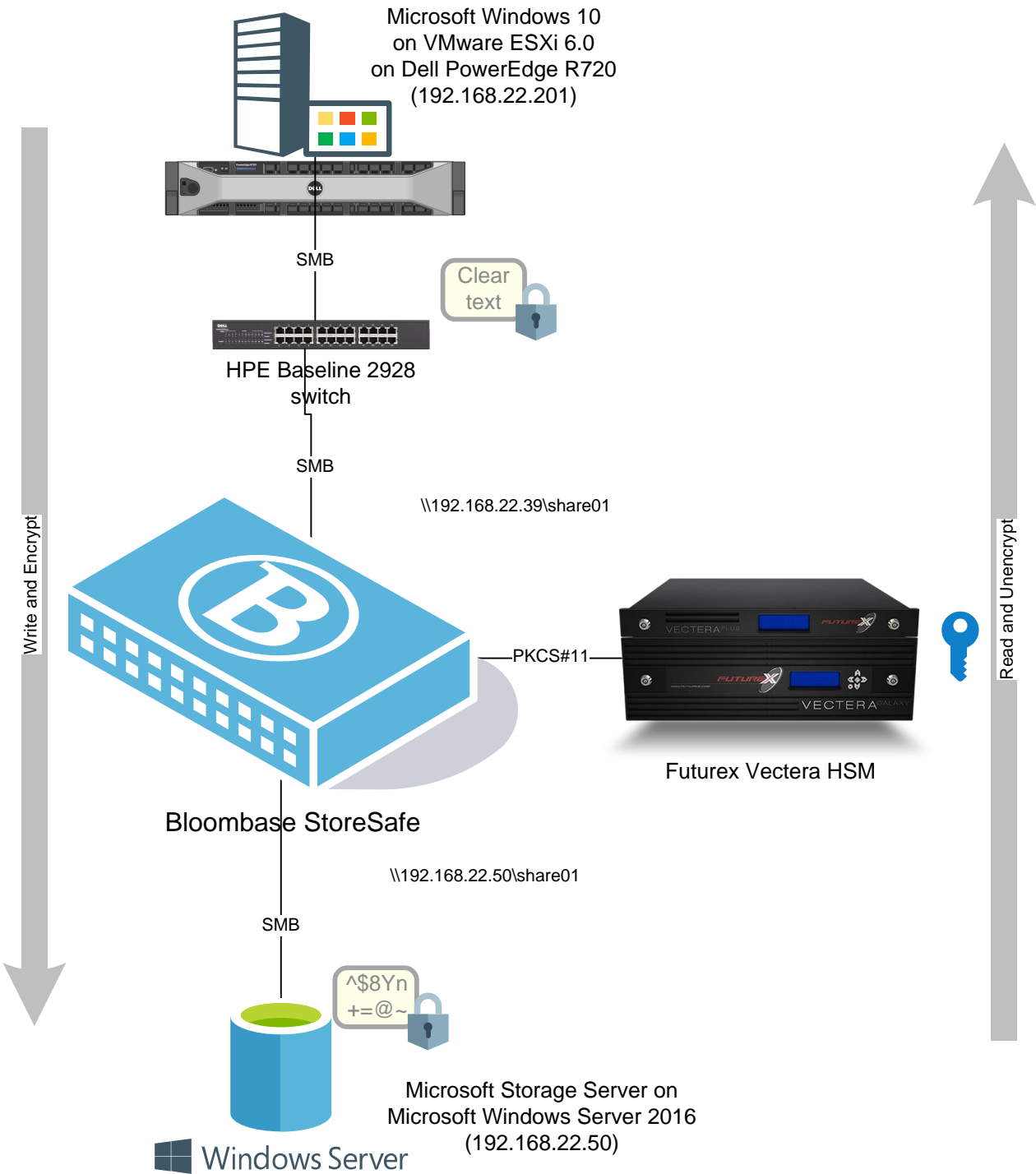
This document describes interoperability testing of Futurex Vectera with Bloombase StoreSafe. Therefore, it is assumed that you are familiar with operation of Futurex Vectera, storage systems and major operating systems including Linux, Microsoft Windows, IBM AIX, HP-UX and Oracle Sun Solaris. It is also assumed that you possess basic UNIX administration skills. The examples provided may require modifications before they are run under your version of operating system.

As Futurex Vectera is third party hardware option to Bloombase StoreSafe data at-rest encryption security solution, you are recommended to refer to installation and configuration guides of specific model of Futurex Vectera for your actual use case. We assume you have basic knowledge of storage networking and information cryptography. For specific technical product information of Bloombase StoreSafe, please refer to our website at <https://www.bloombase.com> or Bloombase SupPortal <https://supportal.bloombase.com>.

Infrastructure

Setup

The validation testing environment is setup as in below diagram



Hardware Security Module

Hardware Security Module	Futurex Vectera HSM
Firmware Version	6.5.3.8

Bloombase StoreSafe

Bloombase StoreSafe	Bloombase StoreSafe Software Appliance v3.4.7
Futurex Client Software Package	4.1
FIPS Mode	Non-strict FIPS security world
Server	VMware Virtual Machine (VM) on VMware ESXi 6.0
Processor	4 x Virtual CPU (vCPU)
Memory	8 GB

Storage System

Storage System	Microsoft Storage Server on Microsoft Windows Server 2016 on VMware ESXi 6.0
----------------	--

Client Hosts

Hardware	Dell PowerEdge R720
Hypervisor	VMware ESXi 6.0
Operating System	Microsoft Windows 10

Configuration Overview

Futurex Vectera

Enabling PKCS#11 communication on Futurex Vectera

In order to utilize the Futurex Vectera as an external key manager, it must allow communication through the PKCS#11 protocol.

This requires the “General-Purpose Cryptographic License” on the Futurex HSM. To check for this license, access the web portal on your HSM. Under the Features tab check the status of the line labelled PKCS11 Ability. It should say Enabled.

Status	COM	Features	Firmware	IP	Misc	Msg Log	SSL/TLS	Time
Update Feature Settings								
Speed:	2250							
CPIN Functions:	Enabled ▼							
Command Set:	Excrypt and Kryptos Command Set ▼							
PCE Mode:	Disabled ▼							
RSA Functions:	Enabled ▼							
ECC Functions:	Enabled ▼							
Excrypt UI:	Enabled ▼							
Clear Keyload:	Disabled ▼							
Bulk Encryption Functions:	Disabled ▼							
EMV Transaction Validation Ability:	Enabled ▼							
EMV Card Issuance Ability:	Enabled ▼							
FPE Ability:	Enabled ▼							
Admin Port:	Enabled ▼							
FIPS Ability:	Disabled ▼							
PCI-HSM Ability:	Disabled ▼							
PIN Mailer Ability:	Enabled ▼							
P2PE/Tokenization:	Enabled ▼							
PKCS11 Ability:	Enabled ▼							
Futurex Signed Certificates Ability:	Enabled ▼							
IRIS Ability:	Disabled ▼							
Command Primary Mode:	GP ▼							
Command Extension Mode:	Financial Extensions ▼							
Multibanco Ability:	Enabled ▼							
SCSA Ability:	Enabled ▼							
Key Block abilities:	AKB:☑ ANSI (TR31):☑							
Feature Update Request:	Download							

Creating a Key Profile

Bloombase StoreSafe requires multi-purpose keys in order to encrypt and decrypt data as well as other keys functions. A custom profile must be created to allow for multi-purpose keys.

Accessing the Futurex Vectera web portal, please select "add usage" under Vectera Plus->Web Portal Configuration Panel->Common Miscellaneous Settings. Note that a profile will need to be created with the following usage: EDWUSVX

Common Miscellaneous Settings

Transactions in log:	Disabled ▾								
Store stats in storage:	<input type="checkbox"/>								
Verify PIN/PIN-Offset lengths:	<input type="checkbox"/>								
Enable distressed PIN (backwards):	<input type="checkbox"/>								
Note: Allows another value for the PIN									
Enable simplified parsing:	<input type="checkbox"/>								
Decimalization table format:	Clear ▾								
Require 4 digit VISA PINs:	<input type="checkbox"/>								
Allow PIN block translation from stronger to weaker formats:	<input type="checkbox"/>								
RSA Blinding:	<input checked="" type="checkbox"/>								
Allow weak keys:	<input checked="" type="checkbox"/>								
Allow access for single operations users:	<input type="checkbox"/>								
Check incoming key integrity:	<input type="checkbox"/>								
Key Usage Combinations:	Authorized Asymmetric ▾ Add usage								
	<table border="1"> <tr><td>ED</td><td>-</td></tr> <tr><td>SV</td><td>-</td></tr> <tr><td>WU</td><td>-</td></tr> <tr><td>X</td><td>-</td></tr> </table>	ED	-	SV	-	WU	-	X	-
ED	-								
SV	-								
WU	-								
X	-								
Max servicer request message length (15360 - 512032):	15360 (1000 max connections)								

Key Usage Combinations: Allows multipurpose keys to be generated. Typically in high assurance environments, keys are bound to a single usage. However, various key usage combinations can be defined if required by an application integration. To define a new key usage combination, first select Authorized Asymmetric or Anonymous Asymmetric from the drop-down to specify which type of user can generate the key. Then select Add Usage. On the dialog window, select the applicable key usage options and select Save.

The above instructions can also be found in your Futurex Vectera user guide.

Futurex Vectera Client Setup

To communicate with the HSM, users must first configure the Futurex PKCS #11 library. This section describes the configuration files, the available options, and the configuration options necessary for establishing connection. The Futurex PKCS #11 library can be configured with a text editor or through the “Futurex Config Tool” application, which provides users a graphical user interface (GUI) through which to edit configuration options.

The configuration file, fxpkcs-11 software, and TLS certificates should be uploaded to the Bloomberg StoreSafe and placed in the correct directories.

The default location where the configuration file is read from is:

```
/etc/fxpkcs11.cfg
```

The fxpkcs-11 software should be extracted to the following directory:

```
/opt/fxpkcs11/
```

Note: it is required to use the `fxpkcs11-redhat` software.

The TLS certificates can be placed in any directory but their paths must be declared in the configuration file under the following options:

```
<PROD-TLS-CA>          </PROD-TLS-CA>
<PROD-TLS-CERT>        </PROD-TLS-CERT>
<PROD-TLS-KEY>         </PROD-TLS-KEY>
```

Run command

```
/opt/fxpkcs11/x64/OpenSSL-1.0.x/PKCS11Manager
```

as the sanity check for if everything is working on the HSM and PKCS#11 layer.

```
Library Information:
    Manufacturer: Futurex
    Library: FxPKCS11
    Cryptoki Version: 2.20
    Library Version: 4.1
    Library Flags: 00000000
[2019-07-25 02:47:50] | INFO | 7F3579A1B880 | C_GetSlotInfo: Slot
0 Flags: 0000
0007.

Slot Information:
    Slot: 0
    Manufacturer: Futurex
    Description: Futurex Cryptoki Slot #0
    Hardware Version: 0.0
    Firmware Version: 4.1
    Flags: 00000007
[2019-07-25 02:47:50] | INFO | 7F3579A1B880 | C_GetTokenInfo:
Token Flags: 0000
064D.

Token Information:
    Manufacturer: Futurex
    Token: us01hsm01test.virtucrypt.com:592
    Model: HSM
    Serial Number: 1831800266
    Flags: 0000064D
    Time on HSM:

Session Information:
    Session: 1
    Slot: 0
    State: 3
    Flags: 00000006
    Device Error: 00000000
```

In this interoperability test, Slot 0 has been used for key protection with the HSM as in the Bloombase StoreSafe registry.

HSM PKCS#11 integration uses standard SunPKCS11 provider. This makes selection of slot customer configurable. This can optionally be reconfigured, by modifying

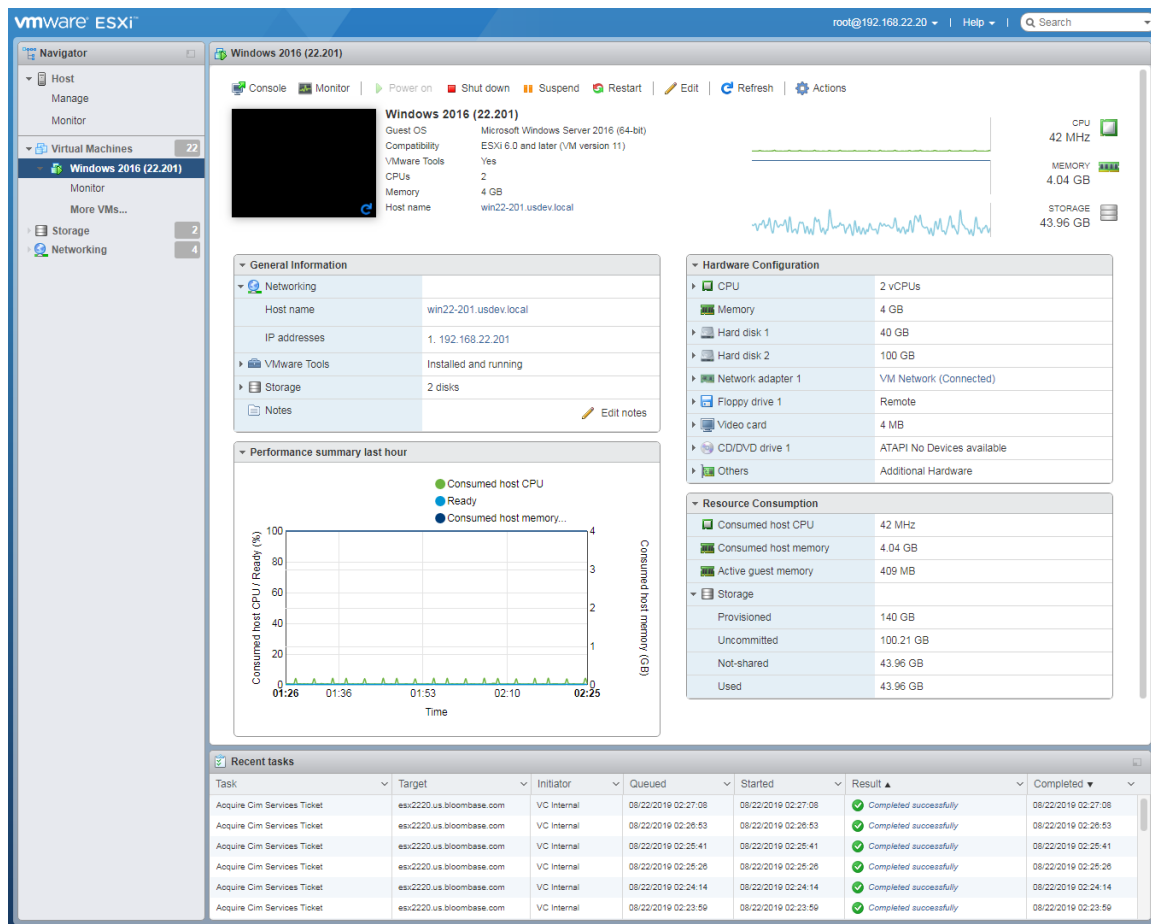
```
slotListIndex
```

entry in Bloombase StoreSafe.

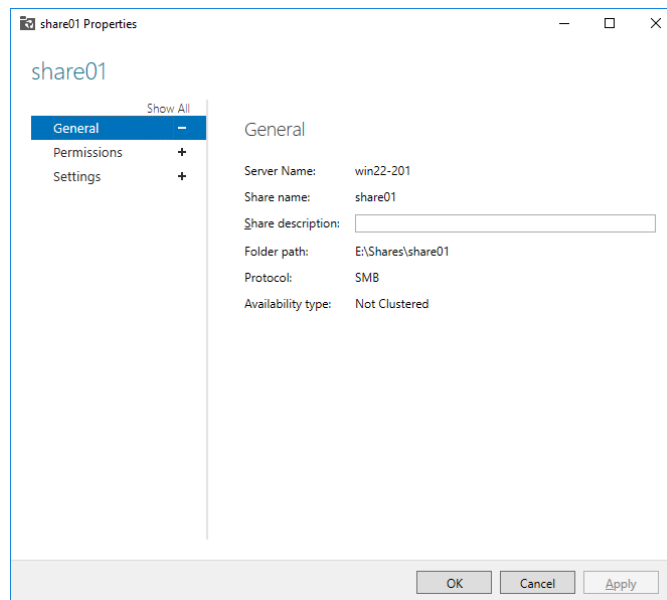
Please refer to “nShield Connect User Guide” for detailed setup and configurations.

Microsoft Storage Server on Microsoft Windows Server 2016

Microsoft Windows Server 2016 is used in this interoperability test which is able to provide storage services over network storage protocols including NFS, CIFS, iSCSI, etc.

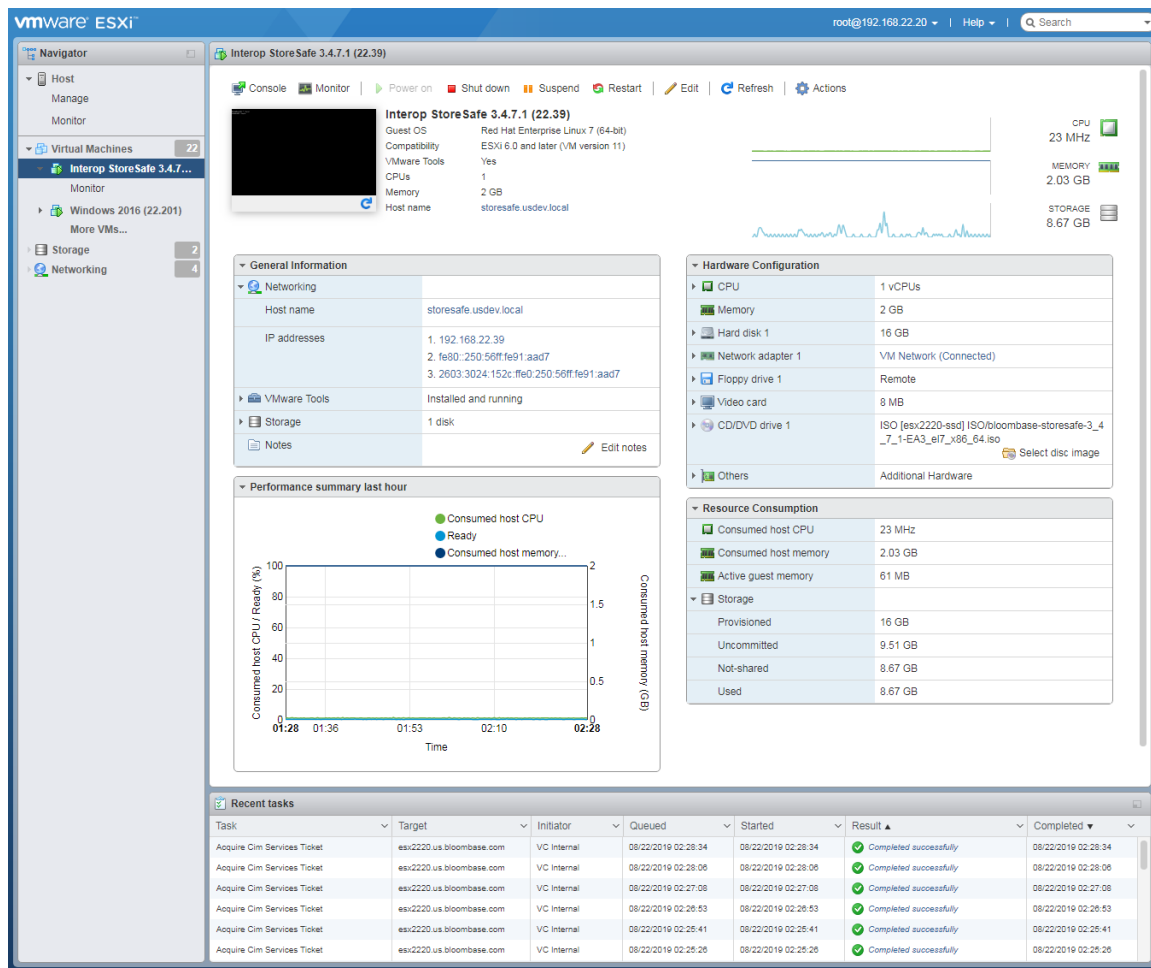


A Windows network share is provisioned for Bloombase StoreSafe encryption using keys from Futurex Vectera HSM.



Bloombase StoreSafe

Bloombase StoreSafe delivers unified data at-rest encryption security of files, block devices, objects, sequential storages, etc. In this interoperability test, file-based encryption security service is validated against Bloombase StoreSafe with keys managed at Futurex Vectera HSM.



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

The screenshot displays the Bloombase StoreSafe Security Server web management console. The interface includes a top navigation bar with links for Main, Logout, Support, About, and Help. The main header shows the Bloombase logo and the title 'Bloombase StoreSafe Security Server'.

On the left side, there is a 'Greeting' section with the following information:

- Host Name: storesafe.usdev.local
- User: admin
- Datetime: 2019-07-28 21:23:34 -0700

Below the greeting is a 'Menu Bar' with the following items:

- System
- Operation
- High Availability
- Administration
- Key Management (expanded)
- Bloombase KeyCastle
- Hardware Security Module
- OASIS KMIP Key Manager
- Cloud Key Managers
- Find Key Wrapper
- Create Key Wrapper
- StoreSafe Configurations
- Storage

At the bottom left, there is a 'Language' section with a dropdown menu set to 'English'.

The main content area is titled 'Find Key Wrapper' and contains a search form with the following fields:

- Name: (text input)
- Type: Asymmetric (dropdown)
- Active: Active (dropdown)
- CA: (dropdown)

Below the search form are buttons for 'Find', 'Reset', and 'Add'. A 'More Options' link is also present.

The search results are displayed in a table with the following columns:

	Name	Type	Key Source Type	Active	Status	CA	Subject DN	Issuer DN	Effective Datetime	Expiry Datetime	Last Update Datetime
1	key01	Asymmetric	Hardware Security Module	<input checked="" type="checkbox"/>	Valid		CN=ssf-key01	CN=ssf-key01	2019-07-25 15:58:31 -0700	2029-07-22 15:58:31 -0700	2019-07-28 21:19:34 -0700

The table shows 1 result out of 1. There are also pagination controls at the bottom right of the table.

At the bottom of the page, there is a copyright notice: Copyright © 2019 Bloombase.

Futurex Vectera and Bloombase KeyCastle Integration

To enable the built-in Bloombase KeyCastle to utilize keys in the network attached Futurex Vectera HSM. The hardware security module configuration at Bloombase web management console must be set up.

Bloombase supports Futurex Vectera out of the box. When a Futurex Vectera is configured at Bloombase web management console, select Module as 'futurex' which allows embedded Bloombase KeyCastle module to utilize Futurex fxpkcs11 driver to access Futurex Vectera HSM over standard PKCS#11 protocol.

In this scenario, the Futurex Vectera HSM is assigned a token label namely 'uso1hsm01test.virtucrypt.com:592'. Again, the use of slot is customer configurable. This can optionally be reconfigured, by modifying entry in Bloombase StoreSafe registry.

When prompted for pins, enter the password of the "CRYPTO-OPR" declared in the cfg file.

Modify Hardware Security Module

Modify Hardware Security Module

Module

Label / Username


Pin

Confirm Pin

When Futurex Vectera HSM resource is properly provisioned at Bloombase StoreSafe, the status would show up as 'Active'.

List Hardware Security Module

List Hardware Security Module

	Label	Present	Slot	Token	Module	Manufacturer	Model	Serial Number	Version	Status
1	us01hsm01test.virtucrypt.com:592	<input checked="" type="checkbox"/>	0	0	futurex	Futurex	HSM	1831800266	0.0 / 101.56	<input checked="" type="checkbox"/>

Encryption Key Provisioning

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

Modify Key Wrapper

Key Wrapper Permissions

Modify Key Wrapper

Name	<input type="text" value="key01"/>
Key Source	Hardware Security Module
Type	Asymmetric
Active	<input checked="" type="checkbox"/>
Module	futurex
Label	us01hsm01test.virtucrypt.com:592
Alias	<input type="text" value="ssf-key01"/>
Algorithm	<input type="text" value="RSA"/>
Key Bit Length	<input type="text" value="2048"/>
Signature Hash	<input type="text" value="SHA256"/>
Key Usage	<input type="checkbox"/> Digital Signature
	<input type="checkbox"/> Non Repudiation
	<input type="checkbox"/> Key Encipherment
	<input type="checkbox"/> Data Encipherment
	<input type="checkbox"/> Key Agreement
	<input type="checkbox"/> Key Cert Sign
	<input type="checkbox"/> C R L Sign
	<input type="checkbox"/> Encipher Only
	<input type="checkbox"/> Decipher Only
Extended Key Usage	<input type="button" value="Add"/> <input type="button" value="Remove"/>
Owner	admin
Last Update Datetime	



To generate key in attached Futurex Vectera HSM, select Key Source Type as “Hardware Security Module”, Module as “futurex” and the assigned HSM token label, in this case “us01hsm01test.virtucrypt.com:592”. Ensure you import a key from the HSM before you submit the key wrapper.

Modify Key Wrapper

Key Wrapper**Permissions**

Modify Key Wrapper

Key Source

Module

Token

Key

Or if key already exists, simply choose from the pull-down box.

Modify Key Wrapper

Key Wrapper**Permissions**

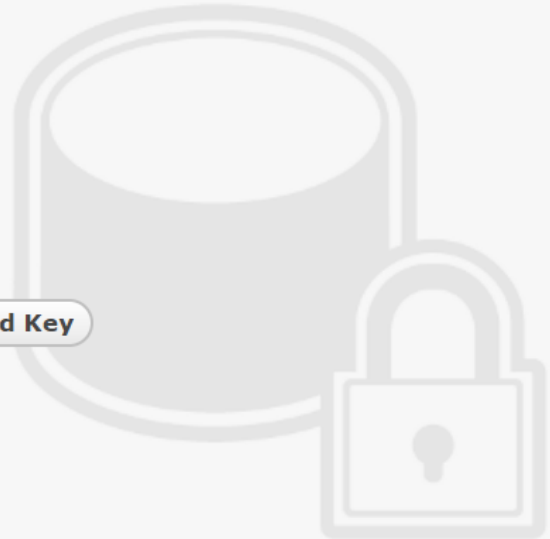
Modify Key Wrapper

Key Source

Module

Token

Key



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

Submit**Delete****Close**



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	<input checked="" type="checkbox"/>
Description	
Active	<input checked="" type="checkbox"/>
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 Microsoft Storage Server storage backend using AES 256-bit encryption and encryption key 'key01' managed at Futurex Vectera.

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

Add Remove

Cryptographic Cipher

Cipher Algorithm AES ▼

Bit Length 256 ▼

Submit Close



SMB/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"/>	user01 ▼	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	2014-02-13 10:09:11 +0800

Add Remove

▼ More Options

Submit Close



Conclusion

Hardware security module

- Futurex Vectera HSM

passed all Bloomberg interopLab's interoperability tests with Bloomberg StoreSafe

Bloomberg Product	Operating System	Hardware Security Module
Bloomberg StoreSafe	Microsoft Windows Server	Futurex Vectera HSM

Disclaimer

The tests described in this paper were conducted in the Bloombase InteropLab. Bloombase 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.

Acknowledgement

Bloombase InteropLab would like to thank Futurex for supporting this interoperability testing.

Technical Reference

Bloombase StoreSafe Technical Specifications, <http://www.bloombase.com/content/8936QA88>

Bloombase StoreSafe Hardware Compatibility Matrix, <http://www.bloombase.com/content/e8Gzz281>

Futurex Vectera HSM, <https://www.futurex.com/products/vectera-series>