Good practice in information handling: Secure remote access

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.

© Becta 2009

Contents

Key points

Educational organisations should use secure remote access technology, where appropriate, to secure the personal data of learners, staff and any other authorised users.

This guide will help to determine when organisations should use secure remote access and the level of security needed.

This guide is intended for staff or contractors in educational organisations who are tasked with putting in place secure remote access to sensitive data.

It contains:

- an explanation of why secure remote access is needed
- an overview of the technologies
- guidance on levels of security
- secure remote access solutions
- additional remote access requirements
- information on online reporting and remote access (maintained schools only)
- examples of third-party solutions.

1 The need for secure remote access

The Government has set out in detail the procedures that all departmental and public bodies should follow in order to maintain security of the data they hold. These include encryption, protective marking, audit and logging, operational controls for use of mobile devices, and a range of measures to ensure secure remote access.

These measures will help educational organisations fulfil their legal obligations under the Data Protection Act 1998[1]. Educational organisations must secure any personal data that is removed or accessed from outside a secure area in the organisation. Educational organisations must also ensure that sensitive and personal data is encrypted when it is in transit from one location to another, including transit from one approved secure area to another.

2 Essential components of secure remote access

Providing secure remote access to systems and the personal data they contain requires multiple technologies that cover:

- **authentication** – who or what system is trying to connect, ensuring that the users and the computers at each end are who they say they are

[1] http://www.ico.gov.uk/what_we_cover/data_protection.aspx

- **authorisation** – ensuring that the users at the remote end are authorised to access the data
- **geographical restrictions** – personal data may not be accessed remotely unless encrypted, and access may requires specific network connections
- **encryption** – to secure personal data in transit, and file or full disk encryption for any storage media that holds personal data
- **audit** – logs of access to secured data.

3 Risk assessment and remote access requirements

Organisations should base their remote access requirements on information risk assessments[2]. Organisations should think carefully about what kinds of sensitive and personal data they are making available remotely and who they are granting access to. Remote access to any personal data should be over an encrypted connection protected by a username/ID and password. Users who are given full, unrestricted access to an organisation's management information system should do so over an encrypted connection and use two-factor authentication.

Organisations may receive data from other organisations – for example, on looked-after children or exclusions – that may have been marked as having specific security requirements. Organisations should include any protective markings on such data in their risk assessments.

Organisations should ensure that users are aware of the need to keep their sign-on credentials secure. This is particularly important when users access systems from a shared computer. For example, users should make sure they sign off when they have ended their session. Users should not save passwords, if offered this option by their browser. Users should ensure that unauthorised users are not able to use their credentials to gain authorised access, for example, another family member at home who may use a shared computer.

4 Secure remote access solutions

The following remote access solutions offer ways for educational organisations to put in place secure remote access.

4.1 DCSF CIO Group strategy for enhancing identity assurance for children, learners and parents

This section provides early information on the DCSF Chief Information Officer's (CIO) Group's work on online authentication and simplified sign-on, which forms part of an overall strategy for identity assurance.

[2] *Good practice in information handling: Keeping data secure, safe and legal* contains more information about risk management and protectively marking data: [http://www.becta.org.uk/schools/datasecurity and http://www.becta.org.uk/feandskills/datasecurity]

© Becta 2009

Changes in the education, skills and children's services sector mean that many services are delivered online, and often involve more than one provider. Examples are where a learner is enrolled at two institutions and wants to use systems and content from both; and a parent/carer who wishes to receive information online about her children who attend three different schools. At the same time, there is a heightened awareness and need for secure online access to information and transactions.

Identity Assurance means the ability for a child, learner or parent/carer to assert their identity when dealing with organisations in our sector with ease and confidence, and for organisations to deal with that identity appropriately, effectively and efficiently.

DCSF CIO Group and Becta are working on the policy, regulations, solutions and guidance to assist local authorities, schools and colleges to enhance identity assurance for children, learners and parents. One important aspect of this is online authentication – the issuing and use of usernames, passwords and other credentials for enrolling and logging in to web-based services.

The intention is that:

- children and learners have secure, appropriate and simple access to a wide range of learning materials and solutions, access to their own records, access to online services such as the MIAP Learner Record, and the ability to use online enrolment- and entitlement-based applications. We want to ensure that, as far as possible, all children and learners can use their school/college log-ins for as many such services as possible, and that there is a common understanding and level of effectiveness and security in such systems and solutions.
- parents/carers have secure, appropriate and simple access to their child's or children's records, and to make online entitlement-based applications for educational services, such as Free School Meals. Many schools, colleges and local authorities issue log-ins to parents through their own systems. Increasingly, parents may have one log-in account for other online dealings with local and central government, and it is the Government's intention that these will be usable in future for any government services the user chooses. Parents will have appropriate control of their usernames and passwords for their dealings with local and central government, and certainty that all such services are effective and secure.

Using one log-in to access more than one service provided by different organisations is often called simplified (or single) sign-on. The future framework for Identity Assurance will include the enabling of simplified sign-on for children, learners and parents/carers across the education, skills and children's services sector.

There are currently two frameworks (or federations) for simplified sign-on that are relevant to schools, colleges and local authorities. The first is specific to the education sector and is provided by the UK Access Management Federation for Education and Research[3] (which is funded by Becta and JISC) and uses the standards-based Shibboleth software (see below).

The second is the Government Gateway[4], which is considered to be the 'cross-government champion asset' and is supported by the Cabinet Office, the Department for Communities and Local Government (CLG) and the Department for Work and Pensions (DWP). In the future, this is likely to be used increasingly by government departments, agencies and local authorities as their standard mechanism for authenticating citizens.

As a sector, we need to recognise that while children and learners are our primary concern, parents/carers are also 'customers' for some online services. And many young people will be in learning at the same time as in work, and may need to use online services which must be accessed through both the UK Access Management Federation and the Government Gateway.

For the education, skills and children's services sector, each of the two federations has distinct advantages. The aim is to join up access to these two federations. So, whether a provider decides to build on a Shibboleth solution, or adopt a solution at local authority level which is built around the Government Gateway, one won't 'lock out' the other. Such technology investment decisions are complex because, for example, simplified sign-on solutions are linked to infrastructure, directory structures, data warehousing, application designs and so on. Our approach will mean that when a local authority, school or college makes an investment in technology that uses one of the federations, it will be interoperable with the other.

DCSF CIO Group is working to establish the business and technical framework for achieving this, which will then become an education, skills and children's services sector-wide solution.

Subject to the requirements of an agreed 'trust framework', service providers within the UK Access Management Federation, whose solutions allow learners and parents/carers to log in via other providers within the federation, will also be able to allow learners and their parents/carers, for example, to log in via the Government Gateway.

A solution which is either UK Access Management Federation or Government Gateway compliant is likely to be much more effective and secure than one that uses neither. Indeed, there are some significant risks attached to using a 'home-grown' or proprietary sign-on solution. Therefore, we hope that by providing this

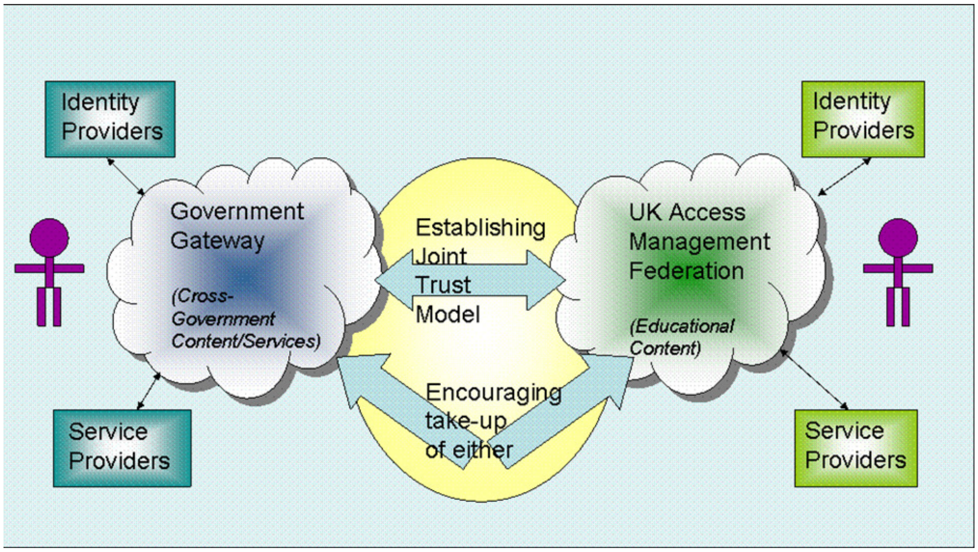
[3] http://www.ukfederation.org.uk
[4] http://www.gateway.gov.uk

© Becta 2009

information now, we will encourage schools, colleges and local authorities to adopt a strategic solution to simplified sign-on.

The future framework, which will include best practice guidance and toolkits for adopters, will be promoted as a standard model of good practice for policy areas and local service providers to adopt (for example, when specifying/procuring online solutions from their ICT providers). It will also help ICT providers to develop solutions that are interoperable, and which can be shown to follow the good practice for security, appropriateness and ease of use.

The approach being taken is to establish interoperability between the UK Access Management Federation and the Government Gateway rather than create a new federation. Service providers in one federation will potentially be able to accept ‘assertions’ from identity providers in the other federation.


Identity Providers
Government Gateway
(Cross-Government Content/Services)
Service Providers
Establishing Joint Trust Model
Encouraging take-up of either
Identity Providers
UK Access Management Federation
(Educational Content)
Service Providers

It is recognised that many schools, colleges and local authorities are already procuring and designing solutions in this area. We are working as quickly as possible to issue further guidance and toolkits. Work is underway on the specification and design of the solution architecture with the aim of completing a proof of concept by the end of 2009 and having an operational interoperable framework available early in 2010.

A parallel stream of work is the Employee Authentication Services project, which is described below. These streams of work address different audiences (employees versus children, learners and parents) but some of the principles are the same, and some of the underpinning standards and technology are common.

Although local authentication solutions may still be developed and maintained, it is anticipated that the benefits to service providers and their customers of federated authentication will reduce the need for local ad hoc solutions. We also recognise that it will take some time for software suppliers to upgrade their solutions, although

© Becta 2009

many educational software providers are already working to join the UK Access Management Federation. This should not be affected by the work to achieve interoperability between the UK federation and the Government Gateway.

For example, online reporting for parents is a key driver within the school sector and will place an additional burden on providers of a ‘parent portal’ if they are to provide support for local parent user accounts and, depending on where their children go to school, may require the parent to manage multiple accounts. The proposed cross-sector authentication model would allow parents to access their child’s records by authenticating via their Government Gateway account instead of logging in to one or more parent portals locally, and allow schools to focus on enrolment and access control, leaving the Government Gateway to provide the registration and account management services for parents.

In anticipation of this approach and to allow new services to take advantage of the federated model, new systems should be specified where possible to support federated authentication using the Security Assertion Mark-Up Language (SAML2) standard. SAML2 is increasingly being adopted as the standard for interoperability and the UK Access Management Federation will cease to support earlier versions of SAML from April 2010.

4.2 Shibboleth and the UK Access Management Federation for Education and Research

Shibboleth provides a mechanism for secure access to online content for the education sector and is supported by the UK Access Management Federation for Education and Research [http://www.ukfederation.org.uk]. It provides secure encrypted authentication and authorisation.

Shibboleth requires SSL certificates to be installed to help maintain security. It provides extended privacy functionality, allowing the 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:

- secure exchange of authentication and authorisation between identity providers and service providers. In combination with SSL websites, the whole process of logging in to and accessing a resource can be encrypted
- devolved authentication (authentication is handled by the institution/local authority/regional broadband consortium)
- authorisation achieved by an exchange of attributes (such as ‘member of an institution’)
- a trust agreement that all providers must sign
- an implementation of SAML2.

© Becta 2009

Educational organisations are encouraged to implement Shibboleth or a compatible solution and join the UK Access Management Federation. In the case of UK schools, they should do this via their local authority or regional broadband consortium.

4.3 Employee Authentication Services (EAS)

Local authorities and schools should also consider how Employee Authentication Services (EAS) can help with two-factor authentication. EAS is endorsed and security accredited as a core government shared asset, meaning that central and local government employees can use EAS to access multiple applications and databases across government through a single authentication process and token. As more shared government databases switch to two-factor authentication as a minimum security standard, EAS will help decrease the burden on users by reducing the number of tokens that they are expected to carry and manage in order to access sensitive information.

EAS is a cross-government project delivered through a DCSF-led strategic partnership supported by the CLG, the DWP and local authorities. The project is engaging with service users (such as local authorities) now and will be offering a range of services through EAS from 2009.

You can find detailed information about EAS on the local authorities section of the DCSF website [http://www.dcsf.gov.uk/localauthorities/index.cfm?action=content&contentID=18622]

5 Other secure remote access requirements

5.1 Encrypting data in transit

Data in transit is any type of data that is transmitted between systems, applications or locations. Organisations must encrypt personal data in transit. Encryption mechanisms to secure data in transit include:

- **Secure Shell (SSH)** – for remote log-in 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 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 regional broadband consortium.

© Becta 2009

- **Wireless Protected Access (WPA2 and WPA)** – to secure Wi-Fi computer networks. Organisations should use WPA2 (or WPA if WPA2 is not available). Organisations should not use Wired Equivalent Privacy (WEP).

5.2 Browser-based server identity assurance

Assurance of server identity (authentication) on the web currently requires a certificate supplied by a third-party Certificate Authority (CA). Using certificates with SSL adds trust to online transactions. Website owners need to be vetted by the certificate authority in order to get an SSL certificate. However, commercial pressures have led some certificate authorities to introduce ‘domain validation only’ SSL certificates for which minimal verification is performed.

Most browsers do not clearly show users the difference between low-validation certificates and those that have undergone more rigorous vetting. Since any successful SSL connection causes browsers to show users the padlock icon, users will assume the website is valid. As a result, fraudsters have started to use SSL to make fake websites seem more credible.

New techniques, such as Extended Validation (EV) certificates, enable filtering to occur within application-level gateways. Once these technologies have gained maturity, they may be more appropriate for use within the educational sector.

5.3 Audit and logging

A basic requirement for educational organisations 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 secured data.

The accompanying guide, *Good practice in information handling: Audit logging and incident handling*, contains more information.

5.4 Remote access approval by the Information Asset Owner

Information Asset Owners are those individuals in an organisation who are responsible for identification of secured 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. Any remote access to secured data must be authorised by the Information Asset Owner of that data.

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

6 Online reporting and remote access requirements – A special note for schools

All maintained schools in England are expected to start the move towards online reporting. Secondary schools should provide parents with online reports by September 2010, and primary schools by September 2012.

Schools need to prepare for online reporting and include secure remote access requirements. Schools should also take the opportunity to look at how they could make better use of their existing data and systems to share secured data. Becta's *Information Management Strategy Framework* [http://www.becta.org.uk/plansustainablesuccess] can help with this.

Schools already collect and manage a range of data. Schools should make as much use as possible of their integrated management information system and learning technologies. As with any move to a new way of working, schools will need to review their own capability – across the whole school – to put online reporting in place.

Schools should provide parents and learners with online access to data about:

- attendance and behaviour (both positive and challenging)
- progress and achievement
- special educational needs.

6.1 Special security considerations for online reporting

As with any remote access to data, it is important to provide summary data that is fit for purpose and on a strictly need-to-know basis. Schools should work out remote access requirements by a risk assessment on the data being reported to ensure the content of the data provided is suitable for the parent to view. In particular, schools should look carefully at the content of the data they are making available to parents, to ensure that it does not reveal the personal data of other learners. It is also good practice to issue each parent with individual usernames/IDs and passwords so that access can be tightly controlled.

The type and amount of data that will be made available online to parents is such that they should not need two-factor authentication for online reporting.

Many portals and learning platforms allow the use of freely available objects such as Web Parts and Widgets. These objects can be installed and executed within web pages by the end user without requiring additional authorisations. In some cases, using these objects can link users directly to systems and allow unintended access. Learning platforms and portals should, therefore, use code-based filtering to help prevent bypassing of security measures.

7 Examples of third-party solutions

The following are examples of technologies that meet the Government secure remote access requirements when combined with two-factor authentication.

Note: Becta has not conducted a formal evaluation of these products and, therefore, does not recommend any specific solution. Other suitable products are available that are not listed in this document.

7.1 MobileXpress (MX) Private Teleworker

MobileXpress (MX) Private Teleworker from BT Global 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 virtual private network (VPN) access options and a choice of encryption and token-based authentication equipment.

[http://www.btglobalservices.com]

7.2 Citrix SSL Access Gateway

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 approved by the Central Sponsor for Information Assurance (CSIA). (The CSIA is a unit within the Cabinet Office providing a central focus for information assurance activity across the UK.)

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

7.3 Check Point SSL VPN

The clientless SSL VPN 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

© Becta 2009

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.

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

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

7.4 CISCO SSL VPN

The SSL/IPSec VPN delivers a comprehensive set of SSL and IPSec (IP security) 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.

[http://www.cisco.com]

7.5 VASCO SSL VPN

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 two-factor authentication so users can establish secure sessions.

VASCO SSL VPN is FIPS 140-2 certified.

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

7.6 RSA SSL VPN

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.

RSA SSL VPN is FIPS 140-2 certified.

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

7.7 Microsoft Intelligent Application Gateway SSL VPN

Intelligent Application Gateway (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.

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.

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, while allowing those same users full access when connecting within protected buildings and local areas networks (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.

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

7.8 SSL-Explorer VPN

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, and 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 on a hardened Linux distribution.

© Becta 2009

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 OS X Tiger (or later) and Linux operating systems.

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

7.9 OpenVPN SSL

OpenVPN accommodates two-factor authentication and a wide range of configurations, including remote access, site-to-site VPNs and 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 Transport Layer Security (TLS)/Secure Sockets Layer (SSL) 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.

[http://openvpn.net]

© Becta 2009