becrypt
DATA SECURITY

CAPS
CESG Assisted Products Service

DISK Protect™ Baseline

Complete full-disk encryption solution for laptop and desktop computers

DISK Protect Baseline is CAPS approved to handle protectively marked data to Baseline

DISK Protect Baseline is an approved solution for protecting data on computers and removable media by encryption, and for enforcing a centrally-defined security policy.

Full disk encryption

DISK Protect transparently encrypts a computer's hard disk(s) using an encryption key supplied by CESG. Once encrypted, data is automatically decrypted and re-encrypted on the fly (as and when required). Encryption overhead is minimal with no noticeable impact on performance.

Strong, flexible authentication

DISK Protect provides strong authentication, using LOGFIRE for hashing and for optional password generation, with the flexibility of a configurable password policy for length and complexity. Smart cards or USB tokens may optionally be used for secondary authentication.

Authenticating the user pre-boot allows DISK Protect to encrypt the entire Operating System and ensure that data cannot be accessed using low level tools. If anyone attempts to bypass Authentication, the data remains encrypted and unintelligible.

Removable media encryption

For safe transportation, DISK Protect secures data on USB-connected storage devices and floppy disks by encryption. Data may be encrypted using a shared key to allow the transfer of data between authorised users. DISK Protect may also be configured to allow the use of unencrypted media.

Easy installation

DISK Protect may be installed and configured on individual client computers or installed on multiple client computers via an Installation Package. Approved key distribution mechanisms, used for large-scale deployments, significantly reduce cost of ownership. DISK Protect is compatible with common management systems, and supports standards-based environments.

Transparency

Once the user has logged in to Windows, DISK Protect operates transparently and the standard applications can be used as normal. Since all data is automatically encrypted, there is no risk that the user will forget to encrypt sensitive files.

System management

An easy-to-use Management Tool simplifies the management of deployed systems, allowing the administrator to update policy and maintain user accounts

Device recovery

If the user forgets his or her password (or loses his or her token or smart card), the protected computer may be accessed with help from an administrator. At no time during the device recovery process is the user's password exposed.

Note that all communication must take place over a crypto-channel or in a crypto-environment.

Please see S(E)N 05/06 for guidance on the use of the Device Recovery features.

As an alternative to Device Recovery, if the administrator can physically access the locked computer, he or she may unlock the machine using his or her own DISK Protect credentials and reset the user's password.

CAPS - approved to BASELINE

Token support

DISK Protect supports **Aladdin R2e** and **eToken PRO** USB tokens, and **RSA 5100, 5200, 6100** and **SID800** smart cards to provide dual-factor authentication. Extended smart card support gives an organisation the option of using a card that is already part of its security systems, issuing its staff with a single Smart Card for all access control and authentication purposes.

DISK Protect™

PC security solution combining full disk encryption with strong boot time authentication and optional removable media encryption.
DISK Protect 4.1 has been awarded the CCT Mark;
DISK Protect Baseline is CAPS approved to Baseline;
DISK Protect Enhanced is CAPS approved to Enhanced grade.

Removable Media Module

Encryption of data on removable storage devices such as USB Flash Drives, memory devices and SD Cards.

PDA Protect™

PDA security solution that enforces strong authentication, secured synchronisation and the encryption of removable memory cards.
PDA Protect 4.1 has been awarded the CCT Mark.

Connect Protect™

Port Controller for desktop and laptop PCs managing access to Plug and Play devices.
Connect Protect 2.0 has been awarded the CCT Mark.

Trusted Client™

Secure, isolated, configurable operating system for use in an unmanaged environment providing functionality customised to an organisation's requirements.
Trusted Client 1.2 has been awarded the CCT Mark.

BeCrypt Enterprise

Centralised, scalable security management suite based on Open Standards.
Provides comprehensive assurance for end-point and infrastructure, with low cost of ownership.

BeCrypt Limited, Wyvols Court, Swallowfield, Reading, Berkshire RG7 1WY UK
Tel: 0845 838 2050 • **Fax:** 0845 838 2060 • **Email:** sales@becrypt.com • **www.becrypt.com**
Outside UK Tel: +44 (0)1189 880 277 • **Fax:** +44 (0)1189 880 377