

DISK Protect™ Baseline

DISK Protect is a full-disk encryption solution for laptop and desktop computers running Windows operating systems.

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

Full disk encryption

When first installed, DISK Protect transparently encrypts a computer's hard disk(s) using an Encryption Key supplied by CESG. From then on, data is automatically decrypted and re-encrypted on the fly (as and when required). If anyone attempts to bypass Authentication, the data is encrypted and unintelligible.

Pre-boot authentication

DISK Protect can be configured to authenticate by password or by password and token. In either case, an embedded password generator provides the level of security required. Authenticating the user pre-boot allows DISK Protect to encrypt the Operating System and ensure that data cannot be accessed using low level tools.

Removable media encryption

Removable media encryption secures data on USB-connected storage devices and floppy disks. Data may be encrypted using a shared Encryption Key or a personal Encryption Key. DISK Protect can be configured to allow the use of both encrypted and unencrypted removable media.

Previously only available as part of a DISK Protect installation, the BeCrypt Removable Media Module can now be purchased as a

standalone product, and encrypts all data on mass storage devices.

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.

Low performance overhead

Encryption overhead is minimal with no noticeable impact on performance.

Multiple users

DISK Protect Baseline supports one or more DISK Protect Administrator accounts and multiple user accounts per protected machine. The hard disk is encrypted using a single Encryption Key but each user has a unique password or password and token.

System management

The DISK Protect Management Tool permits a DISK Protect Administrator to add or remove users, create additional administrators, reset users' passwords, and enable/disable removable media encryption. The Management Tool permits ordinary users to manage their own removable media Keys.

Device recovery

Device recovery permits a user, with the aid of an administrator, to regain access to a locked computer. If the user fails three attempts to enter the correct password or password and token, DISK Protect denies access and displays a challenge code. The user must contact an Administrator (over a crypto-channel or in a crypto-environment), provide the code, and will receive a response code, which must be entered into the computer to regain access.

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

Once the user has logged in to Windows, he or she is required to generate a new password. At no time in this procedure is the user's original password exposed. Note that, if required, the Device Recovery feature must be enabled during installation.

As an alternative to Device Recovery, if the Administrator can physically access the locked computer, he or she may restart the machine, enter his or her own DISK Protect Username and password (and token, if appropriate), log in to Windows, and use the DISK Protect Management Tool to reset the user's password.



Easy installation

DISK Protect may be installed and configured on individual client computers or installed on multiple client computers via an Installation Package.

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 CSIA Claims Tested 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 CSIA Claims Tested Mark; **PDA Protect Baseline** is CAPS-approved to Baseline.

Connect Protect™

Port Controller for desktop and laptop PCs manages 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.

Protect Manager™

Centralised security management and auditing functionality for the enterprise.

© Copyright 2008
by BeCrypt Ltd.

All Rights Reserved.

The BeCrypt Logo and Trademarks
are owned by BeCrypt Ltd.

No material may be reproduced for any
purpose, private or commercial,
without prior written
permission from
BeCrypt Ltd.