BitLocker Management

Vista Full Volume Encryption

Feature Overview

- BitLocker - Full Volume Encryption
  - Vista Enterprise and Ultimate
  - AD management & Key backup options
  - Save recovery password to USB, Printer, or File Share
- TPM 1.2 – Enables Drive Tampering Protection
- WMI Interface
- Vista Tool compatibility
  - MS Boot Loader, System Restore, Disk Management

BitLocker Tools

- Manage-bde.wsf - RTM
  - Add / Remove key protectors

Tools from MS Premier Support Site:

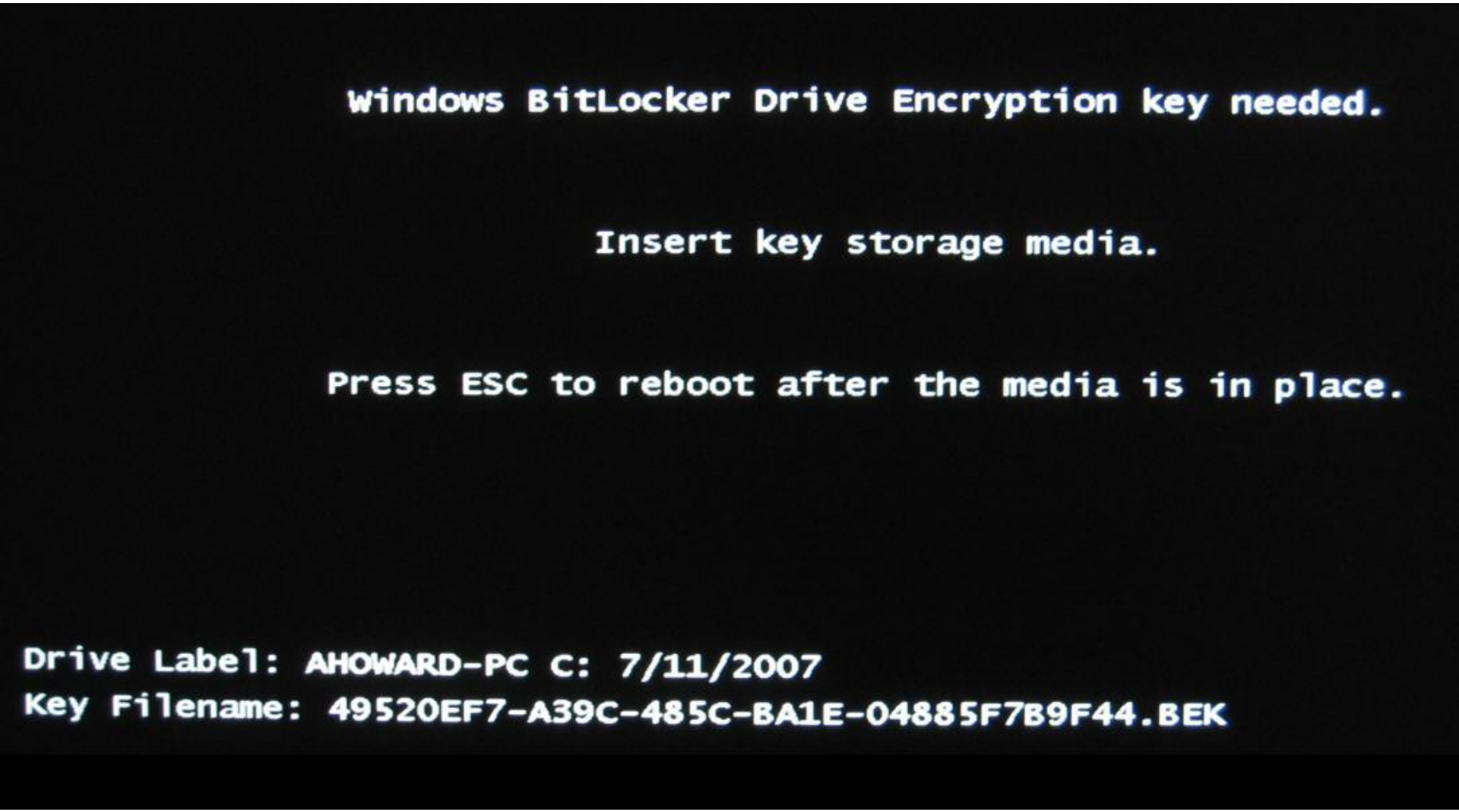
- BitLocker Drive Preparation
- BitLocker Recovery Password Viewer
- BitLocker Repair Tool
  - Searches HD for unlinked FVEKs

BitLocker Group Policy

- Computer Config\Admin Templates\Windows Components\BitLocker Drive Encryption
- AD Key Backup Options
  - Backup Recovery Password to AD
  - Backup Key Package to AD
  - Require Backup to AD before encryption is enabled
- Backup Recovery Password to Share
- Recovery Options
  - Require Creation of Recovery Password - Default
  - Require Creation of Recovery Key Package - Default

BitLocker Group Policy

- Advanced Options
  - Allow BitLocker without TPM
  - Startup Key or Pin with TPM
- Encryption Method AES 128 Diffuser – Default
- Prevent Memory Overwrite on Restart – Disabled
- TPM Platform Validation –7 Default Metrics
  - Rom Code
  - MBR Code – not partition table
  - Boot Manager


Windows BitLocker Drive Encryption key needed.
Insert key storage media.
Press ESC to reboot after the media is in place.
Drive Label: AHOWARD-PC C: 7/11/2007
Key Filename: 49520EF7-A39C-485C-BA1E-04885F7B9F44.BEK

TPM Group Policy

- Computer Config\Admin Templates\System\ Trusted Platform Module
- Backup TPM Owner information to AD
  - Require backup
- 3 settings related to TPM blocked commands
  - BDE Security and Compatibility

BitLocker Tips

- AD Backup only occurs when BDE is enabled
  - Or when TPM is initialized
- Manage-bde does more than the wizard
  - Data volumes or Removable Drives (NTFS only)
    - Auto-unlock feature
  - System volumes on some dual boot machines
- Only simple or basic volumes can be encrypted
- Enabling FIPS compliant encryption disables ability to create recovery passwords

BitLocker Resources

- Tech ED Presentation & Article – Byron Hynes

http://blogs.technet.com/tnmag/archive/2007/06/08/byron-hynes-on-bitlocker.aspx

- MS BitLocker Site

http://technet.microsoft.com/en-us/windowsvista/aa905065.aspx

The Planning and Implementation Guide

http://www.microsoft.com/downloads/details.aspx?familyid=41ba0cf0-57d6-4c38-9743-b7f4ddbe25cd&displaylang=en&tm

Manage-bde

http://blogs.technet.com/steriley/archive/2006/11/25/bitlocker-command-line.aspx

Repair tool

http://support.microsoft.com/kb/928201/en-us

http://helpdesk.its.uiowa.edu/encryption/