

# Security solutions for Central Government

With Central Government departments under pressure to provide more flexible working arrangements for staff, the threat to sensitive data has never been greater.

In the drive for efficiency it is becoming more important to provide workers with access to data from remote locations, either from home, out in the field or while travelling from meeting to meeting. Protecting data from loss, whether accidental or malicious, is now a key issue for Central Government departments.

A UK based company, BeCrypt provides a range of market leading encryption and data protection products and services that can

be tailored to meet the individual requirements of any central government department.

Having worked with Central Government and the Ministry of Defence on many security development projects, BeCrypt is uniquely placed to provide Information Assurance products and services. BeCrypt is able to supply CESS certified products for areas where a high degree of data security is required, and products that carry the CCT

Mark for situations where a more flexible product is appropriate.

BeCrypt's encryption and security products are quick and easy to set up and deploy and enable Her Majesty's Government departments to allow employees the flexibility of working from any location, while still protecting data.



## DISK PROTECT™

**DISK Protect is a full disk encryption solution** (with optional removable media encryption) for laptop and desktop computers.

### **DISK Protect provides:**

**Full disk encryption** - it transparently encrypts a computer's hard disk(s), automatically encrypting and decrypting data on the fly so that applications can be used as normal. If an unauthorised user attempts to access the hard drive directly, without going through the User Authentication process, the data remains encrypted and unusable. If the hard drive is later disposed of, any data it contains is unintelligible, even if specialist data recovery tools are used.

### **Boot-time authentication** -

it can be configured to call for a strong password or a token and a PIN. Authenticating the user at boot-time means that the operating system may be encrypted to prevent unauthorised data access using low-level tools. DISK Protect is compatible with most of the widely used tokens and smart cards.

### **Removable media encryption** -

enables mass storage devices, such as USB memory sticks and floppy disks to protect data in transit.

The latest version of DISK Protect supports up to 26 password protected accounts or an unlimited number of token and PIN protected

user accounts per machine, and each user may have DISK Protect accounts on several machines. DISK Protect v4.1 has been awarded the CSIA Claims Tested Mark.

### **DISK Protect Baseline**

DISK Protect Baseline is CESS approved to Baseline and reduces the protective marking of Restricted data by one level or, when used to enforce dual-factor authentication, reduces the protective marking of Confidential data by one level.

### **DISK Protect Enhanced**

DISK Protect Enhanced is CESS approved to Enhanced Grade and reduces the protective marking of Confidential data by two levels.



## PDA PROTECT™

**PDA Protect is the most comprehensive security and encryption product available** for Personal Digital Assistants (PDAs). PDA Protect is a software solution that protects a PDA by encrypting its removable memory, enforcing strong user authentication, restricting data connection and data transfer and optionally preventing the use of high-risk features.

The latest version of PDA Protect provides support for Microsoft® Windows™ Mobile 5 operating system. This includes compatibility with the new Windows messaging pack that supports Direct Push email. PDA Protect v4.1 has been awarded the CSIA Claims Tested Mark.

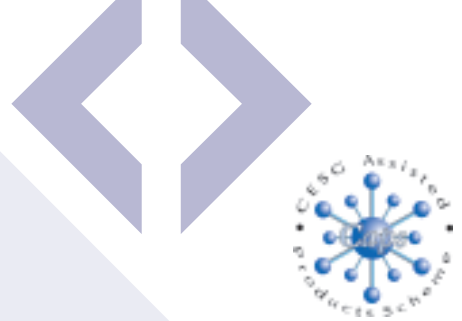
## PROTECT MANAGER™

**Protect Manager is a central management resource** for BeCrypt products designed to simplify the administration of large installations. Protect Manager 2.0 automatically

uploads the recovery data generated during client installation and stores the Encryption Key and the recovery file in a central, secured database; provides a distributed Device Recovery Help Desk with secured access to the Protect Manager database; and provides a comprehensive system management audit trail.

## CONNECT PROTECT™

**Connect Protect is a port control (end-point security) solution**, designed to secure desktop or laptop computers from the introduction of unauthorised material, and from accidental or malicious data leakage, via devices such as removable disk drives, MP3 players, and printers. Connect Protect is remotely installed using standard tools and configured via Active Directory and includes full audit trail facilities. Connect Protect 2.0 has been awarded the CSIA Claims Tested Mark.



## Removable Media Module™

Previously only available as part of DISK Protect or DISK Protect Baseline, the BeCrypt Removable Media Module is now available as a standalone product, and the Baseline version is the first CESG approved solution to encrypt all content on portable devices such as USB Flash Drives and Memory Sticks.

The Removable Media module is a cost-effective way to protect content when the threat is not to the computer itself but to data in transit.



## Commission for Social Care Inspection (CSCI)

Launched in April 2004, the Commission for Social Care Inspection (CSCI) is the single, independent inspectorate for all social care services in England. It was created by the Health and Social Care Act 2003.

As part of the remit to provide a complete picture of social care in England, CSCI is upgrading its core applications and rolling them out to mobile staff. CSCI is part of the Government Secure Intranet (GSI) community which requires that all mobile devices connecting to the network must be encrypted. CSCI selected Fujitsu to deliver the broadband project and BeCrypt was chosen to provide encryption solutions.

Over 1280 people now use BeCrypt DISK Protect across the nine regions and satellite offices. DISK Protect was installed on all laptops and a secure broadband line arranged for each member of staff to be able to connect to the GSI network from home.

Mobile staff are now able to log on to the network securely and gain access to files from the shared areas. Files do not need to be stored locally and so less sensitive data is now held on laptops. Furthermore with DISK Protect software, should the laptop be lost or stolen, the data that is held on the computer is completely inaccessible and unintelligible.