PROTECT

MICROSOFT BITLOCKER

MICROSOFT WINDOWS 7/WINDOWS SERVER 2008 R2

Product Description

BitLocker is a software-based disk encryption feature that is part of Enterprise and Ultimate editions of Microsoft Windows 7 and all editions of Windows Server 2008 R2. It provides confidentiality to data at rest on appropriately powered down computers. BitLocker is typically used with a Trusted Platform Module (TPM).

BitLocker supports a number of different "Key Protectors". A Key Protector defines how many, and what, authentication factors are used. BitLocker supports a number of 1-factor, 2 factor and 3-factor authentication options.

Scope of Common Criteria Certification

The scope of the Common Criteria (CC) certification included the following security functionality:

- Access control
- Data encryption
- Key protection

Common Criteria Certification Summary

The product has met the requirements of the Common Criteria Evaluation Assurance Level (EAL) 4 augmented with advanced flaw remediation (ALC_FLR.3).

DSD's Cryptographic Evaluation

Since the product employs cryptography as a security enforcing mechanism, DSD performed a cryptographic evaluation on the product in addition to the Common Criteria certification.

DSD was able to confirm the implementation of secure data at rest when configured in accordance with the guidance in this consumer guide.

DSD's cryptographic evaluation applies to the following versions of Windows:

- Windows 7 RTM/SP1
- Windows Server 2008 R2 RTM/SP1

PROTECT

DSD's Recommendations

As BitLocker has been evaluated to EAL4+ with a DSD cryptographic evaluation, it can be used to reduce the physical storage and handling requirements of classified data at rest. As such, the product can be used in accordance with the Australian Government Information Security Manual (ISM) for the storage of information of classification:

- PROTECTED
- UNCLASSIFIED

When appropriately used BitLocker can reduce the physical storage and handling requirements of the above classifications to those of UNCLASSIFIED.

Agencies must be aware that the reducing of physical storage and handling requirements for BitLocker protected computers to UNCLASSIFIED only applies when data is at rest. This is only when computers are turned off/hibernated and unauthenticated to. Conversely, when a computer is turned on and authenticated to, it assumes the classification of that data that resides on it and must be handled appropriately.

BitLocker must be enabled before any classified information is written to the HDD.

Sleep mode must be disabled as a BitLocker protected computer that is put to sleep does not require authentication before access is given to data. A computer that is in a sleep state is authenticated to, and does not benefit from any reduction in physical storage and handling requirements.

DSD approves the following Key Protectors:

- TPM + PIN + USB
- TPM + PIN
- TPM + USB
- USB

Where PINs are used, they must be "enhanced" PINs. Windows 7/Windows Server 2008 R2 introduced enhanced PINs. Enhanced PINs allow characters from the full keyboard.

DSD recommends the use of Key Protectors that incorporate PINs over ones that do not.

If TPM + PIN + USB is used the PIN must be at least six characters long. The PIN should consist of at least three of: lowercase characters, uppercase characters, digits and punctuation and special characters.

If TPM + PIN is used the PIN must be either:

- a minimum length of 12 characters with no complexity requirement; or
- a minimum length of nine characters, consisting of at least three of the following character sets: lowercase characters, uppercase characters, digits and punctuation and special characters.

PINs and USB authentication tokens must be handled as per the classification of the data that they protect. They must not be stored with a BitLocker protected computer when it is powered down/hibernated.

Recovery Keys allow for the recovery of data where a user has forgotten their password. The Recovery Key is a 48-digit machine generated key and must be classified at the same level as the information protected by BitLocker and handled appropriately.

If a BitLocker protected computer is put into "disabled" mode it assumes the classification of the data, even when powered off. That is, BitLocker no longer provides a reduction in physical storage and handling requirements. Agencies must sanitise the HDD using an ISM approved mechanism and then reinstall BitLocker before a reduction in physical storage and handling requirements can be applied. This is because when BitLocker is put into disabled mode it will write encryption keys to the HDD in the clear.

DSD recommends that agencies configure BIOS with a "setup" password and disable Direct Memory Access (DMA) controllers such as Firewire/1394. This is to reduce the risk of DMA based attacks.

Additional Resources

Agencies wishing to use BitLocker should refer to the Cryptography chapter in the ISM.

Further information on HDD sanitization can be found in the Media Sanitisation chapter in the ISM.

Further information on DMA threats to BitLocker can be found at:

http://blogs.msdn.com/b/si_team/archive/2008/02/25/protecting-bitlocker-from-cold-attacks-and-other-threats.aspx and http://support.microsoft.com/kb/2516445

Further information on BitLocker configuration for Windows 7 can be found at:

http://technet.microsoft.com/en-us/library/dd835565(WS.10).aspx

Point of contact

For further information regarding certification or compliance with the ISM please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.