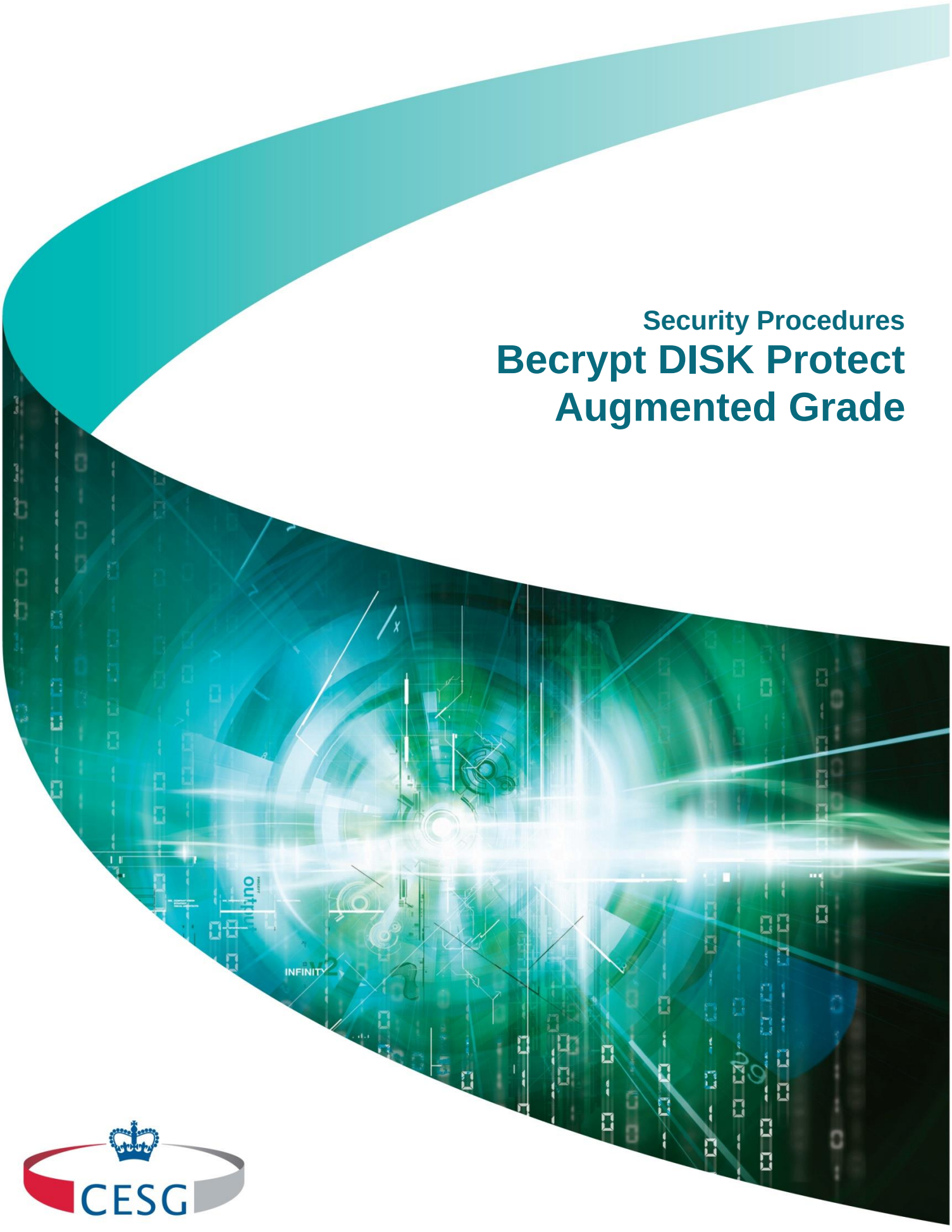
October 2015
Issue No: 1.1

Security Procedures

Becrypt DISK Protect Augmented Grade



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Security Procedures

Becrypt DISK Protect
Augmented Grade

Issue No: 1.1
October 2015

This document describes the manner in which this product should be implemented to ensure it complies with the requirements of the CPA security characteristic that it was assessed against. The intended audience for this document is HMG implementers, and as such they should have access to the documents referenced within. If you do not have access to these documents but believe that you have an HMG focused business need, please contact CESG Enquiries.

Document History

Version	Date	Comment
1.0	May 2013	First issue
1.1	October 2015	First public release

About this document

These Security Procedures provide guidance on the secure operation of Becrypt DISK Protect.

This document is intended for System Designers, Risk Managers and Riask Management Advisors.

The Security Procedures come from a detailed technical assessment carried out by CESG. They do not replace tailored technical or legal advice on specific systems or issues. CESG and its advisors accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed on this guidance.

Related documents

The documents listed in the References section are also relevant to the secure deployment of this product. For detailed information about device operation, refer to the DISK Protect product documentation.

Points of contact

For additional hard copies of this document and general queries, please contact CESG using the following details.

CESG Enquiries
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

enquiries@cesg.gsi.gov.uk
Tel: 01242-709141

CESG welcomes feedback and encourages readers to inform CESG of their experiences, good or bad, in the document please email enquiries@cesg.gsi.gov.uk

Contents:

Chapter 1 - Outline Description

1. DISK Protect comprises software that encrypts all data on a device's hard drive (including operating system files), such that it will only be accessible after successful authentication using a username, passphrase and physical USB token. The entire hard disk data remains protected when the device is hibernated.

2. The software is installed using a CPA product license key that automatically selects the appropriate CPA-compliant configuration. During this process, the software generates all key material required for the operation of the software.

3. Following installation, the Administrator sets configuration options for the DISK Protect software (such as specifying allowable passphrase formats) before creating one or more accounts for the end users, including preparation of a physical USB token for each user account.

4. Note: The following features of DISK Protect have not been evaluated and are beyond the scope of this document:

   - Removable Disk Encryption
   - Device Decommissioning
   - Single Sign-On
   - Enterprise Management

Certification

5. DISK Protect v7.3.3 has undergone CPA assessment and has been certified as meeting the Augmented Grade requirements as described in the Software Full Disk Encryption SC v1.22 (reference [a]). Later versions are automatically covered by this certification until the certificate expires or is revoked, as stated on the product's certificate and on the CPA website.

Components

6. DISK Protect comprises the following components:

Component	Classification Level	Comments
Installation CD	OFFICIAL	
Physical USB Tokens	OFFICIAL	Locally accountable once programmed

Table 1 – Components of DISK Protect

Chapter 2 - Security Functionality

Full Disk Encryption

7. DISK Protect encrypts a device's hard disk(s). Following successful pre-boot authentication, data is automatically encrypted when written to disk and decrypted when read from disk 'on-the-fly'. No further user interaction is required.

Pre-boot Authentication

8. DISK Protect authenticates the user at pre-boot using a username, passphrase and physical USB token. If verified, the device continues to boot into the Windows operating system, otherwise the prompt is repeated.

Multiple User Support

9. DISK Protect supports one or more DISK Protect Administrators and multiple user accounts per protected device. Each user has a unique passphrase and physical USB token. The Administrator manages users and cryptographic keys using a provided tool.

Device Recovery (challenge/response)

10. Data exchanged during the device recovery process has an equivalent protective marking to the maximum protective marking of the data held on the device.

11. CESG does not recommend the use of the device recovery feature. Instead an Administrator should log into an administrator account on a protected device and reset the passphrase for the affected user account, using the DISK Protect management tool.

Chapter 3 - Secure Operation

12. The following recommendations outline a configuration for DISK Protect that is in line with the Security Characteristic for Software Full Disk Encryption. These recommendations should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Risk Management Advisor.

Pre-installation

13. Before installing DISK Protect CESG recommend that you take the following actions:

- The BIOS (legacy and UEFI) configuration menu on the device should be configured so that the protected hard disk is the only permitted boot device for an end user. It is strongly recommended that 'value-add' UEFI functionality, such as fast-boot environments and pre-boot networking, is disabled
- Disable external ports which allow DMA including IEEE 1394 (Firewire), PCMCIA and Thunderbolt
- Set a BIOS passphrase (i.e. separate to any DISK Protect passphrase) to prevent changes to the BIOS configuration. It is acceptable to re-use a single password across an estate of devices, but different passwords should be used on systems accredited for different security domains
- Enable ASLR (Address Space Layout Randomisation) support, if not enabled by default
- Install an up-to-date antivirus product on the protected device
- Consider the use of tamper-evident seals to make entry to system internals detectable by physical inspection

14. Further good practice advice for securing and managing devices can be found within existing CESG guidance, such as CESG Architectural Pattern No. 11, Mobile Remote Endpoint Devices at RESTRICTED (reference]b[(and CESG IA Notice 2011/06 UEFI BIOS Security Considerations.

Installation

15. An installation guide is provided with DISK Protect, which should be followed. Ensure the latest version of DISK Protect is used and a CPA product license key is entered when prompted. This will automatically configure the majority of options in accordance with the requirements of the Security Characteristic.

16. Cloning encrypted disks will duplicate the DEK, so a single DEK compromise will allow access to multiple devices. If disks are to be cloned as part of the build process, they must be re-keyed individually. Alternatively a cloning tool

which is specifically designed for use with the Disk Encryption product which prevents DEK re-use may be used.

Tokens

17. DISK Protect supports a range of USB tokens, each requiring a driver to allow the token to communicate with the operating system. Some drivers may come pre-installed with the operating system while others require separate installation.

18. These drivers have not been evaluated and may introduce vulnerabilities which are not appropriately mitigated in a manner required by an Augmented Grade product. You should conduct your own assessment of the drivers if necessary.

Configuration

19. The DISK Protect Management Tool must be configured such that no user (other than the Administrator) has the 'DISK Protect Administrator' privilege.

20. Passphrase complexity requirements must be set to specify at least 8 characters, including a mixture of upper and lower case, numbers and/or special characters. This requirement must also be implemented by the Administrator when setting a user's initial passphrase, either for the first time or when resetting a forgotten passphrase.

21. Each new user account must be configured with the 'force password change' option set, so as to prompt the user to change their DISK Protect passphrase on first use. The option must similarly be set if the Administrator resets a user passphrase that has been forgotten.

Operation

22. It is strongly recommended that a protected device is allowed to completely encrypt a hard drive before it is issued to users. This ensures no sensitive data can be written to the disk prior to encryption.

23. Users must receive a protected device along with their physical USB token and passphrase by secure means (i.e. such that they cannot be intercepted by another party). Users must change their DISK Protect passphrase following first use, or after an Administrator-instigated passphrase reset for the user.

24. A protected device must not be left unattended when it is powered up or in 'sleep' mode in a non-secured location. If it needs to be left unattended in such situations then it must be powered off beforehand (i.e. shut down or hibernated).

Maintenance and Updates

25. Security updates for DISK Protect must be applied promptly.

26. The antivirus product installed on a protected device must have its virus definitions kept up-to-date.

27. Reviews of a protected device's operating system logs must note any unexpected entries relating to Becrypt audit events. Tamper-evident seals should also be checked if in use.

User Education

28. Users of DISK Protect should be trained in its use and given specific Security Operating Procedures (SyOps). Advice should also include looking for damage to tamper-evident seals if these are in use.

29. CESG recommend that emphasis be placed on the importance of storing the token separately from the protected device; however training should also cover social engineering methods used by attackers and the risks of using protectively marked devices in public or untrusted areas.

30. Users should be reminded that unless the device is powered off or hibernated data is **not** protected.

Disposal and Destruction

31. The destruction, disposal or reuse of a protected device should comply with your decommissioning policies.**Error! Reference source not found.**Although DISK Protect provides a decommission facility this functionality has **not** been evaluated.

Chapter 4 - Security Incidents

32. If evidence of actual or suspected compromise is found, the equipment protected by DISK Protect should be withdrawn from use while the incident is investigated. If the investigation determines that equipment may have been compromised, isolate it from any network, quarantine to preserve potential evidence, and take the appropriate action as outlined in the following Table.

Component	Classification Level	Action if lost or compromised
Installation CD	OFFICIAL	Request a new CD from supplier.
Physical USB Token	OFFICIAL	Provided the protected device and passphrase are still secure, program a new token and issue it to the user with a new initial passphrase.
User Passphrase	Maximum protective marking of the data on the device.	Provided the physical USB token and device are still secure, the user only needs to change his/her passphrase, albeit as soon as is possible.
Device protected with DISK Protect	Powered-down state: OFFICIAL Powered-on and sleep states: maximum protective marking of the data on the device.	Take an audit of all data that was known to be held on the device to determine the true impact of the loss/compromise.

Table 2 - Actions to be taken after actual or suspected Comsec incidents

33. In the event of a security incident that results in the compromise of information protected by DISK Protect, the local IT security incident management policy should ensure that the Department Security Officer (DSO) is informed.

34. Contact CESG if a compromise occurred that is suspected to have resulted from a failure of DISK Protect.

References

Unless stated otherwise, these documents are available from the CESG website. Users who do not have access should contact CESG Enquiries to enquire about obtaining documents.

[a] CPA Security Characteristic - Software Full Disk Encryption latest issue available from the CESG website

[b] CESG Architectural Pattern No. 11, Mobile Remote Endpoint Devices at RESTRICTED – latest issue available from the CESG website.

CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk