

PDA Protect™ 4.1

Security solution for Personal Digital Assistants

PDA Protect 4.1 has been awarded the CCT Mark

PDA Protect is a security solution for mobile devices. It protects data on PDAs by encryption, enforcing a centrally-defined security policy to control the use of high-risk features, prevent data leakage, and support compliance initiatives.

Feature summary

- Allows the administrator to build custom security policies
- Transparently encrypts all data on removable SD and Compact Flash memory cards
- Enforces Secured Synchronisation by restricting connection to authorised users or workstations only
- Logs connection events and selected file transfer events
- May be configured to restrict the use of high risk features, such as Bluetooth and WiFi
- Compatible with handheld devices running Microsoft Windows Mobile 5.0 and Windows Mobile 5.0 with AKU2

Strong authentication

Where required, PDA Protect authenticates the user by password every time the PDA is switched on. Passwords may be chosen by the user (in compliance with the password policy set by the administrator during installation) or generated using an embedded password generator that employs an approved algorithm to generate strong passwords.

The Device Recovery feature allows an authorised user (with the aid of an administrator) to unlock the PDA if he or she has forgotten the password.

Data protection

PDA Protect secures the data on removable Secure Digital and Compact Flash memory cards by encryption. If an encrypted memory card is inserted into another device, the data is inaccessible.

PDA Protect safeguards data in memory by optionally performing a 'secure wipe' following repeated password failure, or if the PDA is switched on after having been

left unused for a certain number of days—both circumstances that may indicate that the device has been lost or stolen. (Secure wipe is not supported by Windows Mobile 5.0).

Secured synchronisation

PDA Protect prevents the unauthorised transfer of data by controlling synchronisation, blocking connection by unauthorised users or to unapproved machines.

Feature control

PDA Protect may be configured to disable high-risk features such as connection to other devices via Bluetooth or WiFi.

Installation options

PDA Protect may be installed on individual PDAs, rolled out to multiple PDAs via a pre-configured Installation Package, or directly installed on the PDA (typically by the user) from a CAB file.

Windows Mobile 5.0 support

PDA Protect safeguards sensitive data used for messaging and related business applications.



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.

© 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.