

S.H.A.U.N

Secure Hospital Access from the University Network

A pilot project to develop secure and authenticated communications between Addenbrooke's NHS Trust and Cambridge University data networks.

January 2004

Dr. Geoffrey D. Smith BSc. PhD.
Senior Project Manager
Addenbrooke's NHS Trust IT Department
Cambridge

Copyright

All copyright to this document resides with the author and with Addenbrooke's NHS Trust. It may not be republished in any context without the written consent of the copyright holder.

Summary.

A significant number of honorary NHS consultants work primarily in offices and laboratories connected solely to the University network. The consultants often have a requirement to access patient identifiable data held on the Trust network. A methodology based on Citrix terminal server technology combined with RSA token-based two factor authentication has been successfully implemented to allow encrypted transport of data from the Trust network to the University network, satisfying the security requirements of the NHS Information Authority (NHSIA).

Introduction.

Addenbrooke's NHS Trust is a local district hospital of approximately 1000 beds, for the approximately 0.5 million people who live in the Cambridge sub-region and the surrounding district. It provides comprehensive acute and maternity services as well as some specialist tertiary referral. It also hosts an extensive research campus and is the teaching hospital for the University of Cambridge, with an annual student intake of 150 undergraduates per annum. The Clinical School and associated university research laboratories and offices are primarily hosted in the Cambridge University Data Network (CUDN).

There are approximately 400 University staff who also have honorary consultant NHS contracts who require access to patient data held on the Trust's network. At present the only approved way for these staff to access this data from their University offices and laboratories is to have either a completely separate network point installed with an associated separate PC on the Trust network or to utilise a NHSIA approved Secure Dial-up link through the Cable and Wireless gateway.

This situation has been recognised by both the NHS and HE establishments as being extremely inconvenient and wasteful on resources and a recent white paper outlining this and associated problems, together with possible generic solutions has been published. (Andrew Cormack, UKERNA. http://www.ja.net/documents/nhs_janet_architectures.pdf).

Addenbrooke's NHS Trust has undertaken an evaluation of the solution put forward for the third scenario outlined in Cormack's paper, namely use of a firewall or router to separate the two networks, an application terminal server on the trust network to provide access to the data and use of SSL to provide encrypted transport.

Factors determining chosen solution.

Following discussion with both University and Trust IT staff and also with external consultants it was decided that the terminal server solution would be based on Citrix Metaframe solution, rather Microsoft terminal server alone. This was influenced by a number of factors, not least of which were the advanced features of Citrix enabling more control of the user environment, the availability of non-Microsoft clients (Unix and Macintosh OS in particular) and an existing Citrix portal (Nfuse) for access to the terminally served resources which would be relatively easy to integrate with the security requirements. The NHSIA have a requirement for 2-factor strong authentication for access from external networks. Use of smartcards or biometrics was considered as the 2nd tier of identification in addition to domain authentication. However, this is relatively new technology and would require additional hardware to be purchased and integrated with the access stations. It was therefore decided to employ 1-time token-based RSA keys, a well-established technology that would be easy to integrate with the rest of the access system. Should there be a future requirement to migrate to a smartcard or biometric authentication mechanism, then it will be relatively easy to integrate this into the overall system, replacing only the 1-time token mechanism.

The NHSIA also require that the firewall separating the two networks be to the EAL-4 standard. Of the possible candidates, the hardware-based PIX secure firewall was chosen, primarily as it would fit best with other aspects of the network architecture employed at Addenbrookes. Since this firewall had the potential to replace the existing firewall between the Trust network and NHSNet, it therefore represented a single point of failure for a critical link. It was therefore decided that this should be implemented as a fully featured failover system even though the project was in essence to be a pilot in terms of external access.

The project requirements were put to external tender and ISC Networks chosen as the preferred supplier (www.iscnet.co.uk). This decision was based not only on cost, but also on the fact that ISC had all the necessary expertise (PIX, Citrix and RSA authentication) as in house teams, ensuring that time spent on development and integration of the components would be minimised. ISC were also able to propose a solution based on an existing development (Project Willamette) that had a number of features closely resembling the required solution.

Note: Since this project was initiated, the NFuse portal has become the Metaframe Web Interface and the functionality of project Willamette has become incorporated into the new version of the Citrix Secure Gateway.

The outline architecture of the solution is shown below in Fig. 1 together with a description of the components. (Full costings are given in Appendix 1).

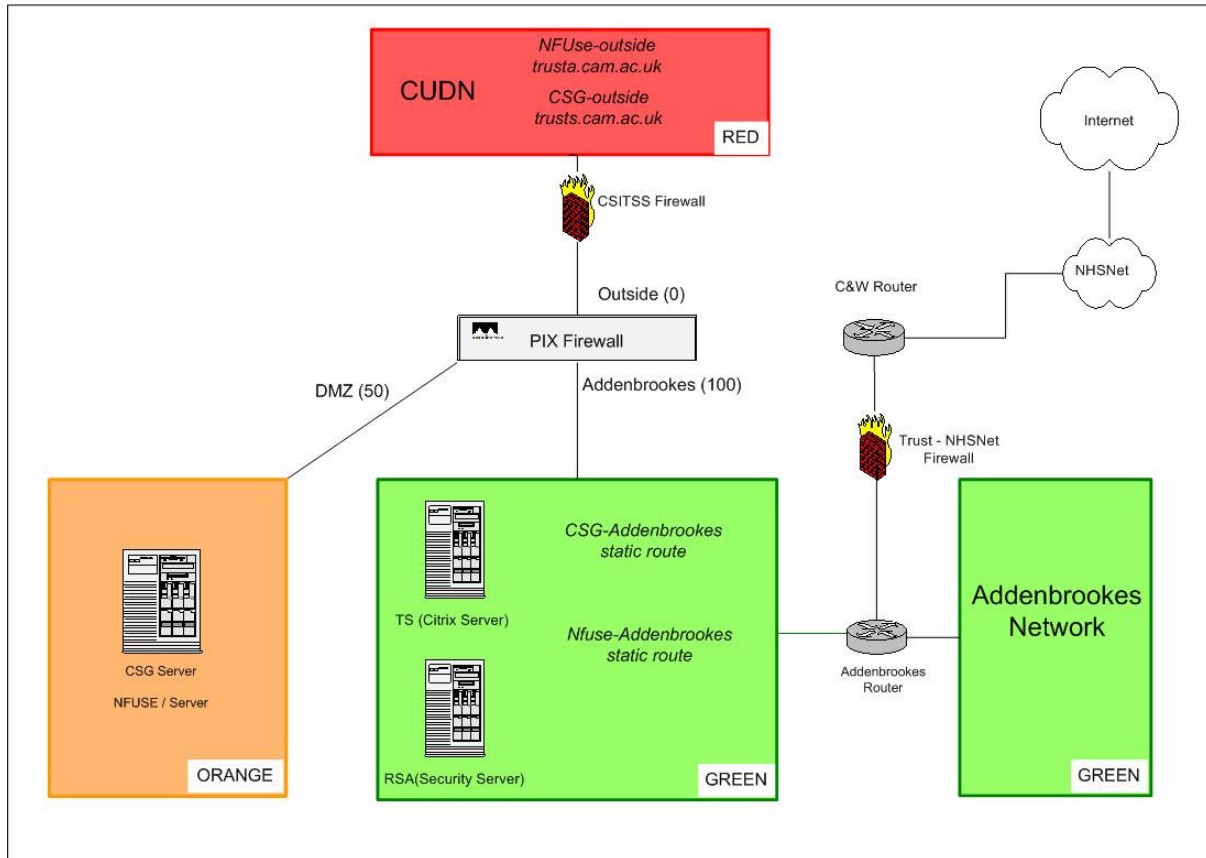


Fig 1. Network Architecture of SHAUN access system.

Areas on a green background represent the secure areas of the Trust network. The red CUDN region represents the 'untrusted' University network on the outside interface of the firewall. The CUDN is also protected from the Trust network by a second firewall, administered by the Clinical School IT support service. The Orange area represents the DMZ, which is isolated from the rest of the Trust network. Connectivity can only be established through the PIX firewall.

Components:

- PIX 515 Firewall with failover.
- Citrix based terminal server.
- RSA token-based authentication server.
- NFuse Web portal running in the DMZ. This is mapped via a static route through the firewall to an address on the Firewall outside interface. This is resolved by a FQDN on the University DNS. Only https traffic is allowed on this route.
- Citrix secure gateway (CSG) running in the DMZ. Also mapped via a static route through the firewall to an address on the Firewall outside interface. This is also resolved by a similar FQDN on the University DNS. Only https traffic is allowed on this route.
- Secure Ticket Authority (STA) running on the RSA server.

Functions of the Citrix Secure Gateway (CSG)

The Citrix Secure Gateway functions as a secure gateway between the MetaFrame servers and ICA Client workstations. All data traversing the network, between the client workstation and the CSG server, is encrypted, ensuring privacy and integrity of information flow.

The CSG provides a single point of entry, and secures access to Citrix server farm. SSL technology is used for encryption, allowing secure transfer of data across public networks.

The CSG also removes the need to publish the addresses of every MetaFrame server, simplifies server certificate management, and allows a single point of encryption and access into the MetaFrame server farm. It does this by providing a gateway that is separate from the MetaFrame servers and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls. The following benefits are achieved:

- Strong encryption (SSL V3 128-bit)
- Authentication (achieved through Nfuse and RSA/ACE)
- Internal network addresses of the MetaFrame servers are hidden
- Firewall traversal through a widely accepted port
- Single-point server certificates
- Large number of servers can be easily supported
- Separate client software is not required; the standard ICA client is sufficient

Components of the Citrix Secure Gateway.

Secure Gateway Service

This component is deployed in a Demilitarised Zone (DMZ) and provides SSL encryption as well as connection routing (gateway) functionality. This component interacts with the Secure Ticketing Authority (STA) to validate/resolve CSG tickets.

Secure Ticketing Authority (STA)

This component is responsible for generating and validating CSG Authorization tickets, as well as storing real destination addresses during ticket generation and recovering that address during ticket resolution.

Nfuse Classic

This component is based on the standard NFuse Java Object component. NFuse will request CSG Authorization tickets from the CSG Ticketing Authority during ICA file generation using STA XML protocol. Along with the ACE Client and Willamette add-in it authenticates the user who supplies an NT Userid and Password and a SecurID Passcode.

Sequence of events leading to the secure connection.

1. A user on the University network launches a Web browser session pointed at <https://trusta.cam.ac.uk> and connects to the mapped external address of the NFuse Webserver on port 443 (https) as presented by the outside interface of the PIX.
2. The NFuse Web portal requires the user to authenticate using strong authentication, ie the user is required to enter Username, Domain Password & Passcode generated from the users PIN and the code presented by the RSA token.
3. The ACE client on the NFuse portal sends a request to the RSA server to authenticate the user against the NT domain and the secure token passcode
4. If authenticated by ACE, the users domain credentials are then presented to the XML listener running on a MetaFrame server (port 8080), the XML service then returns a list of the published applications that the user can have. The NFuse server then creates a web page specific to that user with hyperlinks to their applications within it.
5. When the user selects an application, the NFuse server requests that the STA (Secure Ticketing Authority) issue a 'ticket' for that user, ensuring that their credentials are no longer required. The NFuse server also requests the XML service on the MetaFrame servers provide a MetaFrame Ticket relating to the application – these are both used to create the ICA file which details the application session information – the Citrix servers' real IP address which would normally appear in this file is replaced with the external IP address of the CSG server
6. The browser passes the ICA file to the ICA client , which launches an SSL connection to the CSG server. Initial SSL handshaking is performed to establish the identity of the Secure Gateway Server.
7. The Secure Gateway Server accepts the ticket from the ICA client and uses information contained in the Secure Gateway ticket to identify and contact the STA for ticket validation.
8. If the STA is able to validate the ticket, it returns the IP address of the MetaFrame server on which the requested application resides. If the ticket is invalid, or has expired, the STA informs the Secure Gateway server, and an error message is displayed on the ICA Client device
9. On receipt of the IP address for the MetaFrame server, the Secure Gateway server establishes an ICA connection to the MetaFrame server. After the ICA connection is established, the Secure Gateway server monitors ICA data flowing through the connection, and encrypts and decrypts client-server communications.

The communications routes for this process are represented in Fig. 2 below.

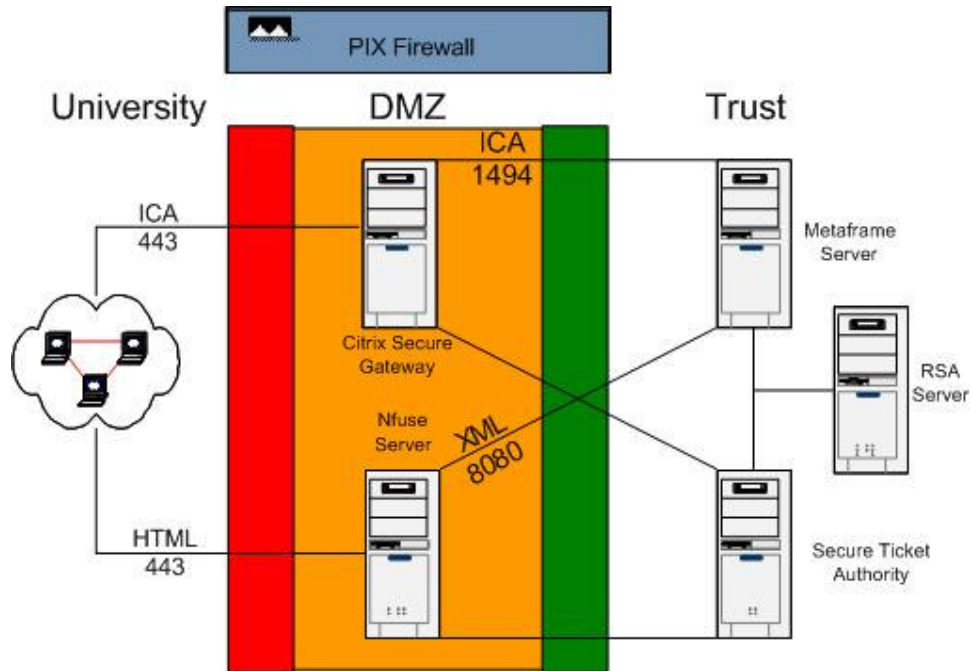


Fig. 2 Communications routes between the different elements of SHAUN together with the message protocols and ports used.

Intrusion Detection (IDS)

The Cisco PIX provides a subset of the Cisco Intrusion Detection System. This is being used in conjunction with 'syslogger' software to provide email-based notification of possible attacks on the firewall.

Time scale for Implementation.

The implementation consultants (ISC Networks) budgeted for 7-man days for the implementation, this to include documentation of the project to facilitate technology transfer. Hardware configuration and initial software (Citrix and RSA) installation was carried out in 1 working day utilising 3 x ISC consultants, specialising in Citrix, PIX and RSA technologies respectively. Further configuration, in particular of the firewall took place over the next 10 working days, partly with consultants on site and partly with IT staff responding to remote communications. Internal testing in close collaboration with University staff was carried out for a further 10 working days before enrolling a small number of relatively IT-enthusiastic users for a 3-month trial.

Policies and Procedures. - BS7799 Gap analysis.

One of the essential ingredients of a secure access system are the administrative policies and procedures that are put in place. To this end we have commissioned a BS7799 analysis of the access procedure, the results of which will be used to formulate the appropriate policies and procedures. It is hoped that the resultant policies and procedures together with the SHAUN architecture will be made available by the NHSIA as a baseline model that can be adapted to other Trust / University modalities.

Problems

No major problems were encountered in the initial implementation. Server identification certificates are required for both NFuse and CSG servers. Addenbrooke's maintains its own certificate authority and issued its own certificates for the servers concerned. This then requires that each terminal from which SHAUN is used, have the Addenbrooke's CA root certificate stored in the trusted root certificate store of either the current user or the machine. This is not a problem for workstations running MS-Windows operating systems but has proved to be troublesome for users wishing access via the MacIntosh platform. If server certificates are obtained from Verisign or other major certificate authorities, these are built into the base operating systems and the root authorities automatically recognised. The MacIntosh platform additionally showed problems concerning the automatic installation of the Citrix client software. These issues can be addressed to provide a workable MacIntosh platform and solutions are discussed in Appendix 2.

Of more concern is the suitability of this solution to one particular group of users. Typical of this group are consultants of the university-based histopathology department. They informed us that their working practices require them to be logged-on in continuous sessions, referring to clinical data whilst observing tissue sections and writing reports. Terminal server sessions are designed primarily for sharing resources and are geared towards users connecting, performing their tasks and then disconnecting, freeing resources for other users. In view of the limited resources of this pilot, we set the Citrix server operating parameters to automatically logoff the connection if no keyboard activity was detected in a 10 min period. Histopathology informed us that this is too disruptive to their working practices. It has been proposed that they fund a separate Citrix server, which just serves their department and has no inactivity limit imposed. Technically this would work, but it may be more cost effective to utilise the broadband secure VPN solution that will shortly be available from Cable & Wireless. The VPN connection is rather better suited to a long period of connection to resources than the terminal server solution.

A further issue concerns enrolment, administration and support of a SHAUN solution. Enrolment and administration of tokens is clearly the responsibility of the Trust IT department. However, the workstations from which access is made, sit on the University network and have University IP addresses. It is clearly not appropriate for Trust IT department to perform the set up of these workstations, which requires administrative privileges. When a fault occurs, it is not easy to determine who has responsibility for 1st line support. It may not be at all clear whose network might be at fault, if it is a problem with the workstations O/S, the Citrix server on the Trust network or the HISS data system which at Addenbrooke's is hosted and supported remotely. It is clear that these are not trivial management issues and require close cooperation between the IT support teams of both networks.

Proposed Extension to SHAUN architecture for broadband access.

Initial design criteria for the SHAUN usage were directed at the requirements of hospital consultants accessing the Trust IT-based resources whilst physically located on the University network. However, this group also often find themselves in the 'on-call' situation, and if given access to test results etc can give professional advice over the telephone. Similarly, IT department staff are often placed in on-call situations where the ability to deal with problems from the home base is required. At present Addenbrooke's staff utilise a Cable & Wireless secure dial-up procedure to achieve this. However there is no inherent difference in accessing the Trust network from the Internet as opposed to accessing it from the University network. We therefore propose that the SHAUN access system might be extended as illustrated in Fig 3 to enable secure access from the Internet as well as the University.

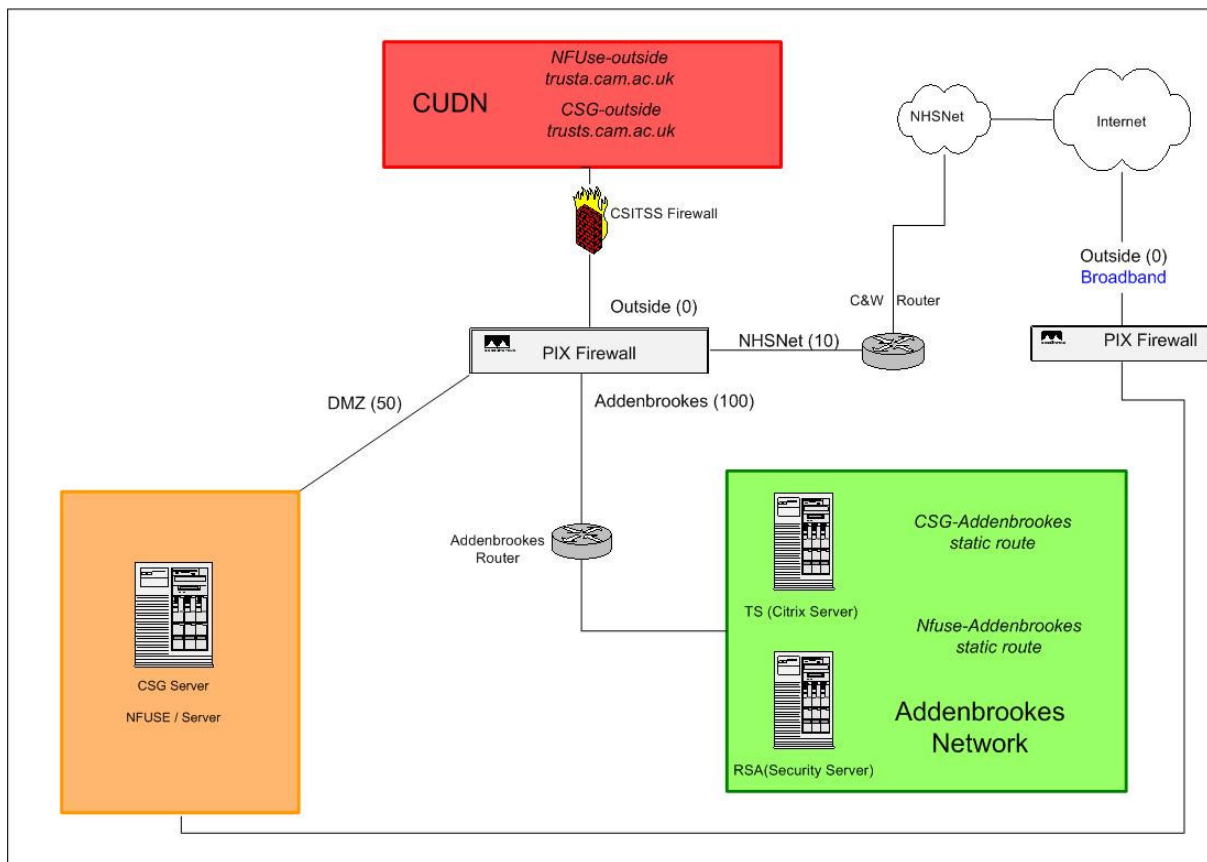


Fig. 3. Extension to SHAUN architecture to allow broadband access. In this illustration the central PIX firewall is also being used to provide security on the NHSNet link.

The extension involves an additional PIX firewall, the inside interface of which is connected to the DMZ of the SHAUN system, the outside interface is connected to the internet via a commercial ISP, providing a fixed IP address mapped to this interface. Two further external addresses are required from the ISP to be statically routed through the secondary PIX to the NFuse server and Citrix secure gateway in the DMZ. These static routes only allow https traffic (tcp 443) to these two specific addresses. All other protocols and ports are denied access. It would be possible to obtain the necessary firewalled access to the internet via an additional interface added to the central PIX (the PIX 515 can

hold a total of 6 interfaces). However, we feel that usage of a secondary PIX provides not only an additional barrier to potential compromise of security, but also makes for easier management both in terms of access control and system logging. This access methodology will provide the same access route whether the user is on standard POTS link or DSL/cable broadband. If a SHAUN type access system is already installed for access from a university network, then secure internet access via the SHAUN extension represents considerable cost savings over the secure dial-up or secure VPN broadband solutions offered by Cable & Wireless. Additionally, if access is by standard POTS modem, the underlying terminal server methodology gives much more responsive access.

Appendix 1. Costs (excluding VAT)

Cisco PIX 515 firewall, failover chassis, additional interface for DMZ	£6304
Citrix Metaframe Xpe 20 User Starter Pack	£4055
RSA ACE server, 50 user licences, 50 x 6 digit, 36-month tokens	£9985
2 Compaq / HP servers for Citrix and RSA	£6135
External consultancy and planning	£5950
Total	£32429

Appendix 2. Connectivity issues for MacIntosh platforms.

The SHAUN project utilises browser technology as the initial connectivity medium and a multi-platform ICA client for display of the Citrix desktop. It should therefore be usable on a MacIntosh platform. However several problems quickly became apparent when SHAUN was trialled under both MacIntosh OS9 and OS-X.

- 1) Authentication of the NFuse and CSG servers requires that the root certificate for the Certificate Authority (CA) be recognised by the client platform. If this is not one of the standard companies, eg Verisign, then the CA's root certificate has to be installed. This does not seem to be possible with the MacIntosh version of IE. It is possible with Netscape, Mozilla and Safari clients.
- 2) The ica client is launched through a file called 'launch.asp'. This introduces three more problems.
 - a. In some versions of the OS and with some browsers, the asp extension is used for the apple system profiler and thus will behave incorrectly when asked to execute this file. There is a fix for this on the Citrix site.
 - b. The safari browser will not automatically execute file types that are not in it's 'approved list'. This list does not include asp files and therefore the ica client does not start automatically with this browser and must be initiated by clicking on the file copy stored on the desktop.
 - c. The launch.asp file contains a specific reference to the CA root certificate as myroot.crt. If a local CA is used to generate the server certificates, then a copy of the CA's root certificate must be placed in the Citrix keystore and renamed as myroot.crt.
- 3) Irrespective of which browser is used, each time an icon on the NFuse desktop representing a published Citrix application is clicked, it will leave a shortcut to launch.asp on the Mac desktop. To minimise this, it is recommended that the only icon on the NFuse desktop is a shortcut to the main Citrix desktop. In this case only one copy of the launch.asp shortcut will be left on the MacIntosh desktop for each complete SHAUN session.