



Technical FAQ

NetApp Storage Encryption FAQ

NetApp
January 2016

FAQ Overview

NetApp® Storage Encryption (NSE) is the full disk encryption product from NetApp. This FAQ addresses questions about how NSE can help your customers meet their regulatory requirements for encryption without sacrificing the NetApp features that provide value to their storage environment.

TABLE OF CONTENTS

1	Introduction	5
2	Overview and Product Details.....	5
	What is NetApp Storage Encryption?	5
	What threats does NSE mitigate?	5
	In what release of Data ONTAP will NSE be supported?	5
	What platforms, shelf types, drive size, and encryption algorithms are supported with NSE?	6
	What NSE-specific hardware and storage part numbers are offered?	6
	Can I mix encrypting and nonencrypting disks in my system?	6
	Can I have NSE and non-NSE nodes as part of the same cluster running clustered Data ONTAP?	6
	Do my customers have to pay more for this technology?	6
	What is the performance impact?	6
	Does NSE provide granular encryption? If so, at what level?	6
	How does the introduction of encryption work with normal cluster or HA pair operations?	6
	What is the operational impact of introducing NSE?	7
	Are there any constraints on downgrading and reverting?	7
	What encryption validations does NSE hold?	7
	How does the built-in 1024 authentication protection mechanism in NSE work?	7
	Is there a way to turn off encryption in NSE and use them as non-encrypting drives?	7
	Can NSE solution be managed through a management GUI?	7
	When replacing a failed NSE drive with a new NSE drive, is it possible to auto rekey the new NSE drive?	7
	Does the authentication key have to be generated manually?	7
	Is it necessary to have a single authentication key per DEK or a single authentication key for all DEKs on a given controller?	8
	Is the authentication key stored in NVRAM?	8
	How are DEKs generated on the NSE drives. Can I update an existing DEK?	8
	I lost my authentication key. Can I still sanitize all the data on the drives if needed?	8
	How do I securely move NSE drives from one FAS system to another?	8
	How mature is this technology?	8
	Where can I find more information on how to quote NSE?	8
3	NSE and Data ONTAP Features	9
	How does NSE affect Data ONTAP features?	9
	Is NetApp Flash Pool supported with NSE?	9
	Is the All-Flash FAS Supported with NSE?	9
	Is NetApp Flash Cache supported with NSE?	9
	Is NetApp MetroCluster supported with NSE?	9
	Is NetApp SnapLock supported with NSE?	9
	Can I take advantage of NetApp deduplication and compression with NSE?	9
	What is the difference between NSE In clustered Data ONTAP and NSE In Data ONTAP operating in 7-Mode?	9

Can I run vol move between NSE and non-NSE systems?.....	9
How does NSE work with NetApp replication technologies such as SnapMirror and SnapVault, and can I replicate data from NSE to nonencrypting storage and vice versa?.....	9
4 Comparison with Existing NetApp Encryption Offerings.....	10
How do the various encryption options from NetApp compare with one another?.....	10
Should I migrate my customers from NetApp DataFort to NSE?	11
My customer uses CryptoShred capability in NetApp DataFort. How can this be accomplished with NSE?	11
5 Key Management.....	11
What is KMIP?	11
How does NSE communicate with the KMIP server?	11
Does NSE require an external key manager?	11
Which key managers does NSE support?	11
Where can I order the various key managers?.....	12
Will NSE operate without a key manager?	12
What happens if a key manager is added at a later time?	12
Does NSE support a local key manager?.....	12
How does key management for NSE work?	12
How many key managers can NSE support?	12
Are keys synchronized between key managers?	13
How does an authentication key work with NSE?	13
6 The Competition	13
What are some products that compete with NSE?	13
7 Connector Licenses	15
What are NSE connector licenses?	15
How is the NSE connector license sold for initial sales of KeySecure k460?.....	15
How is the NSE connector license sold for initial sales of Virtual KeySecure k150v?.....	15
What if my customer already has KeySecure k460 appliances installed?	15
8 Key Contacts and Additional Information.....	16
Where can I find additional information on the NetApp encryption portfolio?	16
Who can I contact for further assistance?	16

LIST OF TABLES

Table 1) Comparison of the features and capabilities of the NetApp encryption options.	10
Table 2) Competitive Fujitsu self-encrypting drives.	14
Table 3) Links to additional information.	16
Table 4) Email contacts for additional support.	16

LIST OF FIGURES

Figure 1) Authentication key use in NSE.....	13
--	----

1 Introduction

The ability to protect and store critical data is a major focus for today's organizations. With the appropriate data protection technologies installed, organization can guard against potential malicious attacks and attempts to steal confidential data.

As government regulations and internal policies drive increasing demands on how corporate data is protected, identifying storage solutions that keep sensitive information secure has become a high priority for IT. And the use of encryption is quickly becoming a vital component for protecting sensitive data across the organization. However, IT is now confronted with the challenge to effectively manage and control disparate solutions, while continuing to provide access to the information by authorized users.

NetApp, working with partners, delivers a comprehensive portfolio of encryption solutions to secure confidential data at rest, while centralizing and simplifying encryption key management across physical and virtual datacenters, disaster recovery sites, and cloud infrastructures. By integrating Gemalto SafeNet appliance-based encryption, Gemalto SafeNet key management, and NetApp disk encryption technologies with NetApp storage solutions, customers can secure important information from unauthorized access or theft, meet data security and compliance initiatives, and preserve company reputation by avoiding publicized loss of data.

This FAQ discusses the positioning of NetApp Storage Encryption (NSE) solutions within the NetApp product portfolio.

2 Overview and Product Details

What is NetApp Storage Encryption?

Answer: NSE is our implementation of full-disk encryption (FDE) using self-encrypting drives from third-party vendors such as Seagate and Hitachi. FDE refers to encryption of all blocks in a disk drive, whether by software or hardware. NSE operates seamlessly with Data ONTAP® features, such as storage efficiencies, because the encryption occurs below Data ONTAP as the data is being written to the physical disk.

What threats does NSE mitigate?

Answer: NSE mitigates several threats, but the primary threat model it addresses, per the Trusted Computing Group (TCG) specification, is the prevention of unauthorized access to encrypted data at rest on powered-off disk drives. That is, it prevents someone from removing a shelf or drives and then attempting to mount them on an unauthorized system. This minimizes the risk of unauthorized access to data if drives are stolen from a facility or compromised during physical movement of the storage array between facilities.

Additionally, NSE prevents unauthorized data access when drives are returned as spares or after drive failure. This includes cryptographic shredding of data for nonreturnable disks, disk repurposing, and simplified disposal of the drive through disk destroy commands, rendering the disk completely unusable. This greatly simplifies disposing of drives and eliminates the need for costly, time-consuming physical drive shredding.

Remember that all data on the drives is automatically encrypted. If a customer doesn't want to keep track of where the most sensitive data resides or doesn't want to risk it being outside of an encrypted volume, NSE is a simple way to make sure that all data is encrypted.

In what release of Data ONTAP will NSE be supported?

Answer: NSE is officially supported with 7-Mode Data ONTAP® 8.1.1 (or higher); and supported with both 7-Mode and clustered Data ONTAP starting with 8.2.1. Refer to question, ["What is the difference](#)

[between NSE In clustered Data ONTAP and NSE in Data ONTAP operating in 7-Mode?](#)” on Page 8 for more details.

What platforms, shelf types, drive size, and encryption algorithms are supported with NSE?

Answer: Please refer to **Hardware Universe** (<http://hwu.netapp.com/Home/Index>) or the current price list for supported configurations and part numbers.

What NSE-specific hardware and storage part numbers are offered?

Answer: Please refer to **Hardware Universe** (<http://hwu.netapp.com/Home/Index>) or the current price list for supported configurations and part numbers.

Can I mix encrypting and nonencrypting disks in my system?

Answer: No. Mixing encrypted with unencrypted drives or shelves across a standalone platform or high-availability (HA) pair is not supported.

Can I have NSE and non-NSE nodes as part of the same cluster running clustered Data ONTAP?

Answer: Yes. NSE and non-NSE nodes can co-exist as part of the same cluster running clustered Data ONTAP. However remember that mixing of NSE and non-NSE drives is not supported across a standalone platform or across high availability HA pair.

Do my customers have to pay more for this technology?

Answer: NSE disks have an incremental cost over nonencrypting disks.

What is the performance impact?

Answer: Based on internal testing the performance impact is negligible (< 1%).

Does NSE provide granular encryption? If so, at what level?

Answer: NSE encrypts at the drive level—that is, each drive has a unique data encryption key (DEK). However, the drives are secured by using a single authentication key (AK) to wrap each DEK. In Data ONTAP 8.1.x GA and later, AKs are supported across entire systems and HA pairs only. Both keys (DEK and AK) can be changed if, or when required.

- **DEK.** Each drive already has a unique DEK and a default passphrase, known as the manufacturing secure ID (MSID). [MSID: keyID 0x0 is the handle NetApp uses to talk about the SED’s default passphrase]. The data is always encrypted with the DEK during write operations, even if it is not wrapped with an AK. We cannot specify a particular DEK; we can only instruct the SED to generate a new one and use that henceforth.
- **AK.** The AK is established in Data ONTAP and loaded onto the KMIP compliant key manager. Once established, the key is used to wrap the DEK. The AK is unique per system. The AK is needed in the event of a key management set-up, power cycle or adding a new HDD.

If AK keys are lost or become corrupted, data cannot be retrieved. It is strongly recommended that a redundant key manager be used for this reason. NSE only protects data-at-rest (on/in disk) when paired with an external KMIP compatible key manager, such as SafeNet KeySecure (SSL exchange of AK). NSE provides no protection for data once it is read from the disk. Other methods of encryption are required for data on the wire.

How does the introduction of encryption work with normal cluster or HA pair operations?

Answer: The introduction of NSE encryption has no effect on HA pair operations because the encryption occurs at a much lower level. However, the FAS administrator must make sure that the same passphrase and SSL certificates are used on both HA pair nodes for failover.

What is the operational impact of introducing NSE?

Answer: NSE requires a completely new system: controller, shelves, and drives. Existing FAS60xx and FAS31xx and older systems do not support the addition of encryption drives or shelves. Existing customers on supported platforms can upgrade to Data ONTAP 8.1.1 GA and higher, but they must purchase encrypting drives and shelves. Also, data must be migrated from existing nonencrypting shelves. NSE is best offered as a net-new installation.

Are there any constraints on downgrading and reverting?

Answer: NSE is officially supported in both 7-Mode and clustered Data ONTAP starting with 8.2.1. FAS platforms supporting NSE should not be downgraded or reverted to any release prior to clustered Data ONTAP 8.2.1. Users of FAS systems that attempt to downgrade will fail to detect the encrypting drives and therefore are not able to boot successfully.

What encryption validations does NSE hold?

Answer: NSE relies on the drive manufacturer for assurance-level certification. Seagate, our first drive partner, provides Federal Information Processing Standards (FIPS) 140-2 level 2 validation for these drives. Use of these drives in a FIPS validated mode is being considered for a future Data ONTAP release. There are currently no plans for Common Criteria (CC) validation, but FIPS at the drive level should provide the necessary security assurances based on the customer's security policy. Seagate's security policy can be found on the National Institute of Standards and Technology (NIST) site at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>.

How does the built-in 1024 authentication protection mechanism in NSE work?

Answer: The built-in 1024 authentication protection mechanism in NSE protects against brute force attacks and prevents unauthorized access to the data. If the drives sequentially fail authentication for more than 1024 times, the firmware within each drive will drop its internal DEK. Once the DEK is dropped, the data on the drives will be lost and there is no way to revert this process. However setting the drives back to the manufacturing defaults can reinitialize the drives.

Is there a way to turn off encryption in NSE and use them as non-encrypting drives?

Answer: The way to look at NSE solution is that it is always encrypting at the drive level. Hence there is no way to turn off encryption capability in NSE and use them as non-encrypting drives. When a KMIP compliant Key Manager such as Gemalto's SafeNet KeySecure or IBM TKLM is used to store and manage the keys from NSE solution, NSE protects against disk theft scenarios. Without the use of KMIP compliant Key Manager, NSE is still encrypting at the drive level, however it does not protect against the disk theft scenarios.

Can NSE solution be managed through a management GUI?

Answer: Currently all the NSE commands need to be executed at the CLI level. A management GUI to manage the NSE solution does not exist at this time.

When replacing a failed NSE drive with a new NSE drive, is it possible to auto rekey the new NSE drive?

Answer: NSE does not support auto rekey on new NSE drive. The rekeying on the new NSE drive is a manual process.

Does the authentication key have to be generated manually?

Answer: There are two ways to generate the authentication key. During the time of NSE setup, you can either input it manually or have the system auto (randomly) generate one for you.

Is it necessary to have a single authentication key per DEK or a single authentication key for all DEKs on a given controller?

Answer: NetApp recommends generation of a single authentication key for all NSE drives on a given controller. Hence if you have two controllers namely controller A and controller B, NetApp recommends generating authentication key AK1 for all DEKs on controller A and authentication key AK2 for all the DEKs on controller B.

Is the authentication key stored in NVRAM?

Answer: No. The authentication key is not stored in NVRAM. The authentication key is available during the time of Data ONTAP boot only. It is stored in volatile memory and backed up to KMIP compliant Key Manager such as SafeNet KeySecure or IBM TKLM. The authentication key is purged from volatile memory on a power loss.

How are DEKs generated on the NSE drives. Can I update an existing DEK?

Answer: Each drive ships with a default DEK generated by the drive manufacturer. NetApp has the ability to generate a new DEK using the “disk encrypt” command set. Note that the generation of a new key will effectively wipe the data on that particular drive.

I lost my authentication key. Can I still sanitize all the data on the drives if needed?

Answer: Yes. If a situation arises where you have lost your Authentication Key and if you feel the need to sanitize all the data on all the drives, you can run the “disk encrypt sanitize – all “ command which will effectively wipe all the data on the drives and reset the drives to the factory default DEKs. The “disk encrypt sanitize – all “ command should be run at the system level.

How do I securely move NSE drives from one FAS system to another?

Answer: From a high level, to securely move NSE drives from one FAS system to another, involves creating clone key of the Key ID belonging to the source NSE disks, making sure the object group system ID of the clone key reflects the destination FAS system ID and making sure that the new key ID is loaded into the Data ONTAP's key table on the destination FAS system. Full details on step by step process of how to securely move NSE drives from one FAS system to another can be found in the Knowledge Base article below:

https://kb.netapp.com/support/index?page=content&id=1014315&actp=search&viewlocale=en_US&searchid=1386636334251

How mature is this technology?

Answer: Full-disk encryption has been around in one form or another for many years. Several major drive vendors such as Seagate and Hitachi have been investing heavily in self-encrypting drives across their entire drivelines. All major drive manufacturers have collaborated to create a Trusted Computing Group specification that standardizes encryption methods across all vendors' drives.

Where can I find more information on how to quote NSE?

Answer: Refer to the “Quoting Storage Security Products” presentation on the Field Portal (<https://fieldportal.netapp.com/safenet-encryption.aspx#150153>) for detailed information on how to quote NetApp security products along with part numbers, software licensing, and sample configurations.

3 NSE and Data ONTAP Features

How does NSE affect Data ONTAP features?

Answer: NSE operates at the disk drive level. Data ONTAP features such as SnapDrive®, SnapMirror®, SnapVault®, SnapProtect®, and even storage compression and FAS deduplication operate above NSE and are supported with NSE. Interoperability with these features is completely transparent.

Note: SnapLock® and MetroCluster™ are not currently supported with NSE.

Is NetApp Flash Pool supported with NSE?

Answer: Yes. NetApp Flash Pool™ is supported with the SSD 800GB NSE drives.

Is the All-Flash FAS Supported with NSE?

Answer: Yes. The All-Flash FAS is supported with NSE SSD drives.

Is NetApp Flash Cache supported with NSE?

Answer: NetApp Flash Cache™ is supported with NSE. However, the contents of the Flash Cache are not encrypted.

Is NetApp MetroCluster supported with NSE?

Answer: MetroCluster is not currently supported with NSE. Support for MetroCluster with NSE is targeted for a future release of Data ONTAP.

Is NetApp SnapLock supported with NSE?

Answer: SnapLock is not currently supported with NSE. Support for SnapLock with NSE is targeted for a future release of Data ONTAP.

Can I take advantage of NetApp deduplication and compression with NSE?

Answer: Yes. NSE supports storage efficiency — FAS deduplication and storage compression. Because deduplication and compression take place at the WAFL® layer and encryption occurs at the disk level, customer can deduplicate and compress their data before it is encrypted at the disk level. The result is great storage savings for the customer.

What is the difference between NSE In clustered Data ONTAP and NSE In Data ONTAP operating in 7-Mode?

Answer: Functionally there is no difference at this point between NSE available in clustered Data ONTAP and NSE in 7-Mode. Architecturally, they are the same. NSE commands in clustered Data ONTAP are same as those available in 7-Mode, except that those commands need to be run from nodeshell in clustered Data ONTAP.

Can I run vol move between NSE and non-NSE systems?

Answer: Yes. You can run `vol move` between NSE and non-NSE systems. Make sure the NSE and non-NSE systems are not part of the same HA pair because you cannot mix encrypted and non-encrypted drives on the same controller or across an HA pair.

How does NSE work with NetApp replication technologies such as SnapMirror and SnapVault, and can I replicate data from NSE to nonencrypting storage and vice versa?

Answer: Yes. You can use NSE with replication technologies such as SnapMirror and SnapVault. NSE encrypts data at the drive level. Therefore when you have an NSE system at the source, the data is

encrypted at the drive level. When you use replication technologies such as SnapVault and SnapMirror for backup and recovery, Data ONTAP pulls the data from the disks and converts it to clear text.

Note: Note that data in transit between the source and destination is not encrypted; that is, data travels over the wire in clear text.

The data can be sent to any target, encrypted NSE system or otherwise. If the destination contains an NSE system, the data is encrypted as it is being written to the self-encrypting drives at the destination. If the destination contains a non-NSE system, then the data on the destination system remains in clear text. You can also replicate from a non-NSE system to an NSE system. Just remember that when using SnapVault or SnapMirror, the data travels in clear text over the wire. However, most customers replicate over secure links between their sites in any case, so encryption between sites is not typically required.

4 Comparison with Existing NetApp Encryption Offerings

How do the various encryption options from NetApp compare with one another?

Answer: Table 4 compares the features and capabilities of the encryption options available from NetApp.

Table 1) Comparison of the features and capabilities of the NetApp encryption options.

Feature	E-Series	SafeNet StorageSecure	NetApp Storage Encryption
Access controls and authentication	Local SANTricity accounts or via external host with AD, LDAP, NIS, etc.	Quorum-base authentication Enforce granular ACLs	Data ONTAP access controls and authorization
Granularity of encryption	Self-encrypting disk drive	SMB (CIFS) share, NFS export, or iSCSI LUN	Self-encrypting disk drive
Data at rest	Yes	Yes	Yes
Data in flight	No	Yes (server-side encrypted)	No
Performance	10k RPM high-performance drives SSD Drives 7.2K RPM high-capacity drives	1GbE and 10GbE ports (StorageSecure)	10k RPM high-performance drives SSD Drives 7.2K RPM high-capacity drives
Simplicity and interoperability	Simple setup via SANTricity. Compatible with SANTricity storage efficiencies such as compression and thin provisioning.	Broad interoperability with multiple vendors, but interop lags behind as new storage products emerge. Management of standalone appliance in the storage network.	Compatible with all Data ONTAP efficiency and management features. Management integrated in Data ONTAP commands.
Cryptographic shredding	Yes	Yes	Yes
Key management	On box key management in SANTricity	SafeNet KeySecure k460	SafeNet KeySecure k460 IBM TKLM/SKLM
Security	AES 256	FIPS 140-2 level 3 AES 256	FIPS 140-2 level 2 (at the drive level) AES 256

Feature	E-Series	SafeNet StorageSecure	NetApp Storage Encryption
Bottom line	Encryption for data at rest for high performance and big data applications	Specialized appliance for high security needs and granular encryption.	Seamless integration into storage array takes full advantage of existing data ONTAP storage efficiency features.

** Use of these drives in a FIPS validated mode is being considered for a future Data ONTAP release.*

Should I migrate my customers from NetApp DataFort to NSE?

Answer: NSE might not be a suitable migration path for all NetApp DataFort customers because DataFort has additional functionality such as additional ACL management and more granular encryption. Migration involves deploying a new FAS platform with NSE and copying the data over from the LUNs or volumes encrypted with DataFort to the new storage array. There is no in-place upgrade or migration, because DataFort and NSE use different encryption data formats. The drop-in replacement for DataFort installations is SafeNet StorageSecure by Gemalto.

Note: NSE is best positioned as a net-new installation.

My customer uses CryptoShred capability in NetApp DataFort. How can this be accomplished with NSE?

Answer: NSE wraps the data encryption key contained in the disk drive with an authentication passphrase. Destruction of this passphrase eliminates access to the data encryption key and effectively shreds all the data. Destruction of the key management server and power cycling the entire system plus drives (not just the controller) disables any ability to access encrypted data. During runtime, Data ONTAP also supports commands to sanitize the drive or to permanently disable it so that further data access is impossible.

5 Key Management

What is KMIP?

Answer: Key Management Interoperability Protocol (KMIP) is an encryption key interoperability standard created by a consortium of security and storage vendors (OASIS). Version 1.0 was ratified in September 2010, and participating vendors have been releasing compatible products since then. KMIP appears to have supplanted IEEE P1619.3, an earlier proposed standard.

How does NSE communicate with the KMIP server?

Answer: NSE uses Transport Layer Security (TLS) certificates to establish secure communications with the KMIP server. These certificates must be in Base64-encoded X.509 PEM format and can be either self-signed or signed by a certificate authority.

Does NSE require an external key manager?

Answer: Yes. NSE does require an external key manager; and can support up to four key managers simultaneously.

Which key managers does NSE support?

Answer: NSE supports the SafeNet KeySecure k460 key management appliance, SafeNet Virtual KeySecure k150v, IBM Tivoli Key Lifecycle Management TKLM server, IBM Security Key Lifecycle Manager (SKLM). The Vormetric Data Security Manager (DSM) is also supported via PVR. We are also

evaluating other KMIP-compliant key managers and will expand support for additional KMIP-compliant key managers as they come onto the market.

Where can I order the various key managers?

Answer: SafeNet KeySecure k460 and Virtual KeySecure k150v can be ordered from NetApp. Refer to the “Quoting Storage Security Products” presentation on the Field Portal (<https://fieldportal.netapp.com/safenet-encryption.aspx#150153>) for more details.

Note: SafeNet Virtual KeySecure k150v was added to the NetApp price list in August 2015.

Note: IBM TLKMv2 and SKLM must be ordered from an external IBM reseller.

Is there a recommended best practice for key management?

Answer: The “best practice” for key management is to install one key manager at each remote site. At a minimum, two key managers in two locations would be the best alternative to provide a cost effective, high availability solution.

If customers want to deploy 2 units in a central location to support remote devices, they need to understand the implication that if the link is down the FAS can't reboot. Or if the central site is destroyed, then those keys are gone forever.

Will NSE operate without a key manager?

Answer: Without a Key Manager, the SED will still encrypt the data during writes to the media. However, without the AK wrapping the DEK, the data can be read based on possession of the drive. In this case, the DEK is freely accessible. Deploying NSE without a key manager provides limited protection of the data-at-rest.

What happens if a key manager is added at a later time?

Answer: If a key manager is added at a later point, setting the AK will wrap the existing DEK. Setting a new DEK is not required. If a new DEK is desired, the data will need to first be migrated to another drive. Setting a new DEK effectively wipes the data from the drive. If you do not desire to use the default DEK generated during manufacturing, it is recommended that a new DEK be generated as part of installation.

Does NSE support a local key manager?

Answer: Data ONTAP does not currently include a local key manager. An external KMIP compliant key manager is required to store the AK. No other methods for AK storage are supported.

How does key management for NSE work?

Answer: NSE drives have built-in DEKs that never leave the drives. The DEKs are used to encrypt and decrypt data on the drive. They are wrapped using an authentication key (AK) generated within Data ONTAP. The AK wraps the DEK, locking the drive and preventing unauthorized access to the DEK. Upon generation, the AK is backed up to the key management server using an SSL connection.

On boot, Data ONTAP requests the AK from the key manager. On successful retrieval, the AK is passed to the drive, which allows the DEK to be unwrapped, and access to the disk can begin.

How many key managers can NSE support?

Answer: NSE supports up to four key managers simultaneously for high availability of the authentication key.

Are keys synchronized between key managers?

Answer: High availability of keys is assured by allowing the NSE client to send keys to up to four key management servers. Key manager synchronization depends on the vendor implementation.

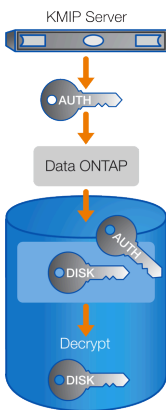
- SafeNet KeySecure k460 provides automatic key synchronization for clustered key managers.
- IBM TKLM offers the ability to export its key database and import it into another TKLM instance for key replication.

NetApp highly recommends backing up your key management servers regularly to make sure that the keys are available. Check with your key management provider for information about how to back up your key management servers.

How does an authentication key work with NSE?

Answer: Figure 1 shows how the AK wraps the DEK and is backed up to an external key management server.

Figure 1) Authentication key use in NSE.



6 The Competition

What are some products that compete with NSE?

Answer: Answer: Here is a list of products offered by Hitachi, EMC, IBM, and Fujitsu that compete with NSE.

Hitachi

- HDS USP V, USP VM, VSP and HUS support controller-based encryption at the controller level and support FC, SAS, SATA, and/or flash drives.
- HDS AMS 2000 family supports self-encrypting hard disk drives, similar to NSE.

EMC

- **VNX:** provides Data at Rest Encryption (D@RE) that encrypts data as it is written to a disk using Controller-Based Encryption (CBE) on VNX systems. Only supports internal key management. Keys cannot be centrally managed across other EMC storage systems.
- **Symmetrix VMAX:** Data at Rest Encryption provides hardware-based, on-array, back-end encryption for Symmetrix VMAX systems: 10K, 20K, 40K. Only supports an Integrated key manager using RSA® Embedded Key Manager. Keys cannot be centrally managed across other EMC storage systems.

- **Data Domain:** DD Encryption is an optional software license, supported on all Data Domain systems, and is designed to protect against unauthorized access to user data as a result of the theft of disk shelves, individual disks, or while failed disks are being returned for repair. No key management is the default, but customers can choose to use an internal key manager, or externally manage using RSA Data Protection Manager. Keys cannot be centrally managed across other EMC storage systems.
- **Isilon:** Teamed with Vormetric for encryption and key management. Vormetric Encryption Expert Agents are software agents that insert above the file system logical volume layers, and are installed on each server where data requires protection. Vormetric Key Management (VKM) provides a robust, standards-based platform for managing encryption keys from disparate sources across the enterprise. Isilon and other KMIP encryption solutions can be centrally managed, however keys cannot be centrally managed across other EMC storage systems

IBM

- IBM System Storage DS8000 series supports self-encrypting drives for every tier to help secure the data at rest, similarly to NSE.

Fujitsu

- Table 2 summarizes competitive Fujitsu branded self-encrypting drives.

Table 2) Competitive Fujitsu self-encrypting drives.

Fujitsu Self-Encrypting Drives	NetApp Self-Encrypting Drives
Fujitsu self-encrypting drives are supported in the following ranges: • Entry range (ETERNUS DX80 S2/DX90 S2) • Mid range (ETERNUS DX400 S2 series) • Enterprise range (ETERNUS DX8700 S2)	NetApp self-encrypting drives are supported in the following ranges: • Entry range (FAS 2040, FAS 2220, FAS 2240) • Mid range (FAS32xx/V32xx) • High range (FAS62xx/V62xx)
Fujitsu encryption by firmware is supported in the following ranges: • Entry range (ETERNUS DX60/DX60 S2, DX80/DX80 S2, DX90/DX90 S2) • Mid range (ETERNUS4000, ETERNUS DX400/DX400 S2 series) • Enterprise range (ETERNUS8000, ETERNUS DX8000 series/DX8700 S2)	
Fujitsu's unique encryption is supported in the following range: • Entry range (ETERNUS DX60/DX60 S2/DX80/DX90)	

What advantages does NSE offer over competitive encryption solutions?

Answer: The following list describes the competitive advantages of NSE:

Complete transparency:

- NSE supports storage efficiencies — FAS deduplication and storage compression. Because all deduplication and compression take place at the WAFL layer and encryption occurs at the disk level, customers can deduplicate and compress their data before the data is encrypted at the disk level. The result is great storage savings for the customer. Array-based AV scanning is also supported by NSE.
- NSE also supports integrated data protection: Backup and recovery, SnapMirror, SnapProtect®, and SnapVault.

Negligible performance impact:

- The performance impact when using NSE is minimal (<1%).

Standards-based key management:

- NSE complies with the OASIS KMIP standard, offering compatibility with key managers such as the SafeNet KeySecure k460, Virtual KeySecure k150v, and IBM TKLM.

NetApp Unified Architecture:

- NSE benefits greatly from the NetApp Unified Architecture, which goes beyond simple multiprotocol storage to provide integrated data management and data protection, support for all tiers of storage, quality of service, and other elements, all in a single platform. The unified storage architecture enables the creation of a common storage pool that can be networked and shared across a diverse set of applications with a common set of management processes. The ability to scale from small to very large storage capacity without compromising application performance or service levels and do it all non-disruptively is a key attribute.

Protocol independent:

- It doesn't matter whether you are using a NAS or a SAN protocol; NSE drives are protocol independent.

7 Connector Licenses

What are NSE connector licenses?

Answer: The NSE connector is a software license that allows SafeNet KeySecure (required for both models: k460 and k150v) to store and serve keys to specific devices.

How is the NSE connector license sold for initial sales of KeySecure k460?

Answer: For initial sales of NSE with SafeNet KeySecure k460, the part number for the appliance comes with a 10-pack NSE connector license. This single k460 can talk to up to five HA pairs (one NSE connector license per controller). Multiple SafeNet KeySecure key managers are allowed to share the licenses as part of the clustering feature. For a second k460, you would order a base k460 (without any licenses). If you exceed 10 controllers, you can purchase a 10-pack NSE Connector license bundle.

Example:

If a customer wants to deploy NSE in a DR environment, NetApp recommends two SafeNet KeySecure k460s, one at each site. Assuming there are five HA pairs of NetApp controllers in the environment, the customer can purchase one SafeNet KeySecure k460 with a 10-pack NSE connector license and one base SafeNet KeySecure k460 without the 10-pack NSE connector license. If the customer decides to purchase more NetApp controllers in the future, they can then purchase a 10-pack NSE connector license bundle.

How is the NSE connector license sold for initial sales of Virtual KeySecure k150v?

Answer: Virtual KeySecure k150 can be sold as either a subscription or perpetual license. Add the part number for the NSE connector License in QuoteEdge as part of the configuration. One connector license is needed for each controller. Order additional 10-pack NSE Connector licenses to cover all controllers in the configuration.

What if my customer already has KeySecure k460 appliances installed?

Answer: As of June 2015, account teams now have the ability to quote NSE connector licenses separately from SafeNetKeySecure appliances. Customers that already own SafeNet KeySecure key managers can now purchase the connector licenses directly from NetApp when adding NSE shelves instead of having to purchase from Gemalto.

8 Key Contacts and Additional Information

Where can I find additional information on the NetApp encryption portfolio?

Answer: The Field Portal has a wealth of information on these technologies. The following landing page and binders of the most relevant collateral are available on the Field Portal:

Table 3) Links to additional information.

Content	Web link
Data at Rest Encryption NetApp Storage Encryption (NSE) Binder	https://fieldportal.netapp.com/collections/212366
Data at Rest Encryption SafeNet Solutions by Gemalto Binder	https://fieldportal.netapp.com/Modules/FieldPortal/Binders/Content.aspx?contentID=77913
SafeNet KeySecure Collection	https://fieldportal.netapp.com/collections/298786
SafeNet Virtual KeySecure Collection	https://fieldportal.netapp.com/collections/298728
SafeNet StorageSecure Collection	https://fieldportal.netapp.com/collections/298733
SafeNet KeySecure Connector License Collection	https://fieldportal.netapp.com/collections/298792
SafeNet Internal Wins Collection	https://fieldportal.netapp.com/collections/298789

Who can I contact for further assistance?

Answer: Additional information can be requested by sending email to the email addresses, based on specific product required.

Table 4) Email contacts for additional support.

Contact	Support Provided
SafeNet Support netapp-sales@safenet-inc.com ng-selling-safenet@netapp.com	- KeySecure and StorageSecure sales assistance, installation, configuration, and support. - Schedule a Web meeting, an in-person meeting, or a demo.
NetApp Encryption xdl-encryption@netapp.com	Further information or sales assistance on NetApp encryption solution portfolio.

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.