



Technical FAQ

NetApp Storage Encryption FAQ

March 2012 | Version 1.5 |

Status: Final

FAQ OVERVIEW

NetApp® Storage Encryption is the next generation in encryption products from NetApp. This FAQ attempts to answer questions about how this solution can help your customers meet their regulatory requirements around encryption without sacrificing many of the NetApp features that provide value to your storage environment.

OVERVIEW AND PRODUCT DETAILS	3
WHAT IS NETAPP STORAGE ENCRYPTION?.....	3
WHAT THREATS DOES NSE MITIGATE?	3
HOW DOES NSE AFFECT DATA ONTAP FEATURES?	3
CAN I REPLICATE DATA FROM NSE TO NON-ENCRYPTING STORAGE AND VICE VERSA?	3
ON WHAT RELEASE OF DATA ONTAP WILL THIS BE SUPPORTED?	3
ON WHAT PLATFORMS/SHELF COMBINATION WILL THIS BE SUPPORTED?	4
WHAT DRIVE SIZES WILL BE AVAILABLE?	4
CAN I HAVE A SYSTEM THAT HAS A MIXTURE OF ENCRYPTING AND NONENCRYPTING DISKS?	4
DO MY CUSTOMERS HAVE TO PAY MORE TO GET THIS TECHNOLOGY?	4
WHAT IS THE PERFORMANCE IMPACT?	4
DOES NSE PROVIDE GRANULAR ENCRYPTION? IF SO, AT WHAT LEVEL?	4
HOW DOES INTRODUCTION OF ENCRYPTION WORK WITH NORMAL CLUSTER OR HA PAIR OPERATIONS?	4
WHAT IS THE OPERATIONAL IMPACT OF INTRODUCING NSE?	4
ARE THERE ANY CONSTRAINTS ON DOWNGRADE/REVERT?	5
WHAT ENCRYPTION VALIDATIONS DOES NSE HOLD?	5
HOW MATURE IS THIS TECHNOLOGY?	5
COMPARISON TO EXISTING NETAPP ENCRYPTION OFFERINGS	5
COMPARE NSE TO DATAFORT/SAFENET STORAGESECURE AND BROCADE ENCRYPTION SWITCH	5
SHOULD I MIGRATE MY CUSTOMERS FROM DATAFORT TO NSE?	6
MY CUSTOMER USES CRYPTOSHRED CAPABILITY IN DATAFORT. HOW CAN THIS BE ACCOMPLISHED WITH NSE?	6
KEY MANAGEMENT	6
WHAT IS KMIP?	6
HOW DOES NSE COMMUNICATE WITH THE KMIP SERVER?	6
DOES NSE REQUIRE AN EXTERNAL KEY MANAGER?	7
WHICH KEY MANAGERS DOES NSE SUPPORT?	7
WHERE CAN I ORDER THE VARIOUS KEY MANAGERS?	7
HOW DOES KEY MANAGEMENT FOR NSE WORK?	7
HOW MANY KEY MANAGERS CAN NSE SUPPORT?	7
ARE KEYS SYNCHRONIZED BETWEEN KEY MANAGERS?	7
FIGURE 1: AUTHENTICATION KEY USE IN NSE	8

OVERVIEW AND PRODUCT DETAILS

WHAT IS NETAPP STORAGE ENCRYPTION?

NetApp Storage Encryption (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 is encryption that operates seamlessly with Data ONTAP® features, such as storage efficiency, because the encryption occurs below Data ONTAP as the data is being written to the physical disk.

WHAT THREATS DOES NSE MITIGATE?

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 drive(s) and then attempting to mount them on an unauthorized system. This minimizes 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 disk (NRD), disk-repurposing scenarios, and simplified disposal of the drive through disk destroy commands, rendering a disk completely unusable. This greatly simplifies the disposal 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 an encrypted volume, NSE is a simple way to make sure all data is encrypted.

HOW DOES NSE AFFECT DATA ONTAP FEATURES?

NSE operates below all Data ONTAP features such as SnapDrive®, SnapMirror®, and even Storage Compression and FAS Deduplication. Interoperability with these features should be completely transparent. SnapVault® and SnapMirror are both supported, but in order for data at the destination to be encrypted, the target must be another NSE system.

The use of SnapLock® precludes the inclusion of NSE; therefore, simultaneous operation of SnapLock and NSE is not permitted. This is being evaluated for a future release of Data ONTAP.

MetroCluster™ is not currently supported. Support for MetroCluster is currently targeted for a future release of Data ONTAP.

CAN I REPLICATE DATA FROM NSE TO NON-ENCRYPTING STORAGE AND VICE VERSA?

Data is only encrypted when it is at rest on the self-encrypting drives. When the data is read off the disk and sent across via technologies like SnapMirror or SnapVault, the data is in the clear. Therefore the data can be sent to any target, encrypted or otherwise. The reverse is also true. A non-encrypting system can send its data to an NSE system. The data will be encrypted as it is being written to the self-encrypting drives at the destination.

ON WHAT RELEASE OF DATA ONTAP WILL THIS BE SUPPORTED?

NSE is officially supported with Data ONTAP 8.1RC3 7-mode only. Cluster-Mode support for NSE is not available in Data ONTAP 8.1, but is targeted for a future release of Data ONTAP.

ON WHAT PLATFORMS/SHELF COMBINATION WILL THIS BE SUPPORTED?

Data ONTAP 8.1RC3 will support FAS2040, FAS2240-2, FAS32xx, FAS62xx, V32xx, and V62xx platforms. We will have support for the following drive and shelf types:

3.5" 600GB Performance HDD with AES-128 bit encryption in the FAS2040 and in the DS4243 shelf

2.5" 600GB Performance HDD with AES-256 bit encryption in the FAS2240-2 and in the DS2246 shelf

Both drive and shelf types are supported in the FAS/V32xx and FAS/V62xx family.

WHAT DRIVE SIZES WILL BE AVAILABLE?

The initial release of NSE will be supported with 600GB Performance HDD. Additional drives will be qualified as they become available from our drive vendors. Encrypted 3TB Capacity HDDs are tentatively scheduled for an upcoming release of Data ONTAP and is depending on drive availability.

CAN I HAVE A SYSTEM THAT HAS A MIXTURE OF ENCRYPTING AND NONENCRYPTING DISKS?

In Data ONTAP 8.1RC3, all drives installed within the storage platform must be self-encrypting drives. We will not be supporting the mixing of encrypted with unencrypted drives or shelves across a standalone platform or high-availability (HA) pair.

DO MY CUSTOMERS HAVE TO PAY MORE TO GET THIS TECHNOLOGY?

NSE disks will have an incremental cost over non-encrypting disks.

WHAT IS THE PERFORMANCE IMPACT?

For the 600GB Performance HDD available in the initial release and based on internal testing and specifications from Seagate, the performance impact is considered negligible (< 1%).

DOES NSE PROVIDE GRANULAR ENCRYPTION? IF SO, AT WHAT LEVEL?

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 8.1RC3, AKs are supported across entire systems and HA pairs only.

HOW DOES INTRODUCTION OF ENCRYPTION WORK WITH NORMAL CLUSTER OR HA PAIR OPERATIONS?

Introduction of NSE encryption will have no effect on HA pair operations because the encryption is occurring at a much lower level. However, the FAS administrator will have to 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?

NSE requires a completely new system: controller, shelves, and drives. Existing 60xx and 31xx and older systems will not support addition of encryption drives or shelves. Existing customers on supported platforms can upgrade to Data ONTAP 8.1RC3, but will need to purchase encrypting drives and shelves. Data migration from existing non-encrypting shelves will need to be performed. NSE is best offered as a net-new installation.

ARE THERE ANY CONSTRAINTS ON DOWNGRADE/REVERT?

NSE is officially supported only on Data ONTAP 8.1RC3. FAS32xx and FAS62xx platforms will not be able to downgrade or revert to any release prior to Data ONTAP 8.1RC3. Users of FAS systems who attempt to downgrade will fail to detect the encrypting drives and therefore will be unable to boot successfully.

WHAT ENCRYPTION VALIDATIONS DOES NSE HOLD?

NSE relies on the drive manufacturer for assurance-level certification. Seagate, our first drive partner, has Federal Information Processing Standards (FIPS) 140-2 level 2 validation for these drives. There are currently no plans for Common Criteria (CC) validation, but FIPS 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 MATURE IS THIS TECHNOLOGY?

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

COMPARISON TO EXISTING NETAPP ENCRYPTION OFFERINGS

COMPARE NSE TO DATAFORT/SAFENET STORAGESECURE AND BROCADE ENCRYPTION SWITCH

Feature	E-Series DataFort/ SafeNet StorageSecure	NSE	Brocade Encryption Switch
Access controls and authentication	Quorum-based authentication 2-factor authentication Enforce granular ACLs	Data ONTAP access controls and authorization	Smart card for administration, encryption zones for access to encrypted targets
Granularity of encryption	CIFS share, NFS export, or iSCSI LUN	Single platform or HA cluster pair	FC LUN or FC tape
Data at rest	Yes	Yes	Yes
Data in flight	Yes (server side encrypted)	No	Yes (server side encrypted)
Performance	1GbE ports	600GB Performance HDDs	8GB FC ports
Simplicity and interoperability	Broad interoperability with multiple vendors, but interop lags behind as new storage products emerge. Management of standalone appliance within storage network.	Compatible with all Data ONTAP efficiency and management features. Management integrated within Data ONTAP commands.	Broad interoperability with multiple vendors, but interop lags behind as new storage products emerge. Initiators and targets managed as well- known fabric objects.

Cryptographic shredding	Yes	Yes	No
Key management	SafeNet KeySecure k460/NetApp Lifetime Key Management™	SafeNet KeySecure k460/IBM TKLMv2	SafeNet KeySecure k460/NetApp Lifetime Key Management
Security	-FIPS 140-2 level 3 -AES 256	- FIPS 140-2 level 2 -Data ONTAP- CC EAL2+ validation targeted -AES 128/AES 256	-FIPS 140-2 level 3 -CC in process -AES 256
Bottom line	Specialized appliance for high security needs and granular encryption	Seamless integration into storage array taking full advantage of existing Data ONTAP storage efficiency features	Integrated in fabric switch and offers high performance for FC environments

SHOULD I MIGRATE MY CUSTOMERS FROM DATAFORT TO NSE?

NSE might not be a suitable migration path for all DataFort customers since 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/volumes encrypted with DataFort to the new storage array. There is no in-place upgrade or migration since DataFort and NSE use different encryption data formats.

NSE is best positioned as a net-new installation.

MY CUSTOMER USES CRYPTOSHRED CAPABILITY IN DATAFORT. HOW CAN THIS BE ACCOMPLISHED WITH NSE?

NSE wraps the data encryption key contained within 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) will disable any ability to access encrypted data. During runtime, Data ONTAP also supports commands to sanitize the drive or also permanently disable the drive so further data access will be impossible.

KEY MANAGEMENT

WHAT IS KMIP?

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. KMIP appears to have supplanted IEEE P1619.3, which was an earlier proposed standard.

HOW DOES NSE COMMUNICATE WITH THE KMIP SERVER?

NSE uses Secure Sockets Layer (SSL) certificates to establish secure communications with the KMIP server. These certificates need to be in Base64-encoded X.509 PEM format and can be either self-signed or signed by a certificate authority (CA).

DOES NSE REQUIRE AN EXTERNAL KEY MANAGER?

NSE does require an external key manager and supports up to 4 key managers simultaneously.

WHICH KEY MANAGERS DOES NSE SUPPORT?

NSE with Data ONTAP 8.1RC3 will support IBM's Tivoli Key Lifecycle Management Version 2 (TKLMv2) server and the SafeNet KeySecure k460 key management appliance. 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?

SafeNet KeySecure k460 can be ordered from NetApp.

IBM TKLMv2 needs to be ordered via an external IBM reseller.

HOW DOES KEY MANAGEMENT FOR NSE WORK?

NSE drives have built-in data encryption keys (DEKs) that never leave the drives. The DEKs are used to encrypt and decrypt data on the drive. The DEKs 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 will request the AK from the key manager. Upon 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?

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

ARE KEYS SYNCHRONIZED BETWEEN KEY MANAGERS?

High availability of keys is assured by allowing the NSE client to send keys to up to 4 key management servers. Key manager synchronization is dependent upon the vendor implementation.

IBM TKLMv2 provides an ability to export its key database and import into another TKLMv2 instance for key replication.

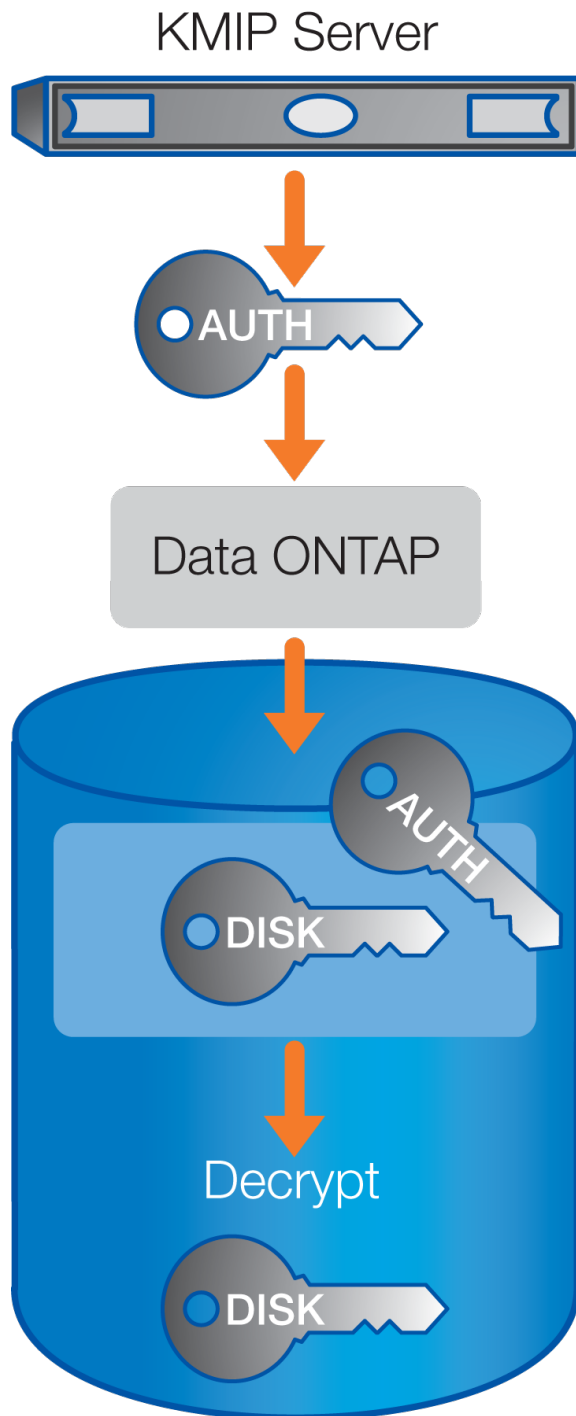
SafeNet KeySecure k460 provides automatic key synchronization for clustered key managers.

It is highly recommended that backups of your key management servers be made on a periodic basis to make sure of availability of keys. Check with your key management provider for information on how to back up your key management servers.

FIGURE 1: AUTHENTICATION KEY USE IN NSE

Figure 1 demonstrates how the AK is used to wrap the DEK and is backed up to an external key management server.

Figure 1) Authentication key use in NSE.



© 2012 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, DataFort, Data ONTAP, Lifetime Key Management, MetroCluster, SnapDrive, SnapLock, SnapMirror, and SnapVault are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.