#becrypt

Data Protection

Disk Protect : CPA

A Commercial Product Assurance (CPA) approved full disk encryption solution for desktops, laptops, tablets and servers to protect OFFICIAL data from theft and loss.

Disk Protect CPA secures organisations' protectively marked data (up to OFFICIAL), whether on desktops, laptops or tablets, with full central management and simple deployment.

Disk Protect CPA ensures that all OFFICIAL data is safely encrypted, with no change to performance or operation. Disk Protect CPA can be used without requiring key material from NCSC during any phase of the setup or installation.

What is CPA?

HM Government's Commercial Product Assurance (CPA) scheme evaluates commercial off-the-shelf security, enforcing products and their developers to be certified against published security and development standards. Becrypt's Disk Protect CPA is the first full disk encryption solution to gain this approval - making it suitable for the majority of data held by local authorities, blue light services, NHS and central government, while avoiding the complexity of managing NCSC key material.

How it Works

Disk Protect CPA works by encrypting every section of the hard drive, preventing unauthorised access to anyone accessing the files without permission. Disk Protect CPA provides strong authentication to load the operating system and access user files, allowing users to protect their existing and new data without any operational impact.

The product can be installed at any time, and will encrypt data while the user works. Once installed, all read/write requests are decrypted/encrypted invisibly, without user interaction, allowing users to continue to use the system as normal.

Full Management

Management capabilities allow recovery data and audit logs to be recorded centrally, while the deployment can take place with no user interaction required, preventing any down time.

Specifications

- CPA accredited
- Touchscreen support
- Removable media encryption
- Pre-boot authentication
- Multi user support at pre-boot
- Secure hibernation
- Single sign-on
- Central key escrow

National Cyber Security Centre
a part of GCHQ

CERTIFIED CPA & FIPS 140-2 & ASSURED

Official supplier to:

HM Government

For more information on Becrypt and our solutions, contact us:

info@becrypt.com

0845 838 2080

#becrypt.com

#becrypt

Data Protection

Disk Protect : CPA

Specifications

Supported Hardware

> Laptops
> Desktops
> Tablets
> Servers

Supported Disk Format Types

> MBR
> GPT (fixed disk only)

Boot Methods

> MBR
> UEFI

Types of Hard Disk Supported

> HDD (spinning)
> SSD
> RAID

Operating Systems

Desktop;
> Microsoft Windows 10
> Microsoft Windows 8.1
> Microsoft Windows 7

Server;
> Windows Server 2012 R2
> Windows Server 2008 R2

Encryption Algorithm

> AES 128 bit

Data Level Protected

> CPA

Accreditation

> CPA
> EUCI
> NATO

Existing Data

Initial encryption of the hard drive(s) does not delete existing data, but it is recommended that existing data is backed up prior to installation, and you may prefer to perform a full system backup.

User Authentication

Authentication is by username, strong password and mandatory token.

When used in the context of an Active Directory domain, Disk Protect CPA supports single sign-on.

Supported Tokens

> RSA SecureID 800
> Safenet 5100
> Safenet 5105
> Aladdin eToken
> Standard USB devices
> TPM

Multiple Users

Disk Protect CPA support up to 20 pre-boot users.

Device Recovery

The Disk Protect computer provides a dynamically-generated challenge code, which is used by a Service Desk operator to generate a response code that the user enters into the computer to gain temporary access and set a new password.

Self Registration

Self registration permits an Active Directory user to register themselves and token on a pre-encrypted Disk Protect CPA device.