LEARNING LIVES HERE

BitLocker: Protecting Portable Data in Windows

Rahul Singh, Harpreet Singh
Global Technical Support Center
Microsoft India

msdn Microsoft® Developer Network

Microsoft TechNet

Agenda

- Introduction to BitLocker in Windows Vista
- Architecture
- Bitlocker and BitLocker To Go in Windows 7
- Using BTG
- Recovering your Data

BitLocker™ in Windows Vista

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System Drives	TPM TPM+PIN TPM+Startup key TPM+PIN+ Startup Key* Startup key	Recovery password Recovery key Active Directory backup of recovery password	Group policy controlled options presented to users	Use of the BitLocker Drive Preparation Tool to create a system partition where boot files are located System partition size: 1.5GB System partition assigned a drive letter NTFS file system
Fixed Data Drives*	Automatic unlocking	Same as OS drive	No policies	Operating System drive must be encrypted NTFS file system

*Introduced in Windows Vista SP1

R2

Disk Layout and Key Storage

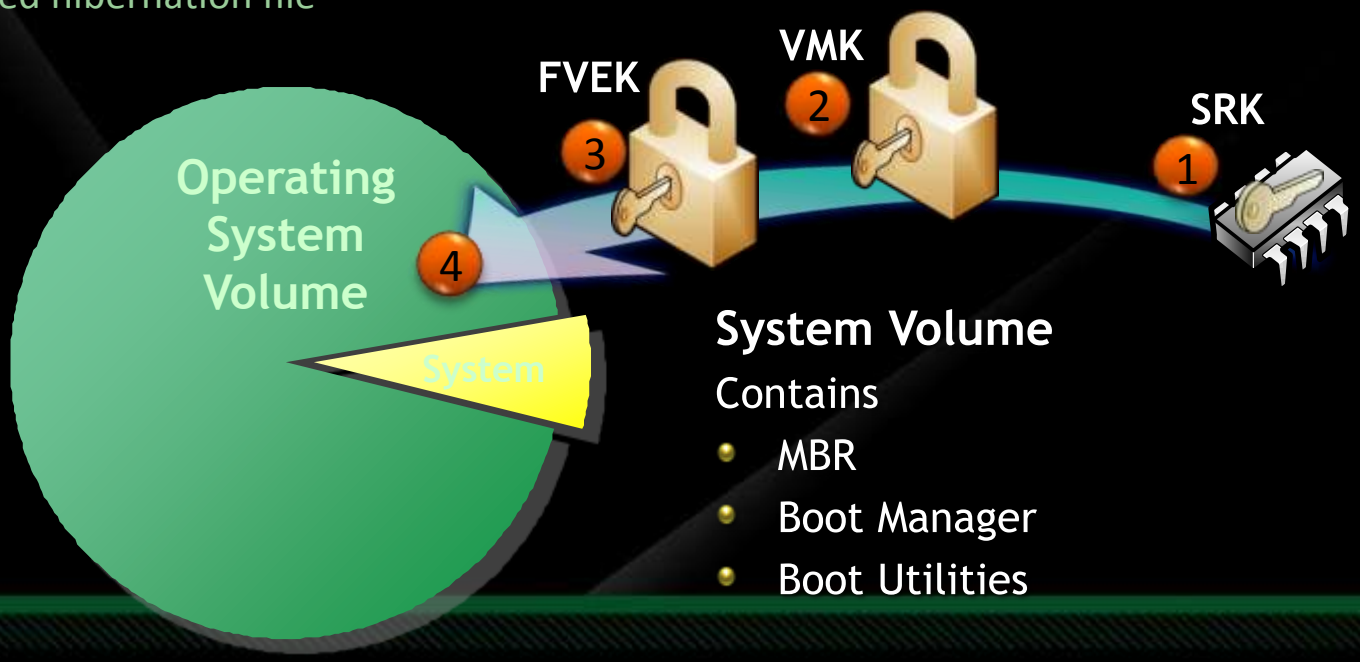
Operating System Volume

Contains

- Encrypted OS
- Encrypted page file
- Encrypted temp files
- Encrypted data
- Encrypted hibernation file

Where's the Encryption Key?

1. **SRK** (Storage Root Key) contained in TPM
2. **SRK** encrypts the **VMK** (Volume Master Key)
3. **VMK** encrypts **FVEK** (Full Volume Encryption Key) – used for the actual data encryption
4. **FVEK** and **VMK** are stored encrypted on the **Operating System Volume**



System Volume

Contains

- MBR
- Boot Manager
- Boot Utilities

BitLocker in Windows 7

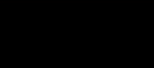
Operating System Drive Overview

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System drives	TPM TPM+PIN TPM+Startup key TPM+PIN+ Startup key Startup key	Recovery password Recovery key Active Directory backup of recovery password Data Recovery Agent	Robust and consistent group policy enforcement Minimum pin length	Drive preparation fully integrated in BitLocker setup. System partition size: 200MB without WinRE 400MB with WinRE System partition is letterless NTFS file system

R2

Setup and Configuration Improvements

- Windows 7 is BitLocker ready
  - A separate system partition is standard in Windows 7
  - System partition is now letterless and hidden
  - BitLocker Drive Preparation Tool now integrated into the BitLocker setup experience
- Upgrade scenarios
  - Windows Vista to Windows 7 upgrades are possible without decrypting the OS partition
- No Additional Tools required
  - Simply right-click and “Turn on Bitlocker” for a volume



BitLocker To Go

Requirements of Roaming

- Work on existing removable drives
- Easy to use
- Meet varied security needs
- Shouldn’t rely on IT departments centrally provisioning drives
- Recovery
- Easy to centrally administer policies
- Roam everywhere – home, work, clients

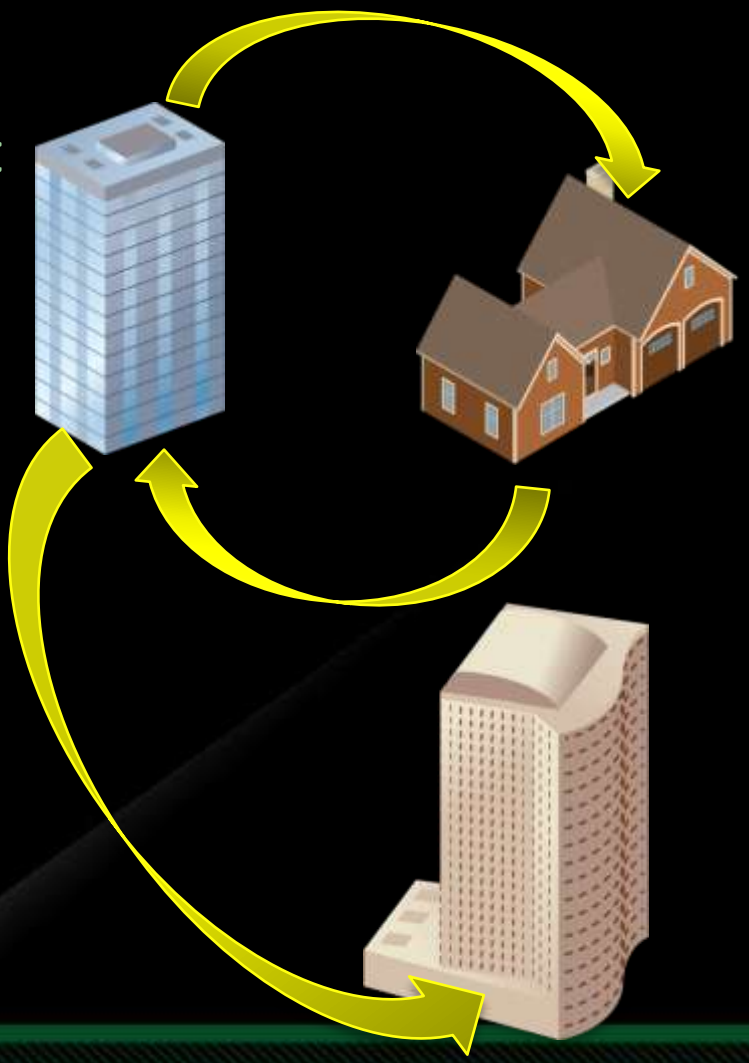
BitLocker on Removable Drives

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Removable data drives E.g.: USB flash drives External hard drives	Passphrase Smart card Automatic unlocking	Recovery password Recovery key Active Directory backup of recovery password Data Recovery Agent	Robust and consistent group policy controls Ability to mandate encryption prior to granting write access	File systems: NTFS FAT FAT32 ExFAT

New Unlock Methods

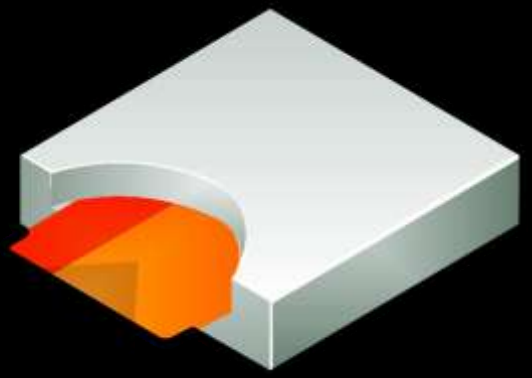
Roaming using a Passphrase

- No specific hardware requirement
- Easily roam inside and outside domains/organizations
- Complexity and length requirements managed by Group Policy



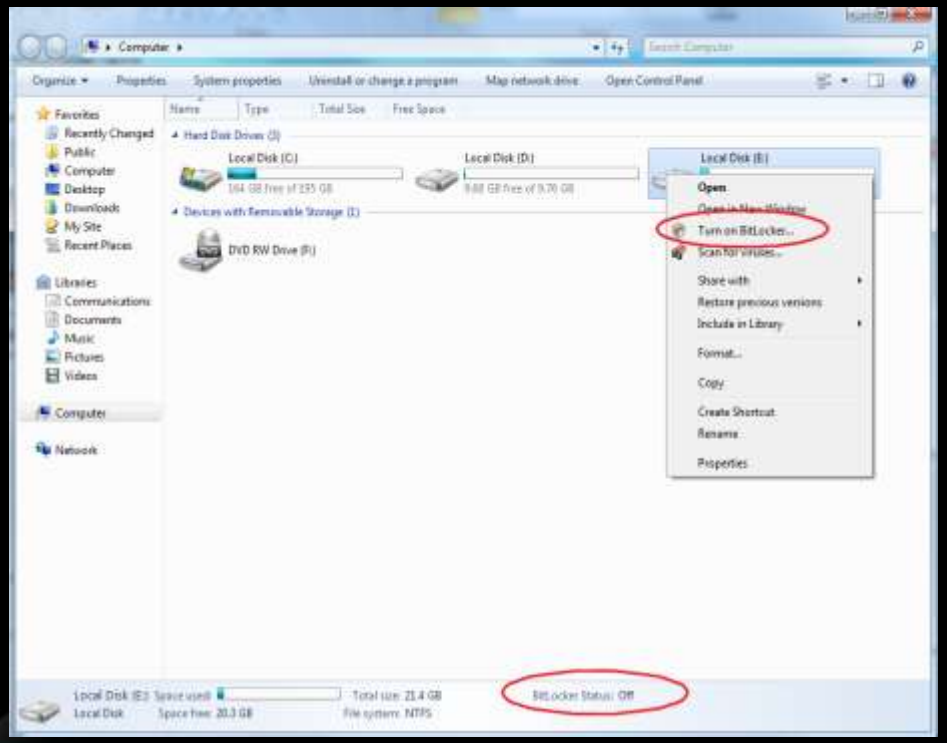
New Unlock Methods

- Roaming using Smart Cards
  - Leverages existing PKI infrastructure
  - Requires specific hardware
  - Can roam to any computer running Windows 7 or Windows Server 2008 RC2
  - Uses much stronger keys than passphrase



Integration

- Control BitLocker from Windows Explorer
- Right click drives in Windows Explorer to
  - Turn on BitLocker
  - Unlock a drive
  - Manage BitLocker
- Choose locking type:
  - Password based
  - SmartCard Base



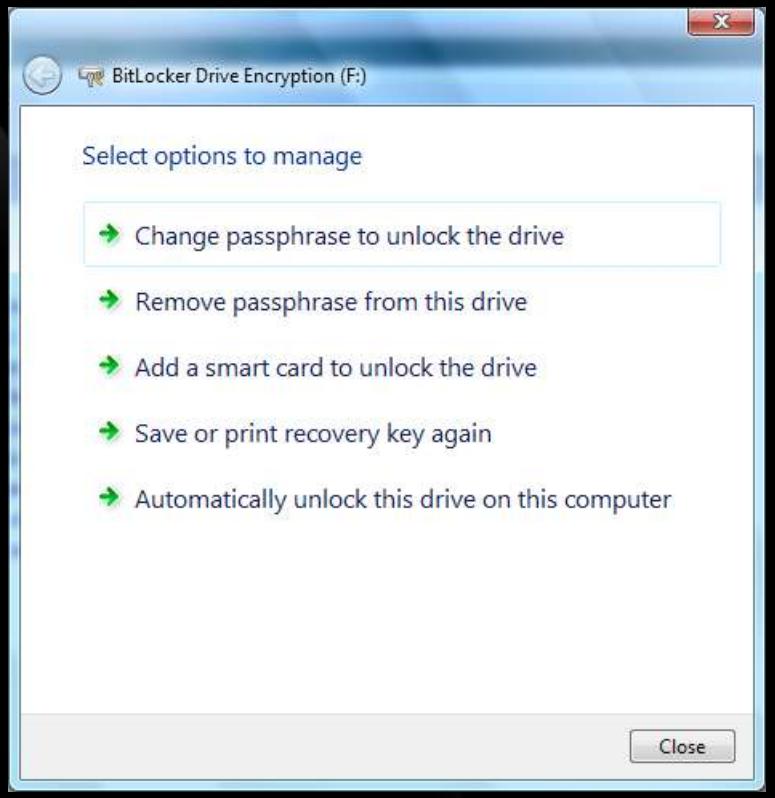
Using BTG

- Win7 allows user to enter password/smartcard to unlock drive
- User can save unlock status on a per-drive/per-user basis
- Password can be changed

Demo

Initializing, Installing and Using BTG

Managing BitLocker



Data Drives

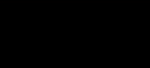
- Add, remove, or change their passphrase
- Add or remove a smart card
- Add or remove automatic unlocking
- Duplicate their recovery key/password

OS Drives

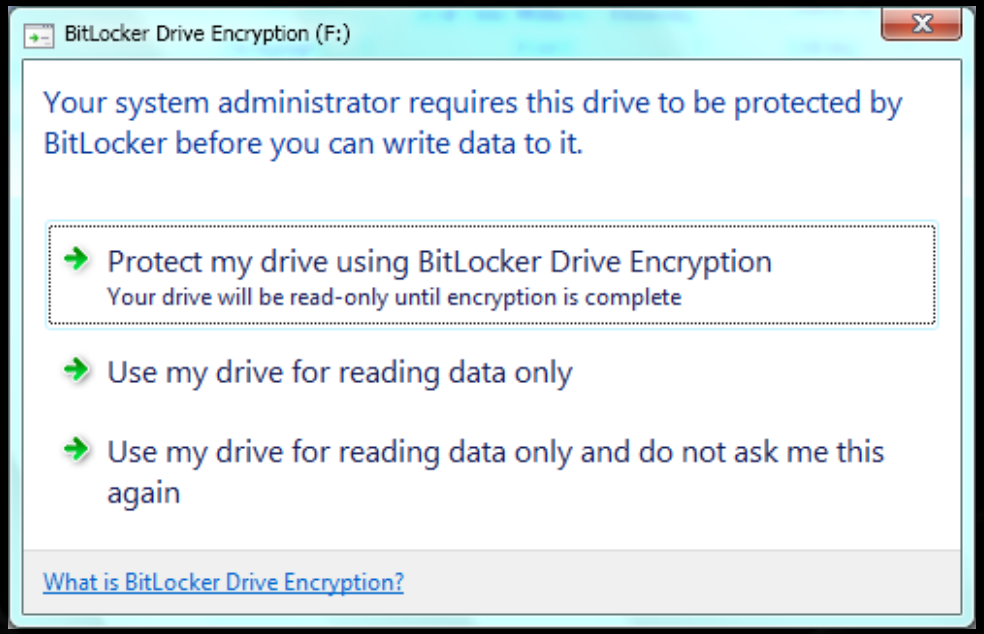
- Duplicate their recovery key/password
- Reset their PIN
- Duplicate their startup key

Mandating BitLocker on Removable Drives

- Requiring BitLocker for removable data drives
  - When this policy is enforced, all removable drives will require BitLocker protection in order to have write access
  - As soon as a drive is plugged into a machine, a dialog is displayed to the user to either enable BitLocker on the device or only have read-only access



Mandating BitLocker on Removable Drives



- The user gets full RW access only after encryption is completed
- Users can alternatively enable BitLocker at a later time

Demo

Managing BitLocker Settings

New Recovery Mechanism

- Data Recovery Agents (DRA)
  - Certificate-based key protector
    - A certificate containing a public key is distributed through Group Policy and is applied to any drive that mounts
    - The corresponding private key is held by a data recovery agent in the IT department
  - Allows IT department to have a way to unlock all protected drives in an enterprise
  - Saves space in AD – same Key Protector on all drives

Recovering Data from a Drive

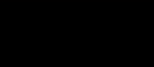
- User can also choose to save the Data Recovery key for a USB Drive
  - When turning BitLocker on
  - Managing BitLocker settings
- Key is not allowed to be saved on the same drive (obviously!)

Demo

Recovering your data from a BTG enabled drive

Working with BTG Drives on Earlier Versions of Windows

- BTG initialization adds a BTG Tool to the drive
- BTG Tool can be used on Windows XP, Windows 2003, Windows Vista and Windows 2008 to view contents of the drive
- The drive contents are read-only
- Data has to be copied off the drive to work with



Demo

Using a BTG drive on Windows XP/Vista

Microsoft®

Your potential. Our passion.™

R2