



Enterprise-Class Key Management For Heterogeneous Storage Security

**Decru Lifetime Key Management™
(LKM) System**

White Paper
August 2006

Table of Contents

Evaluating a Storage Security Solution

Introduction	4
Decru DataFort™ Storage Security Appliances	4
High Availability	5
Strong Authentication Support.....	6
Lifetime Key Management™ (LKM) Software	6
Decru LKM Appliance	7
Key Management Lifecycle	9
Decru OpenKey™ APIs for Third Party Encryption Devices.....	10
System Security Features	10
Migration from LKM Software to LKM Appliance	10
LKM Appliance Deployment Best Practices	11
LKM Deployment Example	12
Conclusion	13
Appendix	14
Decru DataFort Deployment Examples	14
High Availability NAS Deployment.....	14
Inline Fibre Channel Deployment	15
Fabric-Attached Fibre Channel Deployment.....	16

Executive Summary

For many organizations, the business drivers for securing stored data are becoming obvious: high-profile security breaches, identity theft, brand damage, regulatory penalties, and increased legal liability have all underscored the importance of securing large data repositories. As organizations acknowledge their increasing vulnerability to data theft, and the potential costs, they are turning to encryption as a way to lock down sensitive information.

In fact, Gartner Research recently published a study that estimated the costs of a privacy breach, and the costs of prevention. Based on data from actual incidents, Gartner calculated that the cost per identity lost was approximately \$90, not counting brand damage, regulatory penalties, or legal judgments. The study noted that encryption would have prevented many of the breaches, and Gartner estimated the cost of deploying encryption at \$6 per customer record.

Hardware-based encryption solutions like Decru DataFort™ appliances have removed many of the traditional encryption concerns such as performance degradation or application-dependency. For many organizations, encrypting data is now technically and operationally feasible. Increasingly, the larger concern is managing the associated encryption keys that are used across multiple, disparate systems. Data is both persistent and mobile in today's global enterprises, and must be kept for years to comply with mandates, yet it is often stored in many different locations for availability, disaster recovery, and information sharing. Without automated, global access to the keys, the data may as well be lost.

In order to ensure that data is properly secured while remaining available to authorized users, an enterprise-class, secure key management system is critical. You should carefully consider several aspects of an enterprise data encryption and key management system including:

- Support for your infrastructure – today and in the future (e.g. support for strategic vendors, operating systems, applications, networks, etc.)
- Performance, scalability, and support for enterprise disaster recovery requirements
- Ability to manage encryption keys and policies across multiple platforms and vendors
- Security of the key management system, and support for a variety of security policies and auditing procedures

This document will explain Decru's industry-proven encryption and key management architecture, including the capabilities of the Decru Lifetime Key Management™ (LKM) 3.0 Appliance. Further, it will explore how this system allows you to efficiently and securely manage your sensitive data over time and across your enterprise.

Introduction

Decru's storage security solution consists of Decru DataFort™ storage security appliances and Decru Lifetime Key Management™ system.

Decru DataFort™ Storage Security Appliances

Decru DataFort appliances use wire-speed encryption, authentication, and access controls to secure stored data. Decru appliances can be deployed transparently in NAS, DAS, IP SAN, FC SAN and Tape environments, with no changes to servers, desktops, applications, or user workflow. By locking down stored data with strong encryption, and routing all access through secure hardware, DataFort radically simplifies the security model for networked storage.

There are three families of Decru DataFort appliances. DataFort E-Series supports Gigabit Ethernet for NAS and IP SAN environments. DataFort FC-Series appliances support Fibre Channel (SAN) networks for disk and tape encryption. DataFort S-Series appliances support direct SCSI tape encryption.

Decru DataFort appliances are engineered to handle enterprise-class requirements, including:

Strong Security – All encryption and key management are handled in secure hardware, ensuring maximum security with minimum complexity for end users and administrators. Decru DataFort's encryption engine, the Storage Encryption Processor (SEP), has been certified by NIST for compliance with FIPS 140-2, level 3, and is encased in hardened epoxy to thwart physical laboratory attacks on the processor. The chassis is tamper-evident, and armed with intrusion prevention capabilities.

Interoperability –DataFort is compatible all open systems storage environments, and works seamlessly with existing backup configurations and mechanisms, as well as third-party backup software such as Symantec, Tivoli Storage Manager (TSM) and Legato.

Transparency – DataFort can be deployed transparently into the existing infrastructure, without requiring changes to clients, servers or backup processes. In fact, existing data can be encrypted or rekeyed in place with zero downtime for applications.

Performance – Hardware-based encryption and compression enables multi-gigabit, wire speed performance. For example, Decru's FC1020 appliance provides total throughput of 10 Gbps for encryption and compression in tape environments, in a compact 2U chassis.

During normal runtime operation, each DataFort appliance uses the True Random Number Generator (TRNG) encapsulated in its Storage Encryption Processor to generate strong, high-entropy keys. Each appliance generates the keys, associates them with data based on policies, and maintains metadata about which key was used to encrypt each piece of data. When an authorized user or application requests the data, it is transparently decrypted and presented by DataFort, with no changes in user workflow or software.

High Availability

Today's global, distributed enterprises make multiple copies of data to support high availability, disaster recovery, data mining, and information sharing with clients or partners. Encryption provides a powerful enforcement mechanism to ensure sensitive data is not compromised during these activities, but it is critical to have a key management system that can support these requirements. Reference or regulated data may be stored for years, even if it is not regularly accessed.

In addition to security requirements, most organizations have disaster recovery requirements for critical data and applications. The Decru platform, including DataFort appliances and LKM, provide multi-layered recovery capabilities to insure uninterrupted access to encrypted data. Recovery and high availability methods include:

1. **Clustering:** DataFort appliances can be deployed in clusters, securely sharing key material for failover, load balancing and improved throughput. If a cluster member fails, the other DataFort appliances will continue encrypting and decrypting data to insure uninterrupted data access.
2. **Replacing a Cluster Member:** A failed DataFort can be quickly replaced by adding a "factory-fresh" DataFort appliance to the cluster. For this procedure, a quorum of Recovery Cards is needed to inject the required key material. (e.g. 2 out of 5, 3 out of 5 smart cards). There is a more detailed explanation of Smart Cards used in the Decru system further along in this document.
3. **Cloning:** If a DataFort is not part of a cluster, a fresh DataFort can also be cloned by combining a quorum of Recovery Cards with a Configuration Database. This file contains encrypted keys and system configurations, and can be stored independently or in the Lifetime Key Management system.
4. **Software-based Recovery:** Decru also provides a software recovery tool called Decru Decryption Software (DDS) which allows an administrator or business partner to decrypt necessary data from a file, a Cryptainer™ vault, or an entire DataFort, without requiring a

DataFort appliance. A Recovery Card quorum and Configuration Database are needed for this procedure. The Data Decryption Software can be stored on media alongside encrypted data, ensuring ready access to data archives even if no DataFort appliances are available.

Strong Authentication Support

Decru DataFort appliances and the new Decru LKM Appliance both utilize smart card technology to provide strong authentication to administrators for sensitive activities. There are three types of smart cards used in these systems:

System Cards are unique to each LKM Appliance and are used as an 'ignition key' to start key management processes. The System Card is required for the LKM Appliance to boot and provides physical security for the appliance. The System Card can be removed to protect encryption keys during shipment or periods of reduced physical security.

Admin Cards are used to authenticate communication between the administrator and LKM Appliance. Access for each administrator can be tailored to security policies using included Role Based Access Control (RBAC) features, enabling secure and granular delegation of administrative rights to multiple individuals.

Recovery Cards are used in sets to restore encrypted data or disabled LKM Appliances, and to replace other smart cards. Each Recovery Card belongs to a Recovery Officer, who is a highly trusted individual in the organization. Officers must present cards and passwords before a recovery procedure that could threaten data security can be performed.

Lifetime Key Management™ (LKM) Software

Decru has been shipping LKM software since mid-2003, supporting many of the world's largest storage encryption deployments. Through version 2.5, LKM has been implemented as host-based application, leveraging secure hardware in DataFort appliances. DataFort appliances send encrypted keys and configuration information to the LKM server for long term storage, and request keys from LKM as required for data access. All keys and configuration information are encrypted before leaving the DataFort appliance's secure hardware, and all links between appliances and LKM are further secured with SSL encryption to prevent eavesdropping and data access by unauthorized parties attempting to access stored data.

As enterprise encryption rollouts have grown in size, many customers have identified requirements for a key management platform that can support deployments ranging from a

handful of DataFort appliances and scaling up to hundreds of globally distributed encryption devices. Additionally, enterprises have begun to consider centralized key management requirements for handling encryption at multiple layers of the IT infrastructure, including applications, tape drives and storage arrays. Decru's LKM 3.0 Appliance is designed to address these requirements.

Decru LKM Appliance

The Lifetime Key Management™ 3.0 Appliance is Decru's third generation key management platform, delivering centralized, enterprise-class key management for distributed encryption environments.

The LKM Appliance 3.0 is a hardened 2U appliance, providing robust features to automate the key management lifecycle:

Mature platform: The Decru key management platform has been proven in demanding real-world enterprise and government deployments, supporting large clusters of encryption devices across multiple distributed data centers.

Scalability: Each appliance can securely store more than 10 million encryption keys, enabling granular encryption and information sharing policies (for example, a unique key for every backup tape). An LKM fabric consisting of up to 16 clustered appliances can scale to support over a thousand encryption devices.

Secure management: The LKM Appliance is also designed for FIPS 140-2 Level 3 physical security. Administrative access is secured by two-factor authentication, role-based access controls, and smart card quorum requirements for sensitive operations.

Automation: The LKM Appliance securely automates key management functions including key generation for third party encryption systems, key replication, archiving, recovery, and sharing. The LKM Appliance and DataFort appliances automatically and securely propagate encryption keys to other authorized LKM systems and utilize features such as key translation and trustee key sharing to enable secure information sharing across groups or companies. Decru CryptoShred™ secure deletion enables sophisticated lifecycle management of encryption keys, including policy-based key expiration.

Heterogeneous support: The LKM Appliance provides centralized key management across all DataFort appliances, enabling enterprise-wide support for NAS, DAS, IP SAN,

FC SAN, and tape storage environments. The LKM Appliance can also be deployed to support both existing and new Decru DataFort appliances.

Open and standards-based: The Decru OpenKey partner program and APIs enable unified support for heterogeneous encryption systems, simplifying the deployment of encryption across multiple environments.

Secure key generation: Many encryption systems lack the ability to generate strong, random encryption keys, significantly reducing the overall level of security. Decru DataFort and the LKM Appliance use a hardware-based true random number generator (TRNG) to create strong, high-entropy keys.

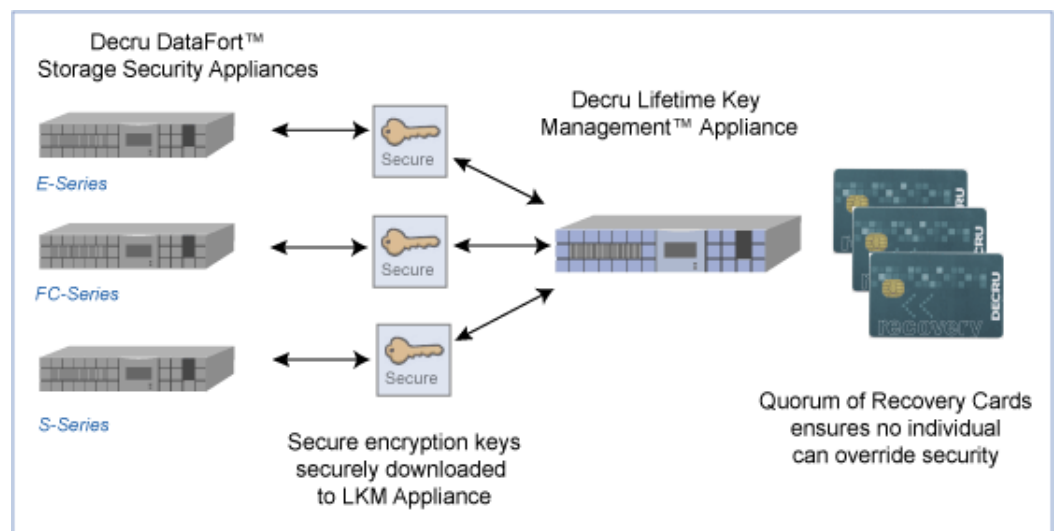


Figure 1: Key Management with Decru LKM

Key Management Lifecycle

The Decru LKM system provides strong security and effective manageability for storage encryption keys throughout their lifecycle:

Key Management Function	Description
Key Generation	LKM Appliance and DataFort utilize hardware-based True Random Number Generation to generate strong, high-entropy keys.
Replication	DataFort appliances can be clustered to automatically replicate encryption keys and policies. Additionally, each DataFort appliance can back up keys to four separate LKM instances. LKM Appliances can create clusters of up to 16 nodes, distributed across multiple sites, providing an additional layer of high availability and failover.
Archiving	LKM Appliance provides a centralized archive of 10 million+ keys per appliance, allowing encryption devices to purge unused keys without affecting archive access.
Recovery	DataFort and LKM Appliance provide sophisticated recovery capabilities. For scenarios where a clustered appliance fails, a new appliance can be added; once a quorum of Recovery Cards are presented, keys and configurations are automatically synchronized to the new cluster member. When local cluster recovery is unavailable, LKM Appliance can provide keys and configuration data to clone a disabled unit.
Sharing	The Decru platform offers multiple functions to enable secure information sharing across business units or partners. LKM Appliance can export or automatically synchronize keys to support remote DataFort appliances and LKM Appliances. Partners can use either Decru Data Decryption Software (DDS) or DataFort appliances to access shared data sent in either tape or electronic formats.
Deletion	Decru CryptoShred™ key deletion features enable “no touch” deletion of distributed data. By deleting associated encryption keys using either manual or automated procedures, CryptoShred features allow organizations to streamline the handling of data lifecycles.

Decru OpenKey™ APIs for Third Party Encryption Devices

Responding to customer demand for greater security, many storage and data management vendors have announced plans to incorporate encryption and security features into their products. For large enterprises, however, the prospect of operating proprietary key management systems for every system and vendor presents substantial challenges.

To address these challenges, Decru has announced new application programming interfaces (APIs) for LKM Appliance that enable centralized, standards-based key management services for multiple third-party encryption systems across the enterprise

The Decru OpenKey program provides partners with standards-based APIs, developer kits, reference implementations, and technical support to facilitate development of interoperable encryption and key management solutions. The OpenKey program builds upon Decru's unique role as an independent security vendor to facilitate development and standards cooperation among competing data management vendors. For more information on the Decru OpenKey partner program, visit: <http://www.decru.com/partners/openkey.htm>

System Security Features

The DataFort and LKM Appliance platforms incorporate a variety of features for secure administration and operation. Many of these features combine electronic security measures with suggested processes to insure appropriate checks and balances within a multi-user enterprise environment.

The LKM Appliance incorporates Decru's FIPS 140-2 Level 3 Storage Encryption Processor (SEP) and includes physical security controls including epoxy-encased encryption processors, battery-backed memory, intrusion detection, and configurable defense settings.

Migration from LKM Software to LKM Appliance

End user organizations that have already deployed LKM software can migrate to LKM Appliance. Decru will provide an upgrade utility to import encryption keys and configuration information from current LKM software installations into an LKM appliance deployment.

LKM Appliance Deployment Best Practices

All security and encryption deployments require procedures to insure the security and resilience of systems across a variety of failure and disaster scenarios. These procedures are incremental to practices that you already employ such as Uninterruptible Power Supplies, redundant network ports, fire control, air conditioning and physical access control for critical systems.

Decru LKM Appliances include a number of configuration and deployment choices that can be adapted to enterprise operational requirements. Decru Professional Services can also offer valuable information and deployment recommendations to ensure optimal security and functionality.

Redundancy – Consider both the number and location of your LKM appliances.

DataFort appliances and LKM Appliances should be geographically and electronically segmented to ensure that disasters do not compromise key availability.

Manageability – LKM appliances are accessed over a secure link from a management utility, which can be installed on a number of systems. Administrators use smart cards to authenticate themselves to the system. It is important to configure your network to maximize availability of the connection to the appliance and availability of workstations with smartcard readers where you will need them.

Logging – DataFort appliances and LKM appliances can both be configured to send log information to external archives for storage, using either Syslog or Windows Events formats. DataFort and LKM Appliance logs are crypto-signed, providing a tamper-evident record of relevant operations. These records of user and administrative actions provide a valuable forensic resource for investigation into events on your network. Environments with high data access traffic should ensure that the archive devices have sufficient storage resources available.

RBAC – DataFort and LKM appliances support a hierarchy of predefined roles such as:

- Full Administrator
- Storage Administrator
- Security Administrator
- Machine Administrator
- Accounts Administrator
- Key Administrator
- Backup Administrator
- Read-Only Administrator

These roles provide granular control over administrative access. Users should consider role definition options to maintain a balance between effective management and strong separation of responsibilities.

Physical Measures – While the LKM appliances themselves are hardened against attack with multiple protection mechanisms including smartcards, they should ideally be maintained in a location that provides physical security for the devices themselves. This practice applies to all major infrastructure components, in order to prevent sabotage or denial-of-service attacks.

Secondary Key Archive – Although not required, you may wish to archive keys outside of the LKM appliance infrastructure. For example, as keys age, you may still need to maintain them, but they are likely to only be used in abnormal situations. In this case, it may make sense to archive them to an offline location and remove them from the appliances themselves.

LKM Deployment Example

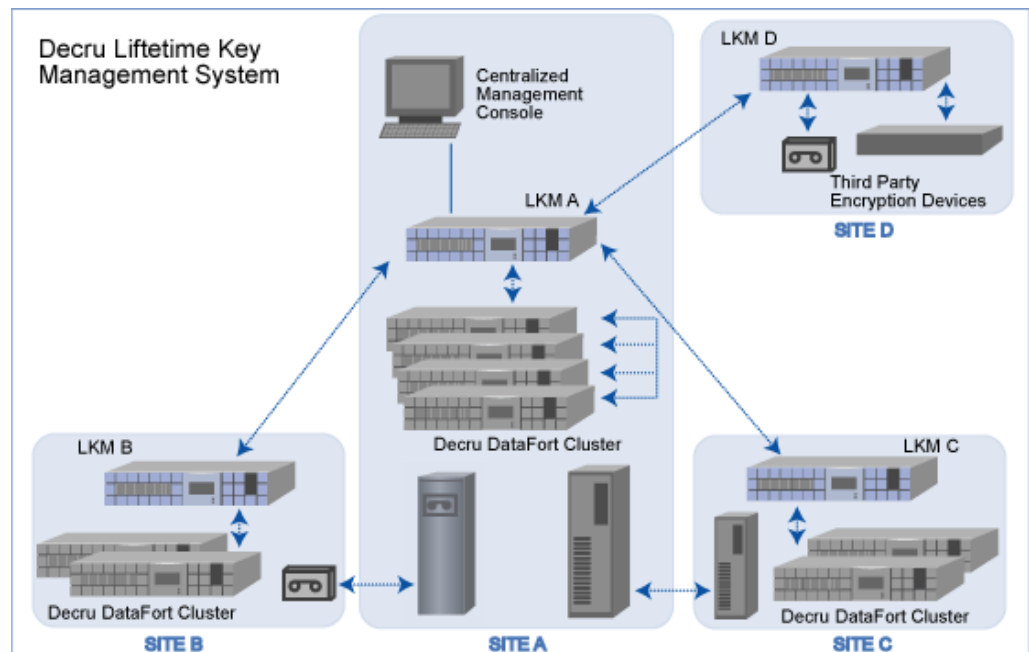


Figure 2: Distributed DataFort and LKM Appliance architecture

Conclusion

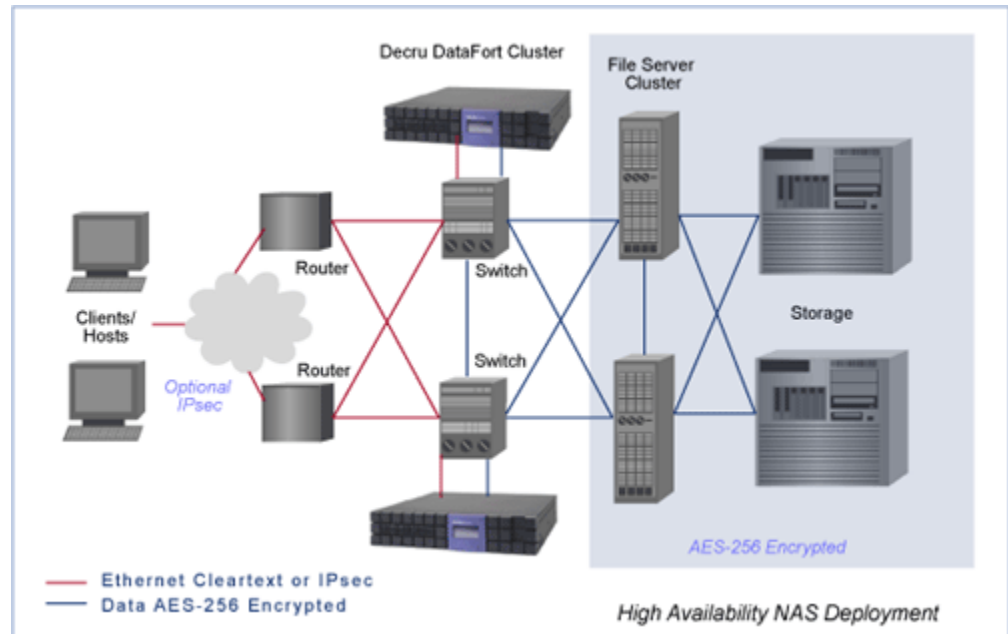
Data encryption is becoming increasingly ubiquitous throughout enterprise storage infrastructures. As new options for encryption devices come to market, your decisions regarding key management investments will affect your long-term security and operational posture.

Decru, the leader in the storage security market, has broken new ground in storage key management since 2003 when LKM software was released. Now, with the release of LKM Appliance, we are further advancing the state of the art for key management systems. With support from leading 3rd party encryption vendors, increased scalability, performance and high availability, and by integrating management capabilities for enterprise DataFort encryption device deployments, LKM appliances will meet your requirements for storage security key management now and in the future. For more information about Decru solutions, visit www.decru.com, or call 1-877-22DECURU.

Appendix

Decru DataFort Deployment Examples

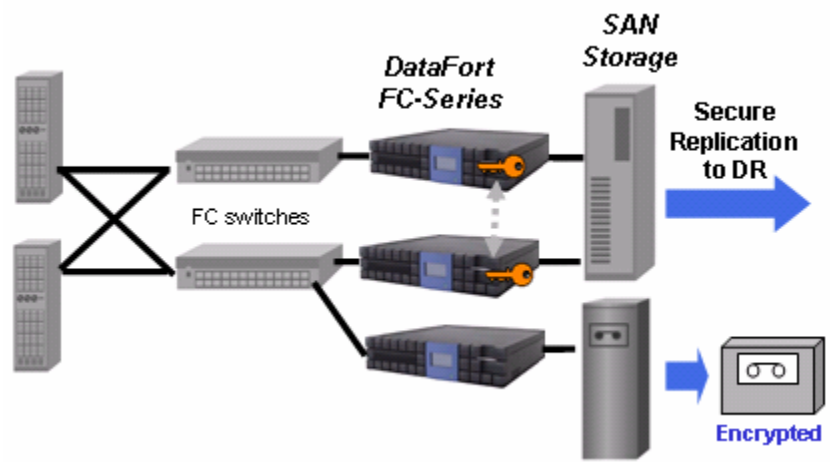
High Availability NAS Deployment



- Provides high-availability storage security in NAS environments
- DataFort appliances are placed on the IP network between department clients and files servers

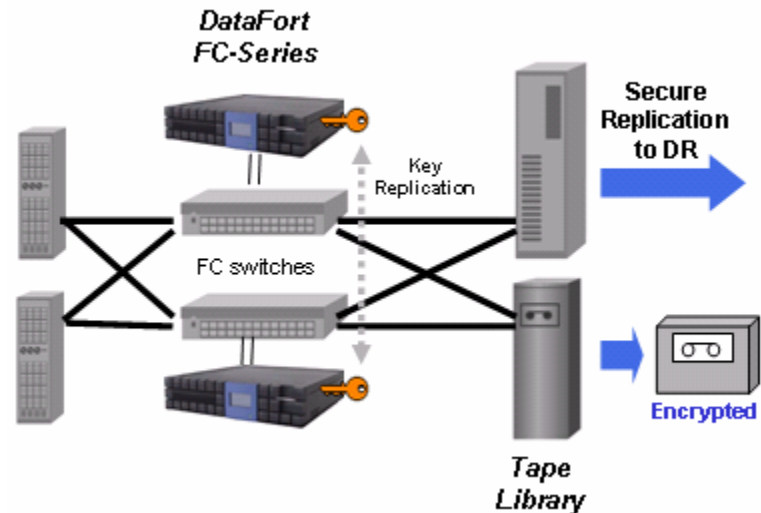
In-line direct connections are also supported

Inline Fibre Channel Deployment



- Enables deployment with no zoning/ reconfiguration of hosts or switches
- All traffic passes through DataFort, can select cleartext/encrypted and access controls per LUN
- DataFort ports used for each data path
- Supports transparent rekeying (zero app downtime for encrypting existing data)
- Can be inserted anywhere between host and storage target

Fabric-Attached Fibre Channel Deployment



- Hosts & storage are selectively zoned to access DataFort
- Only secured traffic flows through DataFort
- Allows fan-in/fan-out, shared utilization, and incremental rollout of encryption
- Supports transparent rekeying (zero app downtime for encrypting existing data)
- Can be deployed with VSANs and other fabric security features

Decru, Cryptainer and CryptoShred are registered trademarks of Decru. Decru DataFort and Lifetime Key Management are trademarks of Decru, a NetApp company. All other trademarks are the property of their respective owners.