DELL EMC® VMAX3™ AND VMAX ALL FLASH™ DATA AT REST ENCRYPTION

ABSTRACT

In the interconnected world, data and intellectual property is the highest value currency which can be held by corporations. From recent newsworthy examples, it is still evident that this currency is still vulnerable to intrusion and theft within the modern corporate data center. Often, this data is compromised by physical theft, misplacement, or the inappropriate redeployment or disposal of internal storage from computers or storage arrays. Dell EMC VMAX3 and VMAX All Flash Data at Rest Encryption (D@RE) provides an industry leading solution to protect and secure customer data from drive loss and theft. This white paper explains the features and operations behind D@RE and how it secures customer data.

May, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
Audience 4
Terminology 4
DATA AT REST ENCRYPTION 5
KEY MANAGEMENT 5
EMBEDDED KEY MANAGER 6
EXTERNAL KEY MANAGER 6
KEY MANAGER COMPONENTS 7
Embbedded Management Components 7
External Key Management Components 7
Data Encryption Key Protection 7
Data Encryption Key Recovery 8
Data Encryption Key Integrity 8
VAULTING WITH D@RE 8
OPERATIONAL EXAMPLES 8
Installation of a VMAX3 and VMAX All Flash System 8
Installation with Embedded Key Manager 8
Installation with External Key Manager 9
Replacement of a Drive 9
Decommissioning of a VMAX3 and VMAX All Flash System 9
Decommission with Embedded Key Manager 9
Decommission with External Key Manager 10
DATA AT REST ENCRYPTION CONSIDERATIONS 10
CONCLUSION 10

EXECUTIVE SUMMARY

Securing sensitive data is one of the greatest challenges faced by many enterprises. Increasing regulatory and legislative demands and the constantly changing threat landscape have brought data security to the forefront of IT issues. Several of the most important data security threats are related to protection of the storage environment, where drive loss and theft are primary risk factors. Dell EMC VMAX3 and VMAX All Flash Data at Rest Encryption (D@RE) protects data confidentiality by adding back-end encryption to the entire array.

D@RE provides hardware-based, on-array, back-end encryption for VMAX3 and VMAX All Flash arrays with FIPS 140-2 validated SAS I/O modules that use the 256-bit AES-XTS encryption algorithm. These modules encrypt and decrypt data as it is being written to or read from physical drives, which protects information from unauthorized access even when physical drives are removed from the array.

AUDIENCE

This white paper is intended for:

- Customers, including IT planners, storage architects, and administrators involved in evaluating, acquiring, managing, operating, or designing security for a Dell EMC networked storage environment.
- Dell EMC staff and partners, for guidance and development of proposals.

TERMINOLOGY

Terms	Definition
Drive Array Enclosure (DAE)	Storage module that contains fully redundant drives, link control cards (LCCs), and power supplies and cooling components.
HYPERMAX OS	Dell EMC VMAX3 and VMAX All Flash arrays run HYPERMAX operating environment.
Audit Log	An immutable audit log that tracks security events on a VMAX3 or VMAX All Flash array. The audit log allows administrators to identify any breaches in the array and prove compliance with data protection policies.
Management Module Control Station (MMCS)	A component that monitors the array environment, provides remote notification and remote support capabilities, and allows Dell EMC personnel to access the array locally or remotely.
SymmWin Application	A graphics-based tool used by Dell EMC personnel for configuring and monitoring VMAX3 and VMAX All Flash arrays.
SAS I/O Module	Component that contains a 256-bit AES-XTS encryption controller and provides connectivity to DAEs. The Key Encryption Key is programmed into write-only, non-volatile memory in the I/O module.

Term	Definition
AES-XTS Algorithm	An XEX-based Tweaked Codebook (TCB) mode with Cipher Text Stealing (XTS) disk encryption used for the encryption of sector-based storage devices.
Data Encryption Key (DEK)	Used by VMAX3 and VMAX All Flash encryption algorithms to encrypt and decrypt data and apply confidentiality protection to information.
Key Encryption Key (KEK)	Keeps DEKs secure during storage and transmission. The approved technique to protect DEKs is to use KEKs along with the AES Key Wrap algorithm.
RSA Embedded Data Protection Manager	Embedded Data Protection Manager (eDPM) provides onboard set-and-forget data at rest encryption services.
Key Management Interoperability Protocol Client	Client software that allows for separation of key management between VMAX3 or VMAX All Flash arrays and a KMIP based key management server.

Table 1 - Terminology

DATA AT REST ENCRYPTION

Data at Rest Encryption (D@RE) provides hardware-based, on-array, back-end encryption for VMAX3 and VMAX All Flash systems. Back-end encryption protects your information from unauthorized access when physical drives are removed from the system. D@RE provides encryption on the back-end using SAS I/O modules that incorporate 256-bit AES-XTS data encryption. These modules encrypt and decrypt data as it is being written to or read from a physical drive. All configured drives are encrypted, including both data and spare drives using a unique DEK per drive. In addition, all cached user data stored in Power Vault is encrypted.

D@RE incorporates RSA Embedded Data Protection Manager (eDPM) for on-board set-and-forget key management.

D@RE can also be deployed with an external key manager using KMIP, which provides external centralized key storage and management which simplifies key generation and recovery management for VMAX3 and VMAX All Flash and other KMIP compatible encryption solutions.

By securing data on VMAX3 and VMAX All Flash systems, D@RE ensures that the potential exposure of sensitive data on discarded, misplaced, or stolen media is reduced or eliminated. As long as the key used to encrypt the data is secured, encrypted data cannot be read. In addition to protecting against threats related to physical removal of media, this also means that media can readily be repurposed by process of data cryptoshredding, which destroys the encryption key used for securing the data previously stored on that media.

D@RE is compatible with all VMAX3 and VMAX All Flash system features, allows for encryption of any supported drive type or volume emulation, and delivers powerful encryption without performance degradation or disruption to existing applications or infrastructure.

KEY MANAGEMENT

Because encryption offers protection for the data itself rather than for a device or host, it is a powerful tool for enforcing security policies. However, the data security provided by encryption is only as good as the generation, protection, and management of the keys used in the encryption process. Encryption keys must be available when they are needed, but at the same time access to the keys during decryption activities must be preserved for the lifetime of the data. This is especially important for the enterprise storage environments where encrypted data is kept for many years. D@RE offers flexible key management options with both Embedded and External Key Managers.

EMBEDDED KEY MANAGER

Because of the critical importance of key management in encryption solutions, D@RE was designed to be integrated with RSA Embedded Data Protection Manager (eDPM). RSA eDPM provides enterprise key management for a broad range of encryption environments, establishing a pervasive and secure infrastructure for this essential component of data security. All key generation, distribution, and management capabilities required for D@RE are provided by RSA Embedded Data Protection Manager, according to the best practices defined by industry standards such as NIST 800-57 and ISO 11770.

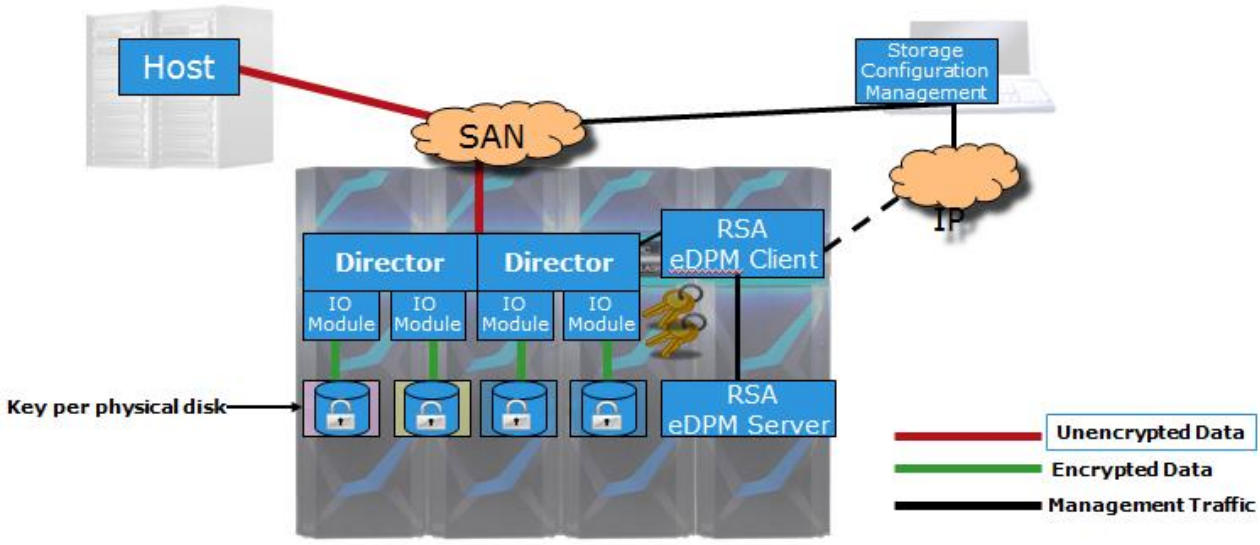

Figure 1 - Embedded Key Manager Architecture

EXTERNAL KEY MANAGER

D@RE can also be deployed with external key managers using KMIP (Key Management Interoperability Protocol) which will allow for a separation of key management from VMAX3 and VMAX All Flash arrays. KMIP is an industry standard that defines message formats for the manipulation of cryptographic keys on a key management server. External key managers provide support for consolidated key management and allows integration between VMAX3 and VMAX All Flash arrays with an already existing key management infrastructure with the ability to non-disruptively migrate keys from embedded key manager. External key management also offers the ability to cluster multiple key servers appliances and separate key ownership and management individually while providing a centralized audit log. Depending on the specific capabilities of the external key manager, HSM integration can provide FIPS 140-2 Level 3 compliance.

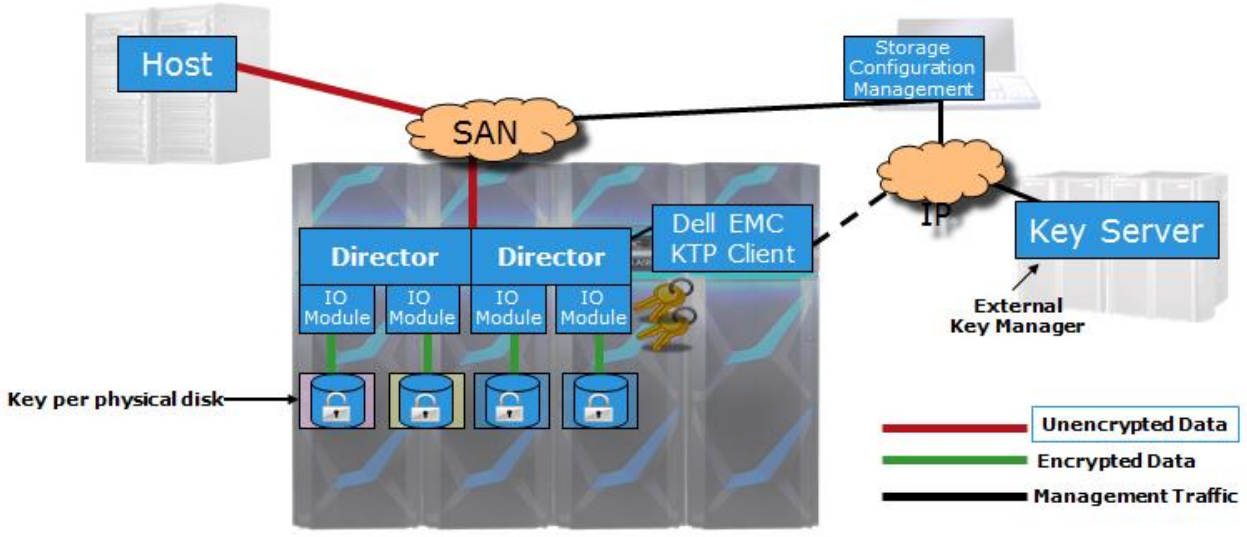

Figure 2 - External Key Manager Architecture

KEY MANAGER COMPONENTS

The following are the components for embedded and external key manager:

EMBBEDDED MANAGEMENT COMPONENTS

Embedded management utilizes the following RSA software, which resides on the primary Management Module Control Station (MMCS):

- eDPM Server – Embedded Key Manager which provides encryption key management capabilities such as secure key generation, storage, distribution, and audit.
- eDPM Client– Client software that handles communication with the Embedded Data Protection Manager Server.
- BSAFE® Cryptographic Libraries – This provides foundational security functionality for Embedded Data Protection Manager Server and Embedded Data Protection Manager Client.
- Common Security Toolkit (CST) Secure Lockbox – An encrypted repository that securely stores passwords and other sensitive key manager configuration information.

EXTERNAL KEY MANAGEMENT COMPONENTS

External management unitizes the following:

- Key Trust Platform (KTP) Client – Client software that runs securely on the MMCS and facilitates communication between the external key manager and VMAX3 or VMAX All Flash system.
- BSAFE® Cryptographic Libraries – This provides foundational security functionality for the external key management server and KTP Client.
- Common Security Toolkit (CST) Secure Lockbox – An encrypted repository that securely stores passwords and other sensitive key manager configuration information.

VMAX3 and VMAX All Flash can interoperate with the following external key manager platforms:

- Gemalto (SafeNet) KeySecure
- KeySecure, IBM Secure Key Lifecycle Manager

Note: The above external key managers are offered as of publication date. Please check with Dell EMC to confirm support for any additional external key managers.

DATA ENCRYPTION KEY PROTECTION

The following ensures the protection of DEKs:

- For embedded D@RE, the local key repository is encrypted with 256-bit AES using a random generated password which is saved in the secure lockbox.
- Lockbox is protected by PKCS#12 using Primary MMCS-specific stable system values (SSVs).
  - Removal of an MMCS will not allow file access without valid SSC credentials.
  - Copying lockbox repository files will fail SSV tests.
- For D@RE with external key management, the secure lockbox contains the PKCS#12 password that protects the VMAX3 or VMAX All Flash client's TLS authentication private key.
- All persistent key storage locations either contain wrapped or encrypted keys.
- There are no backdoor keys or passwords to bypass security.

DATA ENCRYPTION KEY RECOVERY

The following is information on recovery of the encryption keys:

- External key managers only need to be available during initial installation, back-end maintenance or upgrades, or in an unlikely system recovery event.
- The array can come online without the MMCS being available, using keys persistently cached on the array itself.
- MMCS key management components can restore the D@RE configuration and keys directly from the array, in most cases.

DATA ENCRYPTION KEY INTEGRITY

The following features ensure the integrity of the DEKs:

- Data keys exported to the array include a unique keytag identity alias along with the key metadata, which is appended to key data during the keywrap process along with an AES Key Wrap required constant Initial Value (IV).
- During encryption I/O, the expected keytag associated with the drive is separately supplied along with the wrapped key.
- During key unwrap (prior to starting an I/O) the encryption hardware checks for both valid IV and matching keytag to ensure the correct key is being used to protect data on a specific drive.
- Arrays with data encryption enabled have a special Physical Information Block (PHIB) located in a reserved system area at the beginning of each drive. Before the drive is made available for normal I/O operation, the PHIB contents are used to validate that the key being used to encrypt the drive matches the last known key in use by the array.

VAULTING WITH D@RE

VMAX3 and VMAX All Flash arrays have the capability to encrypt data in cache during the vault process in the event of the system being powered down. The vault image is encrypted and then saved on the Flash I/O modules. The back-end SAS I/O modules running in loopback mode provide services to encrypt/decrypt the Power Vault image during vault operations. There is a unique DEK for each director board's set of Flash I/O modules in the system and flash DEKs are managed similar to normal drive DEKs.

For more information on vaulting in VMAX3 and VMAX All Flash arrays, see the Vaulting section of the *Dell EMC VMAX ALL Flash and VMAX3 Reliability, Availability, and Serviceability* Technical Notes.

OPERATIONAL EXAMPLES

This following sections describe how Data at Rest Encryption works during common VMAX3 and VMAX All Flash operations.

INSTALLATION OF A VMAX3 AND VMAX ALL FLASH SYSTEM

Once the VMAX3 or VMAX All Flash system has been properly sized, D@RE can be enabled in the BIN file from Dell EMC Manufacturing or onsite prior to installation:

Note: If the system is currently installed and customer wants to upgrade to D@RE, the customer will need to work with their account team and an RPQ will need to be submitted.

Installation with Embedded Key Manager

1. Once the VMAX3 or VMAX All Flash is at the customer site, the Dell EMC field personnel will start the installation process.
2. The installation script automatically installs the RSA software on the Primary MMCS.
3. The RSA Embedded Key Manager Server generates DEKs for each drive that is installed in the system and a KEK that is unique to that system.
4. HYPERMAX OS generates an entry in the VMAX Audit Log for every key generation event.
5. The RSA Embedded Data Protection Manager Server encrypts the keys and stores them in the local key repository file (lockbox) as non-volatile copies.

6. The RSA Embedded Data Protection Manager Client wraps each DEK with the KEK, and HYPERMAX OS stores all of the keys on the system as encrypted, persistent backup copies.

7. HYPERMAX OS initializes volumes using DEKs and writes any incoming host data to the drives as encrypted data.

Installation with External Key Manager

1. Once the VMAX3 or VMAX All Flash is at the customer site, the Dell EMC field personnel will start the installation process.

2. Enterprise Key Server option will be selected during installation script.

3. IP address and port number as well as certificate authentication information and application registration name will be input by the Dell EMC field personnel.

4. The script performs the following:

    a. Verifies the supplied server configuration information

    b. Verifies that the external key manager is correctly configured.

    c. Asks the key manager to generate a KEK for the array and HMAC key.

    d. Asks the key manager to generate a DEK for each drive.

    e. Initializes the VMAX array with these D@RE objects, and performs the rest of the generic initial configuration steps such as cable verification and VTOC.

    f. Backs up the KTP Client configuration details to the array for use during an MMCS replacement or during a HYPERMAX OS non-disruptive upgrade.

    g. Populates the VMAX Audit Log with D@RE security events pertaining to this installation.

REPLACEMENT OF A DRIVE

In the event of a failed drive:

1. The Dell EMC field personnel will remove the failed drive from the system.

2. Once the drive has been removed from the array, the RSA Embedded Data Protection Manager Server securely deletes that key from the key repository on the MMCS. If using an external key manager, the KTP client will request the KMIP server to securely delete the key.

3. After the Dell EMC field personnel installs the new drive and HYPERMAX OS verifies that the new drive is functional, the RSA Embedded Data Protection Manager Server generates a new DEK for the drive and wraps the DEK using the KEK. For external key manager configurations, the KMIP server will generate a new DEK and return it to the array to be wrapped with the KEK by the KTP client.

4. HYPERMAX OS generates an entry in the Audit Log for the deletion of the old DEK and the creation of the new DEK.

5. HYPERMAX OS caches the new DEK, which replaces the previous DEK.

6. HYPERMAX OS rebuilds the drive data using the new DEK.

DECOMMISSIONING OF A VMAX3 AND VMAX ALL FLASH SYSTEM

In the event a VMAX3 or VMAX All Flash array will be decommissioned by a Dell EMC field personnel:

Decommission with Embedded Key Manager

1. The Dell EMC field personnel will start the D@RE Array Decommission script.

2. The RSA Embedded Data Protection Server securely deletes all persistent copies of the keys in the key repository.

3. HYPERMAX OS securely deletes the cached keys that are stored within the system, making the Audit Log irretrievable.

4. A certificate file is produced detailing the deletion of all keys during the decommissioning of the system.

Decommission with External Key Manager

1. The Dell EMC field personnel will start the D@RE Array Decommission script.
2. The KTP client instructs the KMIP external key manager server to securely delete each of the array's keys.
3. The system is taken offline.
4. All keys and authentication credentials are zeroized within the array.
5. A certificate file that details the decommission results is produced on the MMCS.

DATA AT REST ENCRYPTION CONSIDERATIONS

The following options apply to D@RE for the VMAX3 and VMAX All Flash systems:

- Because Data at Rest Encryption can only be configured during initial install, the system will need to be properly sized and the D@RE flag set when the array is initialized at Dell EMC Manufacturing.
- Once the D@RE flag has been set it cannot be disabled without the VMAX3 or VMAX All Flash system being initialized again which will erase all data on the system.
- Mixing encrypted and unencrypted data on the system is not supported.

Note: If the VMAX3 or VMAX All Flash system has already been installed and the customer wants to enable D@RE as an upgrade, the customer will need to work closely with their account team.

CONCLUSTION

Data At Rest Encryption is an easy-to-use solution that keeps sensitive data safe from drive theft or loss by providing back-end encryption for the entire system. The VMAX3 and VMAX All Flash systems can utilize either RSA Embedded Data Protection Manager or external key management using the standard KMIP protocol. Embedded key management allows the system to self-manage encryption keys. External key management allows the end user to manage keys on an external management server for centralized key storage. D@RE incorporates other important key management components such as Embedded Data Protection Manager, BSAFE Cryptographic Libraries, and CST Secure Lockbox. VMAX3 and VMAX All Flash also offer encryption during a vaulting operation in the event of a system power down, securing all data in cache to flash I/O modules. Through these components, D@RE offers Data Encryption Key protection, recovery and integrity to ensure all sensitive data is secure.