

GCSx Data Handling and Secure Access

How BeCrypt can help Local Authorities meet the requirements



BACKGROUND

The new Government Connect Secure Extranet (GCSx), is scheduled to go live by 31 March 2009. To connect to GCSx Local Authorities need to conform to the GCSx and Code of Connection guidelines.

This guide describes three main areas where BeCrypt can help, highlighting the relevant guidance and detailing how BeCrypt provides a solution.

BeCrypt has a strong track record in local Government, numerous local authorities rely on BeCrypt to protect sensitive data and reduce the risks of data loss. Our DISK Protect product is CESG CAPS approved for handling Restricted data and above.

MOBILE DATA SECURITY

BeCrypt can help with the guidance for remote access in two ways. Firstly by offering approved encryption for mobile devices namely laptops and PDA devices.

Secondly through BeCrypt Trusted Client, a low cost secure remote access tool which is CCT Mark approved, allowing access from unmanaged PCs such as a users home PC.

SECURING MOBILE DATA

The guidance on securing remote access to IT systems is detailed in CESG Memo 35. For Impact Level 2 (IL2) a cryptography product preferably evaluated to FIPS 140-2 standard and meeting the CCTM requirements should be used to protect data on a client device.

BeCrypt DISK Protect meets the standards for FIPS 140-2. For Impact Level 3 (IL3) i.e. Restricted data, a cryptography product evaluated to FIPS 140-2 standard and CCTM requirements should be used. Also additional controls need to be in place such as an evaluated firewall.

BeCrypt DISK Protect Baseline meets the standards for FIPS 140-2, meets CCTM requirements and is CAPS approved. BeCrypt DISK Protect secures data on laptop and desktop computers by enforcing strong User Authentication and by encrypting all data on the hard disk(s) and secures data on removable media, such as USB memory devices, by removable media encryption.

SECURING REMOTE ACCESS

Again the guidance is detailed in Memo 35. There are two areas relating to network access to highlight. When connecting to a server or network as a whole, it is recommended that the server should only allow access from approved and 'suitably authenticated clients'.

Memo 35 also makes the recommendation that remote access clients be officially owned, if personal devices are to be used to connect additional security controls are needed to mitigate against the increased risk.

BeCrypt Trusted Client is a CCTM and FIPS approved, low cost secure access device. Trusted Client transforms an unmanaged internet enabled PC into a trusted secure access point. By simply inserting a low cost Trusted Client USB stick a totally isolated environment is created, all data is encrypted, no trace of Trusted Client is left on the host machine.

HANDLING RESTRICTED DATA

The guidance for electronic storage of data marked Restricted is very clear and is laid out in the GCSx Operational Support Guide:

Electronic Storage

Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms:

- a. User challenge and authentication (username/password or digital ID/Certificate)
- b. Logging use at level of individual
- c. Firewalls and intrusion-detection systems and procedures; server authentication
- d. OS-specific/application-specific security measures.

BeCrypt DISK Protect Baseline is a CAPS approved disk encryption solution. It transparently encrypts a computer's hard disk(s) using an encryption key supplied by CESH.

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.

DEALING WITH PHYSICAL MEDIA IN TRANSIT

Again the guidance is very clear and is outlined in GCSx Operational Support Guidance. It states: HR, the ITSM and the IT Department should ensure that media containing information marked PROTECT and RESTRICTED is protected against unauthorised access, misuse or corruption during transportation beyond the Customer premises in accordance with MPS.

Recent data loss incidents have reinforced the need to protect data if it physically moves outside the organisational boundary. BeCrypt Media Client secures data while on the move.

BeCrypt Media Client is a file-level encryption software solution that protects data in transit (on CDs, DVDs, or USB devices) by encryption and strong passphrase protection. Designed to be easy to use, users simply select files or folders to be encrypted, they then write the data to the chosen media with an assigned passphrase.

The recipient of the protected media, for instance a CD, does not have to have BeCrypt software installed on their PC. Media Client has an extractor application which allows the recipient of the protected CD to recover and open the encrypted data.

ABOUT BECRYPT

BeCrypt provides a suite of market leading encryption and data protection products and services that can be configured to meet the individual requirements of each local authority.

Having worked with the UK Government and the Ministry of Defence on many security development projects, BeCrypt is uniquely placed to provide local authorities with Information Assurance products and services. BeCrypt is able to supply CAPS certified products for areas where a high degree of data security is required, and products that carry the CCT Mark and FIPS 140-2 validation for situations where a more flexible product is appropriate. The CSIA Claims Tested (CCT) Mark scheme helps Local Authorities implement secure mobile working strategies

Our suite of Products includes:

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 remote access device 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 Media Client™

A 'zero footprint' software security solution that protects data in transit on CDs, DVDs and USB devices. It uses encryption and strong passphrases protection and adds file level encryption to BeCrypt's product portfolio.

BeCrypt Enterprise Manager™

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

For more information and to talk further about the issues highlighted please contact us on 0845 838 2050 or visit www.becrypt.com