Good practice in information handling: Data encryption

For staff and contractors tasked with implementing data security

This document is one of a series of good practice guides to help schools, colleges and universities protect personal and sensitive data. Building on good practice from industry and central government these guides describe procedures and possible technical and operational solutions that can help organisations reduce the risks of data security incidents and comply with current legislation.

Produced by Becta on behalf of the Department for Children, Schools and Families, these guides have been reviewed and updated with feedback from a number of cross-sector organisations including DCSF, DIUS, JISC Legal, The Information Authority and JANET(UK), as well as from schools, local authorities, RBCs and suppliers.

For further information on these guides, please see http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity.

Contents

Key points

Educational organisations should use data encryption to help maintain the security of the personal data they hold on learners, staff and others.

In most cases, electronic transmission and storage of data is more secure than paper-based systems.

Encryption does not work in isolation from the other good practice in data handling.

This guide is intended for those staff or contractors in educational organisations who are tasked with putting in place a system of encryption and secure deletion of data. It contains:

- information on when encryption is required
- information on the types of encryption software available and their advantages and disadvantages
- information on common examples of encryption software
- methods of encryption for data in transit
- detailed information on data handling policies
- guidance on taking encrypted data overseas.

1 What should organisations do?

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends[1] that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Data Handling Procedures in Government [http://is.gd/lUbc], published by the Cabinet Office, also sets out the measures that government organisations should adopt to protect personal and sensitive data:

- when sensitive or personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if

[1] See the ICO website [http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx].

the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

- Organisations or users must securely delete sensitive personal data or personal data when it is no longer required[2].

Government recommendations are that the Government Protective Marking Scheme should be used to indicate the sensitivity of data. The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most sensitive or personal data that is used within educational institutions will come under the PROTECT classification. More information about the Government Protective Marking Scheme can be found in *HMG Security Policy Framework* [http://www.cabinetoffice.gov.uk/spf/sp2_pmac.aspx#18].

Specific rules apply to how data within each classification should be secured. Data that is classified as PROTECT should be encrypted if removed or accessed from outside any approved secure space or transferred between secure spaces. Examples of approved secure spaces include physically secure areas in schools, colleges, universities, local authorities and the premises of support contractors.

Note that access to sensitive data must also be controlled according to the role of the user, with access granted on a need-to-know basis. For example, not every member of staff should need access to the whole management information system.

2 Encrypting devices and media

2.1 What needs to be encrypted?

The Government's and the ICO's guidelines are that encryption should be applied to personal data that is held on hard drives, portable media (such as DVDs, CDs and USB drives), back-up tapes, computer networks (such as storage area networks) and off-site back-up services.

The encryption solutions you choose will depend on your organisation, your users, the ICT infrastructure, staffing and technical capability, and the applications that you use, but it should be noted that encryption does not work in isolation from the other good practice in data handling. Installing and configuring encryption software on every member of staff's laptop, as well as putting in place new authentication tokens and any additional technology (if applicable), is not just time-consuming, it also requires a change of culture for all users.

Note that if your organisation does not have encryption now, we strongly recommend that you stop all copying, removing or accessing PROTECTED data

[2] Retention times will differ depending on the specific data, the organisation's own policies and, where appropriate, statutory requirements. The Records Management Society provides some guidance for schools and local authorities on retention periods [http://www.rms-gb.org.uk/resources].

until you have software to encrypt files and protect the communication links accessing this data.

3 An overview of encryption solutions

A number of encryption solutions are available, some of which may be certified as CAPS (CESG Assisted Products Service) – CESG stands for Communications-Electronics Security Group, the Government's national technical authority for information assurance, CCTM (CESG Claims Tested Mark) approved, FIPS (Federal Information Processing Standards) 140-2 compliant or have no formal certification.

Certified products have been independently evaluated to verify that they operate correctly and are robust. Ideally, organisations should use certified products where possible. The certification process, however, is expensive and time-consuming, so certified solutions tend to be more expensive and respond more slowly to changes to operating systems or applications. Non-certified solutions can also provide effective data security. We suggest that organisations ask for further advice from their supplier or technical support service (if available).

3.1 Full disk encryption and file/folder encryption

Organisations and individuals can encrypt personal data on a device – for example, a laptop – using either full disk encryption (also known as whole disk encryption) or file/folder encryption (also known as file system level encryption).

In full disk encryption, almost all of the contents of a laptop's hard drive are encrypted. Usually only the Master Boot Record remains unencrypted, and this does not contain personal data.

Full disk encryption has the big advantage of being user-friendly. Users can continue to use their laptop in much the same way as they did before it was encrypted. It also encrypts almost all of the data on the device, including temporary files.

However, full disk encryption has the disadvantage that it only secures data while it stays on the laptop. If a user copies it to an unencrypted portable USB drive or removable media, it is decrypted and is no longer secure. It is also decrypted if a user sends the data as an attachment in an email. File/folder encryption overcomes this by encrypting the files and/or folders individually, so that they stay secure throughout their life. Data stays secure even if a user copies it to a portable USB drive or other removable media, or sends it to someone as an attachment in an email.

File/folder encryption must be set up with great care. Personal data is sometimes contained in the temporary files created by operating systems and applications. File/folder encryption solutions must be set up to encrypt these files. As users mostly do not know that these files exist, they will need help to do this.

Furthermore, file/folder encryption does not always encrypt the metadata associated with a file (metadata includes the attributes of a file such as its name, size, type and so on).

You should also note that if a laptop is put to sleep or hibernated, rather than being shut down, data may not be properly secured.

Full disk encryption and file/folder encryption slow down laptop performance by up to 10 per cent. Full disk encryption provides faster individual file/folder access compared to file/folder encryption, but it increases start-up times for booting and applications.

In many cases, organisations should use a combination of full disk encryption and file/folder encryption to achieve a balanced, secure solution.

With both options, it is critical to test operating system patches and application updates for compatibility with encryption solutions before implementing them.

Finally, there is the issue of equipment disposal. Provided strong authentication credentials are used, full disk encryption may reduce the need to securely delete data on media before disposal. Anyone accessing the media will find, what looks like, random data. With file/folder encryption, it is necessary to securely delete all the data held on media before disposal to make sure the data cannot be recovered (including account details, history/log information and temporary files).

3.2 Enterprise solutions compared with stand-alone solutions

Whichever technology is deployed, organisations need to be sure that:

- the technology has been thoroughly tested on the platform(s) they use
- the technology will be relatively future-proof
- there is someone to call when something goes wrong.

While it is possible to conform to current privacy legislation using the stand-alone solutions explained later in this document, there are significant issues that need to be understood before using them. Enterprise solutions, such as those supplied by Entrust, Microsoft, PGP and others, provide a manageable and reliable infrastructure that is designed to address these issues.

In terms of one-off costs, stand-alone solutions are usually free or low cost. However, the total cost of ownership for an enterprise solution may well be lower when other long-term costs (for example, manageability) are considered.

3.2.1 Recovering information after losing passwords, passphrases or tokens

Not all stand-alone encryption solutions provide reliable information recovery because encryption relies on a credential (password, passphrase or token) that belongs to an individual user. If the user forgets or loses the credential, it is not possible to recover the encrypted data. If organisations encrypt entire servers this way, the impact of losing a credential is high.

Organisations using stand-alone solutions must be careful to select solutions that offer methods for resetting passwords and managing keys, or have additional procedures in place to make sure they do not permanently lose credentials.

Enterprise solutions get around this by creating keys that can be used to recover encrypted data. This needs to be a strictly managed and regulated process, usually involving more than one person; most enterprise identity management and provisioning systems provide the technology to achieve this ‘out of the box’.

3.2.2 Ease of use

Once set up, enterprise solutions tend to be user-friendly and come with comprehensive help, support and training material because they are aimed at a broad market. They do, however, require expert support to install and set up correctly.

Stand-alone solutions are usually easy to use once installed and set up correctly. However, users will need some training before using them and, like enterprise solutions, need expert help to install and set up the software correctly.

3.2.3 Non-repudiation

An enterprise solution provides the significant benefit of non-repudiation, which means that a user cannot deny they created a document or performed an action affecting it. This also provides an audit trail.

Digital signatures provide a robust way of confirming the identity of the creator of a document or piece of content or an individual user who has performed an action on a system. This means organisations can guarantee that a document was created or a transaction was started by a particular user and that it has not been altered in any way since.

3.3 Using enterprise solutions

The ideal enterprise solution for organisations will provide:

- full disk encryption for all laptops and file/folder encryption (so that files retain their protection if they are moved, copied or emailed)
- key management and recovery capabilities

- the capability to address multiple platforms – Windows, Linux and Apple Mac – as well as mobile devices with the same product
- secure automatic file deletion
- ease of use, requiring little intervention or knowledge of the underlying technology by the average user
- compatibility with various two-factor authentication mechanisms
- certification to FIPS 140-2.

4 Encryption products

NB: Becta has not conducted formal evaluation of these products and, therefore, does not recommend any specific solution. The products listed here are to demonstrate some of the types of solutions currently in use within the education sector. Other suitable products are available that are not listed in this document.

4.1 Table showing examples of encryption products

Example products (in alphabetical order)	**Windows**	**Mac**	**Unix/Linux**	**Symbian**	**Windows Mobile**	**USB**	**Ad hoc file encryption**
BeCrypt DISK Protect	X					X	
BeCrypt PDA Protect					X	X	
BestCrypt			X				
Check Point	X	X	X			X	
CREDANT Mobile Guardian	X	X		X	X	X	X
DESlock+	X					X	X
Disk Utility		X					
Eclypt and Eclypt Freedom	X		X			X	X
Eclypt PICO Freedom						X	
Entrust Entelligence	X	X	X			X	X
FileVault		X					
IronKey						X	
Kanguru MicroDrive						X	
Kingston DataTraveler BlackBox						X	
Knox		X				X	
McAfee Endpoint Encryption				X			
MS BitLocker	X					X	
MS Windows EFS	X						
PGP Desktop Professional	X	X	X	X	X	X	X
Pointsec Mobile				X	X		
Redstor Protector	X					X	X
SanDisk Cruzer						X	
Stealth MXP						X	
TrueCrypt	X	X	X			X	
WinZip	X	X				X	X

The sections below provide manufacturers' descriptions of various encryption products and the functions they perform. There are also links to each manufacturer's website for extra information.

Some of the products discussed here are listed in the CESG's *Directory of Infosec Assured Products* [http://www.cesg.gov.uk/publications/media/directory.pdf]. Other products will meet the intent of *Data Handling Procedures in Government*, but may not yet have undergone the assurance testing required to become listed in the *Directory of Infosec Assured Products.*

We recommend that a technically competent person installs and sets up encryption products. You may lose important data permanently if you do not install or set up the software correctly.

4.2 BeCrypt DISK Protect

DISK Protect is listed in the CESG *Directory of Infosec Assured Products* and has been developed under the CAPS (CESG Assisted Products Service) scheme to provide security assurance coupled with reduced physical handling requirements for PCs containing Protectively Marked information.

DISK Protect provides full disk encryption for either fixed disk or removable media devices. Boot-time authentication is also provided. Optional token-based secondary authentication is supported using a range of smartcards and USB tokens. Following user authentication, encryption is transparent, and the user needs to take no further action. All data written to disk is automatically encrypted using the Advanced Encryption Standard (AES). Removable device support includes memory sticks, USB drives and Firewire drives.

[http://www.becrypt.com/uk/home/index.php]

4.3 BeCrypt PDA Protect

PDA Protect is listed in the CESG *Directory of Infosec Assured Products*. PDA Protect is a software security solution for Personal Digital Assistants (PDAs) running Pocket PC and Windows Mobile for Pocket PC (2000 and 2003) operating systems. PDA Protect allows the administrator to create a custom-built security policy, including:

- setting password lifetimes and the number of password attempts
- setting a synchronisation policy
- controlling the use of permanent (Flash) memory
- controlling the use of high-risk features, such as connection to other devices, audio facilities, Wi-Fi, cameras, Bluetooth and infra-red capabilities.

However, it should also be noted that:

- data is only encrypted on the CF or SD memory cards, and not encrypted in the PDA's memory
- all data written to the protected volume, the hibernation file, or a crash dump file, is encrypted using 128-bit AES.

[http://www.becrypt.com/uk/industry/education.php]

4.4 BestCrypt

BestCrypt creates and supports encrypted virtual volumes for Linux. A BestCrypt volume is accessible as a regular file system on a corresponding mount point. The data stored on a BestCrypt volume is stored in the container file. A container is a regular file, so it is possible to back up, move or copy it (to a CD-ROM or network, for instance) and continue to access encrypted data using BestCrypt.

The preferred BestCrypt algorithm to choose is AES 256-bit Rijndael.

[http://www.jetico.com/linux.htm]

4.5 Check Point

Check Point Endpoint Security Full Disk Encryption provides data security through strong encryption in multi-platform solutions that include handheld wireless devices and portable storage media. The product works on Windows, Mac and Linux-based computers and functions transparently to the user. It is capable of using smartcards and tokens, and includes either single sign-on or Windows Integrated Login. Check Point Full Disk Encryption is FIPS 140-2 certified and CESG approved.

[http://www.checkpoint.com/products/datasecurity/index.html]

4.6 CREDANT Mobile Guardian

The policy-based intelligent encryption technology of CREDANT Mobile Guardian (CMG) delivers full data encryption for laptops, desktops, handhelds and external media. Enterprises can now implement the thorough protection needed to secure their corporate data no matter where it is stored, yet have the flexibility and ease of use not found in older, first-generation encryption technologies, such as full disk and file/folder encryption.

With CREDANT Intelligent Encryption, a security administrator can easily establish and enforce policies governing the application of encryption on all mobile endpoints. Centrally defined policies can protect entire drives or be more granular to control certain file types for a particular user or group – whatever the environment dictates. Policy definition is simple yet powerful, and encryption is enforced transparently, without changing the way users or IT administrators interact with their systems. There are no special utilities, and all processes and procedures can continue unchanged after CMG has been deployed. CMG has FIPS140-2, Common Criteria EAL3 and CCTM accreditations.

[http://www.credant.com]

4.7 DESlock+

Data Encryption Systems (DES) has been providing customers with encryption technology designed for everyday PC users for 20 years. In partnership with RM Education, a customised version of DESlock+ has been developed for use within schools. Designed to secure data in the school office and on teacher laptops, the education version complies with guidelines and provides easy-to-use data encryption for local and removable storage and secure file deletion.

To make compliance with data handling regulations simpler, RM also provides telephone support, and remotely manages licensing, user rights, encryption keys and key recovery where passwords are forgotten. The product is currently CCTM approved and is also undergoing FIPS 140-2 approval with certification expected in late 2009.

[http://www.deslock.com/deslockp_products.php]

4.8 Eclypt

This product is in the CESG Directory of Infosec Assured Products. Eclypt is a hardware encryption solution and a direct replacement for a computer's standard hard drive. Eclypt provides full disk encryption that is transparent to the user after pre-boot authentication. All data is then automatically encrypted using AES 256-bit technology. As a hardware solution, Eclypt offers superior performance and security as it does not run on the PC processor and keys are not stored on the hard disk itself.

Eclypt Freedom is a hardware-encrypted portable hard drive, which is also in the CESG Directory of Infosec Assured Products. Available in capacities of 320GB or 500GB, it provides full disk encryption after authentication upon plug-in. All data is automatically encrypted using AES 256-bit technology.

Eclypt and Eclypt Freedom are available in several variants: Corporate (FIPS 140-2 validated), Baseline (IL3 – RESTRICTED) and Enhanced (IL6 – TOP SECRET).

[http://www.eclypt.com/products.aspx]

4.9 Entrust Entelligence

The Entrust Entelligence product portfolio is an integrated suite of security solutions that deliver a single security layer across multiple enterprise applications, enabling strong authentication, authorisation, digital signatures and encryption.

Entrust Entelligence helps empower employees to work efficiently, communicate effectively, improve corporate and regulatory compliance, and use products and services online.

[http://www.entrust.com/entelligence/index.htm]

4.10 FileVault and Disk Utility

Apple’s FileVault secure storage application, introduced in Mac OS X 10.3 in 2003, has been incrementally updated in both the 10.4 and 10.5 releases.

The FileVault application uses AES 128-bit encryption technology to secure the data located in a user’s Home folder, the default storage location for user data. Under normal conditions, FileVault will protect all data for typical users. If encryption of data located outside of the Home folder is required, the standard DiskUtility application can be used to create encrypted disk images.

Disk Utility also offers higher-grade AES encryption with 256-bit keys. However, it is not possible to encrypt the entire disk, as currently the system is unable to start up from an encrypted boot volume.

As with Knox below, Disk Utility can be used to decrypt and unpack the data set held within the file.

[http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1877.html]

4.11 Knox

Knox is a commercial application for data protection on the Mac. The software uses the native encryption technology built into Mac OS X. It allows the user to encrypt data sets and entire volumes using either AES 128-bit or 256-bit encryption.

Knox runs on both PowerPC and Intel-based Mac computers running Mac OS X 10.4.9 or above. However, 256-bit encryption is only available in the current release of Mac OS X 10.5.

A user-friendly interface is provided to the encryption functionality and the user is able to encrypt both data sets and entire volumes, such as a USB removable storage device. Unlike FileVault, there is no concept of a secondary master password in the event that a user forgets the primary password used to encrypt the data. Like Disk Utility, Knox can be used to decrypt and unpack the data set held within the file.

The Knox application can be configured to run at system start-up, so that it automatically detects when an encrypted volume is inserted and prompts for a password. The password can be stored in the Mac’s key store, known as the Keychain, but a strict security policy would not recommend this, since a compromise of the user machine could lead to an attacker gaining access to all passwords in the Keychain.

[http://www.knoxformac.com]

4.12 MS BitLocker

BitLocker is a logical disk encryption tool for workstations and laptops and is listed in the CESG *Directory of Infosec Assured Products*. It is not intended for use on server systems. It performs the following core functions:

- encryption of the complete operating system logical disk, encapsulating user, system, swap and hibernation files to ensure that data may not be easily accessed by any software or hardware based measures taken.
- checking and verification of early boot components and configuration data. Systems using Trusted Platform Module (TPM) version 1.2 hardware are granted additional assurance of pre-start-up system integrity checking security, as the hardware may also verified.

Security is ensured via the implementation of 256-bit AES encryption and the required two-factor authentication can be provided by several different tokens.

[http://technet.microsoft.com/en-us/library/cc766295.aspx]

4.13 MS Windows EFS

EFS is a long-established encryption solution for the Windows platform that protects files and/or folders selected by the end-user. Because of this approach it cannot guarantee to include all the data that needs to be secured. For example, when hibernated, a Windows machine writes all active data to the hard disk in temporary files whose locations may not be known to the user. These files are not encrypted.

EFS is only as robust as the user’s Windows password. Hard to guess passwords or preferably pass phrases consisting of 10 or more characters and numbers and symbols should be used.

[http://technet.microsoft.com/en-gb/library/bb457065.aspx]

4.14 PGP Desktop Professional

PGP Desktop Professional is listed in the CESG *Directory of Infosec Assured Products*. It provides a comprehensive set of encryption applications to protect sensitive data on disk or removable media and in emails and instant messages. It includes PGP Whole Disk Encryption, which locks down the entire contents of a system, external drive or USB flash drive, including system and swap files and boot sectors. The encryption is transparent to the user.

[http://www.pgp.com/products/index.html]

4.15 Redstor Protector

Redstor Protector is designed to allow users to secure the data that resides across all of their personal storage and computing devices. By combining back-up, encryption, synchronisation and data destruction within an easy-to-use service, it is possible to cover accidental or malicious data loss scenarios.

Designed with large-scale deployments in mind, Redstor Protector is designed to be sold by service providers. The service allows consumers to sign up online and create an account. The service creates an encrypted folder on the laptop or desktop as well as on USB storage devices. Should the user have data that is deemed sensitive, they can choose to store the data in a secure folder on the desktop.

If a secure folder is created on the USB device, then it will also synchronise that data with the secure folder on the host system. Redstor's online back-up service then automatically performs daily remote back-ups across a secure internet connection and in the event of data loss or corruption will allow the user to recover their data.

Redstor can also embed a data shredding and destruction technology that can be remotely activated by the service provider.

[http://www.redstor.com]

4.16 TrueCrypt

TrueCrypt is a free and open source encryption software package for Windows Vista/XP, Mac OS X and Linux platforms. A guide to installing TrueCrypt is available from [http://opensourceschools.org.uk].

We recommend that a technically competent person installs and sets up TrueCrypt. Users may lose important data permanently if they set up TrueCrypt incorrectly.

[http://www.truecrypt.org]

4.17 WinZip

WinZip, version 9.0 or later, and WinZip E-Mail Companion support 128-bit and 256-bit AES encryption, which provide much greater cryptographic security than the traditional Zip 2.0 encryption method used in earlier versions of WinZip.

Note that recipients of AES-encrypted Zip files must have a compatible Zip file utility in order to decrypt the files.

[http://winzip.com/wzdaes.htm]

5 Encrypting mobile devices

5.1 USB portable drives

The recommended approach for encryption on USB portable drives is to purchase drives that are FIPS 140-2 certified. The following are widely available:

- Eclypt PICO Freedom (FIPS 140-2 Validated)
- IronKey (all variants)
- KanguruMicro Drive
- Kingston DataTraveler BlackBox
- SanDisk Cruzer (Enterprise FIPS edition)
- Stealth MXP.

It is also necessary to support this with policies or tools to prevent users from using other (unencrypted) USB portable drives.

5.2 Symbian-based mobile devices

5.2.1 McAfee Endpoint Encryption

McAfee Endpoint Encryption (formerly SafeBoot) for Symbian encrypts files, local folders, databases, removable storage and even emails through its FIPS 140-2 certified implementation. Encryption and decryption can be performed on the fly, and a user can access encrypted data only after authenticating. Data can be encrypted and decrypted automatically (and transparently to the user).

[http://www.mcafee.com/us/enterprise/products/data_protection/data_encryption/endpoint_encryption.html]

5.2.2 Pointsec Mobile

Pointsec Mobile secures data on the Symbian, Pocket PC, Windows Mobile Smartphone and Palm operating systems by encrypting files on the devices as well as their related memory cards. Pointsec Mobile is designed to meet the requirements of both enterprise business and service provider environments. It provides:

- transparent, on-the-fly encryption for handheld files/folders and related memory cards
- Open Mobile Alliance (OMA) enabled encryption clients delivered or managed by any OMA device management solution
- a central interface to create, deploy, update and enforce settings
- wireless deployment, updates and support using the over-the-air (OTA) standard
- a simple, secure challenge/response procedure for password resets

- PicturePIN, alphanumeric passwords or numeric PIN authentication.

[http://www.checkpoint.com/pointsec]

5.3 Personal entertainment devices

Personal entertainment devices such as portable music and video players, games consoles and low-end mobile phones are very popular and have increasingly large data storage capacities. Currently, there are no commercial, certified or open source products available to secure these devices. We recommend that users do not store sensitive data on them.

6 Encrypting protected data in transit

Data in transit is any type of information that is transmitted between systems, applications or locations. The secure transmission of data in transit relies on both encryption and authentication. The critical functions provided by this technology are:

- encryption of the data itself
- ensuring that the computers at each end are the computers they say they are
- ensuring that the user at the remote end is who they say they are
- ensuring that the user is authorised to access the requested data.

The following encryption mechanisms can be used to put in place systems that comply with government standards to protect data in transit:

- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) or IPSec – for remote login and remote command execution over Transmission Control Protocol/Internet Protocol (TCP/IP) networks.
- Secure Shell (SSH) – for remote login and remote command execution over Transmission Control Protocol/Internet Protocol (TCP/IP) networks.
- SSH File Transfer Protocol (SFTP) – for encrypted file transfers and manipulation functionality over any reliable data stream. It is typically used with the SSH protocol to provide secure file transfer, but is intended to be usable with other protocols as well.
- Secure Copy (SCP) – for securely copying files between a local and a remote host, or between two remote hosts, using the SSH protocol.
- Public Key Infrastructure (PKI) – a PKI is the combination of software, encryption technologies and services that creates and manages the use of public keys.
- Wireless Fidelity (Wi-Fi) Protected Access (WPA and WPA2) – used to secure Wi-Fi computer networks.

6.1 TLS/SSL

The de facto internet standard for encrypting web-based information interchanges is Transport Layer Security (TLS), previously known as Secure Sockets Layer (SSL). Both the client and server software need to support TLS. All major web browsers and servers support it. However, legacy applications without a web front end may not provide it.

6.2 IPSec

IPSec is designed to provide authentication, integrity and confidentiality. As it operates at the network layer, IPSec has an advantage over SSL and other methods that operate at higher layers. Applications must be written to be aware of, and use, SSL, while applications can be used with IPSec without being written to be aware of it. Thus, encryption occurs transparently to the upper layers.

IPSec is not a single protocol; it is made up of two protocols, which can be used separately or together:

- AH (Authentication Header) – AH is used to authenticate the identity of the sender, and to provide integrity of the data to ensure that it has not been modified. It does not encrypt data and provides no confidentiality. AH signs the entire packet.
- ESP (Encapsulating Security Payload) – ESP can provide confidentiality by encrypting the data itself, along with authentication and integrity. However, ESP generally does not sign the entire packet, only the data.

To protect the IP header and the data, AH and ESP can be used together. There are two modes of operation for both AH and ESP:

- Tunnel mode, which is used to create a virtual private network. Tunnel mode provides gateway-to-gateway (or server-to-server) protection.
- Transport mode, which is used to encrypt data inside a tunnel that is created by Layer Two Tunnelling Protocol (L2TP). Transport mode provides end-to-end security, all the way from the sending computer to the final destination.

Once two computers that are communicating via IPSec establish a security association, this represents the ‘agreement’ between the two about the way the data will be exchanged and protected. Thus, both these computers must support IPSec.

6.3 Server identity assurance

Assurance of a server’s identity (authentication) on the web currently requires the use of a certificate supplied. Using digital certificates with SSL provides the security necessary to protect online interactions. This is the mechanism most typically used in organisations.

Since any successful authenticated SSL session causes a web browser padlock icon to appear, users are not likely to be aware of whether the website has been validated or not. As a result, Extended Validation (EV) certificates have been introduced.

Browsers with EV certificate support display more information for EV certificates than for previous SSL certificates. Internet Explorer 7 is EV certificate-ready (however, in Windows XP and Windows Server 2003, the ‘phishing filter’ must be turned on to show it). Firefox 3.0 (and higher) and Opera 9.5 (and higher) include EV support as well. When a browser receives an EV certificate:

- the address bar turns green
- a special label will appear that alternates between the name/summarised address of the website owner and the certificate authority that issued their certificate.

Using an EV certificate on a web server:

- provides 128-bit or 256-bit SSL link-level encryption
- provides authentication of a web server to a web browser, as well as server-to-server authentication
- provides the ability to secure two virtual web servers using the same SSL certificate via the Subject Alternative Name (SubjectAltName) extension.

EV certificates may also used to incorporate Impact Level labels and remote access restrictions in many gateway applications, including Microsoft’s Intelligent Application Gateway and BT’s Global Network Services.

7 Securely deleting protected data

A normally deleted file can be recovered, since only the directory entry and not the file contents are removed from the disk. Even if the file is later overwritten by a new file, it may still be possible to recover part of the content.

For example, in a simple file system, with 1Kb blocks, if a file of 973 bytes is overwritten by a file of 744 bytes, there will be 229 bytes of the original file which will not be overwritten. Depending on how sensitive that data was, this may be a problem.

Government guidelines mandate the secure deletion of files (when they are no longer needed) by randomly overwriting files to government standards (usually seven times). This functionality is provided by the use of encryption software.

Examples of products and applications that can securely delete data include:

- Compost (Mac)
- DESlock+ Shredder (Windows)

- Eraser (Windows)
- File Shredder (Windows)
- PGP (Mac)
- SDelete (Windows)
- Shred (Linux)
- Wipe (Linux)
- Secure Empty Trash (Mac).

NB: Becta has not conducted formal evaluation of these products and therefore does not recommend any specific solution. The products listed here are to demonstrate some of the types of solutions currently in use within the education sector. Other suitable products are available that are not listed in this document.

7.1 Compost

Compost operates as a Mac OS X System Preferences pane. Its most obvious benefits are the automatic deletion features. Compost automatically deletes files that have been in the Trash longer than a user-defined number of minutes, hours or days. It can also limit the Trash to a certain size: for example, if you limit the Trash to 512MB and later place an item in the Trash that pushes the size of the Trash over that limit, Compost deletes the oldest items until the Trash size is below your limit.

7.2 DESlock+ Shredder

The DESlock+ Shredder is installed onto the Windows desktop. It uses cryptographic random numbers and DoD 5220-22.M (the shredding method used by the US Department of Defense). Files may be dropped onto the shredder for secure deletion, or alternately the shredder can be set to shred the following items:

- My Recent Documents
- Internet Explorer history and cache
- the contents of the Windows temporary files folder
- the contents of the recycle bin
- the Windows page file (on shutdown).

7.3 Eraser

Eraser is a security tool for Windows that completely removes sensitive data by overwriting it several times with carefully selected patterns. Eraser is free software and its source code is released under GNU General Public Licence. The application:

- works with Windows 95, 98, ME, NT, 2000, XP (32/64), Vista (32/64), Windows Server 2003 and DOS.
- It works with any drive, including IDE, SCSI and RAID, and CD-RWs.
- uses DoD 5220-22.M
- erases files and folders

- erases files and folders that were only previously ‘deleted’
- erases all hard drives
- erases Index.dat on reboot
- erases free space on Windows 95, 98, ME, NT, 2000, XP and DOS
- erases contents of the Recycle Bin
- erases compressed files and drives
- erases Windows temporary files
- erases internet cache and cookies
- erases paging (swap) files.

[http://www.heidi.ie/node/6]

7.4 File Shredder

File Shredder provides the secure deletion of files in various partitions and supports Wipe Hard Drive. Supported shredding methods include Peter Gutmann’s method, DoD 5220.22-M and random overwrite algorithms. The application’s functions include:

- secure (unrecoverable) shredding of files and directories
- shredding of file and directory names
- shredding of free space on disk
- supporting shredding on NTFS (New Technology File System), FAT32, FAT16 and FAT12 partitions
- shredding of cluster tips and ADS (Alternate Data Streams) on NTFS partitions.

[http://www.fileshredder.org]

7.5 SDelete

You can use SDelete to securely delete existing files, as well as to securely erase any file data that exists in the unallocated portions of a disk (including files that you have already deleted or encrypted). SDelete uses clearing and sanitising DoD 5220.22-M standards to be sure that once deleted with SDelete, the file data is permanently removed. Note, however, that although SDelete securely deletes file data, it does not delete file names located in free disk space.

[http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx]

7.6 Secure Empty Trash

Within the Mac OS X operating system, items can be moved to Trash or selected for ‘Move to Trash’, and can then be permanently deleted through ‘Secure Empty Trash’. Once that button has been clicked, OS X will run a 35-pass overwrite of the file, essentially going well beyond the basic recommendations of any government security department. And once it is done, there will be no going back.

If you intend to securely erase large files, it could take a substantial amount of time in order to complete the secure erase process, given that a large file would have to be overwritten 35 times.

This application is free as it is native to Mac OS X.

8 Taking encrypted data overseas

8.1 Encryption restrictions

Encryption is controlled or restricted in many countries. Many have passed laws, or are considering laws, to maintain law enforcement and national security capabilities through regulation of these technologies. In some countries, encryption technologies are treated in the same way as weapons or munitions.

Guidelines published in 2002 by the Organisation for Economic Co-operation and Development, *OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, provide a set of principles that apply to all participants (including businesses, governments and individual users) at all levels, and promote a culture of security as a means of protecting information systems and networks. These principles apply to educational ICT systems.

Although recommended for protecting data in the UK, some countries ban the use, or severely regulate the import, export or use of, encryption technology. You should always check current restrictions before leaving the UK with encryption software or encrypted data – you can find out about current restrictions from the two websites below. It may be safer to remove the software and data from your laptop or mobile device than to risk violating compliance requirements in these countries. Not doing so could risk imprisonment or confiscation.

When travelling to countries where encryption is permitted, it is still good practice to store encrypted data on media, laptops or mobile devices in a hotel room safe.

These two general reference sites provide current information on encryption restriction guidance:

- http://rechten.uvt.nl/koops/cryptolaw/index.htm
- http://www.wassenaar.org

Countries with encryption import and use restrictions (information correct at August 2008; before travelling you should check whether the information is still current):

- Afghanistan
- China (import, export and transit controls)

- Hungary (import controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is personal)
- Morocco (stringent import, export and domestic controls enacted)
- Pakistan
- Russia (you must apply for a licence)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls).

Embargoed countries (where approval from the UK government is unlikely):

- Burma (you must apply for a licence)
- Belarus (import and export of cryptography is restricted; you must apply for a licence from the Ministry of Foreign Affairs or the State Centre for Information Security or the Security Council before entry)
- China (you must apply for a licence)
- Cuba
- Ivory Coast
- Indonesia
- Iran (strict domestic controls)
- Iraq
- Liberia
- Libya
- North Korea
- Sudan
- Syria
- Vietnam (personal-use exemption for travellers with cryptography software on a laptop or mobile device)
- Yemen
- Zimbabwe.

It is recommended that you remove any encryption software and encrypted data from your laptop or mobile device if you are travelling to any of the above countries, or apply in advance for the appropriate licence before leaving the UK.