



STORAGE AREA NETWORKS

HP StorageWorks Secure Key Manager with Brocade Encryption Solutions

The HP StorageWorks Secure Key Manager ensures trusted key management that integrates with Brocade encryption solutions. HP Secure Advantage and Brocade provide a full range of services to assist in the successful implementation of data-at-rest encryption solutions.



CONTENTS

Introduction.....	3
Overview	3
Key Exchanges	4
Key Management.....	6
Integration Scenarios	6
Disk Encryption Upgrade	6
Decentralized Tape Backup	9
Summary	10

INTRODUCTION

Brocade® and HP® have formed a solid team to enable data-at-rest encryption solutions using the HP Secure Key Manager™ (SKM) with Brocade encryption devices. The Brocade encryption devices and the SKM provide Federal Information Processing Standards 140 (FIPS 140-2) compliance to enable trusted key sharing between remote sites in a comprehensive solution. This fabric-based solution offers data-at-rest encryption at up to 96 Gigabits per second (Gbps).

NOTE: The term “Brocade encryption device” is used in this paper to reference both the Brocade Encryption Switch and the Brocade FS8-18 Encryption Blade.

Brocade and HP offer superb management interfaces and monitoring capabilities. The SKM cluster integrates into the Compliance Log Warehouse (CLW) to offer enterprise-level management of encryption keys and other security events. For regulatory compliance and confidential data sharing, encrypted data and data encryption keys are often required to be transported between sites. The trusted relationship between the Brocade encryption device and the SKM cluster enables simple yet secure key sharing among multiple sites. The HP SKM and its trusted relationship with the Brocade encryption device enable secure and automated key sharing for encrypted data.

This paper focuses on key management with the HP SKM and assumes a basic understanding of the Brocade data-at-rest encryption solutions. White papers that discuss the basics of encryption and aspects of Brocade encryption solutions can be found at www.brocade.com.

OVERVIEW

A quick overview of the equipment in the solution is helpful in understanding the context of the discussion. Brocade recommends deploying encryption with redundant encryption devices and redundant HP SKM nodes. As shown in Figure 1, the components of this scenario include:

- An initiator to read and write the data
- A target to store the data
- A Fibre Channel (FC) fabric, which in this example consists of two Brocade Encryption Switches
- Fabric-based encryption device to secure data-at-rest
- Redundant SKM nodes to manage and store the data encryption keys (DEKs)
- Brocade Data Center Fabric Manager (DCFM™) to manage the fabric and encryption
- A management Local Area Network (LAN) to link the management station and fabric devices (including the encryption devices and other equipment)
- A separate cluster LAN of Gigabit Ethernet (GbE) links between the encryption devices for exchanging DEKs (not shown in Figure 1)

The HP SKM nodes communicate with the Brocade encryption devices via the SKM Application Programming Interface (API). The SKM API is the interface for exchanging DEKs between HP SKM nodes and Brocade encryption devices. The Brocade encryption device generates the DEKs and wraps (encrypts) them before sending them to the SKM node within a Secure Socket Layer (SSL) / Transport Layer Security (TLS) session. SKM nodes manage the DEKs and perform other tasks, which are discussed in the next section.

Figure 1 shows how the DEKs are exchanged between devices in the encryption solution. The DEK is first generated by the Brocade encryption device and sent to the primary SKM appliance. The encryption device then synchronizes DEKs with the other encryption devices in the fabric through the cluster LAN. The SKM nodes are also synchronized between themselves to ensure access to keys if one fails. These redundant key exchanges are crucial to ensuring that the data can be encrypted or decrypted without a single point of failure.

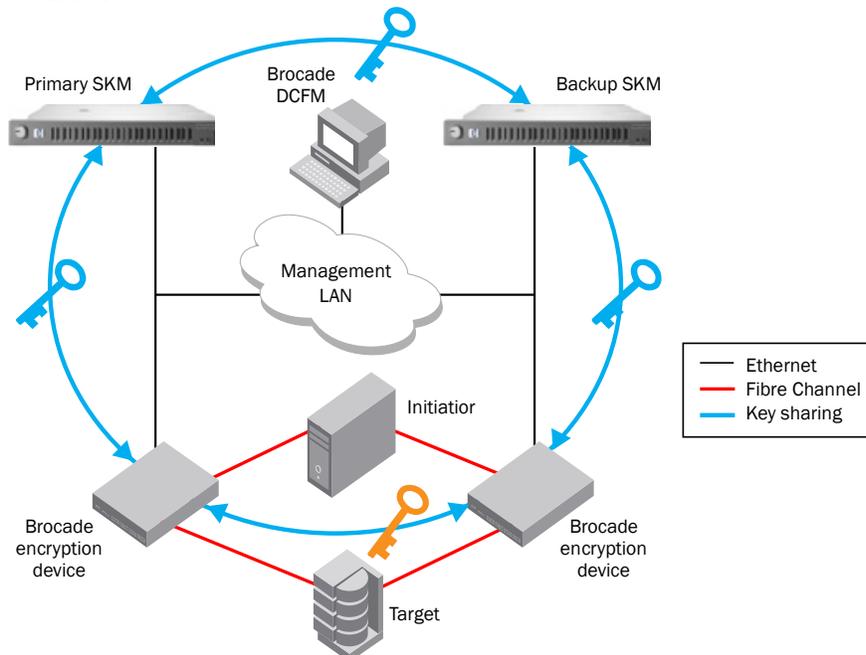


Figure 1. Components of the Brocade-HP solution

KEY EXCHANGES

One of the strengths of this solution is that data encryption keys are protected whenever they leave the FIPS 140-2 Level 3 security boundary in the Brocade encryption devices. The SKM appliance manages the wrapped key that is encrypted as shown in Figure 2. The SKM Appliance manages the various aspects of the key as discussed in the next section.

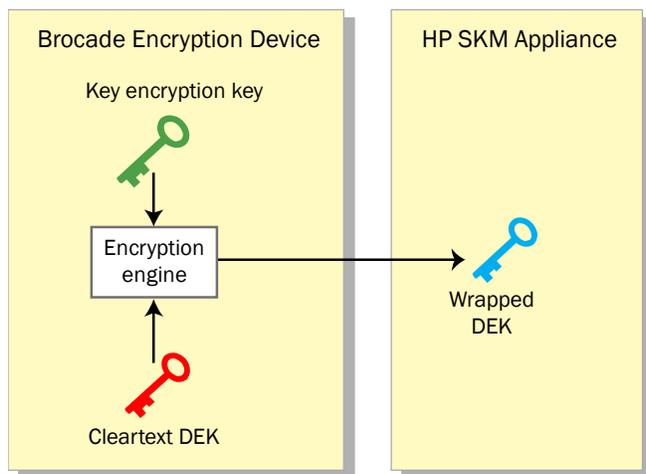


Figure 2. Key exchange between Brocade encryption devices and the HP SKM

When a key needs to be exchanged between Brocade encryption devices, another process is followed so that the encryption device has access to the unwrapped key. The process is described in the following steps and Figure 3.

1. A trusted relationship is created through a secure exchange between the Brocade encryption devices. The trusted link generates a symmetric link key, (shown in green) which is stored in each device and will be used to wrap and unwrap the DEK for secure transport.
2. The Brocade encryption device creates a new DEK in cleartext (shown in red) within its security boundary.
3. The DEK is encrypted (wrapped) with the link key to create a wrapped DEK (shown in orange) before it leaves the encryption boundary.
4. The wrapped key is sent to the other Brocade encryption device in the Secure Socket Layer (SSL) session with a key strength of 256 bits. (Note that the DEK has already been wrapped with the 256-bit strength key so the SSL session key does not weaken the key strength of the system.)
5. After the wrapped key arrives inside the security boundary of the Brocade encryption device, the Brocade encryption device uses its link key to unwrap the DEK to discover the DEK in cleartext (shown in red).

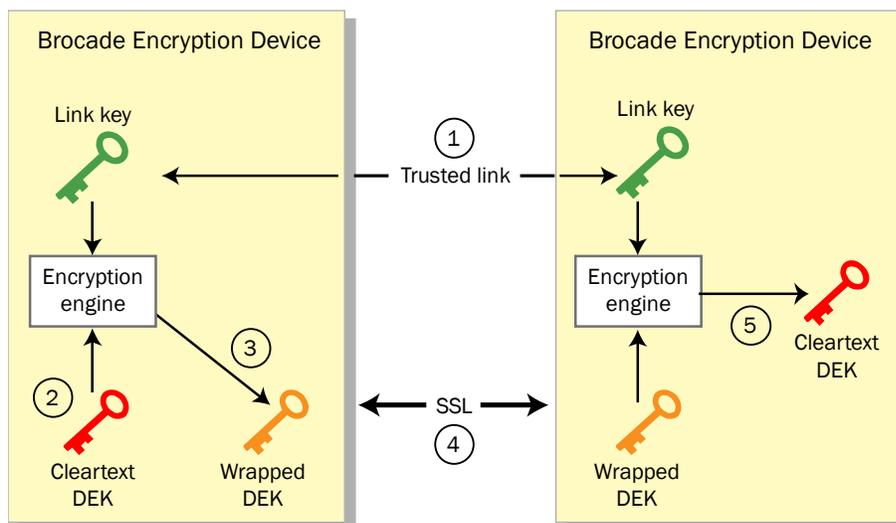


Figure 3. Key exchange between the Brocade encryption devices

KEY MANAGEMENT

The HP StorageWorks Secure Key Manager provides secure centralized encryption key management services for HP LTO-4 enterprise tape libraries and Brocade encryption devices. It is a hardened appliance with digitally signed logs and the following enterprise-class features and functionality:

- Ease of deployment and management
- Operating system and application transparency
- Flexible, secure key enrollment for encrypting devices
- Role-based delegation and multi-admin support
- High availability through cluster failover and remote key replication

The Secure Key Manager has been validated by the National Institute of Standards and Technology (NIST) as compliant with the FIPS 140-2 standard. NIST is a non-regulatory U.S. federal agency established to provide standards in technology; FIPS (Federal Information Processing Standards) 140-2 was developed by NIST to define security requirements for cryptographic modules.

The minimum configuration in a Secure Key Manager deployment consists of two SKM nodes configured in a clustered relationship. For higher availability requirements (including multi-site configurations for disaster recovery), expansion nodes can be added to the initial SKM cluster. Encryption keys, key generation policies, client information, and other settings are automatically replicated asynchronously between nodes within seconds of their creation or alteration (the nodes communicate via Secure Sockets Layer (SSL) connections for all transactions). Each node has its own set of digitally-signed logs that record all events involving the node. These logs are suitable for audit verification and for providing evidence of compliance to security policies. The Secure Key Manager logs can be pushed out to the HP Compliance Log Warehouse for optimal tracking of SKM activities. For more information on the Compliance Log Warehouse, visit www.hp.com/go/clw.

INTEGRATION SCENARIOS

The Brocade-HP partnership offers encryption solutions to meet the needs of the varied environments of corporations and institutions. Whether the customer needs a point product or an international deployment of encryption resources, HP and Brocade offer a solution to help companies become regulations compliant.

Two data-at-rest encryption scenarios are described in this section:

- Disk encryption upgrade
- Remote tape

Disk Encryption Upgrade

Figure 4 shows an initial deployment with a pair of HP Ultrium 1840 LTO-4 tape drives that offer encryption of data-at-rest. The LTO-4 drives are housed in an HP EML 245e tape library to automate backup operations and allow integration with the SKM cluster. This first deployment scenario is a modest step into the world of encryption, which lets the information technology (IT) staff and security officer become familiar with encrypting data for offsite archiving with HP Data Protector. The security officer established policies for DEK sharing between SKM appliances and was confident that they could apply the techniques to other applications and scale the infrastructure to encrypt several more applications as well as encrypting disk. The IT staff decided to use their existing SKM infrastructure and encrypt EVA storage arrays as well as more LTO-4 tape drives.

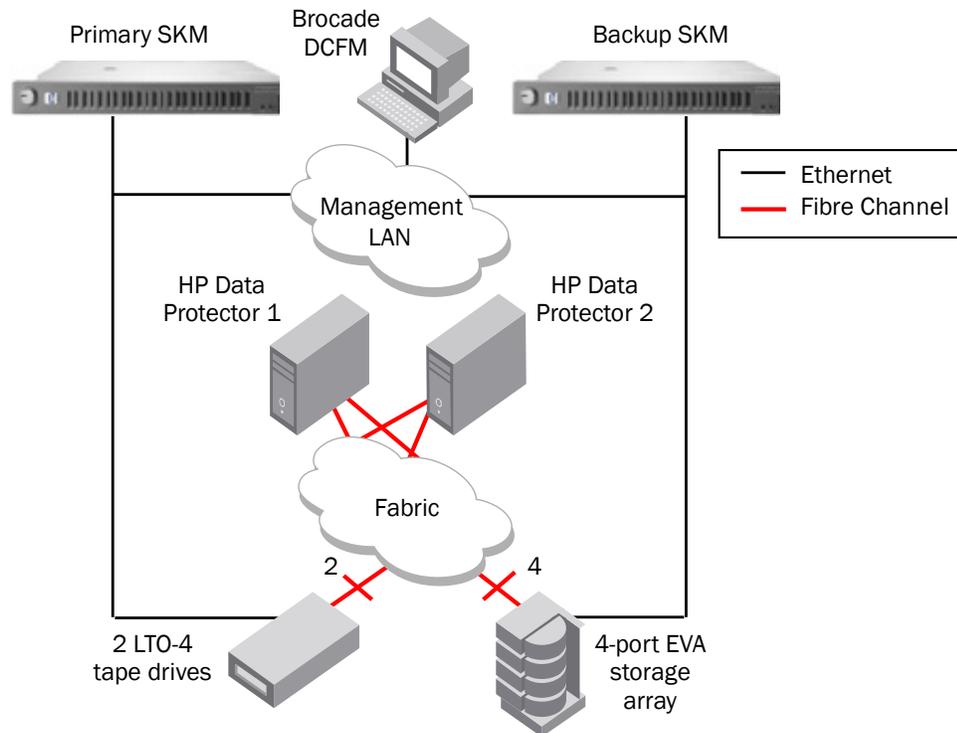


Figure 4. Initial encryption deployment

Figure 5 shows how the organization expanded their encryption solution with more LTO-4 tape drives, blade servers, EVA storage, and Brocade encryption devices. The security officer upgraded the solution to encrypt multiple applications and continued to use the installed base of servers, EVA storage, SKM appliances, Data Protector, and Brocade DCFM management software. The 4-port 4 Gigabit Fibre Channel (4GFC) EVA storage array with 2 terabytes (TB) of storage was upgraded to a 8-port 4GFC EVA array with 64 TB of storage by adding more controller cards and disk arrays. HP BladeSystem servers with server virtualization were used to create flexible deployment of servers that could access encrypted data through the Brocade encryption devices. The IT staff scaled their existing infrastructure with new hardware and software that integrated with their existing solutions.

Since the staff was already familiar with their existing management software (Brocade DCFM) for their storage area network and LTO-4 encryption solution, they were able to quickly encrypt new applications without changing their key management system or backup software. The SKM managed the keys for the LTO-4 tape drives as well as the Brocade encryption devices, which encrypted the disk-based storage. The keys are shared between the redundant Brocade encryption devices and the redundant SKM nodes. As part of a complete encryption ecosystem, the application data was stored in encrypted form on both disk and tape.

The logical view of the encryption process, shown in Figure 6, illustrates how flexible the virtual infrastructure is. The unencrypted data flows start from the virtual servers and flow to Virtual Target 1 (VT1) in the Brocade encryption device. The encryption engine encrypts the data and sends the encrypted data to Logical Unit 1 (LUN 1) from Virtual Initiator 1 (VI1). The encryption is configured on a per-LUN basis so that the users can encrypt only the data that needs to be encrypted. Each virtual server that accesses the LUN must be configured for encryption. The logical infrastructure can easily scale for new applications and new physical infrastructure. The virtual world in the data center has the new capability of ensuring data-at-rest confidentiality at unprecedented data rates.

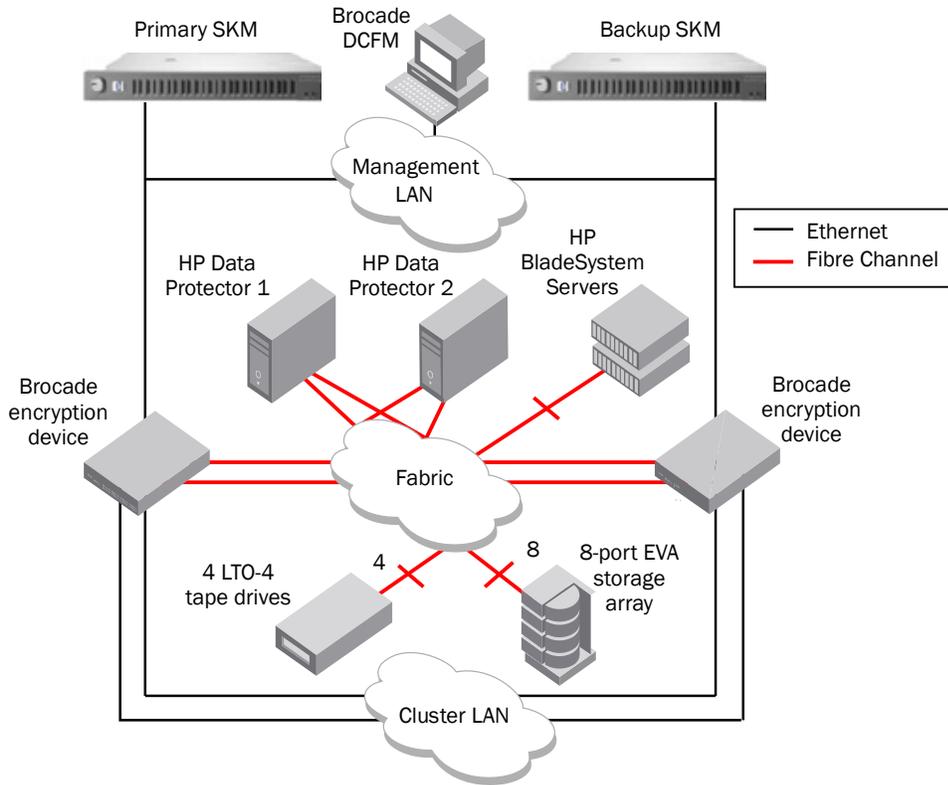


Figure 5. Upgraded encryption deployment

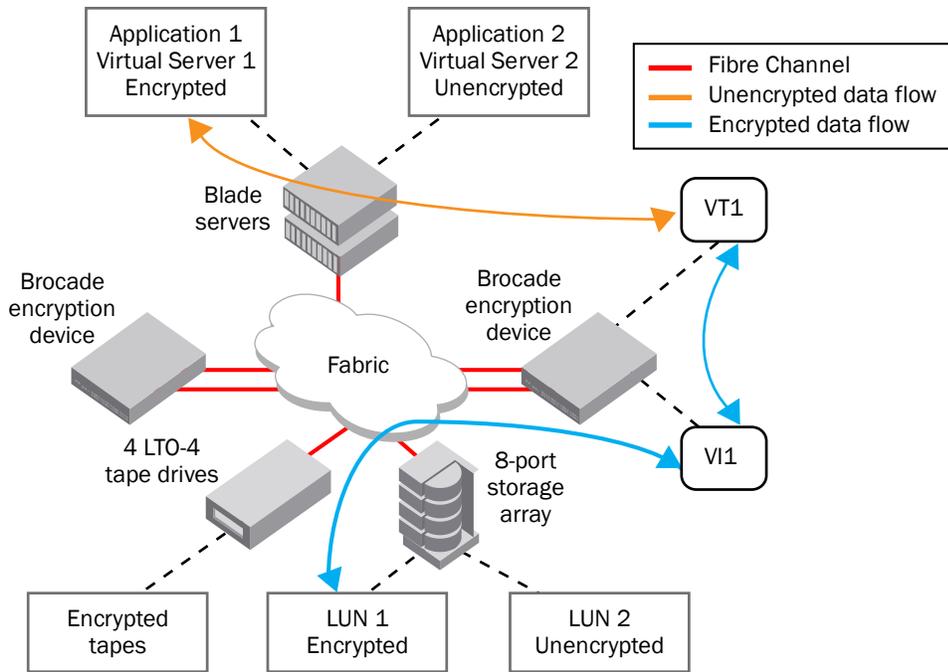


Figure 6. Logical view of upgraded deployment

Decentralized Tape Backup

Tapes are often required to be shipped to multiple locations for auditing and disaster recovery. After mergers and acquisitions, large enterprises often have a number of different systems that need to be integrated. This scenario shows how DEKs from both LTO-4 tapes and Brocade encryption devices can be managed with the SKM appliance. The Brocade encryption device can encrypt data sent to non-encrypting tape drives using AES256-GCM encryption. An Internet connection is required between the remote sites to exchange the keys between SKMs and Brocade encryption devices.

SKM manages encryption keys for tapes from multiple sites and multiple tape environments via trusted key sharing. As shown in Figure 7, the SKM at the tape warehouse stores DEKs for LTO-4 tape drives from Site 1 and Brocade encryption devices from Site 2. The tapes are sent to the tape warehouse and the DEKs are distributed to the heterogeneous tape drives to decrypt the correct tapes. The DEKs are opaquely exchanged between the SKM appliances and transparently exchanged between the Brocade encryption devices over the cluster LAN (the cluster LAN in Figure 7 has dashed lines because the synchronization between the Brocade encryption devices actually occurs over the IP network). The SKM appliance manages the DEKs while the Brocade encryption devices exchange the DEKs.

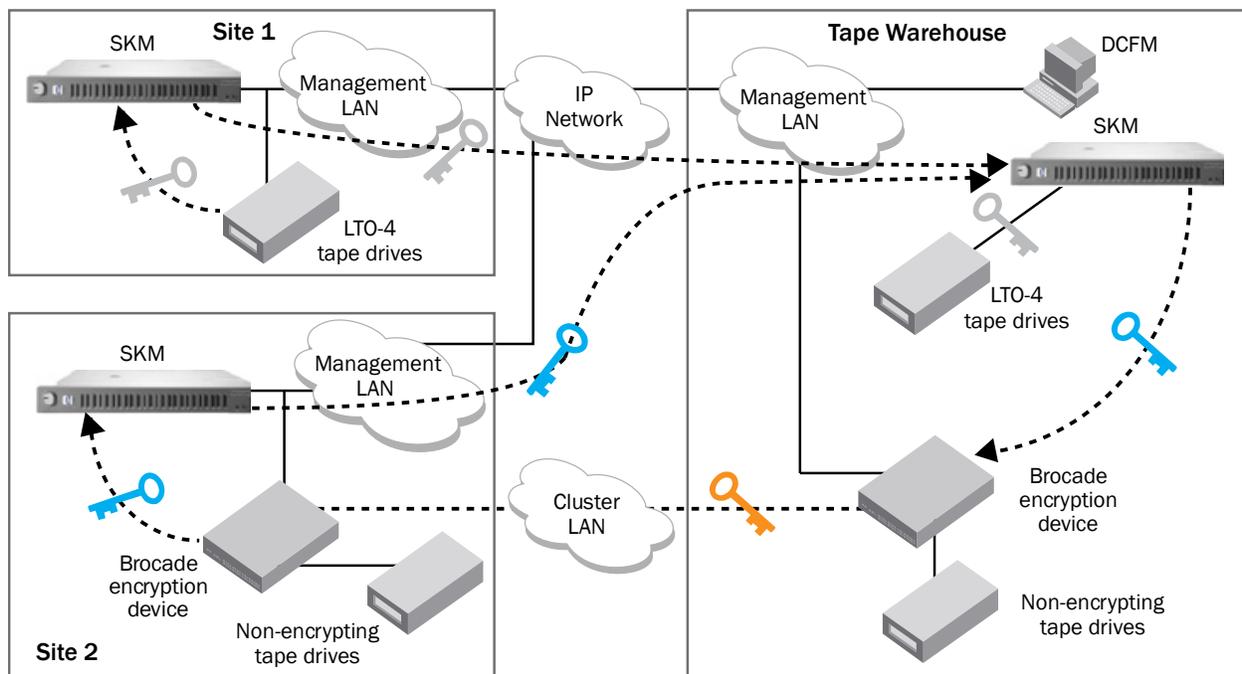


Figure 7. Key exchange between remote sites (redundant SKMs and Brocade encryption devices not shown)

SUMMARY

Brocade and HP have designed solutions for encryption of data-at-rest so that existing systems can easily be upgraded to achieve regulatory compliance. The scenarios in this paper illustrate how Brocade encryption devices and the HP SKM work together to provide reliable encryption solutions. The basic configuration with redundant HP SKM appliances and Brocade encryption devices shows how the joint solution ensures high availability encryption. IT staff can take advantage of the latest hardware running at 8 Gbps per port and encryption processing power of up to 96 Gbps. Combining power and ease of use, these encryption solutions also deliver compliance to the most stringent regulations.

NOTE: The initial release of the HP-Brocade solution does not support tape encryption, but it will be supported in a future release.

With products designed for FIPS 140-2 certification, customers can be assured of the highest level of security. HP and Brocade also provide consulting services to make it easier to plan and deploy these encryption solutions. With years of experience standing behind their storage networking and encryption solutions, HP and Brocade can assure customers that their data is secure and protected using the latest encryption technology.

© 2009 HP. All rights reserved.

© 2009 Brocade Communications Systems, Inc. All Rights Reserved. 02/09 GA-TB-130-00

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and Turbolron are registered trademarks, and DCFM and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.