February 2018

IBM® Virtualization Engine TS7700 Series Disk Encryption Overview Version 1.3

By: Felipe Barajas
IBM Senior Engineer
Tucson, Arizona

Introduction

The IBM Virtualization Engine TS7700 Series is the latest in the line of tape virtualization products that has revolutionized the way mainframe customers utilize their tape resources. Security of the information stored on the internal disk subsystem used to virtualize tape has become important to many customers. The TS7740, TS7720 and TS7760 (collectively called TS7700 hereon) internally use a disk subsystem to store or cache virtual tape volumes. The IBM TS7700 disk subsystem models 3956-CC8, 3956-CS9, 3956-CC9 and 3956-CSA have been enhanced to support disk encryption. Additionally, these subsystem models support externally managed disk encryption since September 2015. This white paper describes the general use of data encryption on these disk subsystems when used in the TS7700 Virtualization Engine (VE).

Summary of Changes

1.0. This is the initial version of this document.

1.1. Updated to reflect 3956-CC9 models.

1.2 Updated to reflect 3956-CS9, CSA and external encryption

1.3 Updated to reflect external encryption configuration and setup

Overview

The importance of data protection has become increasingly apparent with news reports of security breaches, loss and theft of personal and financial information, and government regulation. Encryption of the disk subsystem internal to the TS7700 helps control the risks of unauthorized data access without excessive security management burden or subsystem performance issues.

The disk encryption solution for tape virtualization consists of several components. IBM's disk encryption solution uses Full Disk Encryption (FDE) disk drives inside the disk subsystem. These drives are Self-Encrypting Drives (SEDs). The specific models that support the disk encryption function include: 3956-CC8, 3956-CC9, 3956-CS9, 3956-CSA (including their corresponding expansion drawers).

These disk drives or Disk Drive Modules (DDMs) contain the cryptographic chipset necessary to implement a hardware-based encryption solution. This solution is based on the AES-256 bit encryption standard and adheres to the Trusted Computing Group (TCG) enterprise security requirements. Additionally, this solution complies with National Security Agency standards by implementing government-grade encryption.

The disk subsystem can be encrypted using two methods of key management: Local or External. Local key management minimizes management burden by locally managing the disk encryption implementation. Using local encryption management fully automates the encryption solution by not requiring external key servers or additional software to maintain. External key management on the other hand, isolates the encryption key away from the TS7700 and onto an IBM Secure Key Lifecycle Management (ISKLM) server. Using external encryption management adds another layer of security by ensuring that all copies of the encryption keys are only permanently stored inside an ISKLM server. This additional layer of security however, requires additional maintenance of the ISKLM software and hardware.

Because disk drive modules routinely fail, both, local and external disk encryption ensure any failed drives can be safely disposed of knowing that their contents are encrypted and thus unreadable.

Code Requirements

Disk encryption was first introduced with the TS7700 Virtualization Engine microcode version 8.21.0.119 in January 2012. This first version only supports Local key encryption management. However, starting with microcode version 8.33.0.45 introduced in September 2015, the TS7700 added support for External key management. There are no additional host software updates required for the local disk encryption management function. The external key management function requires an ISKLM server. The current version of ISKLM supported includes ISKLM 2.7 for Linux and Windows only. There is currently no support for ISKLM on zOS as of this writing.

The communication between an ISKLM and the TS7700 is established using the IBM Proprietary Port (IPP) over standard TCP. The port used for this communication is customer assignable with the default set to 3801 as of this writing. Some newer ISKLM versions also support IPP over standard secure channels such as SSL over TLS. However, IPP over SSL/TLS is currently not supported on the TS7700. As of this writing only IPP over TCP is supported by the TS7700.

Disk Encryption Introduction

Disk encryption protects data at rest. The TS7700 uses multiple Redundant Array of Independent Disk (RAID) Drives in the internal disk subsystem to protect and store virtual tape volumes. In the case of a 3956-CSA system, the disk drives are pooled into Dynamic Disk Pools instead of Arrays but the function is similar. The disk subsystem is the only subcomponent of the TS7700 that stores the data sensitive virtual tape volumes. Virtual tape volume data and information is protected by encrypting the individual drives that form the RAID arrays or Pools. This solution therefore protects the data at rest in the TS7700, that is, it protects the individual drives that form all RAID arrays or Pools in the subsystem where the data is stored. This solution complements other types of encryption solutions that may be available such as tape encryption or encryption of data while in transit.

The disk encryption is implemented by hardware inside each disk drive module. Each disk drive module (DDM) inside the TS7700 disk subsystem contains a cryptography chip that encrypts its own data. Using this hardware based approach ensures optimal performance. If one or more DDMs become exposed to unauthorized third parties the data contained within that drive will be unavailable and unreadable without the proper encryption key.

There are two types of keys each disk drive module (DDM) supports: an encryption key and the unlock key. The encryption key inside each DDM is contained inside the cryptographic chipset of the DDM. The encryption key is used to encrypt and decrypt data stored in the DDM. The unlock key, on the other hand, is used to lock or unlock the DDM. The unlock key does not play part in the actual encryption algorithm used by each disk drive module (DDM). The unlock key when enabled locks the encryption key such that the DDM cannot properly initialize without the correct unlock key. The unlock key thus renders the DDM unavailable for any type of I/O (read or write) without the proper unlock key. The unlock key can be changed at any time without having to wait for the drive to re-encrypt itself. This is a double protection mechanism. With encryption enabled, every single DDM in the TS7700 will be physically encrypted and every single DDM will only initialize if the correct unlock key is provided.

Encryption can be enabled on-demand since the unlock key can be set independent of the encryption key. This minimizes configuration time to virtually minutes instead of waiting for days for existing data to be encrypted. However, once unlock keys are enabled they cannot be disabled; this ensures permanent data protection.

Encryption keys can be locally managed. A locally-managed key is contained internally by the TS7700 in a non-volatile memory area that is only accessible by the internal disk subsystem controllers' memory (non-volatile RAM). When this key is copied to areas outside this protected memory, the key is encrypted with its own algorithm in order to further obfuscate and thus avoid being intercepted unknowingly. An obfuscated copy of this key is stored as a backup inside the TS7700 pSeries subsystem. This backup copy can only be accessed manually by higher levels of service personnel during disaster recovery scenarios, for example, in the rare event both disk controllers need to be replaced at once. At customer requests, this obfuscated key can be optionally backed up to media outside the TS7740 (such as CD or DVD disks).

Encryption keys can also be externally managed. An externally-managed key is not stored in either non-volatile memory, the TS7700, nor DVD backup disks. An externally-managed key is only permanently stored in an ISKLM server which is managed by security administrators separately from the TS7700.

The main advantage of Local vs External key management is that Local key management is fully automated. It is completely managed internally by the TS7700.

The main advantage of External vs Local key management is that the key is permanently stored outside of the TS7700. Therefore, the encryption key is only available to security administrators of the ISKLM server. The administrators of the ISKLM server may be different than the administrators or users of the TS7700. This adds another layer of security at the cost of the additional administration and maintenance of the ISKLM server.

Locally Managed Encryption

Locally managed encryption stores the lock key to the encryption key inside the disk subsystem controller's non-volatile memory. Locally managed encryption key configuration and maintenance is automated by the TS7700 microcode. The TS7700 microcode supports enabling locally managed encryption, modifying keys, and backing up the key.

Features

On-Demand Enablement

Disk-encryption can be enabled with Locally Managed Encryption Keys concurrent with customer operations. This ensures no customer downtime. Additionally, there is no performance degradation during or after encryption enablement even on systems with large amounts of active stored data in the disk subsystem.

EKM Migration Support

Any TS7700 configured with Local Key Management can be easily migrated to External Key Management for future needs. Migration to External Key Management is also concurrent with customer operations.

Re-key Support

Any TS7700 configured with Local Key Management encryption can be re-keyed with new encryption keys on-demand with no downtime and no performance loss during or after the re-key operation. Additionally, the key(s) can be externally stored to media such as DVD discs for backup and safekeeping. The re-key and backup operations can be initiated from the TS7700 service menus.

Always-on Encryption

Once encryption is enabled it cannot be disabled unless Cryptographic Disk Erase is performed.

Cryptographic Disk Erase

Cryptographic Disk Erase allows customers to erase the disk subsystem by securely erasing all copies of the encryption keys only. This feature does not do Secure Data Overwrite as actual data is not erased. Instead, this feature code securely erases only the encryption keys such that any knowledge of such keys is forgotten. Without any means of retrieving the encryption key all previously written data inside every DDM will be undifferentiated from random or meaningless data. Cryptographic Disk Erase is meant to complement the Cluster Cleanup feature code. Cryptographic Disk Erase in conjunction with Cluster Cleanup is the only means available of disabling encryption and returning the system to its un-encrypted state.

Prerequisites

While the feature for disk encryption support is customer-installable, actual enablement may require configuration by an IBM Service representative.

TS7700 Virtualization Engine Microcode

The Virtualization Engine (VE) must be running microcode level 8.21.0.119 or higher. The disk encryption feature code must be installed to access the encryption settings.

TS7700 Virtualization Engine Hardware

The TS7700 Virtualization Engine (VE) must contain compatible hardware in order to enable disk encryption. This compatible hardware must include only disk subsystems populated with FDE capable drives. TS7700 systems shipped before January 2012 may not contain this new hardware. TS7700 vital product data (VPD) can be analyzed by IBM service representatives to ensure existing hardware meets these requirements.

Installation

The disk encryption feature code provides explicit instructions on setting and enabling disk encryption. These illustrated instructions are not repeated in this paper. Briefly, the installation steps are:

- Customer installs the proper feature code using the Management Interface (MI)
- IBM Service Representative enables encryption from the TS7740 VE service menu

Encryption is completely transparent to the operation of the TS7700. Once activated, encryption cannot be disabled. However, keys can be re-generated or backed to external media at any time by IBM service representatives from the VE service menu.

Maintenance

There are no additional maintenance requirements with locally managed disk encryption. All disk drive modules (DDMs) that form the RAID arrays or DDP pools must be Full Drive Encryption (FDE) capable. When a FDE capable DDM fails, the TS7700 will automatically inform service personnel the replacement part number needed. Note that the system will not allow a non-FDE drive to be inserted as a replacement to an FDE drive. Due to the transparency of locally managed encryption, other TS7700 subcomponent upgrades, part replacements etc. are not affected and will continue to work the same way as systems without disk encryption enabled.

Externally Managed Encryption Keys

Externally managed encryption stores the lock key to the encryption key inside an IBM Secure Key Lifecycle Manager (ISKLM) server. An ISKLM server is separate and independent from the TS7700 system. Externally managed encryption key configuration consists of two phases. In the first phase, the ISKLM server is setup to accept key requests from the TS7700 disk subsystem. In the second phase, an IBM Service representative enables external key encryption from the TS7700 service panels.

Features

On-Demand Enablement

Disk-encryption can be enabled with Externally Managed Encryption Keys concurrent with customer operations. This ensures no customer downtime. Additionally, there is no performance degradation during or after encryption enablement even on systems with large amounts of active stored data in the disk subsystem.

Locally Managed Keys Migration

Migrating from External to Local Key Management is not supported.

Re-key and Key Backup

Any TS7700 configured with External Key Management Encryption will depend on the ISKLM server to manage the encryption keys. The TS7700 does not support backing up the encryption keys to external media such as DVD discs. Instead, the ISKLM itself must be used to perform key backups. The TS7700 supports re-key however. From the TS7700 service menu, a request can be sent to the ISKLM to issue a new key to the disk subsystem for re-key. The TS7700 does not store any encryption key permanently. All copies of the encryption keys will remain only in the ISKLM indefinitely. The TS7700 supports up to two synchronized ISKLM servers for redundancy.

Single ISKLM Primary Key Store

The disk cache models used by the TS7700 are assigned encryption keys by the ISKLM primary key store using sequential key labels. Two or more independent primary key stores connected to two or more TS7700 clusters can be used, but their key stores must remain independent forever. Any future merging of primary key stores when two or more key stores have assigned keys to different TS7700s can lead to key label collisions. Though the actual encryption keys are unique, the labels associated with them can conflict. Therefore, it's best to use a single primary key store, which can have many synchronized children, secondaries or clones. If two primary key stores are required, the keys handed out to the attached TS7700s can never be consolidated through key store merging.

Always-on Encryption

Once encryption is enabled it cannot be disabled unless Cryptographic Disk Erase is performed.

Cryptographic Disk Erase

Cryptographic Disk Erase allows customers to erase the disk subsystem by securely erasing all copies of the encryption keys only. This feature does not do Secure Data Overwrite as actual data is not erased. Instead, this feature code securely erases only the encryption keys such that any knowledge of such keys is forgotten. Without any means of retrieving the encryption key all previously written data inside every DDM will be undifferentiated from random or meaningless data. Cryptographic Disk Erase is meant to complement the

Cluster Cleanup feature code. Cryptographic Disk Erase in conjunction with Cluster Cleanup is the only means available of disabling encryption and returning the system to its un-encrypted state.

Prerequisites

While the feature for disk encryption support is customer-installable, actual enablement may require configuration by an IBM Service representative.

TS7700 Virtualization Engine Microcode

The Virtualization Engine (VE) must be running microcode level 8.33.0.45 or higher. The disk encryption feature code must be installed to access the encryption settings. Additionally, a second feature code that installs an ISKLM communication certificate in the TS7700 may be needed as well.

TS7700 Virtualization Engine Hardware

The TS7700 Virtualization Engine (VE) must contain compatible hardware in order to enable disk encryption. This compatible hardware must include only disk subsystems populated with FDE capable drives. TS7700 systems shipped before January 2012 may not contain this new hardware.

ISKLM Microcode

The TS7700 currently only supports ISKLM servers running on Linux or Windows. ISKLM for zOS is not currently supported. The minimum version supported of ISKLM is 2.7.

The ISKLM server must be configured to communicate with the TS7700 using IPP over TCP. Any version of KMIP or IPP over SSL/TLC is not currently supported.

TS7700 vital product data (VPD) can be analyzed by IBM service representatives to ensure existing hardware, software and feature codes meet the above requirements.

ISKLM Configuration

An administrator of the ISKLM server is required to enable and setup the ISKLM in order for key exchanges to be handled by the ISKLM. The TS7700 has no control of the ISKLM configuration. The TS7700 will simply act as a proxy to pass internal requests for keys by the DDMs to the ISKLM and vice versa. Therefore, the first step is to setup the ISKLM server for key exchanges. The actual steps to configure the ISKLM can vary based on operating system or ISKLM version. Because of that reason, please consult with an ISKLM administrator for the correct or updated instructions. As a general guideline, the following instructions can be used to configure an ISKLM server:

1. Open the ISKLM management window and log in using an Admin ID.

2. Create a new keystore if not done already. On some versions of ISKLM servers this reads as "**click here to create the master keystore"**. The Keystore settings window is displayed.

3. Type and retype (if needed) the password for the keystore. Keep the default values for the other keystore settings, and click **OK**.

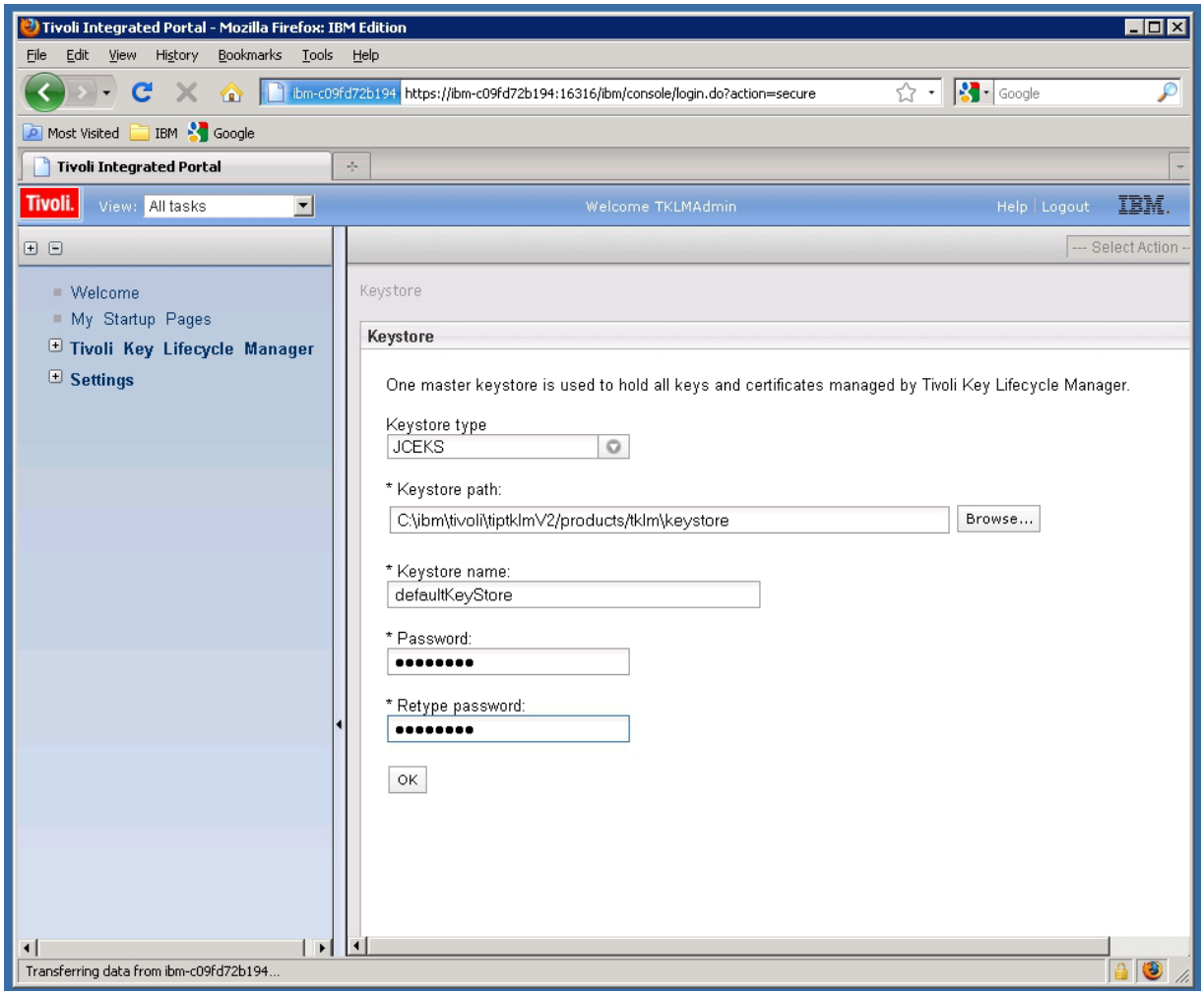

Figure 1 - Creating a Keystore

4. Click the **Welcome** link on the left side of the window. The Welcome window opens.

5. In the **Key and Device Management** box, select **DS5000** from the **Manage keys and devices** menu, and click **Go**. The Key and Device Management window opens. The DS5000 is the generic term the ISKLM uses for DDM key requests coming from a multitude of compatible systems which include the disk subsystems inside the TS7700 such as the 3956-CC9, CS9, CSA etc.

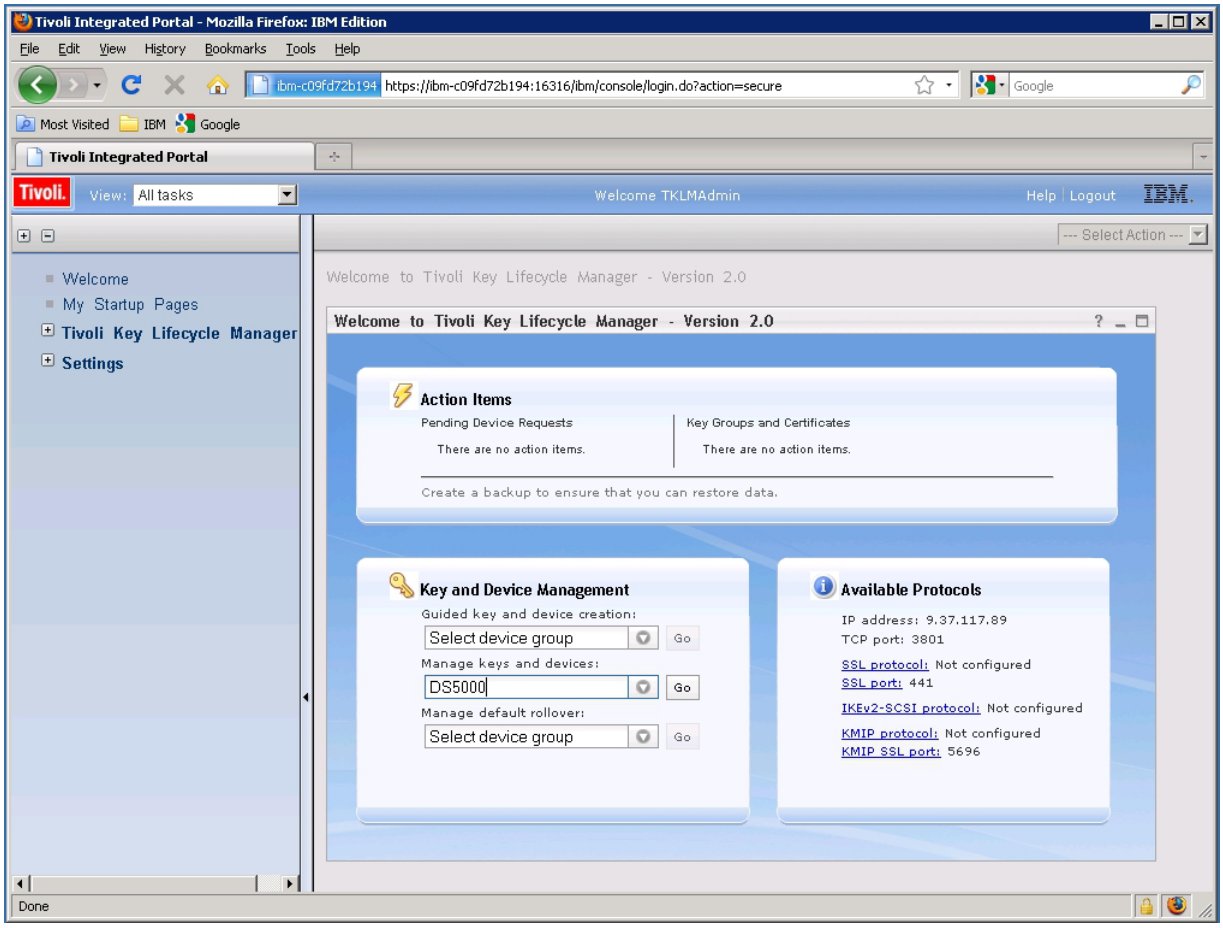

Figure 2 - Key Device Management

6. When the Confirm prompt is displayed, click **Cancel**.

7. In the drop-down menu at the bottom of the window, select either the option to **Automatically accept new device requests** or select the option to **Hold new device requests pending my approval**.

8. If the option to automatically accept new device requests is chosen then the ISKLM server is ready to accept key requests from the TS7700. However, if the option to hold a new device request is chosen, the first time the TS7700 tries to store a key, the operation will fail because the ISKLM server will deny access until the device is approved manually. Follow these additional steps if the option to hold a new device request is chosen:

   8.1. First instruct the IBM Service representative to enable external key management from the VE service menus. This will generate a request for access to the ISKLM server. However, the IBM Service representative may see the operation fail because the ISKLM denied the communication. Once the TS7700 request has been completed by the IBM Service representative click the **Pending devices** link in the **Action Items** box in the ISKLM interface.

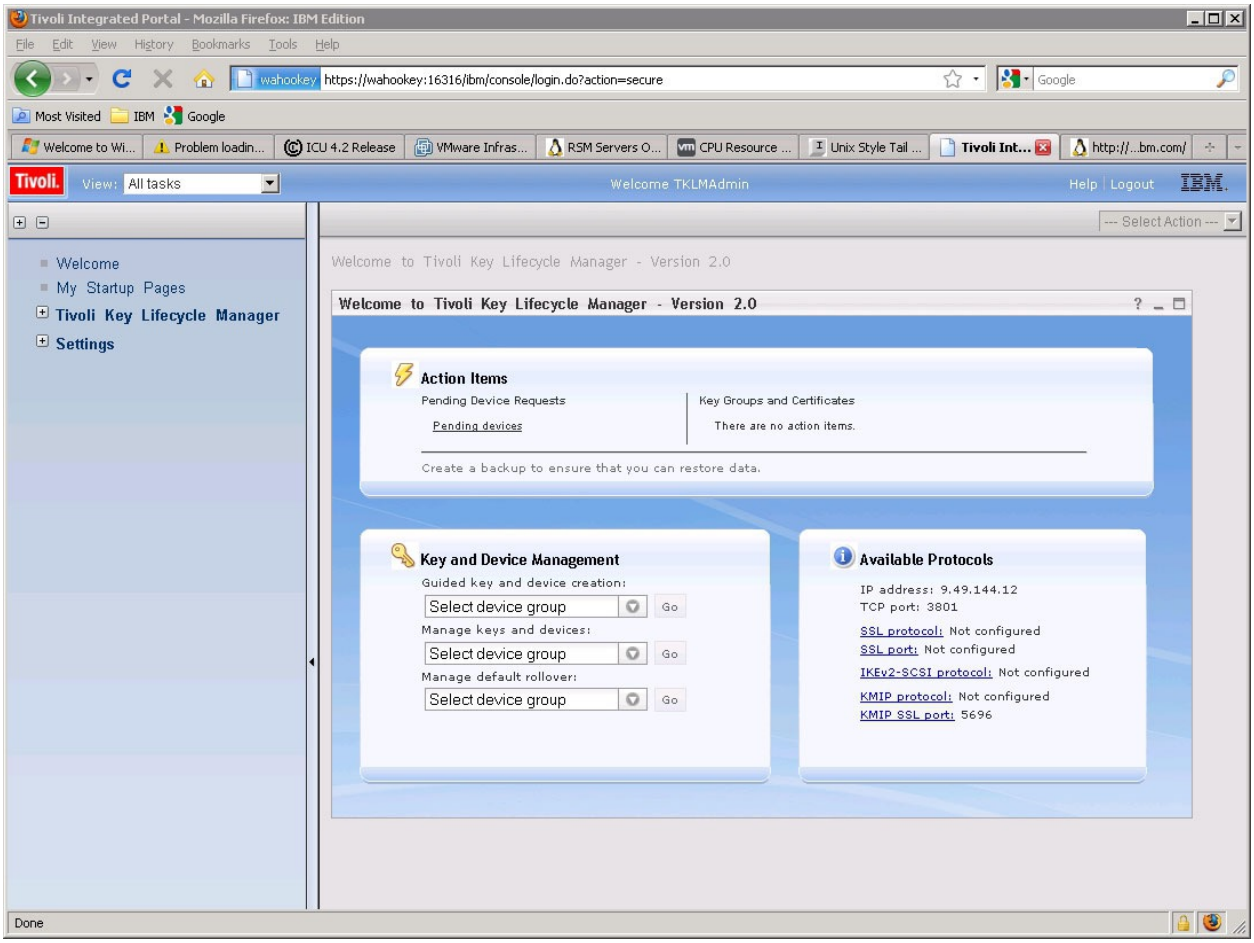

Figure 3 - Pending Service Requests

8.2. The Pending Device Requests window should open. Select the device in the list and click **Accept**. The Accept Device Request window opens

8.3. Click **Accept** on the Accept Device Request window for each TS7700 disk subsystem string that appears. The TKLM server should now be configured and manage all keys for the TS7700 disk subsystem(s). A second attempt to enable encryption from the TS7700 may be required if the first attempt failed due to the device being denied access until manually approved. If that was the case, instruct the TS7700 Service Representative to retry the disk encryption enablement from the TS7000 VE support menus.

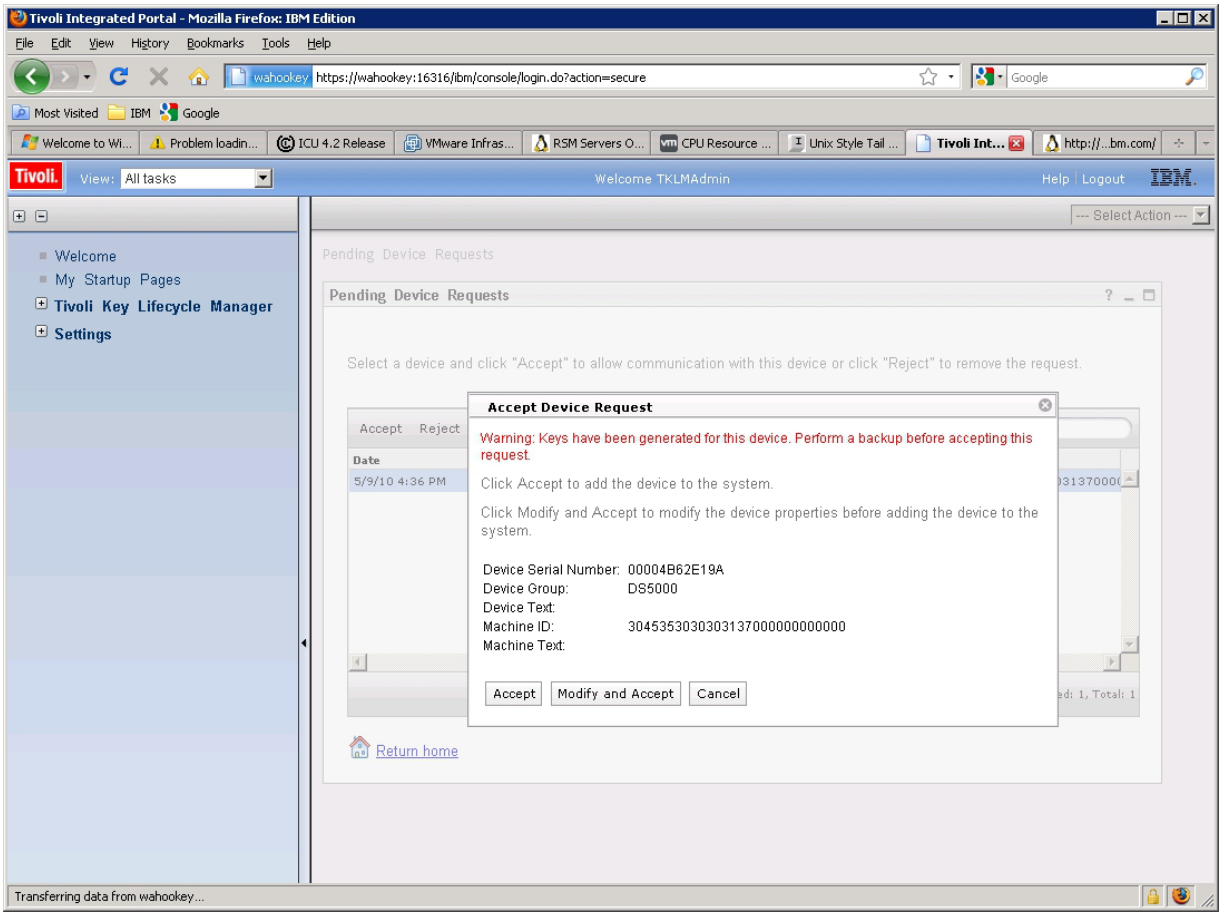

Figure 4 - Accepting Device Request

TS7000 Configuration

Once the ISKLM server has been configured the next step is to enable externally managed encryption from the TS7700. These are the main steps:

- If not already installed, the customer installs the proper features code using the Management Interface (MI)
- IBM Service Representative enables encryption from the TS7740 VE service menu. This may include installing any needed ISKLM-based certificates if not already present.

Maintenance

There are no additional TS7700 maintenance requirements with externally managed disk encryption. All disk drive modules (DDMs) that form the RAID arrays must be Full Drive Encryption (FDE) capable. When a FDE capable DDM fails, the TS7700 will automatically inform service personnel the replacement part number needed. Note that the system will not allow a non-FDE drive to be inserted once encryption is enabled. Due to the transparency of locally managed encryption, other TS7700 subcomponent upgrades,

part replacements etc. are not affected and will continue to work the same way as systems without disk encryption enabled. The ISKLM server however, may require additional maintenance.

RAID Arrays and Disk Pools

The TS7700 disk subsystem uses disk drives that form part of a Redundant Arrays of Independent Disks (RAID) or Dynamic Disk Pools (DDP). The number of RAID arrays or DDP pools varies depending on the specific storage capacity of the TS7700. Disk subsystem models 3956-CC8 (and its 3956-CX7 expansion drawers) use RAID5 arrays which can withstand one disk failure in the same array. Disk subsystem models 3956-CC9 (and its 3956-CX9 expansion drawers) or 3956-CS9 (with 3956-XS9 expansion drawers) use RAID6 arrays which can withstand two disk failures in the same array. Disk subsystem models 3956-CSA (and its 3956-XSA expansion drawers) use DDP pools which like RAID6 provide protection from up to two drive failures in the same pool. Additionally, all systems come with spare drives to mitigate disk failures. When a disk fails, a spare drive automatically takes over for the failed drive. When a spare drive has fully taken over, the RAID array (or DDP pool) is fully protected again. When the failed drive is physically replaced, the new drive will copy over from the spare drive. The spare drive then goes back to being an unused spare drive (in DDP pools the pool will rebalance). This behavior is consistent between encryption capable and non-encryption capable disk subsystems.

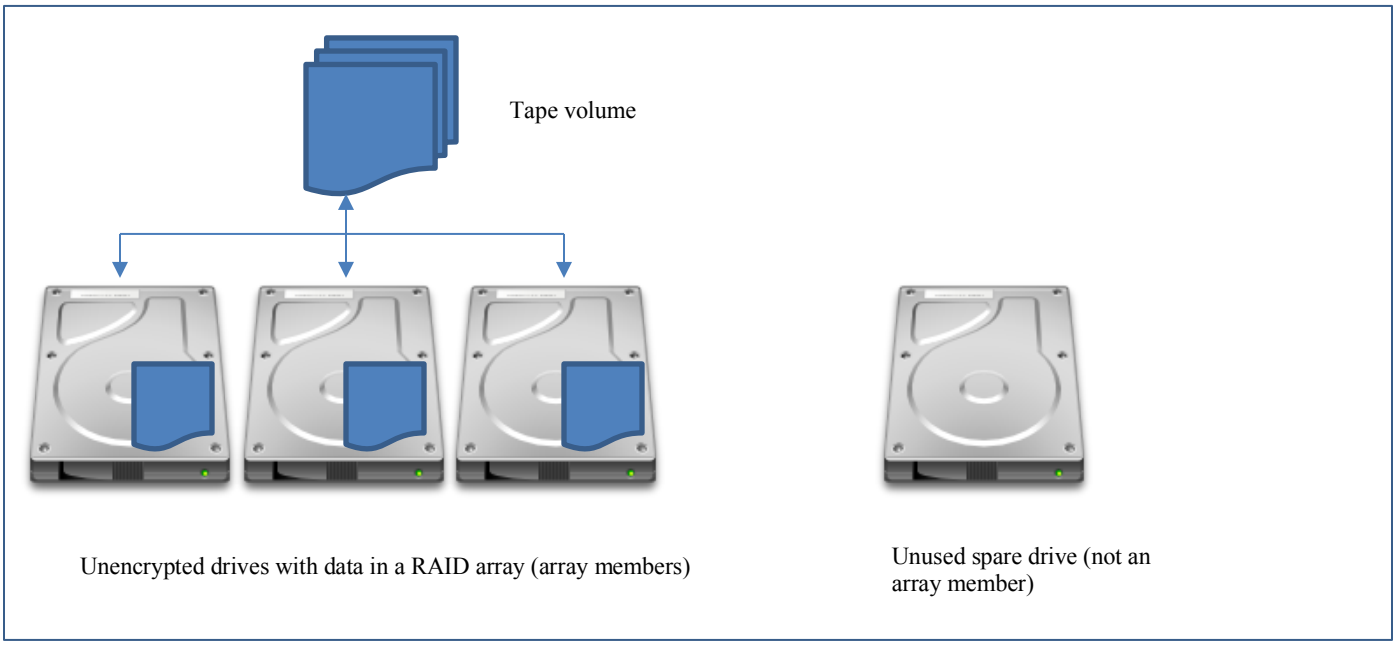

Figure 5 – Disk Array

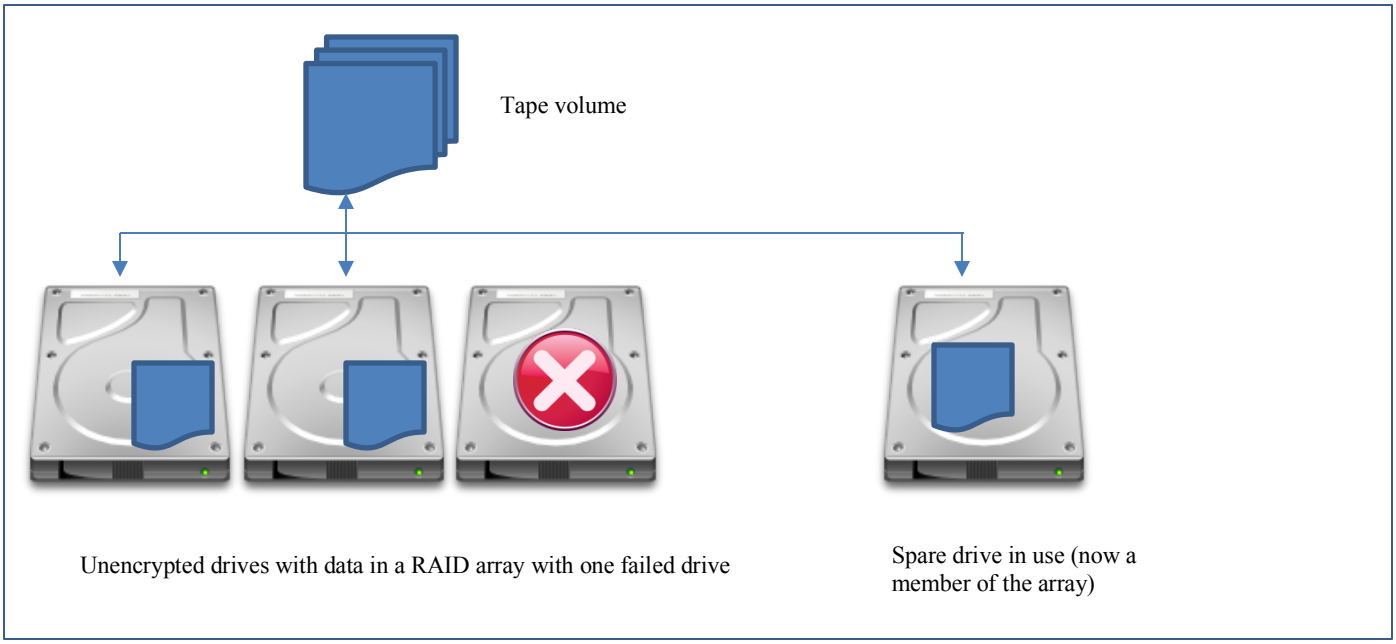

Figure 6 – Disk Array With a Failed Drive

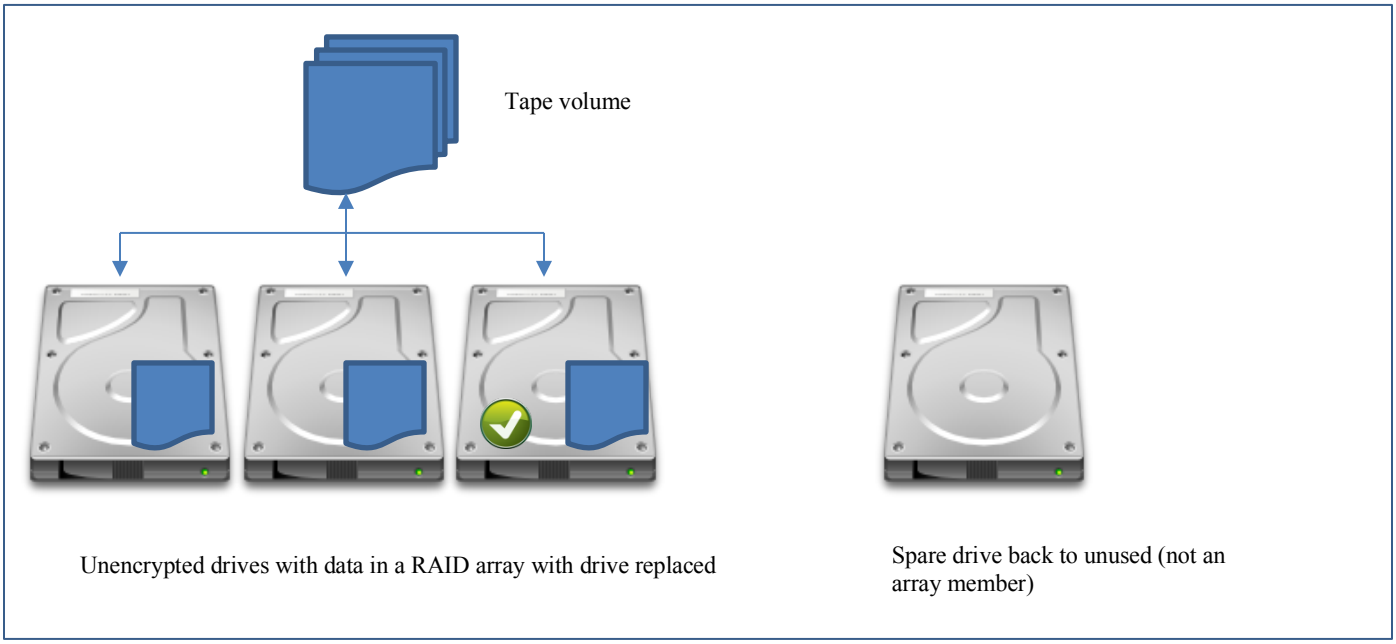

Figure 7 – Disk Array With Drive Replacement

When disk encryption is enabled, all disk members of the RAID arrays (or pools) are individually encrypted. When a spare drive takes over for a failed drive, it automatically turns on its encryption and any data that is being rebuilt will therefore be encrypted on that spare drive. When the failed drive is physically replaced, the replacement drive will also automatically turn on its encryption and form part of the RAID array. The spare drive then goes back to being a spare but will remain encrypted.

With disk encryption enabled the failed drive can be safely disposed of knowing that its contents are encrypted and thus unreadable.

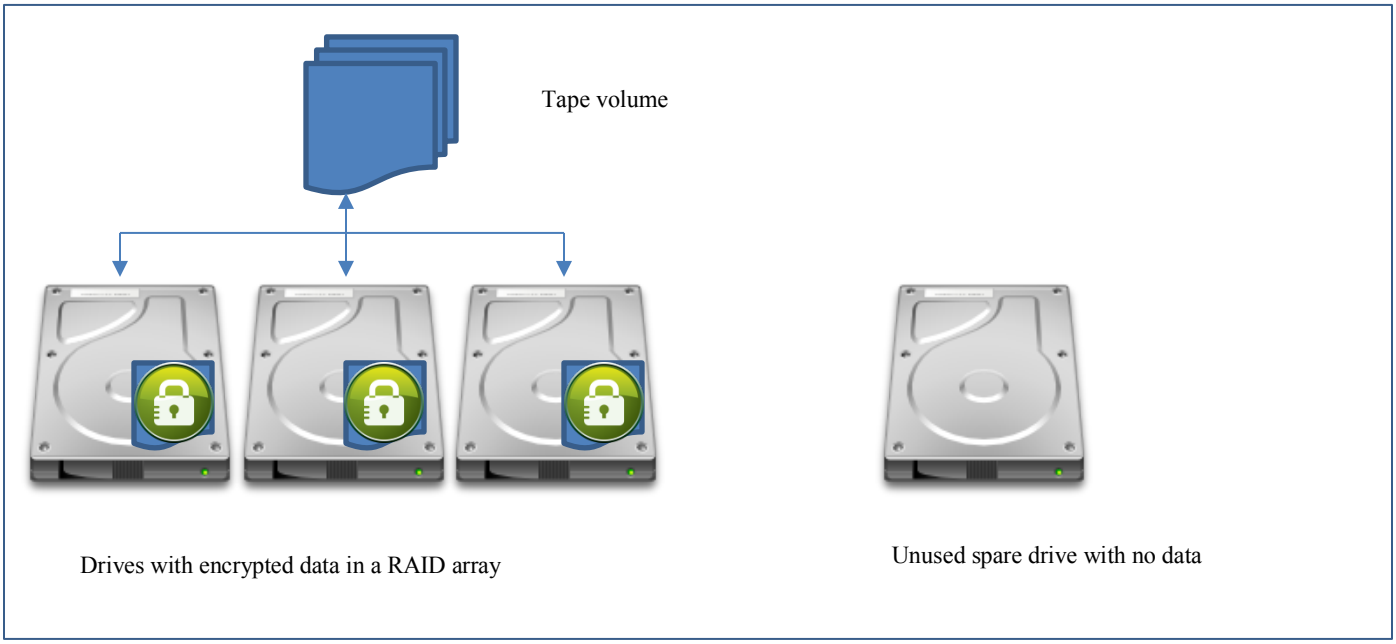

Figure 8 – Encrypted Disk Array

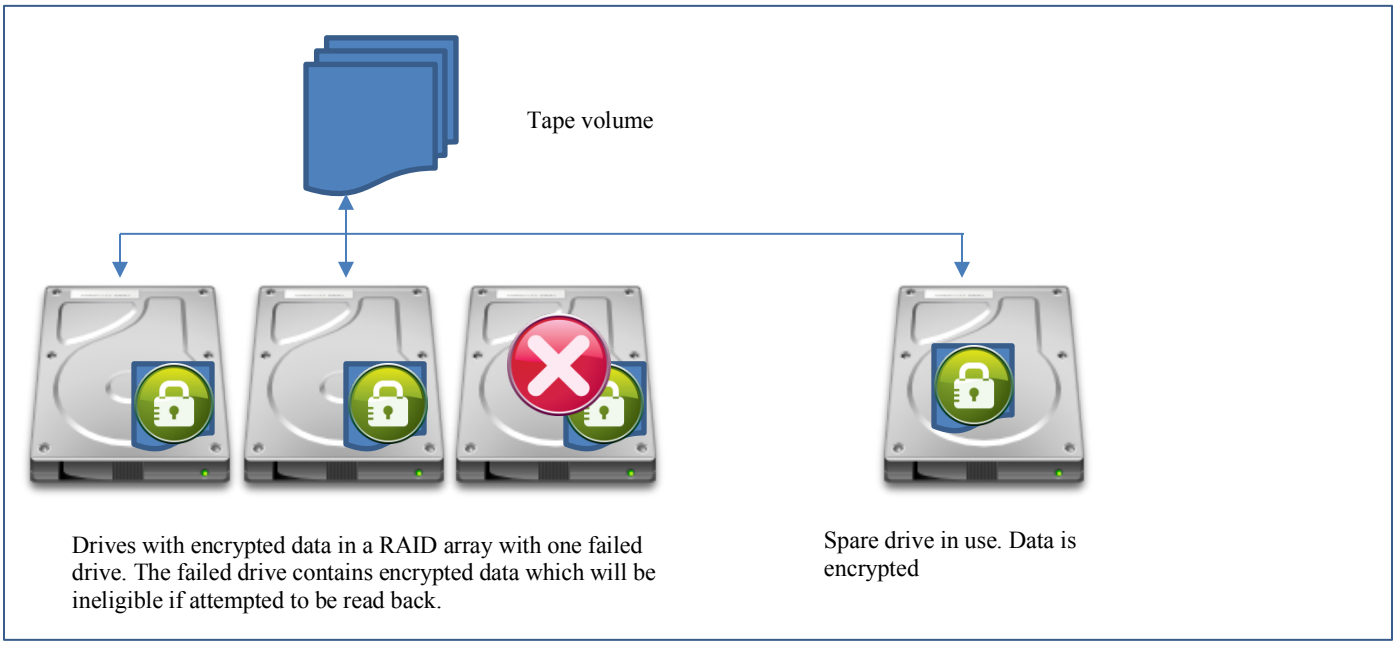

Figure 9 – Encrypted Disk Array With a Failed Drive

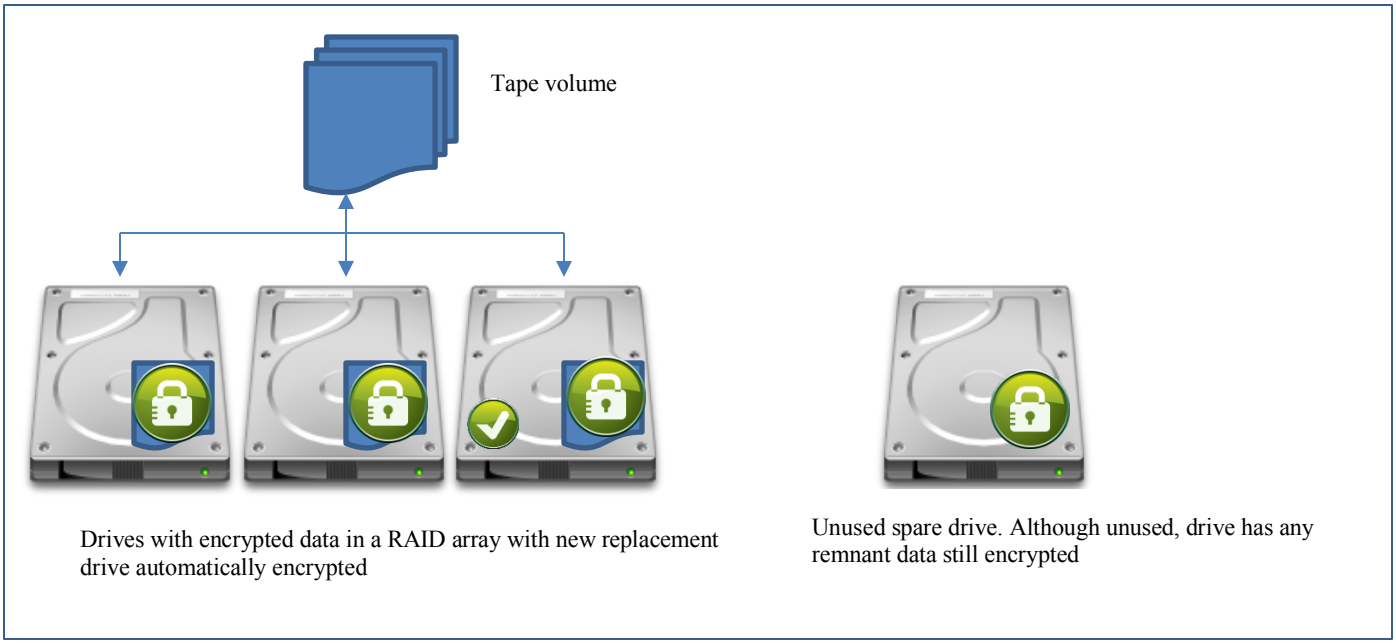

Figure 10 – Encrypted Disk Array with Drive Replacement

Key Exchanges

When disk encryption is first enabled, all physical drives (DDMs) will be locked with a lock key (also called unlock key). The lock key safeguards the encryption key of each DDM such that the DDM will be unusable without the correct lock key. This lock key is independent from the encryption key. The encryption key is unique for each DDM and is stored only in the cryptographic chipset of the DDM. The encryption key is never externalized outside the drive. The lock key is used to protect the encryption key. Several DDMs could have the same lock key but never the same encryption key. After encryption is enabled each DDM will ask for a lock key during the first initial I/O such as during power-ups, when a spare drive becomes an array member, etc. If the lock key is invalid, the DDM will be unable to retrieve the encryption key from its cryptographic chipset and the DDM will fail to initialize (no I/O will be possible).

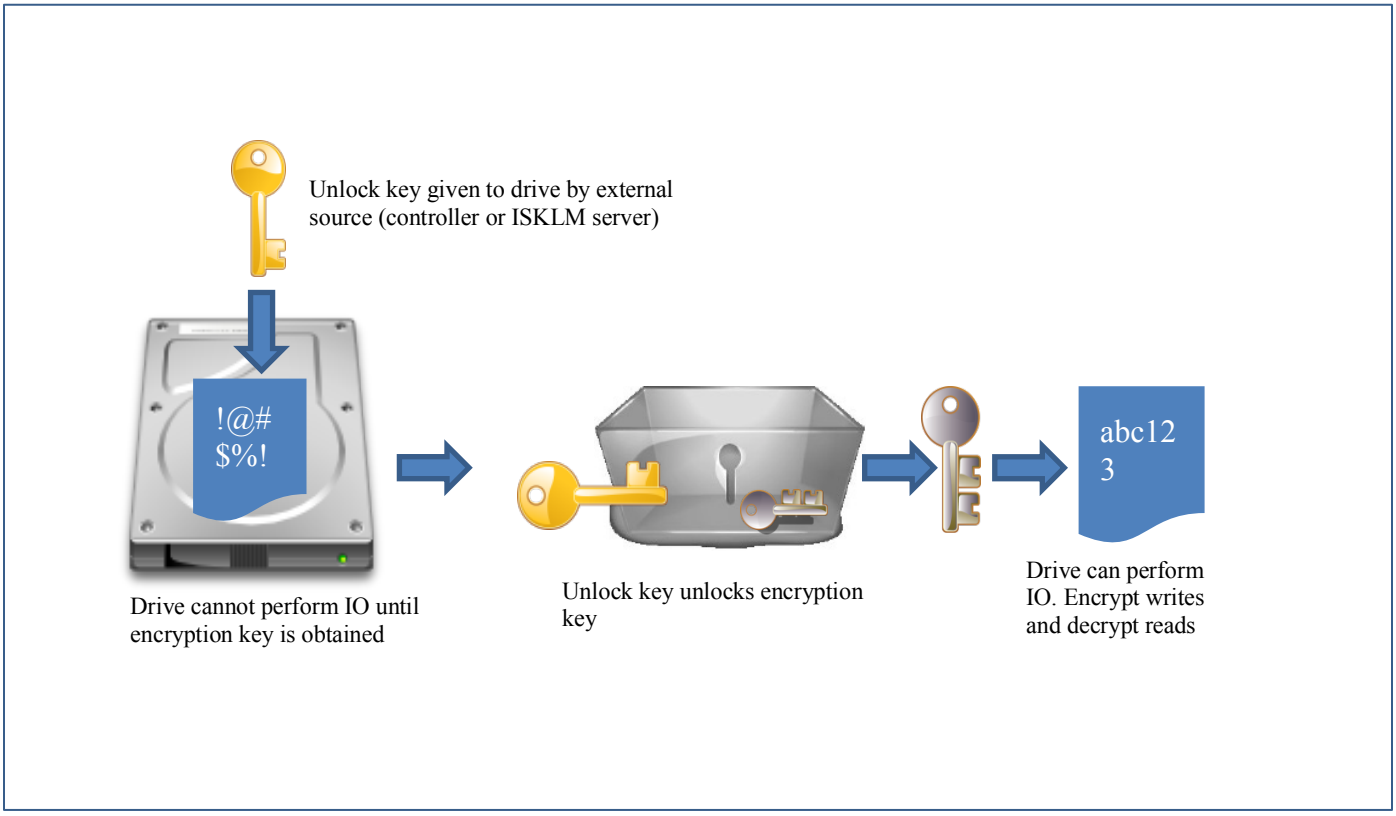

Figure 11 – Lock Key Exchange

The encryption itself however is done individually by each drive's on-board cryptography chipset. The unlock key stored by the drive is not part of the algorithm used to encrypt its contents. The unlock key is instead used to obfuscate the encryption key so that not even the drive can obtain the encryption key without the proper unlock key. Once the drive is unlocked all write I/O operations will be encrypted by the drive's cryptography hardware before they get written to physical media. Similarly only drives that are unlocked will be allowed to read from the physical media. The read I/O operations will get decrypted by the drive's cryptography chipset before being presented to the disk subsystem controllers.

The strength of the encryption key is AES-256. The strength of the unlock key is AES-256. The strength of the encrypted communication channel between the controller and the DDM is AES-256. The strength of an externalized (obfuscated) unlock key is AES-128. The externalized (obfuscated) unlock key only applies to Local Key Management where the key can be backed up to storage outside the disk subsystem such as a DVD disc.

Using this approach enables the TS7700 to protect the data inside the DDMs while automating the encryption and the management of the keys in a way that is transparent to the user. Performance is maximized and downtime is minimized by using a hardware based cryptography chipset localized to each individual disk drive.

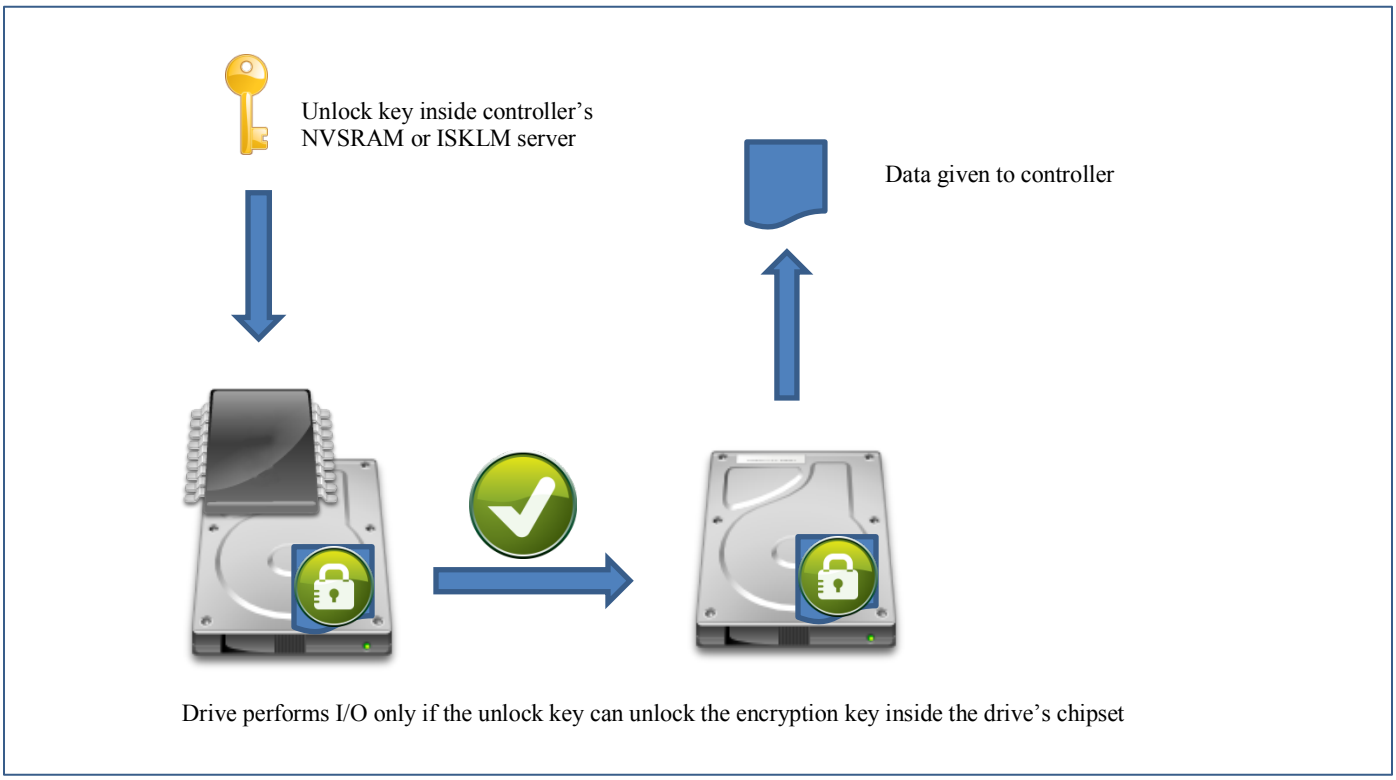

Figure 12 – Valid Key Exchange

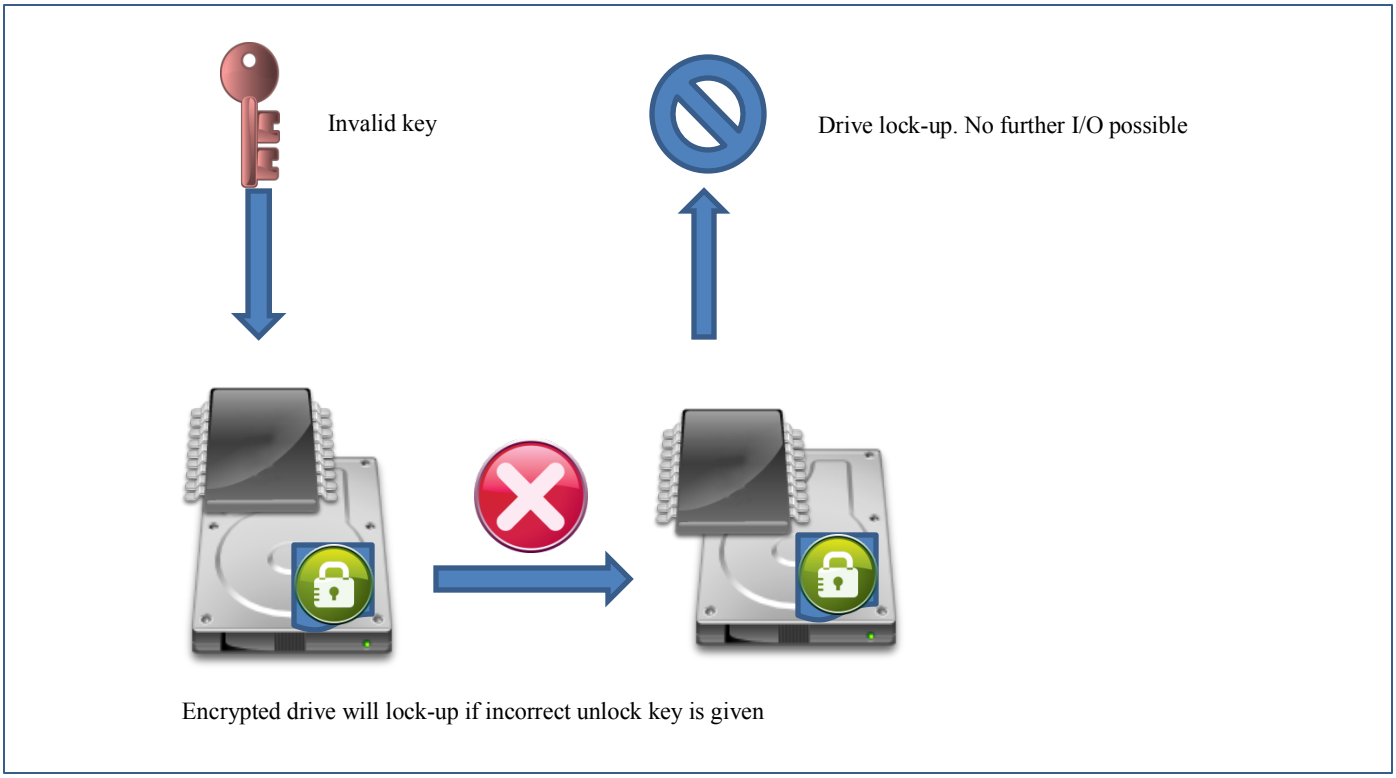

Figure 13 – Invalid Key Exchange

References

IBM System Storage Installation and Host Support Guide, GA32-0963-01

TS7700 Virtualization Engine Information Center,
http://publib.boulder.ibm.com/infocenter/ts7700ic/v1r0/index.jsp

IBM TotalStorage Virtual Tape Server – Using 3592 In a VTS – Version 5,
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100488

IBM Virtualization Engine TS7700 Series Bulk Volume Information Retrieval Function User's Guide Version 1.0, http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100828

IBM Virtualization Engine TS7700 Series Statistical Data Format White Paper,
http://03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100829

Disclaimers:

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This information could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or programs(s) at any time without notice.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead. It is the user's responsibility to evaluate and verify the operation of any non-IBM product, program or service.

The information provided in this document is distributed "AS IS" without any warranty, either express or implied. IBM EXPRESSLY DISCLAIMS any warranties of merchantability, fitness for a particular purpose OR NON INFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted according to the terms and conditions of the agreements (*e.g.*, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. IBM is not responsible for the performance or interpretability of any non-IBM products discussed herein. The customer is responsible for the implementation of these techniques in its environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. Unless otherwise noted, IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The provision of the information contained herein is not intended to, and does not grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Trademarks

The following are trademarks or registered trademarks of International Business Machines in the United States, other countries, or both.

IBM, TotalStorage, DFSMS/MVS, S/390, z/OS, and zSeries.

Other company, product, or service names may be the trademarks or service marks of others.

