HP Enterprise Secure Key Manager with HP StorageWorks B-Series encryption solutions

Storage Area Networks

Technical white paper

Table of contents

The HP Enterprise Secure Key Manager provides trusted, high availability key management services that integrate with B-Series encryption solutions. HP Secure Advantage and B-Series encryption solutions provide a full range of services to assist in the successful implementation of data-at-rest security controls and encryption solutions.

Introduction

HP has developed a unified approach to enable data-at-rest encryption solutions using the HP Enterprise Secure Key Manager (ESKM) with HP StorageWorks B-series encryption devices and other encryption solutions. The B-series encryption devices and ESKM provide Federal Information Processing Standards 140-2 (FIPS 140-2) compliance to enable trusted key sharing between multiple sites and data centers in a comprehensive, scalable solution. This fabric-based solution offers data-at-rest encryption for disk and tape at up to 96 Gigabits per second (Gbps).

NOTE:
The term “B-series encryption device” used in this paper is with reference to both the HP StorageWorks Encryption SAN Switch and the HP StorageWorks DC Switch Encryption Blade.

HP offers excellent management interfaces and monitoring capabilities. An ESKM cluster provides comprehensive security audit logging and integrates into HP's ArcSight and other SIEM solutions to offer enterprise-level management of encryption keys and auditing of all 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 B-series encryption device and the ESKM cluster enables simple yet secure key and data sharing among multiple sites.

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

Overview

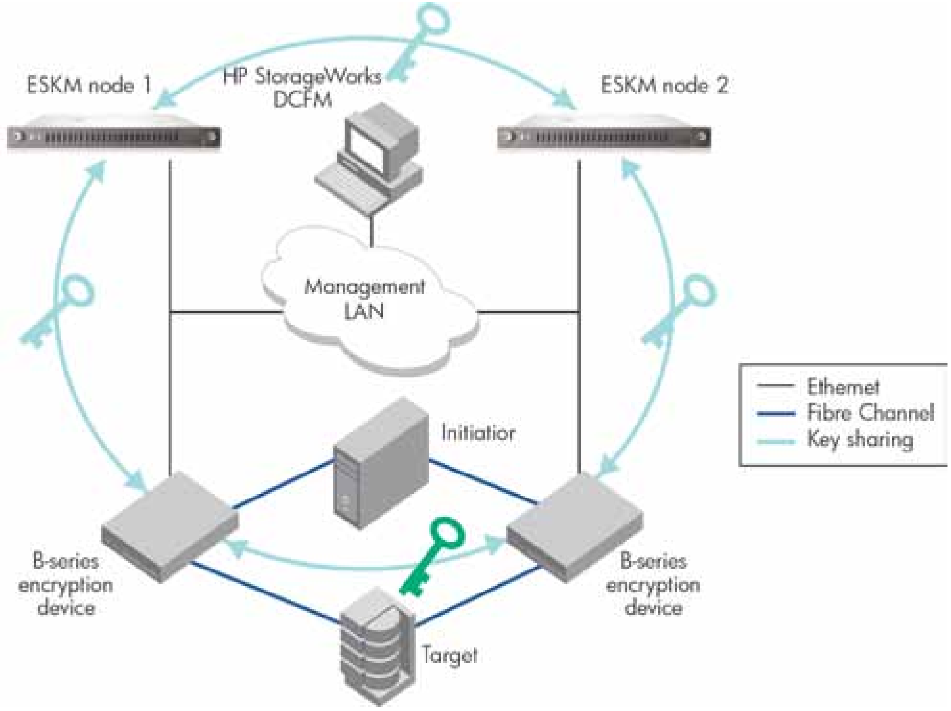
A quick overview of the equipment in the solution is helpful in understanding the context of the discussion. HP recommends deploying encryption with redundant encryption devices and redundant HP ESKM nodes in a high-availability cluster configuration. As shown in Figure 1, the components of this scenario 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 B-series encryption switches
- A fabric-based encryption device to secure data-at-rest
- Redundant ESKM nodes in a cluster configuration to manage and store the data encryption keys (DEKs)
- HP StorageWorks 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 ESKM nodes communicate with the B-series encryption devices via the ESKM client application programming interface (API). The ESKM API is the interface for exchanging DEKs between HP ESKM nodes and B-series encryption devices. The B-series encryption device generates the DEKs and wraps (encrypts) them before sending them to the ESKM node within a secure socket layer (SSL)/transport layer security (TLS) session. ESKM 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 B-series encryption device and sent to a primary ESKM appliance. The encryption device then synchronizes DEKs with the other encryption devices in the fabric through the cluster LAN. The ESKM cluster nodes are also synchronized between themselves to enable access to keys if one fails. These redundant key exchanges help ensure that the data stays encrypted or decrypted without a single point of failure.

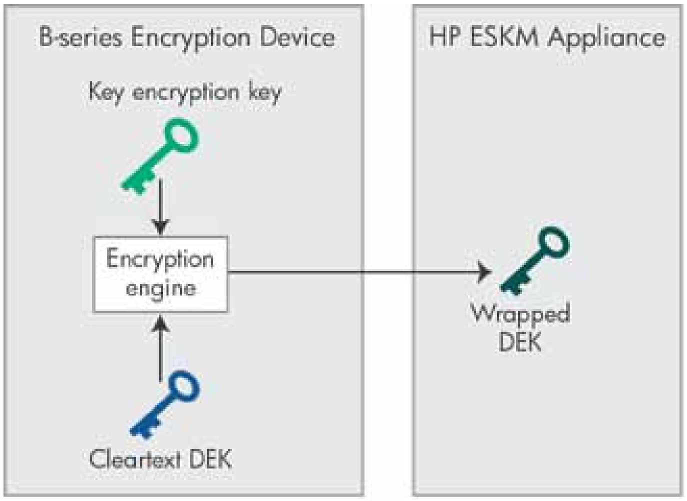
Figure 1: Components of the HP B-series encryption and HP ESKM solution



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 B-series encryption devices. The ESKM manages the wrapped key that is encrypted as shown in Figure 2.

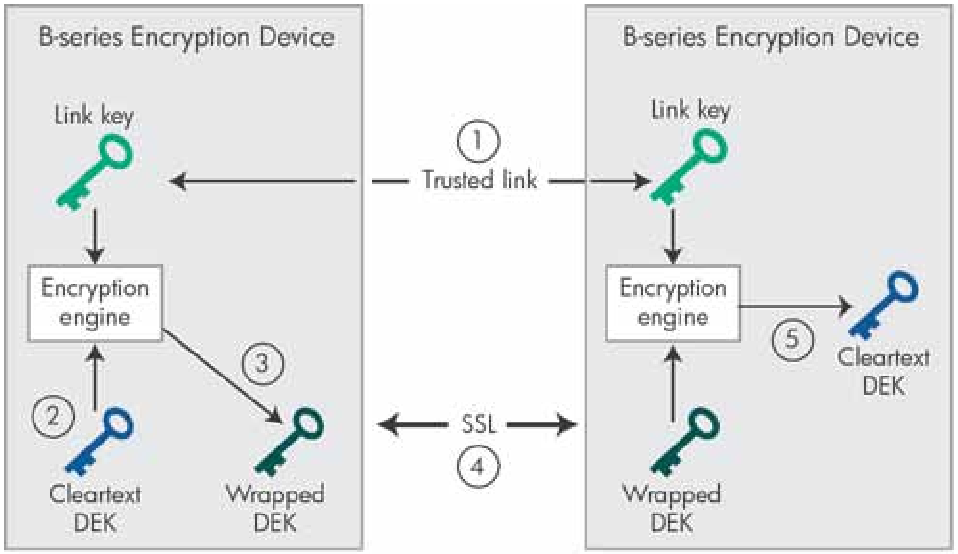
Figure 2: Key exchange between B-series encryption devices and the HP ESKM



When a key needs to be exchanged between B-series 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 in Figure 3.

1. A trusted relationship is created through a secure exchange between the B-series encryption devices. The trusted link generates a symmetric link key, (shown in dark blue) which is stored in each device and will be used to wrap and unwrap the DEK for secure transport.
2. The B-series encryption device creates a new DEK in cleartext (shown in dark green) within its security boundary.
3. The DEK is encrypted (wrapped) with the link key to create a wrapped DEK (shown in light green) before it leaves the encryption boundary.
4. The wrapped key is sent to the other B-series encryption device in the 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 B-series encryption device, it uses its link key to unwrap the DEK to discover the DEK in cleartext (shown in dark blue).

Figure 3: Key exchange between the B-series encryption devices



Key management

The HP Enterprise Secure Key Manager provides secure, centralized encryption key management services for HP LTO-4/LTO-5 enterprise tape libraries, B-series encryption devices, and other HP and partner encryption solutions. It is a hardened appliance with digitally signed logs and the following enterprise-class features and functionality.

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

The HP Enterprise 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 140-2 was developed by NIST to define security requirements for cryptographic modules.

The minimum configuration in an ESKM deployment consists of two ESKM 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 ESKM cluster. Encryption keys, key generation policies, client information, and other settings are automatically replicated between nodes within seconds of their creation or alteration (the nodes communicate via mutually authenticated 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 ESKM logs can be pushed out to the HP ArcSight SIEM solution for better tracking of ESKM activities. For more information on ArcSight, visit www.hp.com

Integration scenarios

The B-series encryption devices and HP ESKM combination offers encryption solutions to meet the needs of varied environments of corporations and institutions. Whether the customer needs a point product or a global deployment of encryption resources, HP offers a solution to help companies become compliant with industry and government regulations.

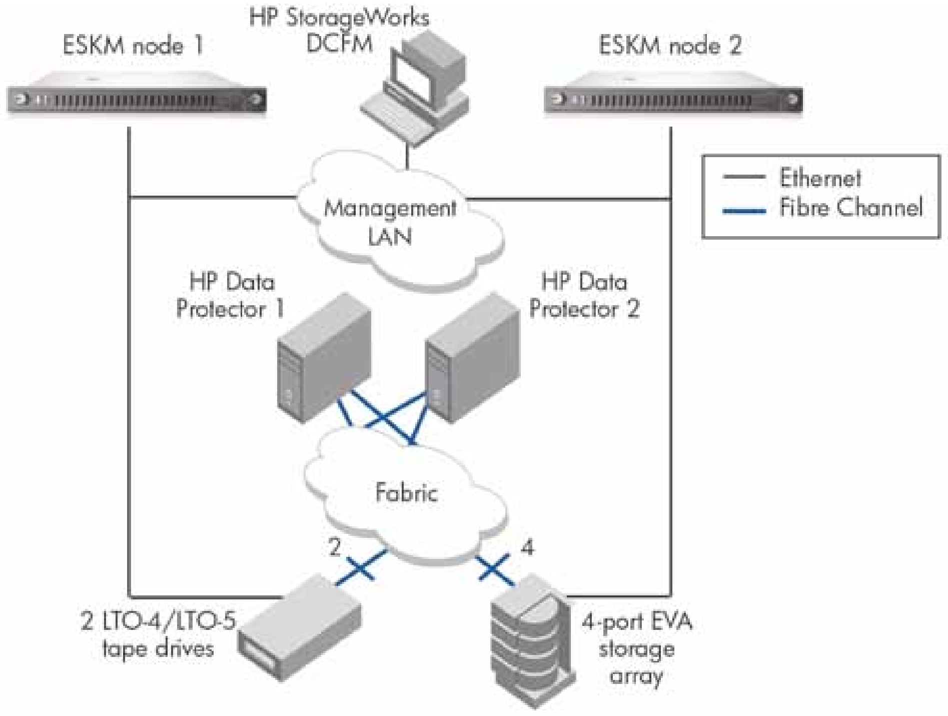
Two data-at-rest encryption scenarios are described in this section:

- Disk encryption upgrade
- Remote tape

Disk encryption upgrade

The Figure 4 shows an initial deployment with a pair of HP Ultrium LTO-4/LTO-5 tape drives that offer encryption of data-at-rest. The tape drives are housed in an HP EML 245e tape library to automate backup operations and allow integration with the ESKM cluster. This first deployment scenario is a modest step into the world of encryption, which lets the technology staff and security officer become familiar with encrypting data for offsite archiving with HP Data Protector. The security officer then establishes policies for DEK sharing between ESKM appliances and is confident that they can apply the techniques to other applications, and scale the infrastructure to encrypt more applications as well as disks. The IT staff decides to use their existing ESKM infrastructure and encrypt EVA storage arrays as well as more LTO-4/LTO-5 tape drives.

Figure 4: Initial encryption deployment



The Figure 5 shows how the organization expands their encryption solution with more tape drives, blade servers, EVA storage, and B-series encryption devices. The security officer upgrades the solution to encrypt multiple applications and continues to use the installed base of servers, EVA storage, ESKM appliances, Data Protector, and DCFM management software. The 4-port 4 Gigabit Fibre Channel (4GbFC) EVA storage array with 2 terabytes (TB) of storage is upgraded to an 8-port 4GbFC EVA array with 64 TB of storage by adding more controller cards and disk arrays. HP BladeSystem servers with server virtualization are used to create flexible deployment of servers that can access encrypted data through the B-series encryption devices. The IT staff scales their existing infrastructure with new hardware and software that integrates with their existing solutions.

Since the staff is already familiar with their existing management software (DCFM) for their storage area network and LTO-4/LTO-5 encryption solution, they are able to quickly encrypt new applications without changing their key management system or backup software. The ESKM manages the keys for the LTO-4/LTO-5 tape drives as well as the B-series encryption devices, which encrypts the disk-based storage. The keys are shared between the redundant B-series encryption devices and the redundant ESKM nodes. As part of a complete encryption ecosystem, the application data is 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 B-series 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 enabling data-at-rest confidentiality at unprecedented data transfer rates.

Figure 5: Upgraded encryption deployment

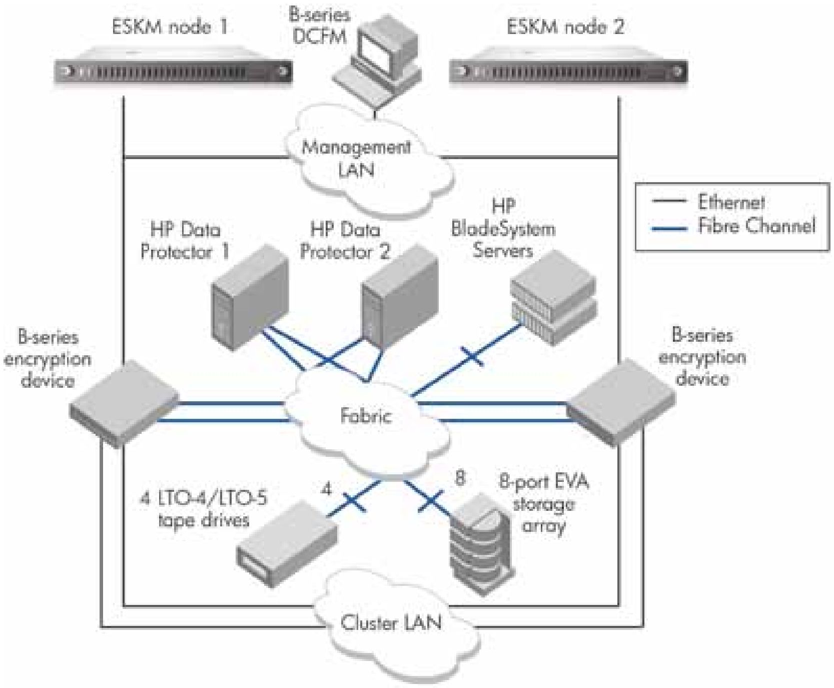
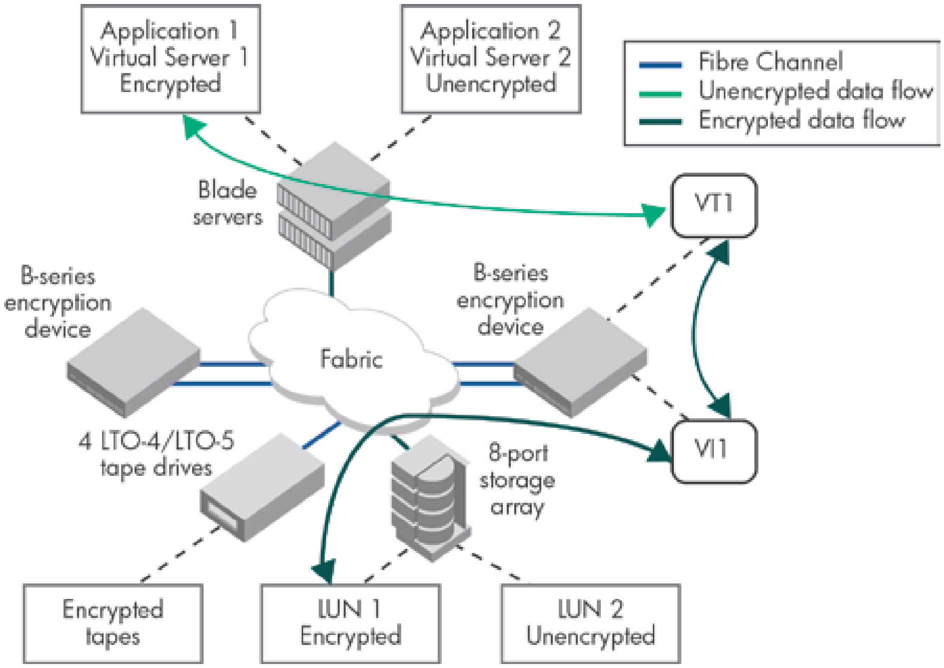


Figure 6: Logical view of upgraded deployment

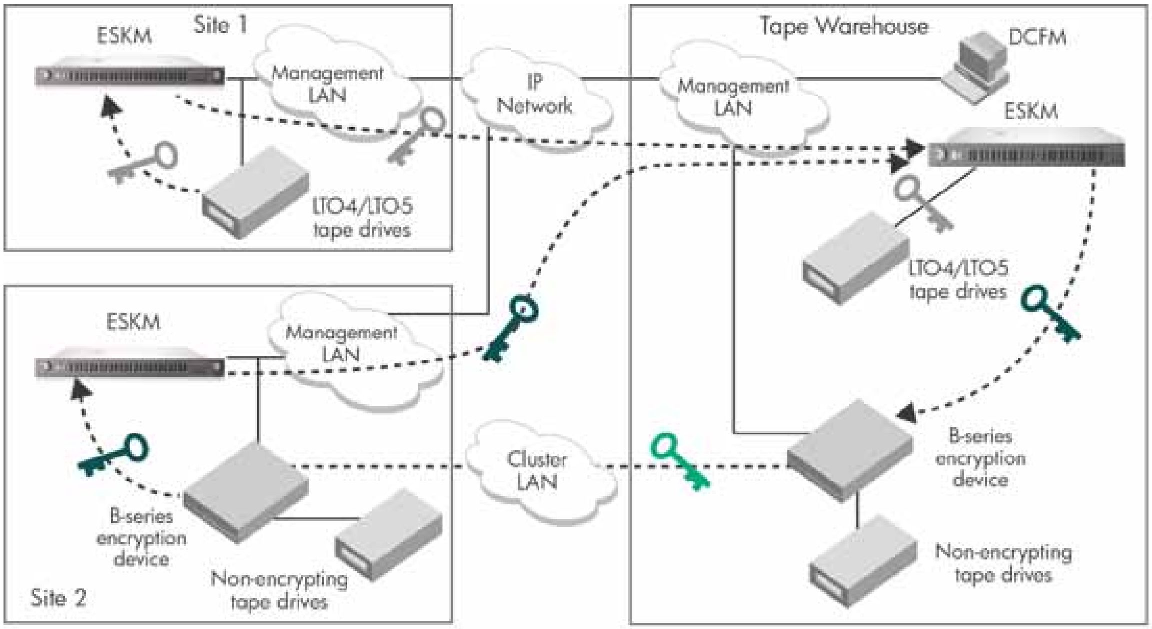


Decentralized tape backup

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/LTO-5 tapes and B-series encryption devices can be managed with the ESKM appliance. The B-series 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 ESKMs and B-series encryption devices.

ESKM manages encryption keys for tapes from multiple sites and tape environments via trusted key sharing. As shown in Figure 7, the ESKM at the tape warehouse stores DEKs for LTO-4/LTO-5 tape drives from Site 1 and B-series 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 ESKM appliances and transparently exchanged between the B-series encryption devices over the cluster LAN (the cluster LAN in Figure 7 has dotted lines because the synchronization between the B-series encryption devices actually occurs over the IP network). The ESKM appliance manages the DEKs while the B-series encryption devices exchange the DEKs.

Figure 7: Key exchange between remote sites (redundant SKMs and B-series encryption devices not shown)



Summary

HP has 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 B-series encryption devices and the HP ESKM work together to provide reliable encryption solutions. The basic configuration with redundant HP ESKM appliances and B-series encryption devices shows how the solution facilitates high availability encryption. Technology 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.

With products achieving FIPS 140-2 certification, customers are offered the highest level of security. HP also provides 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 can help assure customers that their data is secure and protected by using the latest encryption technology.

For more information

For more information on HP's complete Secure Advantage portfolio, please visit: http://www.hp.com/go/security.

For more information on the HP StorageWorks Encryption SAN Switch, please visit: http://h18006.www1.hp.com/storage/saninfrastructure/switches/encrypt_sanswitch/index.html.

For more information on the HP Enterprise Secure Key Manager, please visit: http://www.hp.com/go/eskm.

4AA3-3297ENW, Created May 2011