

Good practice in information handling in schools

Secure remote access

A guide for staff and contractors tasked with implementing data security

Contents

1 The need for secure remote access	3
2 Quick wins for compliance with UK data handling procedures.....	6
2.1 Shibboleth	6
2.2 The Employee Authentication Service (EAS)	7
3 Other secure remote access requirements.....	8
3.1 Encryption-only options for protecting data in transit.....	8
3.2 Browser-based identity assurance	8
3.3 Audit and logging.....	9
3.4 Remote access approval by the Information Asset Owner.....	9
4 Online reporting and remote access requirements.....	10
4.1 Special security considerations for online reporting	10
Appendix A – Exemplar third party solutions.....	11
Appendix B – Exemplar open source solutions	14

1 The need for secure remote access

The report Data Handling Procedures in Government published in June 2008, sets out in detail the procedures that all departmental and public bodies – including schools – should follow in order to maintain security of the data they hold. This includes encryption, protective labelling of sensitive data, audit and logging, operational controls for use of mobile devices – and a range of measures to ensure secure remote access.

Together with the requirements of the Data Protection Act 1998, these measures place new obligations upon schools in relation to any data that is classified as Impact Level 2 (IL2–Protect) or higher if this data is removed or accessed from outside the school. Education organisations must also ensure that data classified as IL2–Protect or higher is encrypted when it is in transit from one location to another, including transit from one approved secure location to another.

Providing secure remote access to educational systems and the protected data they contain requires multiple technologies that address:

- **authentication** – who or what system is trying to connect (identity management); ensuring that the users and the computers at each end are who they say they are
- **authorisation** – the types of tasks you wish to perform and ensuring that the users at the remote end are authorised to access the data
- **geographical restrictions** – protected data may not be accessed remotely unless encrypted, and access requires specific network connection
- **encryption** – to protect sensitive data in transit, and file or full disk encryption for any storage media that holds protected data
- **audit** – logs of access to protected data must be held at evidential quality for seven years.

Remote access requirements are based on data protection Impact Levels (IL). These are derived from the information classification guidance produced by the Central Sponsor for Information Assurance (CSIA) referenced in both Data Handling Procedures in Government and the Data Protection Act 1998. Within the education sector, Impact Levels are being recommended as the means of labelling the sensitivity of data, and have been mapped against the CSIA Levels as shown below.

CSIA Level		Impact Level
CSIA Level 0	equivalent to	IL1–Not Protectively Marked (IL1–NPM)
CSIA Level 1	equivalent to	IL2–Protect
CSIA Level 2	equivalent to	IL3–Restricted
CSIA Level 3	equivalent to	IL4–Confidential

The majority of typical school management information system (MIS) reports or teacher access is to data that is protected at 'IL3–Restricted'. Aggregating data elements into typical reports – data on special educational needs, for example – generally increases the Impact Level.

Some data elements that schools receive from external sources – on looked-after children or exclusions, for example – will have been labelled by the originating agency. Any data elements used must be protected at that Impact Level, and if aggregated with other data, are highly likely to require protection at a higher Impact Level.

There are also special conditions which mandate the use of stronger multi-factor access controls for the higher Impact Levels used in education.

As an example of this, DCSF has co-sponsored the Employee Authentication Service (EAS). It is proposed as a pan-government authentication service that will enable strong authentication of users to multiple government applications at central and local level. EAS works in conjunction with various secure remote access solutions by providing the required two-factor authentication.

EAS represents the Government's desired target state for user authentication services facilitating secure remote access to services by staff across all levels of government. It is delivered by the Government Gateway and initially intended to provide access to central Government services such as ContactPoint. EAS is expected to be launched later in 2008.

Several other cross-Government remote access schemas are being extended to include education, as shown in the table below. These programmes offer remote access solutions which are provided as a managed service and compliant with Data Handling Procedures in Government.

External access in schools by Impact Level

Impact Level	Example data types	eGIF requirements		Example networks	External access			
	Aggregated reports	Registration level	Authentication requirements		Gov PC to www	Internet café	PDA	Home Gov PC LAN
					Wi-fi	3G card	Bluetooth	Bootable USB
IL4 Confidential	<ul style="list-style-type: none"> National Pupil Database Looked-after children Witness protection SEN IL4 data elements 	Level Three ID verification with vetting and 'need to know' measures	Physical/ personal/ procedural protection with appropriate authorisation	GSI CJX	Y ¹	N	N	Y ²
					N	N	N	Y ³
IL3 Restricted or NHS Confidential	<ul style="list-style-type: none"> School MIS Teacher access to learning platform/ portals Special educational needs (with no IL 4 data elements) Pupil characteristic Contact point Health records 	Level Two ID vetting and 'need to know' measures	Mandatory two-factor user ID, password and token	N3 GSI GCSx CJX	Y	N	Y ⁴	Y ⁵
		Information Asset Owner approval	Internet/ Virtual Private Network and token	Encrypted internet VPN	Y ⁶	Y ⁷	N	Y ⁸
IL2 Protect	<ul style="list-style-type: none"> General student data Learning platforms/ portals 	Level One basic ID verification	User ID and password	Internet	Y ¹	N	Y	Y
					Y	Y	Y ²	Y
IL1/ IL0	<ul style="list-style-type: none"> Google search BBC News 	Anonymous	Authentication not required	Any	Y	Y	Y	Y

1Via thin client internet browse-down

2Via hard-wired Government-issued secure laptop (RAS)

3Requires a strong business case and CESG advice

- 4Via CESG-approved product such as Blackberry
- 5Via CESG-approved VPN or validated Manual T or Manual V solutions
- 6Implementations must be compliant with CESG Manual Y
- 7Via Government issued secure laptop with software encryption (RAS)
- 8Using software-based cryptography
- 9Requires strong business case and CESG advice

2 Quick wins for compliance with UK data handling procedures

The following remote access solutions offer methods via which you can achieve compliance with the spirit of Data Handling Procedures in Government.

2.1 Shibboleth

Link encryption and authentication can be achieved through the use of SSL for link-level encryption and Shibboleth for implementing identity standards to provide secure remote access, federated single sign-on and an attribute exchange framework.

Shibboleth provides a mechanism for secure access to online content for the education sector and is supported by the UK's Access Management Federation for Education and Research [<http://www.ukfederation.org.uk/>]. It is essentially a transport mechanism built on top of an institution's existing infrastructure that allows organisations to exchange information about their users in a secure and privacy-preserving manner.

Shibboleth requires SSL certificates to be installed to help maintain security. It provides extended privacy functionality allowing the browser user and their home site to control the attributes released to each application. Using Shibboleth-enabled access simplifies management of identity and permissions for organisations supporting users and applications.

In summary, Shibboleth provides for:

- both the Identity Provider and Service Provider (secure exchange of messages between two parties)
- devolved authentication (authentication is handled by the institution/LA/RBC)
- authorisation achieved by an exchange of attributes (such as 'member of an institution')
- a trust agreement that all providers must sign
- an implementation of Security Assertion Mark-Up Language (SAML).

Schools are encouraged to implement Shibboleth and join the UK Access Management Federation via their local authority or regional broadband consortium.

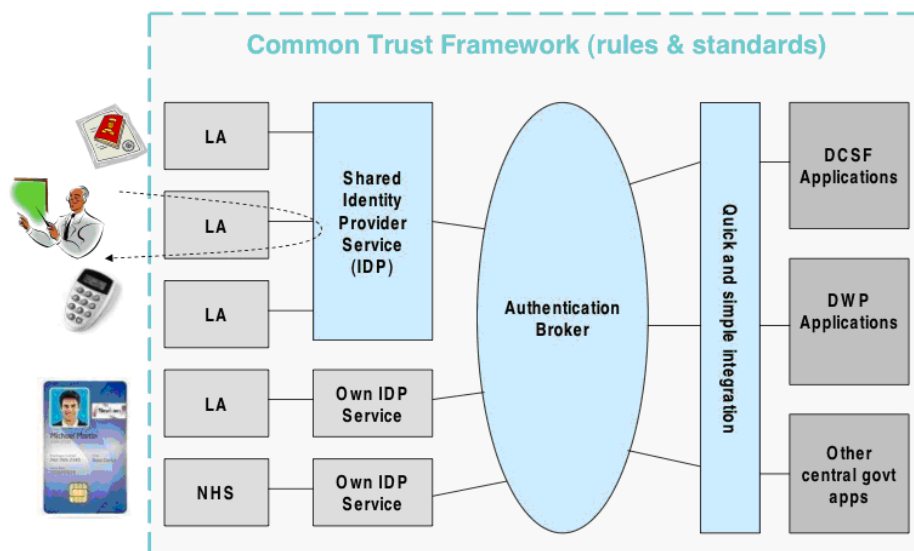
2.2 The Employee Authentication Service (EAS)

EAS is a scalable, sustainable, secure solution that will enable local government, schools and other organisations to access and share sensitive information in order to improve services for the benefit of children, learners and citizens. DCSF is leading the development of EAS, with the aim to make this a pan-government service.

It is intended that the service will be available to users in children's services from November 2008. EAS will be implemented through a phased approach to ensure that the functionality meets the requirements for different types of users. EAS will be delivered through the Government Gateway which currently provides online accounts to 13 million citizens and businesses for 150 government services.

The key EAS components include:

- **Local Authorities** – a registration function to register new users on the system and Enrolment function to enrol users on services
- **Identity Provider** – the part of the system which will verify a user's identity when they try to log on to a service
- **Authentication Broker** – the hub of the system which co-ordinates requests for identification between Identity Providers and Services
- **Service Providers** – these are the central government resources which users will access through the scheme.



This project has been set up as an exemplar and champion asset under the CIO Council initiative to maximise the opportunity for re-use by other government departments and local authorities.

EAS will deliver a common strong authentication platform for local government, teachers and third-sector users. EAS offers a number of benefits for schools:

- A user will only need one token to access a series of Government services
- It offers greater integration of education and children's services to improve access to services, support and resources for children and learners, using a common single sign-on for all services
- It offers safe and secure access to information and sharing of resources to support the learner (including hard-to-reach or disadvantaged groups)
- With robust access security controls, it allows pupil-level data to be shared, including between Children's Services and education practitioners.

3 Other secure remote access requirements

3.1 Encryption-only options for protecting data in transit

Data in transit is any type of information that is transmitted between systems, applications or locations. Encryption of data in transit is a critical mechanism to protect that data and is required by Data Handling Procedures in Government for all data that is at IL2–Protect and above. Encryption mechanisms to protect data in transit include:

- **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 used in public key cryptography. For further information regarding the applicable standards, contact your local authority or RBC.
- **Wireless Protected Access (WPA and WPA2)** – to be deployed to secure Wi-Fi computer networks. Either WPA or WPA2 is to be enabled and chosen in preference to wired equivalent privacy.

3.2 Browser-based identity assurance

Assurance of identity (authentication) on the Web currently requires the use of a certificate supplied by a third-party Certificate Authority (CA). Using digital certificates with SSL adds trust to online transactions by requiring website operators to undergo vetting with a CA in order to get an SSL certificate. However, commercial pressures have led some CAs to introduce 'domain validation only' SSL certificates for which minimal verification is performed of the details in the certificate. This is the mechanism most typically used in schools.

Most browser user interfaces do not clearly differentiate between low-validation certificates and those that have undergone more rigorous vetting. Since any successful SSL connection causes the padlock icon to appear, users are not likely to be aware of whether the website owner has been validated or not. As a result, fraudsters (including phishing websites) have started to use SSL to add credibility to their websites.

Techniques are becoming available such as EV Certificates that enable filtering to occur within application level gateways. Once these technologies have gained a level of maturity, they may be more appropriate within the educational sector.

3.3 Audit and logging

The logging of audit and event data is required to assure compliance with Data Handling Procedures in Government and ISO 27001. Collection of these logs forms a critical part of providing a safe and secure ICT infrastructure for educational environments. It is critical to providing secure remote access.

Gathering event data and the ability to interpret that data (behavioural data forensics) will provide significant value during incident response activities. This value can only be realised if the correct data is gathered and stored in a secure manner. It is also desirable to gather this data in such a way as to not cause performance problems on the monitored systems or run out of system resources.

A basic requirement for schools and/ or local authorities will be to configure secure remote access systems in a manner that facilitates the evidential quality collection and consolidation of event data related to remote access of protected data.

In order to meet the current UK minimum standards, a basic infrastructure that collects this information is required. Additional software tools will be required to analyse this information. Remote access auditing is required for school MIS, learning platforms, portals, operating systems, network devices, wireless access points, firewalls, application-specific events, messaging, chat sessions and email amongst others. The Audit logging and incident handling guide outlines how event data should be recorded.

3.4 Remote access approval by the Information Asset Owner

Information Asset Owners (IAOs) are those individuals in your institution who are responsible for identification of protected information assets (data and applications). Their role is to understand what information is held, what is added or removed, who has access to the data and why. They are the responsible parties for granting remote access to any protected data.

These individuals are key to implementation of secure remote access, the operational and technical procedures facilitating compliance, and reporting on and auditing the information assurance programme within the school.

4 Online reporting and remote access requirements

From September 2008, all maintained schools in England will be expected to start the move towards online reporting with:

- all secondary schools providing parents with online reports by September 2010
- all primary schools meeting the requirement by September 2012.

Schools need to start preparing for online reporting and consider it alongside the secure remote access requirements. This is also an opportunity for schools to look at how they can use their existing data and systems more efficiently and effectively to share protected information.

Schools already collect and manage a range of information. The emphasis should be on maximising the use of their integrated MIS and learning technologies. As with any move to new ways of working, schools will need to review their own capability – across the whole school – to implement online reporting.

Parents and learners should be provided with online access to information about:

- Attendance and behaviour (both positive and challenging)
- Progress and achievement
- Special educational needs

Remote access reporting requirements are determined by the impact level of the data being reported. Therefore, the types of information provided should be appropriate for the parent/learner.

For example, some special needs information may contain data that should be protected at IL3 and above (which would require two-factor authentication to access remotely). Reports for parents to access online must, therefore, be chosen carefully so that only information that is IL2 or below is made available.

If a school wishes parents to have remote access to IL3 data then parents will require two-factor authentication tokens and the use of password-protected files to enable secure communication between the school and themselves.

4.1 Special security considerations for online reporting

It is important that online reporting remote access is designed to provide summary data fit for purpose, on a need-to-know basis.

Reporting must access only authorised data. Unless circumstances or applications allow controlled access, direct access to the school's MIS should be prohibited.

Note: Today's portals and learning platforms facilitate the use of Web Parts and Widgets that are freely available via the internet. These objects are code modules that can be installed and executed within web pages by the end user without requiring additional authorisations. Certain uses of these objects may enable direct linkages to systems and facilitate unintended access. Code-based filtering within learning platforms and portals must be in place to prevent the execution of insecure code in order to prevent the by-passing of security measures.

Appendix A – Exemplar third party solutions

The following are examples of technologies that meet the Data Handling Procedures in Government secure remote access requirements when combined with a two-factor authentication token.

Becta has not tested these solutions and they are presented as examples. Other available solutions may also meet the requirements.

MobileXpress (MX) Private Teleworker

<http://www.btglobalservices.com/>

MobileXpress (MX) Private Teleworker from BT Global Network IT services is a managed service solution available from existing government frameworks, It provides a combination of network connectivity, security and service management capabilities designed with home/remote workers in mind. It also provides a range of broadband VPN access options and a choice of encryption and token-based authentication equipment.

Citrix SSL Access Gateway

<http://www.citrix.com/English/PS2/products/product.asp?contentID=15005>

Citrix's SmartAccess technology means that when a user connects, the system collects data to determine how the user is attempting to access the educational resources. SmartAccess policies provide a fine level of policy-based control over actions users can take with applications, files, web content, printing and email attachments.

It extends access by allowing users to access network file shares, web email and internal websites from devices that are locked down and do not permit the downloading of software. It supports a wide variety of platforms including Windows 2000 Professional, Windows XP, Windows Vista, Linux and numerous small form-factor devices.

This product suite is certified to FIPS 140-2 and CSIA certification.

Check Point SSL Virtual Private Network

[\[http://www.checkpoint.com/products/connectra/index.html\]](http://www.checkpoint.com/products/connectra/index.html)

The clientless SSL Virtual Private Network requires no specialised software to be downloaded on the user's device. All VPN traffic is transmitted and delivered through a standard web browser and its native SSL encryption.

The Check Point SSL VPN provides secure remote access, endpoint security and integrated intrusion prevention. Remote educational users can access a range of enterprise applications. Check Point also supports SSL Network Extender Application Mode where the client is based on an ActiveX or Java applet and a transparent proxy mechanism, which provides a solution for secure remote access to corporate resources through most TCP/IP applications, including non-web applications.

The Check Point SSL VPN solution is FIPS 140-2 compliant and CSIA approved.

CISCO SSL VPN

[\[http://www.cisco.com/\]](http://www.cisco.com/)

The SSL/IPSec VPN delivers a comprehensive set of Secure Socket Layer (SSL) and IP security (IPSec) Virtual Private Network (VPN) features. Support is provided for unrestricted full-network access as well as controlled access to select web-based applications and network resources offering both client and clientless options.

This solution delivers secure remote access to authenticated users on both managed and unmanaged endpoints.

CISCO SSL VPN is FIPS 140-2 certified.

VASCO SSL VPN

[\[http://www.vasco.com/products/range.html\]](http://www.vasco.com/products/range.html)

SSL VPN technology provides secure access for remote users without the requirement of a pre-installed client. SSL VPN provides an additional level of protection through complete content inspection, which ensures the integrity of customers' VPN traffic. Solutions may utilise either CSIA-certified SSL VPN or CSIA-certified IPSec VPN technology.

VASCO and Fortinet offers both a secure IPSec client and clientless SSL VPN for hotspot access in areas where IPSec may be blocked by a firewall. The VASCO token provides the second factor authentication so users can establish secure sessions.

The VASCO SSL VPN solution is FIPS 140-2 certified.

RSA SSL VPN

[\[http://www.rsa.com/node.aspx?id=1155\]](http://www.rsa.com/node.aspx?id=1155)

Used in combination with RSA SecurID authenticators, the RSA SecurID Appliance is designed to validate the identities of users by requiring the user to present a PIN along with their token code before granting access to sensitive network resources. Each user is assigned a unique RSA SecurID authenticator which generates a random code every 60 seconds. The RSA SecurID Appliance validates the user's PIN and token code, confirming the user's identity.

The RSA SSL VPN solution is FIPS 140-2 certified.

Microsoft Intelligent Application Gateway (IAG) SSL VPN

[\[http://www.microsoft.com/forefront/edgesecurity/iag/en/us/overview.aspx\]](http://www.microsoft.com/forefront/edgesecurity/iag/en/us/overview.aspx)

IAG is an enterprise-wide solution with a customisable SSL VPN portal defined by user identity. It restricts client access based on endpoint security profile and provides secure remote access to users by pre-authenticating users before they gain access to any published servers

For users who need access to IL3–Restricted data contained in an aggregated database, such as a school MIS, it provides:

- application-specific data protection
- blocking of specific functions and/or areas within applications based on endpoint profile
- endpoint security verification
- client-side cache and session clean-up
- multiple policy-based portal configurations with link translation.

While this is an effective solution designed to severely restrict remote access and limit information flows to IL3 levels, it requires a significant investment in configuration management, co-ordination with CESG and the approval of the accreditation authority for your systems.

This solution supports Windows Active Directory integration with full support for LDAP and RADIUS. IAG can combine authentication against one repository (such as RSA SecurID) with authorisation data from another (such as Active Directory). Custom authentication, geographic location, and individual data element access schemas can be configured to enable controlled remote access security by users whilst allowing those same users full access when connecting within protected buildings and LANs. Authentication mechanisms support X.509 client certificates (typically for student access to learning platforms and portals) and industry standard two-factor authentication tokens.

This solution is FIPS 140-2 certified and in use in the MoD Government gateway.

Appendix B – Exemplar open source solutions

The following provide compliant solutions, but only when combined with a separate two-factor authentication mechanism. This list is provided for indicative purposes only and is not exhaustive.

SSL-Explorer VPN

[\[http://sourceforge.net/projects/sslexplorer/?abmode=1\]](http://sourceforge.net/projects/sslexplorer/?abmode=1)

This software-based SSL VPN solution offers enhanced multi-layered authentication methods, hardware authentication token support, full IPSec replacement, finely-grained policy-based access control along with auditing and reporting tools.

Users can be granted access to their files, applications and email from virtually any location with an internet connection. It can also provide secure remote access to manage servers, routers and other network hardware securely using industry-standard encryption technology.

A virtual appliance edition of SSL-Explorer VPN is available as a free download. This version is based upon a hardened Linux distribution.

Multi-factor authentication is available using LDAP, RADIUS, SSL client certificates or one-time-password via SMS to a mobile device or PDA. These authentication modules provide additional security layers to protect critical information assets and protected data. SSL-Explorer Enterprise Edition is compatible with SafeNet 2032 and Aladdin two-factor authentication devices.

The product's network extension feature allows you to extend full network layer access beyond the physical boundaries and is available for both the Windows and Linux client operating systems.

Versions are available for Microsoft Windows 2000/XP/2003/Vista/2008, Apple Mac OSX Tiger (or later) and Linux operating systems.

OpenVPN SSL

[\[http://openvpn.net/\]](http://openvpn.net/)

OpenVPN accommodates a wide range of configurations, two-factor authentication, including remote access, site-to-site VPNs, Wi-fi security and provides enterprise-scale remote access solutions with load balancing, failover, and fine-grained access controls.

OpenVPN implements OSI layer 2 or 3 secure network extensions using the industry standard SSL/TLS protocol and allows a user or user group specific access control policies by using firewall rules applied to the VPN virtual interface. OpenVPN's drawback is that it is not a web application proxy and does not operate through a web browser.