

Reducing the Risk of Data Theft with BitLocker and EFS

Zeb Bowden, Systems Architect
Virginia Tech

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Where I'm coming from...

- Microsoft Implementation Group –
(<http://vtmig.w2k.vt.edu>)
- Adopt, Adapt, Improve MS technologies – particularly Active Directory related
- Encrypted Data Storage group – focused on a solution for at rest data.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Agenda

- The Threat of Data Theft/Unintentional Disclosure
- BitLocker Overview
- TPM Introduction
- BitLocker Keys and Management
- Potential Problems
- EFS
- Questions/Discussion

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

The Good News

- Operating System security is not perfect, but it is better
- Windows NT → Windows 2000 → Windows XP → XP SP2 → Vista
- Laptops and tablets are more popular than ever and that trend looks to continue.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white and have ornate capitals. The entire slide is framed by a dark brown border.

So Are We More Secure?

- We have smaller, easier to carry devices that house more secure operating systems (and hopefully applications).
- This results in more secure, easier to carry computing devices?
- “Not so fast my friend” ...

- *Lee Corso*

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Bad News

- Smaller, easier to carry = easier to steal and conceal
- Most/almost all of the security improvements have been focused on protecting data in use (online data).
- Very little has been done to protect data “at rest” (offline).
- Physical access = all bets off

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

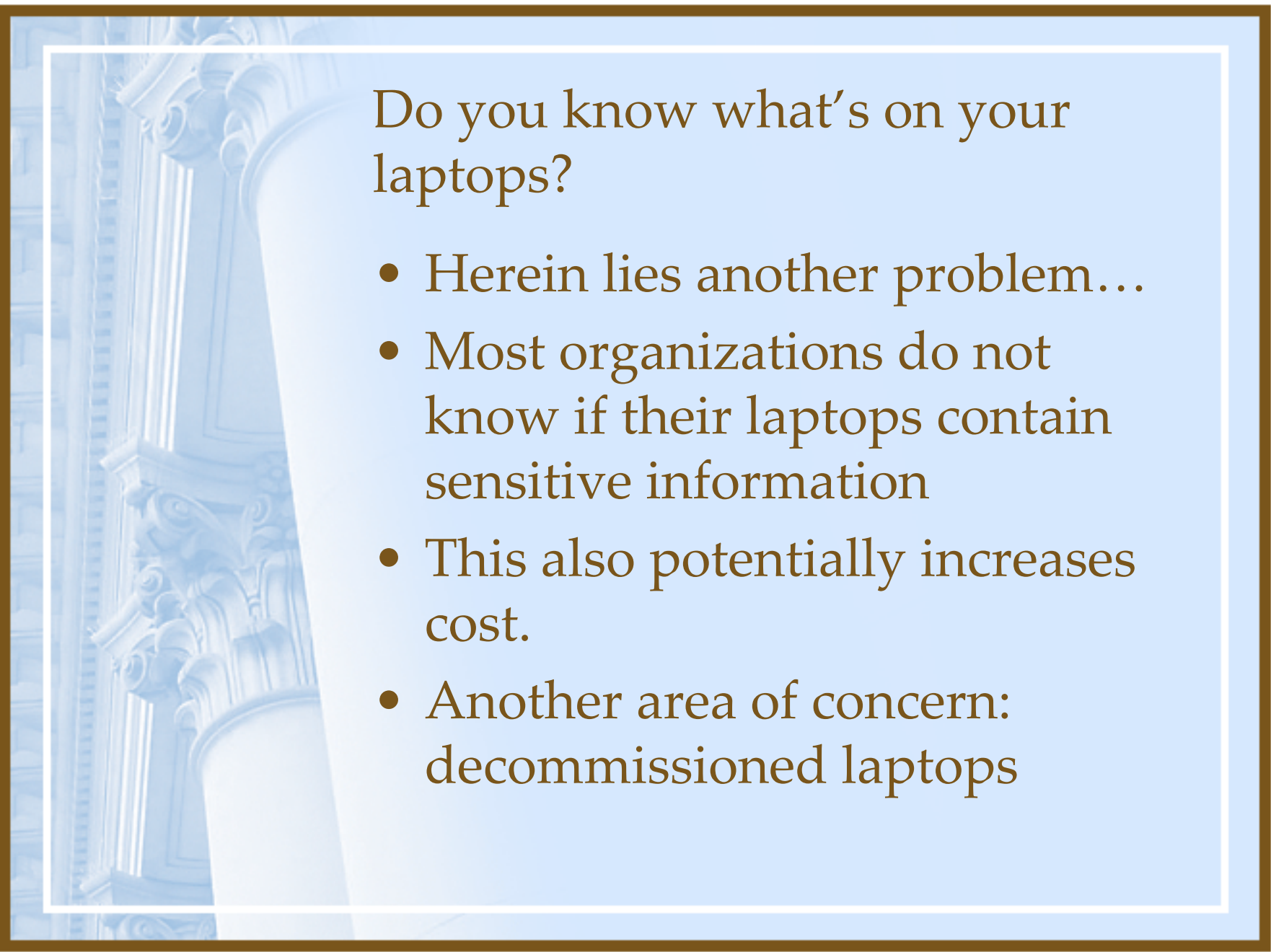
The Threat

- If you've got a machine or just the hard drive, it is a trivial process to get to the data.
- Stolen or lost laptops are nothing new
- Replacing the laptop is a problem but the real threat is the unintentional disclosure of "sensitive" data.



Threat (cont.)

- The cost to deal with incidents however has greatly increased
- Hardware costs are real but relatively small
- The potential for high cost is realized in things like:
 - Bad publicity
 - Loss of revenue (funding, grants, etc)
 - Cost to cleanup/contain
 - Government fines

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Do you know what's on your laptops?

- Herein lies another problem...
- Most organizations do not know if their laptops contain sensitive information
- This also potentially increases cost.
- Another area of concern: decommissioned laptops

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

In Higher Education

- We face additional challenges that may not be addressed by typical enterprise solutions
 - Large amounts and diverse nature of data
 - Decentralized management
 - Lack of accountability
 - Missing/weak policies
 - Popularity of laptops, tablets, etc.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Addressing the Threat

- Data Encryption – best way so far
- Various ways to implement this, each with its own set of challenges:
 - Deciding what to encrypt
 - Accidental storage of unencrypted files
 - System files
 - Key management (lost keys, secure storage)
 - Encryption policy enforcement

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker

- Full disk (volume) encryption
- Seamless experience for the user
- Available on Enterprise and Ultimate
- Utilizes a Trusted Platform Module (TPM) for key protection
- Secure Startup - Integrity checking of boot components
- Initiated at each startup/boot
- Protects data in the “at rest” state.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker Encryption

- Uses AES 128 (w/ diffuser) by default
 - Can use AES 256
 - Can use with or without diffuser
- Sector level encryption – below the file system

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker Prerequisites

- Setup isn't a simple wizard
- You need 2 volumes:
 - your Windows volume, which will be encrypted
 - A 1.5GB unencrypted volume to be used to boot the system
- Your system BIOS needs to support reading/writing to USB devices
- TCG compliant TPM v1.2 (optional)



TPM explained

- Like a smart card attached to your motherboard
- TPM requires certain environmental conditions to be met before keys are accessible.
- This is known as sealing and unsealing.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

More TPM Information

- TPM needs to be enabled, activated, and owned
- TPM Initialization Wizard can walk you through this
- What does ownership give you?
 - Administrative tasks – unlocking the TPM
 - Remote operations
 - It's not the equivalent of root, does not have full control of the TPM or the keys



Why TPM v1.2?

- Only needs one universal driver (that Microsoft wrote)
- Wouldn't this be nice for smart cards/tokens?

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white and have ornate capitals. The entire slide is framed by a dark brown border.

BitLocker and the TPM

- BitLocker uses the TPM to seal keys which protect your data
- Environment must be appropriate for the TPM to unseal.
- Unsealing is performed on the TPM

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker Keys

- Full Volume Encryption Key – this is the key actually used to encrypt data, it is stored (encrypted) in the encrypted volume's metadata.
- Volume Master Key – this key protects the Full Volume key, it is protected by the TPM (or startup/recovery key). Picture

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker Keys (2)

- Recovery Key – a key stored on a USB device that can be used in “recovery situations”. PIN or startup key unavailable OR something in the integrity check failed.
- Recovery Password – a 48 numerical character password used in “recovery situations”. Human readable recovery key
- Startup Key – a key stored on a USB device that can be used to boot the system.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker Modes

- Standard Mode: uses TPM, requires no user interaction on boot
- TPM + PIN: user must enter a numerical PIN on each boot
- TPM + Startup Key: user must insert a USB device on each boot
- Startup Key Only: for systems without a TPM
- PINs and Startup Keys do not replace the need for strong passwords

BitLocker Management

- Active Directory integration
 - Policy via Group Policy
 - UI Configuration
 - Recovery information stored in AD (Screen Shot)
- Technical Management done via WMI (manage-bde.wsf).
- Ultimate Extra: “Secure Online Key Backup” (Screen Shot)
- FIPS compliance = no recovery password

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Group Policy Configuration

- GUI changes:
 - Control Panel Setup: Configure recovery folder
 - Control Panel Setup: Enable advanced startup options
 - This allows you to use BitLocker in the advanced modes.

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Group Policy Config (2)

- Security Changes:
 - Configure encryption method
 - Changes to this setting require that the drive be decrypted and then re-encrypted, doesn't happen automatically.
 - Prevent memory overwrite on restart

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Group Policy Config (3)

- Recovery Information Settings
 - Turn on BitLocker backup to Active Directory Domain Svcs
 - Takes effect when a new recovery password (or TPM owner password) is created.
 - Control Panel Setup: Configure recovery options
- TPM Validation
- TPM Configuration

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Backups

- BitLocker will backup recovery information to AD, Digital Locker, USB device, etc.
- Actual data backups will still be necessary
- Careful, BitLocker doesn't protect network traffic
- BitLocker Repair Tool (928201)
 - for damaged devices

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker - Decommissioning

- Reduce the speed at which you can decommission or reuse machines.
- Scrubbing/multiple overwrites no longer necessary
- Just delete the keys – the data is unavailable
- Vista format is BitLocker aware, and will delete the keys

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.


Legitimate System Changes

- Situations arise that change the conditions the TPM verifies
 - Motherboard replacement
 - BIOS upgrade
- These can be addressed by turning BitLocker off, make changes, turn it back on (Screen Shot)
- Volume master key available – encrypted with a Clear Key

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Attacking BitLocker

- Hardware based – specialized
- Software based –
 - Vulnerability in the boot environment
 - Attack the OS to reveal recovery information
- Simple PIN or storing USB device with laptop

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

BitLocker (High Level) Walkthrough

- Schema/permission modifications
- Configure BitLocker group policy
- Install Vista, correctly configure volumes on the client machine
- Join the machine to your domain
- Enable, activate, and take ownership of the TPM
- Turn on BitLocker (via manage-bde or GUI)

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white and have ornate capitals. The entire slide is framed by a dark brown border.

BitLocker Problems

- Order of implementation matters.
 - BitLocker off prior to joining domain
- An additional volume is required
 - BitLocker Drive Preparation Tool
- Policy changes require turning BitLocker off and back on
- No policy to enforce BitLocker being turned on
- TPM's are new

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Windows Volume only

- Not supported on volumes other than your Windows vol.
- Works really well with Encryption File System (EFS)

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

EFS improvements

- EFS isn't new but is being improved upon
- Available in Enterprise, Ultimate and Business
- New in Vista
 - More control through policy
 - Pagefile encryption
 - Document's folder and offline files cache encryption
 - Smart cards for key storage

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

EFS and BitLocker

- BitLocker compliments EFS quite nicely.
 - Protects the keys used by EFS
- EFS is more versatile than BitLocker
 - Multiple keys to encrypt
 - Sharing supported
 - Remote encryption

The background of the slide features a light blue gradient with a faint, semi-transparent image of classical architectural columns on the left side. The columns are white with detailed capitals and are set against a darker blue background. The entire slide is framed by a thin brown border.

Other options

- Other products are available
 - PGP
 - TrueCrypt
 - PointSec
 - Hardware based
- Easy to Manage?
- Recovery?

Resources

- **Step-by-Step Guide to BitLocker:**
<http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true>
- **TPM Information:**
<https://www.trustedcomputinggroup.org/home>
<http://technet.microsoft.com/en-us/windowsvista/aa905092.aspx>
- **System Integrity Blog:**
http://blogs.msdn.com/si_team
- **BitLocker Repair Tool:**
<http://support.microsoft.com/kb/928201/>

Resources (2)

- **BitLocker Encryption Algorithm:**
<http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/BitLockerCipher200608.pdf>
- **Tracking data exposures:**
<http://www.privacyrights.org/ar/ChronDataBreaches.htm>
- **BitLocker in AD:**
<http://technet2.microsoft.com/WindowsVista/en/library/3dbad515-5a32-4330-ad6f-d1fb6dfcdd411033.msp?mfr=true>
- **VTmig Presentations:**
<http://vtmig.w2k.vt.edu/publications.html>



The End

- Questions, Comments, etc.?



Encrypting File System



Which type of certificate do you want to create?

Select an option below to automatically create and store a file encryption certificate.

- A self-signed certificate stored on my computer
Select this option unless you are using a smart card or a certification authority.
- A self-signed certificate stored on my smart card
Insert your smart card in the card reader.
- A certificate issued by my domain's certification authority
Make sure your computer can access its domain. If you are storing the certificate on a smart card, insert the card in the reader.

[Which type of certificate should I choose?](#)

Next

Cancel

BitLocker Recovery Password Viewer

The screenshot shows the MSBITLOCKER Properties dialog box with the BitLocker Recovery Passwords tab selected. The dialog box has a title bar with a question mark and a close button. Below the title bar are four tabs: General, Operating System, Member Of, and Location. The BitLocker Recovery Passwords tab is active, showing a table with two columns: Date Added and Password ID. The first row is highlighted in blue. Below the table is a section labeled Details, which contains the Recovery Password, Computer name, Date, and Password ID.

Date Added	Password ID
2007-02-16 10:47	1AC046AF-0AFC-4DE3-AB4E-1C94428B8435

Details:

Recovery Password:
249755-524678-600578-162547-
702592-281479-712239-321640

Computer: MSBITLOCKER.zeb.vt.edu
Date: 2007-02-16 10:47:13 -0500
Password ID: 1AC046AF-0AFC-4DE3-AB4E-1C94428B8435

OK Cancel Apply

Administrator: Command Prompt

Microsoft Windows [Version 6.0.6000]

Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cscript manage-bde.wsf -protectors -add c: -tp 13579

Microsoft (R) Windows Script Host Version 5.7

Copyright (C) Microsoft Corporation. All rights reserved.

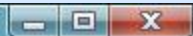
Key Protectors Added:

TPM And PIN:

ID: <0F2E031E-0285-4ABC-9B1E-D68E8142172D>

Key protector with ID "<741CF7F8-9B2F-4594-960A-CC0DA93AEFES>" deleted.

C:\Windows\system32>_



Control Panel > Security > Secure Online Key Backup

Search

Save your BitLocker recovery password or EFS recovery certificate in digital locker

Save your Windows BitLocker Drive Encryption recovery password or Encrypting File System (EFS) recovery certificate on a free Microsoft website called digital locker. You can retrieve your password or certificate from this website at any time, from any computer that's connected to the Internet.

[Read the digital locker privacy policy.](#)



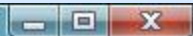
Save your BitLocker recovery password

You can store a copy of the recovery password in digital locker if your hard drive is encrypted using BitLocker Drive Encryption.



Save your EFS recovery certificate

You can store a copy of the EFS recovery certificate in digital locker if you have EFS encrypted files.



Security > Secure Online Key Backup > BitLocker

Search

Store your recovery password on the digital locker website

 Your hard disk is encrypted with Windows BitLocker Drive Encryption, but your recovery password is not stored on the website.

Enter your Windows Live ID below to store a copy of your recovery password in digital locker. Instructions for signing into digital locker and retrieving your recovery password will be sent to the e-mail address you provide.

[Why do I need a recovery password?](#)

Description

Windows BitLocker Drive Encryption Recovery Password for the disk volume MSBITLOCKER C: 3/2/2007

Enter your Windows Live ID _____

[Sign up for Windows Live!](#)

[Help](#)



Works with MSN, Office Live and Microsoft Passport sites

Email address:

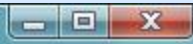
(example: someone@example.com)

Password:

[Forgot your password?](#)

Submit

Cancel



Control Panel > Secure Online Key Backup > Status

Search

Your recovery password has been successfully sent to digital locker



Instructions about how to retrieve your recovery password have been sent to the e-mail address that you provided on the previous screen.
[Click here to go to your digital locker.](#)

The following recovery password has been backed up in digital locker.

Recovery Password

612073-094930-124256-654027-569096-033825-703186-074679

Disk Volume

MSBITLOCKER C: 3/2/2007

Click "Print" to print the information on this page. Because the printout contains your recovery password, be sure to store it in a safe place.

Print

Disable BitLocker

BitLocker Drive Encryption



What level of decryption do you want?

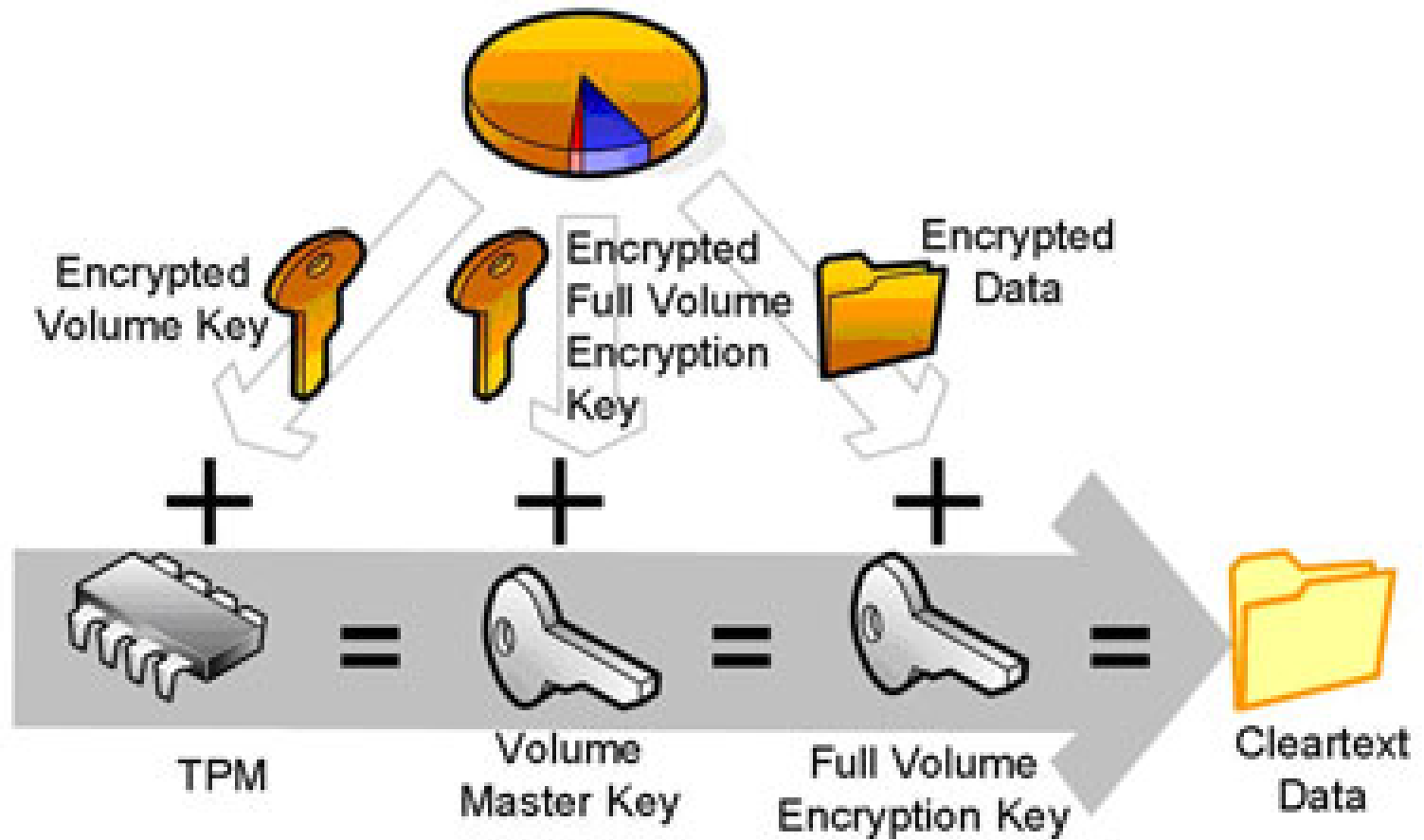
The type of decryption you choose will affect the security of your data.

- ➔ **Disable BitLocker Drive Encryption**
BitLocker Drive Encryption will be disabled. Your encryption key could be exposed with possible security risks if any changes are made to your system.
- ➔ **Decrypt the volume**
Your volume will be decrypted. This may take considerable time. You will be able to monitor the status of your volume decryption.

Cancel

[What is the difference between disabling BitLocker Drive Encryption and decrypting the volume?](#)

BitLocker Keys



© 2007 Microsoft Corporation – image taken from:

<http://technet.microsoft.com/en-us/windowsvista/aa906017.aspx>