FEBRUARY 2015

Microsoft BitLocker and BitLocker To Go for Windows 7, Windows 8 and Windows Server 2012

Product Description

1. Microsoft BitLocker is a software Full Disk Encryption (FDE) program which provides confidentiality to Data-at-Rest (DaR) on appropriately powered-down x86 and x86_64 computers. Microsoft BitLocker is typically, but not always, used with a Trusted Platform Module (TPM).

2. Microsoft BitLocker To Go is a software Full Disk Encryption (FDE) program which provides confidentiality to Data-at-Rest (DaR) on removable media.

3. Microsoft BitLocker and BitLocker To Go support a number of different "Key Protectors". A Key Protector defines the authentication factors required to decrypt data stored on a protected volume. ASD has approved a subset of the available Key Protectors for use.

ASD's Cryptographic Evaluation

4. As Microsoft BitLocker and BitLocker To Go rely on cryptography as a security enforcing mechanism, ASD performed an ASD Cryptographic Evaluation on the product in addition to its Common Criteria Certification.

5. ASD's Cryptographic Evaluation applies to the following versions of the product:

   a. Microsoft BitLocker and BitLocker To Go for Windows 7 on x86 and x86_64

   b. Microsoft BitLocker and BitLocker To Go for Windows 8 on x86 and x86_64

   c. Microsoft BitLocker and BitLocker To Go for Windows Server 2012 on x86 and x86_64

6. This Consumer Guide does not apply to Microsoft BitLocker and BitLocker To Go for Windows 8.1 on x86 and x86_64, as these products have not completed a Common Criteria certification.

ASD's Recommendations

7. Recommendations in this Consumer Guide supersede any conflicting ISM requirements.

8. When appropriately used, Microsoft BitLocker and BitLocker To Go may be used to reduce the physical storage and handling requirements of storage media classified PROTECTED (and below) to UNCLASSIFIED.

9. Microsoft BitLocker and BitLocker To Go must be enabled before sensitive data is written to the storage media.

10. ASD approves the following Key Protectors for use with the evaluated versions of Microsoft BitLocker:

a. TPM + Startup Key (USB) + (enhanced) PIN

b. TPM + PIN

c. TPM + USB

d. USB

11. ASD approves the following Key Protectors for use with the evaluated versions of Microsoft BitLocker To Go:

a. Password meeting the complexity and length requirements detailed below

12. The escrow of recovery information, such as recovery password, TPM Owner password, and the BitLocker Key Package, should be used to ensure that devices can be recovered, if required. Agencies should ensure that this is performed while connected to a network accredited to the maximum classification of data that will be protected by Microsoft BitLocker or BitLocker To Go.

13. ASD was not able to evaluate Key Protectors not detailed above. These additional key protectors do not form part of the evaluated configuration for Microsoft BitLocker and BitLocker To Go and should not be used.

14. Sleep mode must be disabled as a Microsoft BitLocker protected computer that is put to sleep retains cryptographic material in memory. A computer that is in a sleep state is thus effectively unlocked (regardless of the state of a screen lock), and does not benefit from any reduction in physical storage and handling requirements.

15. Passphrases used for Microsoft BitLocker and BitLocker To Go must be a minimum length of 13 alphabetic characters, or a minimum length of 10 characters consisting of at least three of the following character sets:

a. Lowercase alphabetic characters [a-z];

b. Uppercase alphabetic characters [A-Z];

c. Numeric characters [0-9]; or,

d. Special characters [!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~].

16. If Microsoft BitLocker or BitLocker To Go is put into "disabled" mode, the storage media assumes the classification of the data, even when the device is powered-off and unauthenticated. That is, BitLocker and BitLocker To Go no longer provide a reduction in physical storage and handling requirements. Agencies must sanitise the storage media using an ISM approved mechanism and then enable Microsoft BitLocker or BitLocker To Go before a reduction in physical storage and handling requirements can again be applied. This is because Microsoft BitLocker and BitLocker To Go write encryption keys to the storage media when it is put into disabled mode.

Further Information

17. This guidance is given in accordance with the ISM April 2014 release.

18. This guidance was issued by ASD on 10 February 2015.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).