

ICT Data Transfer systems within LSICT: Implemented Solution

Context

Under the Data Protection Act of 1998, the LEA is required to ensure that data maintained within its systems is both secure and processed in accordance with the data subject's rights - thus it is the responsibility of Learning Services ICT to protect relevant electronic data from:

- Data modification during transfer;
- Interception, viewing, or copying if intercepted;
- Being accessed by unauthenticated/unauthorised parties.

It was noted in point 113 of the LEA's Ofsted inspection report of January 2003 that "pupil-level data and transfer information is handled using diskettes" – this has been long regarded as an unsatisfactory system by Learning Services, due to the time taken to receive required data and the potential for data loss inherent within such a procedure; Ofsted also noted in point 113 that "plans for the transfer of electronic data via an intranet for schools have been delayed by at least 18 months because of inadequacies in corporate IT systems" and in point 111 that "electronic transfer of data and web developments are hampered by an out-dated corporate infrastructure".

Recent updates to both hardware and software in conjunction with Council restructuring have resulted in Learning Services ICT now having the facility to implement an effective system of Electronic Data Transfer (EDT) for client sites, thereby enabling the secure transfer of information (anything from a PULSE return to a Training Evaluation Form) between the LEA and the establishments that it serves: this document details the solution that is to be implemented and the factors influencing the selection of this solution. Please note that, in the interests of security, some details are given by way of example rather than being fully descriptive of the actual structures and processes employed.

Implemented Solution

After a process of consultation, followed by the evaluation and testing of potential systems, it has been decided that implementation of a secure file server accessed by clients through a secure website will provide the most effective return on investment with regard to ease of client use, minimising administrative overheads and increasing data security. Data security at the physical server level will be maintained through the use of Windows NTFS directory security permissions, with website security being maintained through

1. The use of Microsoft® Internet Information Services v6 Secure Sockets Layer (SSL)
2. Use of a Public Key Infrastructure (PKI) involving the controlled issue of digital certificates allowing access to the secure site to be restricted to authorised users only.

It is felt that the implementation of this method will provide the greatest scope for future expansion whilst at the same time providing a method of usage that is familiar to the target users.

The SSL and PKI combination is an industry-standard methodology employed in situations where data security is paramount: the commonest examples of its usage being in internet banking facilities and secure online shopping, where the transfer of information such as bank account or credit card details must be done as secure as possible. SSL provides a secure communications channel to prevent the interception of critical information, while PKI provides a method of verifying and authenticating the validity of each party involved in the electronic transaction.

In addition to providing effective security, the use of this combination ties in with recent software upgrades recommended by LSICT and implemented within client sites – e.g. the upgrade of Internet Explorer to 128 bit versions to allow access to the DfES secure site for CTF transfer and the upgrade of admin workstation operating systems to Microsoft® Windows 2000/XP to increase security and prepare for the migration of SIMS onto a SQL-based platform.

ICT Data Transfer systems within LSICT: Implemented Solution

The chosen solution differs slightly from the recommendations of previous Learning Services documentation on this subject (Evaluation of ICT Data Transfer systems within LSICT; ICT Data Transfer systems within LSICT: IPSec): this is as a result of user feedback and security improvements that have been implemented within Microsoft® Internet Information Services with the release of Microsoft® Windows Server 2003.

The previously recommended wholly-IPSec based solution, whilst ensuring security of data in transit, would have been site-based, i.e. any user authenticated in the domain 'School A' could initiate secure communication with the LSICT secure server: to restrict access to specific users would therefore have required the implementation of -

1. Further password authentication;
2. User-specific NTFS access permissions on secure server data folders.

Through conversations with school Admin Officers it became clear that the need to maintain another password (in addition to those currently required for workstation logon, SIMS, FMS, DfES transfers, LSICT website) would not be viewed favourably: this factor, in conjunction with the need for any allocated password to meet complexity requirements to be deemed secure, would have increased the possibility that the password would be written down and therefore increase the risk of security being compromised. Use of a PKI with certificates being allocated by LSICT to only specific authorised users allows -

- Greater centralisation of resource management and thus less administrative overhead;
- Greater transparency and ease of use for the school users;
- Better data security and effective auditing of secure resource access.

The implementation of user-specific NTFS access permissions on secure server data folders would have required a high degree of LSICT administration: permissions would have needed to be amended if admin staff changed job roles or schools, each site-specific secure folder would have required the maintenance of several user access control lists with these users being required to login to the LSICT domain to ensure security. Use of a PKI with certificates being allocated by LSICT to only specific authorised users allows -

- Access permissions on secure server data folders to be set more effectively, thereby reducing administrative overhead;
- Greater transparency and ease of use for the school users;
- Reduction in network traffic, thereby compensating for the overhead introduced by using a PKI.

In this case, the PKI method is being used as a way of authenticating users and allowing or denying access to secured areas – it has, however, also been selected as it will facilitate the use of data encryption if this is deemed necessary at a later date: this element of future-proofing has been another factor influencing selection.

ICT Data Transfer systems within LSICT: Implemented Solution

The solution to be implemented relies on the established secure data channel through the use of SSL, with access to the secure server across this channel being possible only if the school user has a public key supplied with a site-specific digital certificate issued by LSICT (the Certificate Authority). This public key has a corresponding unique private key which is held only by LSICT. When initiating communication, the school user supplies their public key to the LSICT secure server: if this key matches with the corresponding private key, the server is able to verify the authorised status of the school and allow access. Similarly, the school will be issued with a certificate from the Certificate Authority (CA) which contains a private key identifying the LSICT secure server: when the server initiates communication with the school, it supplies the LSICT public key. Matching the public key with the CA supplied private key enables the school user to identify that the attempted communication comes from the secure server and is therefore valid. All this interaction is invisible to the user at the school – once the relevant certificates have been installed for the necessary users. Users who are not issued with certificates will not be able to provide the necessary credentials to permit communication with the secure server.

The digital certificate is analogous to a passport - all UK passports contain a unique key, the registered passport number from the issuing authority: also included on every passport are the passport holder's credentials on the laminated information page. Any country that has agreed to accept these passports trusts that the information on the document is true as long as the passport does not seem to have been illegally altered. This means that foreign countries are relying on the UK Passport Service to ensure that the UK citizen's passport is authentic, just as the user of a public key relies on the issuer's certificate.

Public key cryptography can provide authentication instead of privacy. In Windows 2000, the receiver of the information sends a challenge. The challenge can be implemented one of two ways. In the first authentication method, a challenge to authenticate involves sending an encrypted challenge to the sender. The challenge is encrypted by the receiver, using the sender's public key. Only the corresponding private key can successfully decode the challenge. When the challenge is decoded, the sender sends the plaintext back to the receiver. This is the proof for the receiver that the sender is truly the sender.

For example, when LSICT receives a document from School A, LSICT needs to authenticate that the sender is really School A. LSICT sends an encrypted challenge to School A, using the school's public key. When School A receives the challenge, it uses its private key to decrypt the information. The decrypted challenge is then sent back to LSICT. When LSICT receives the decrypted challenge, it is convinced that the document received is truly from School A.

Rollout

Controlled testing has been carried out within school sites, however the first stage of live use is limited to the schools outlined below. This will allow the removal of potential teething problems on a much smaller scale before the system is configured in all schools throughout Hull.

Bellfield
Bricknell
Buckingham
Cleave
Endsleigh
Fifth Avenue
Frederick Holmes
Thanet

Hall Road
Kelvin Hall
Malet Lambert
Neasden
Parkstone
Spring Cottage
Trinity

ICT Data Transfer systems within LSICT: Implemented Solution

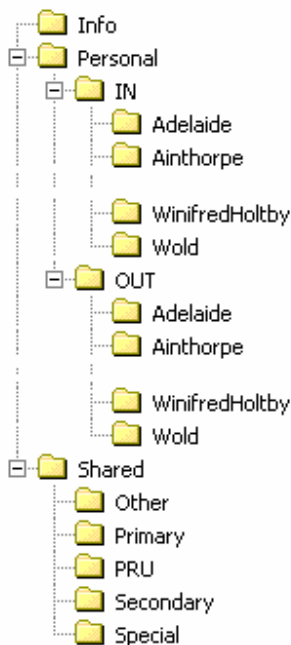
Structure

The structure of the secure area has been created as in Figure 2 below: client schools have been organised into five relevant administrative groupings (Primary, Pupil Referral Units, Secondary, Special and Other), thus providing schools with access to:

- a shared download area for LEA-wide data transfer to schools.
- individual folders for each school site, located within a folder indicating the direction of the data transfer in/from Essex House.
- A group specific download area for data transfer pertinent to school type.

This structure is of concern for administrative purposes only as the user will work with an web based interface.

Figure 2: Secure Area structure



The shared download folder is accessible to all schools, while the group folders being accessible only to their respective groups. The site-specific folders are accessible only to the relevant school, thereby ensuring greater data security and reducing administrative overhead by removing the possibility of users uploading files into the wrong areas.

This is achieved using NTFS permissions as shown below:

`\Info` = Read & Execute, List Folder Contents, Read

`\Personal\IN\schoolName` = Modify, Read & Execute, List Folder Contents, Read, Write

`\Personal\OUT\schoolName` = Read & Execute, List Folder Contents, Read

`\Shared\groupName` = Read & Execute, List Folder Contents, Read