

## JISC DEVELOPMENT PROGRAMMES

### Project Document Cover Sheet

#### FINAL REPORT

#### WORKPACKAGE 3 : SHIBBOLETH and NHS WALES

#### Project

<b>Project Acronym</b>	ASMIMA	<b>Project ID</b>	
<b>Project Title</b>	Adoption of Shibboleth for Multiple Identity Management Applications		
<b>Start Date</b>	April 2005	<b>End Date</b>	March 2006
<b>Lead Institution</b>	Cardiff University		
<b>Project Director</b>	Hugh Beedie		
<b>Project Manager &amp; contact details</b>	Joan Wright <a href="mailto:wright@cardiff.ac.uk">wright@cardiff.ac.uk</a> 029 2087 4496		
<b>Partner Institutions</b>	n/a		
<b>Project Web URL</b>	<a href="http://www.cardiff.ac.uk/insrv/shibboleth/">http://www.cardiff.ac.uk/insrv/shibboleth/</a>		
<b>Programme Name (and number)</b>	JISC Core Middleware Programme (Shibboleth Early Adopters)		
<b>Programme Manager</b>	Nicole Harris		

#### Document

<b>Document Title</b>	Workpackage 3 : Shibboleth and NHS Wales		
<b>Reporting Period</b>	November 2005 – May 2006		
<b>Author(s) &amp; project role</b>	Rhys Smith, IT Officer		
<b>Date</b>	9 June 2006	<b>Filename</b>	WP3 Shibboleth and NHS Wales.rtf
<b>URL</b>			
<b>Access</b>	<input type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

#### Document History

Version	Date	Comments
1.0	9 June 2006	Completed report sent to JISC

## **Work Package 3 – Shibboleth and NHS Wales**

### **A1.2.1 Introduction**

Cardiff University (CU) has a strong connection with NHS Wales via its University Hospital of Wales site and elsewhere. It has regular contact with two NHS Trusts: Cardiff & Vale Trust, through the University Hospital of Wales site, and the Velindre Trust, through Velindre Hospital and elsewhere.

CU has some personnel that are both members of CU (staff and students) and members of one of the two trusts, and are therefore entitled to access both CU and NHS resources: CU resources usually sitting on the CU network and internet, and NHS resources usually sitting on NHSnet and the internet.

The initial method used which allowed joint CU/NHS personnel to access both types of resources was simply have two computers on their desk, one connected to a CU network outlet and one connected to a NHS network outlet. This is obviously an inelegant solution to the problem.

In an attempt to improve this situation, the All Wales Citrix Service was implemented, using technology from Citrix Systems Inc. This service allows CU members to gain access to the CU network from off-campus, and therefore to resources that are restricted to users on the CU network.

However, a solution for access the other way – i.e. to access NHS resources from outside the NHS network has not yet been implemented; the only way to access these resources currently is to use a computer directly on the NHS network. Such a solution is highly desirable.

The aim of this work package is to explore practical solutions for assuring secure and accurate access for joint CU/NHS personnel to all resources they are entitled to.

### **A1.2.2 Background**

#### **Cardiff University**

Cardiff University is one of Britain's major teaching and research universities, and is a member of the Russell Group of premier UK universities. Located in the centre of the capital city of Wales, it has an international reputation for the quality of its work and a mission to be a world class research-led institution and a centre of excellence in its teaching. CU recently merged with the University of Wales College of Medicine (UWCM), resulting in an institution now comprised of approximately 5,000 staff and 22,000 students spread across 28 academic schools and 5 administrative directorates.

CU's Directorate of Information Services (INSRV) is a division of CU that aims to deliver superior computer, library and media services that make a distinctive contribution to CU's research, learning, teaching, community activities and administration functions.

#### **NHS Wales**

NHS Wales is a separate entity to NHS England, with different strategies and policies (though these often converge). NHS Wales' strategy is led by the Welsh Assembly under a programme named "Informing Healthcare" (IHC). IHC intends to improve healthcare in Wales by making better use of information and technology. A key IHC project was Access To Knowledge (A2K). A2K was a project working to ensure healthcare staff in Wales have easy access to healthcare knowledge and evidence, and have the tools they require to retrieve such evidence. Healthcare staff in hospitals, GP surgeries and NHS Dental practices will be able to electronically access the latest and the best evidence to support them as they care for patients. The A2K project was, however, terminated 11 months early in May 2006 under orders of the Welsh Assembly. The A2K project was responsible for consolidating the National e-Library for Wales, which increased the number of electronic

resources available to NHS personnel, which consequently saw NHS Wales Athens usage roughly quadruple within one year<sup>1</sup>.

The Cardiff & Vale NHS Trust is the largest NHS Trust in Wales and one of the largest in the UK. It provides day to day health services to a population of around 500,000 people living in Cardiff and the Vale of Glamorgan who need hospital treatment, mental health care, care for elderly people and children as well as a growing range of community-based services, including specialist dental services, and new therapies as alternatives to hospital admission.

The Velindre NHS Trust, headquartered in Cardiff, was established in 1994 and has steadily grown to manage a budget of over £130M in 2004/05 and provides a range of specialist services at local, regional and all Wales levels. The Trust comprises of a variety of Divisions who specialise in services as diverse as caring for cancer patients in Velindre Hospital to managing the Digital All Wales Network for NHS Wales from Health Solutions Wales in Brunel House.

### **NHS-HE Connectivity Project - NHS-HE Forum**

The NHS-HE Forum was set up in 2001 for IT and networking managers from both the NHS and Higher Education, with an interest in achieving two-way communication between NHSNet and JANET, the network for education and research, managed by UKERNA.

It meets twice a year to discuss case studies and best practice by Medical and Health Sciences Schools, Universities and NHS Trusts. The meetings focus on enabling two-way integration between the NHS and HE networks and the Forum promotes electronic access to medical content via journals, knowledge databases and papers through secure anytime, anyplace and anywhere access.

Through the NHS-HE Forum, Phil Leahy, Business Development Manager, Eduserv Athens Access Management, is leading the Athens Account Linking Project in collaboration with the JISC NHS-HE Procurement Group. The purpose of this project is to allow NHS staff with joint NHS and HE status to have full access to all their e-resources from whatever login account they are using. A healthy number of HE and NHS bodies are keen to act as pilot sites in this project.

### **NHS-HE Connectivity Project - N3 JANET Gateway Working Group**

The working Group is a collaboration between the NHS and UKERNA and was set up in the summer of 2005 to examine the potential and take forward the proposal that one or more network gateways should be created between the new NHS network in England, N3, and the Joint Academic Network, JANET and is currently developing a pilot proposal for a 'national' gateway.

Although the main focus is on the N3 Gateway(s) in England, Scotland has its own N3 contract and it is also hoped that any gateway will assist the whole of the UK, including Wales.

The activities of the NHS-HE Forum are being more widely broadcast and the Forum has its own website at <http://www.nhs-he.org.uk/> and recently its own JISCMail discussion Forum at <http://www.jiscmail.ac.uk/lists/NHS-HE-FORUM.html>

## **A1.2.3 Aims and Objectives**

The main aims and objectives for this Work Package were to:

1. Develop a working prototype implementation giving improved access-control for joint CU/NHS staff to restricted resources on the NHS network;
2. Document the prototype system and a detailed report on its development.

---

<sup>1</sup> Access to Knowledge: comments from health library & information staff, Project Board meeting 26th May 2006

## A1.2.4 Implementation

### Initial steps

The first action taken in this work package was to explore many avenues of communication with NHS Wales, attempting to contact relevant people. This action was met with limited success – we managed to quickly set up meetings with personnel who were very helpful, but who turned out to not be key personnel able to help us move the work forward. The major issue highlighted here is that when working with the NHS, finding out who “relevant” people actually are is a major task in of itself.

The first person we met up with was Bernadette Coles, librarian for Velindre Trust and a Cardiff University member of staff: one of the members of staff having the problem highlighted by this work package. Bernadette introduced us to the resources available through the Velindre Trust, which included the “Health of Wales Information Portal” (HOWIS), and a small collection of Athens resources. HOWIS has an outward facing internet presence aspect<sup>2</sup> containing public information, and an inward facing (to the NHS network) intranet presence aspect containing additional internal information.

We realised here that we instantly had two types of resources where federated access management would be an ideal solution to solving access problems across domains. Firstly, we thought we could score a quick win by adding Velindre Athens resources to the Cardiff University Athens resource set and adding a “Velindre” entitlement attribute to joint CU/Velindre trust personnel (thus giving joint staff access to both CU and Velindre resources); secondly, the HOWIS portal would be an ideal target to shibbolise, as it is a fairly simple web portal with an intranet aspect that joint members of staff would like to be able to use from off the NHS network – and does not contain patient records. This left us with two tasks – seeking permission from the Velindre Trust and Athens to add Velindre resources to the CU Athens permission set; and meeting with someone who managed the HOWIS portal.

### Velindre and Athens resources

This first task was accomplished quickly, however, the result was not what we were hoping. Firstly, the ASMIMA project wrote to the Chief Executive of the Velindre Trust, explaining the nature of our project and our ideas. The response we received was positive in nature, indicating the Velindre Trust was willing to work with us on improving access management techniques, however, the precise details of the request were slightly misunderstood. We then realised that neither CU, Velindre or Athens had the right to assign Velindre resources to the CU Athens permission sets according to Athens licensing terms – permission would have to be sought from the publishers of each resource directly. This idea was abandoned for now due to the effort that task would entail.

### Meeting with HSW

To accomplish our second task, we met up with Steve Finn from Health Solutions Wales (HSW), a division of Velindre Trust that manages NHS Wales IT resources, including the HOWIS portal. Steve Finn is the Web Services Manager and Athens administrator for HSW. He was very interested in Shibboleth, and left out meeting with a working knowledge of federated access management and how it could fit in with his resources. He left us with a recommendation that we should pursue our enquiries further up the NHS chain, as such a big project as enabling federated access management with the NHS would need support from high up.

In another development supporting this avenue of exploration, the University Librarian, Janet Peters, was a member of the (now defunct) A2K Project Board and at a meeting raised the aims of our project; in particular the needs of medical students and joint University/NHS staff. The advice from the A2K project was that these issues should be discussed with the senior members of the IHC Programme.

---

2 <http://www.wales.nhs.uk/>

Thus, we decided to follow this advice and attempted to set up a meeting with senior IHC personnel.

### **CU Dental School**

Meanwhile, whilst we were attempting to set up this meeting, we also had discussions with the CU Dental School. They have a requirement for CU staff who are honorary consultants and specialist registrars to access the Cardiff & Vale Trust Clinical Portal from the CU network. Two solutions are under consideration:

- Implement a Citrix Service similar to the All Wales Citrix service but in reverse. Permission for this is already in place but the costs are expected to be high;
- Implement a secure proxy server (EZproxy, which has inbuilt native Shibboleth support) to access the NHS network. This is a lower cost solution but would require political agreement.

We are advising the use of the secure proxy server option as it has a greater cost-benefit ratio. The document produced and passed to the Dental School is attached to this document, in Appendix 2.

### **Meeting IHC**

By now, after much legwork, our attempt to set up a meeting with IHC staff had been successful, and a meeting was conducted.

Our understanding at this point of NHS Wales strategy for access management was this: the technical architects at IHC had investigated Shibboleth and concluded it was as good, if not a better, strategic option for sign-on access to the NHS e-library per se (but that would need to be confirmed by a strategic assessment). However, they were looking for one integrated solution to solve all of their access management needs and in their assessment so far Shibboleth was deemed unlikely to be sophisticated enough for individual health record single sign on, so they decided to not progress with it. The (now defunct) A2K project which managed the NHS e-library was using Classic Athens for access to its e-library portal.

At the IHC meeting, we met two extremely relevant people – John Sluiter and Robin Mann. John Sluiter is chief strategist for NHS Wales on security and access management, and Robin Mann is a project manager. In this meeting we discovered the following pertinent information:

- NHS Wales strategy differs from NHS England strategy;
- The IHC programme is developing a single-sign on authentication for the individual health record, which will use Smartcard technology;
- This single sign-on will invoke a series of further permissions, one of which is the electronic resources in the/ an national e-library.

We passed on the view to IHC that they should give greater consideration to the role of Shibboleth as a component of access management, rather than considering it as an all encompassing access-management solution in of itself, and that running a small pilot project to show the capabilities of federated access management would be a good idea. IHC were very interested in this idea and asked us to provide a short written brief for them on this. This brief is attached in Appendix 1.

We have since received a response from IHC stating that the document was very useful, and it is being passed onto the Clinical Director for IHC (copied to the head of Health Informatics Development for IHC, and the ex-A2K project manager) with a recommendation to pursue this further, as the Shibboleth security model appears to be in keeping with their proposed approach. They recognise that the NHS/academia staff issue is an important piece of work and an important problem to resolve, and that our project is an appropriate approach to testing a solution. We at CU are delighted with this response from IHC, as it is an enormous step forward in possibly future interoperability between Academia and Health information systems. Another meeting to discuss how to take this to the next step and implement our ideas is currently being set up.

## NHS-HE Forum

Finally, David Harrison (Assistant Director, INSRV) and Carol Leonard (Principal Consultant & User Enablement Manager INSRV) attended the recent meeting of the NHS-HE forum. Carol focused on 'Building upon Collaboration', which included an overview of the Shibboleth project at Cardiff, our extensive links with the NHS, and our requirement for co-ordination between development teams so that we understand each others approaches, and can identify possible areas for collaboration as we move towards joint access and interoperability between HE and the NHS. The Shibboleth driven 'proof of concept' proposal for access to e-resources, our discussions with IHC and our desire for policy clearance to enable us to enter into dialogue with NHS Trusts throughout Wales was emphasised.

Points highlighted were that the ASMIMA project had raised not only policy questions but also questions of a non-technical nature. This gave rise to the formation of a working group (the MCE Working Group) with a remit to make recommendations to the University on those groups of staff and students (particularly those with a dual University and NHS role including honorary contract holders) who legitimately should be given membership of Cardiff University.

Carol outlined the work of this group and the progress made to date on categorisation/entitlement, and also covered licensing issues and the mechanisms required to provide data feeds into Cardiff University systems from diverse communities together with procedures that need to be put in place to enable all of the above to happen.

At the end of the presentation Carol and David were thanked by the Chair for their great contribution to the Forum meeting and the Chair highlighted that both the all Wales public network, the implications of Shibboleth and the work of the MCE Working Group, where Cardiff appeared to be leading the way, were very relevant and of much interest to the attendees as signalling paths for others to follow.

Many questions/comments were raised, followed by a show of hands indicating commonality and in support of the work of the MCE Group which was considered to be of great relevance to all.

## A1.2.5 Outcomes and Results

The outcomes of this Work Package were:

1. A proposal has been submitted to the Dental School of CU/NHS to implement a pilot Shibboleth compliant proxy server (EZproxy) to access resources (specifically the Dental School Clinical Portal) on the NHS network;
2. An idea on how to share Athens resources between NHS trusts and academic establishments, (e.g. the Velindre Trust and CU) by adding the NHS trust's resources to the academic establishment's permission set, and the academic establishment adding an entitlement attribute to relevant join personnel was formulated. However, this would require permission from the publishers of each resource, or a change in the Athens agreements to allow this to be done;
3. A proposal has been submitted to the NHS Wales Informing Healthcare programme to begin discussions aimed at exploring the use of federated identity management to help with accessing NHS resources from off the NHS network; this proposal has been accepted and had a recommendation to pursue the proposal further. A meeting is currently being set up to take this proposal to the next level – implementation. This is an enormously positive step forward!;
4. If this pilot project we have suggested goes well, then we may have helped influence NHS Wales plans with regards to access management to interoperate with the developments in the UK education sector by embracing the idea of federated access management.

### **A1.2.6 Lessons Learned**

During the progress of this work package we have learned several important lessons.

Firstly, a major administrative lesson learned is that dealing with the NHS is hard work: it takes a significant amount of time and effort both to identify relevant people within the organisation to talk to and to then set up a meeting with them. Perseverance is the only answer to this problem!

If a member of staff/student is both a member of an education institution and an NHS trust, both with their own Athens resources, it would be technically fairly straightforward to enable the user to access all resources they are entitled to, however, it would need either a political/legal agreement from the individual publishers or a change in the Athens agreements. It could work by adding the NHS trust's resources to the academic establishment's permission set, and the academic establishment adding an entitlement attribute to relevant join personnel.

The NHS controls access to its internal network very tightly – and rightly so, as it contains highly personal patient information. This, however, means that interoperating with resources on the network, whether they have patient information on or not, is very difficult to do and requires a lot of political agreement and technical setup.

We consider THE major lesson learned as an outcome of the work package to be learning that NHS Wales strategy regarding access management is still in the process of being defined, and that we have a excellent opportunity to influence these decisions as they are being made.

### **A1.2.7 Conclusions**

We at CU feel that this Work Package, while not fulfilling the original aims and objectives defined at the beginning of the project, has nevertheless been a great success. Underestimating the difficulty of working with the NHS was the major downfall in not achieving these objectives.

We have, however, explored several areas where we can make access to NHS resources for joint CU/NHS staff/students easier, and we made highly important headway in relations with the NHS, and our proposal to the NHS to explore a pilot implementation of accessing NHS resources through a federated access management approach has been accepted. This is a vitally important first step in the drive towards making the experience of accessing all resources a particular user is entitled to access as friendly, transparent and useful, as possible.

The problem of joint Academic/NHS staff/students currently not being able to access all resources they are entitled to is a problem encountered further afield than just Cardiff University, and was informally agreed to be the biggest problem facing Academia/NHS relations at the moment at the recent NHS-HE Forum meeting.

## Appendix 1 – Document given to IHC outlining our project and ideas

# Cardiff University, NHS Wales and Federated Access Management Proposal

### ***The need for Federated Access Management***

Cardiff University (CU) has staff and students who are members of both CU and the NHS Trust and may therefore be entitled to access resources on both networks. However, many CU resources are only accessible via the CU network and the same rule applies to NHS resources and, since a single computer may only have permission to connect to one network at any one time, access to resources for joint staff and students is often restricted.

Historically, the method used by joint CU/NHS staff and students to access both networks was to have two computers on a desk with one connected to a CU network outlet and one connected to a NHS Trust network outlet. This is obviously an inelegant and inconvenient way of working.

In an attempt to resolve this situation, the All Wales Citrix Service was implemented to facilitate web access to CU networked resources for CU staff and students from off-campus and NHS locations.

A reverse solution i.e. access to NHS resources for CU staff and students from a computer not directly connected to the NHS network is desirable.

A possible solution is achievable through the use of newly emerging Federated Access Management techniques. This consists of building a trust relationship between Identity Providers (organisations where users require access to electronic resources) and Service Providers (organisations with electronic resources they wish to make available to users).

Responsibility for authentication is devolved to a user's home institution and establishes authorisation through the secure exchange of information (known as attributes) between the two parties.

The need for trust leads to the concept of federations. Federations are groups of similar organisations such as universities who have agreed to a common set of policies. They are typically being established at a national level. The UK's access management federation for educational organisations will be based on a technology called "Shibboleth" and will be run by UKERNA on the behalf of the JISC (Joint Information Systems Committee) and is due to be launched in July 2006. Under orders of the DfES, this will be the national federation for all UK educational establishments – Higher Education, Further Education, and Schools.

### ***Cardiff University's Proposal***

CU has extensive links and liaison channels with the NHS throughout Wales and would like to enter into a dialogue with NHS Wales to resolve the issue of access to NHS resources from a computer not directly connected to the NHS network for joint CU/NHS staff and students. We consider that dialogue should centre around (but not be limited to) a federated access management (using Shibboleth technology) solution, to provide benefit for staff and students within the academic community and the NHS in Wales:

Long term, a full federated access management implementation would allow staff and students of the wider academic and the NHS communities easy access to electronic resources, irrespective of their physical location.

Short term, we believe that a small pilot implementation of Shibboleth for one or two NHS resources would be of great benefit on two fronts. First, the immediate benefit to selected CU/NHS staff and students, able to access resources chosen for the pilot when not on the NHS network. Secondly, a pilot project, if successful, would give NHS and CU staff and students experience in

federated identity access management between the two different organisations, an experience which may prove invaluable when considering future interoperability between education establishments and the NHS as the whole UK Education sector adopts Shibboleth over the coming few years.

We feel that a suitable resource for such a pilot project would be the HOWIS portal to NHS Wales

Ultimately, CU is hoping that the dialogue opened between CU and NHS Wales may lead to collaboration on implementing such a pilot project which would only require support (not funding) from NHS Wales and time from the appropriate personnel. This support could either be direct support from Informing Healthcare, or simply the backing and approval from Informing Healthcare to enable us to enter into direct dialogue with the relevant NHS Trusts hosting electronic resources.

## ***Further Information***

### **Shibboleth**

Shibboleth is an initiative to develop an open, standards-based solution to meet the needs for organisations to exchange information about their users in a secure, and privacy-preserving manner.

The initiative is facilitated by Internet2, a US consortium of 207 universities partnered with industry and government, and a group of leading campus middleware architects from member schools and corporate partners (such as IBM and Sun Microsystems).

The organisations that may want to exchange information include higher education, their partners, digital content providers, government agencies, etc. The purpose of the exchange is typically to determine if a person using a web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla) has the permissions to access a resource at a target resource based on information such as being a member of an institution or a particular class.

Shibboleth does not carry out authentication itself but defines a set of protocols for the secure passing of identity information between institutions and service providers. It relies on the institution to establish identity and on the service provider to confirm access rights, given information about institutional affiliation. It is written in SAML (Security Assertion Markup Language), an international standard developed by the OASIS Security Services Technical Committee.

How authentication is carried out by the institution, and how rights management is carried out by the service provider is left up to the respective parties. In so doing, Shibboleth depends on a certain level of trust. Service providers need to be confident that the institution or organisation that the user belongs to has a robust and up-to-date authentication system in place.

This need for trust leads to the concept of federations. Federations are groups of similar organisations such as universities, who have agreed to a common set of policies. They are typically being established at a national level.

The USA, Australia and a number of European countries, including Switzerland, Finland and the Netherlands have already adopted a Federated Access Management technology known as “Shibboleth” or are in the process of doing so. A number of commercial service providers are planning to create interfaces to their services using Shibboleth technology or already provide them.

For example, US higher education has established a federation known as InCommon. The equivalent in Switzerland is known as SWITCHaai and in Finland as HAKA. The UK access management federation will be run by UKERNA, building on the experiences of a successful pilot federation. The pilot federation is available to join now, and members will be seamlessly migrated to the new UK access management federation on its launch in July 2006.

The JISC UK access management federation will ultimately be the national federation for all UK educational establishments – Higher Education, Further Education, and Schools.

## **Cardiff University and Shibboleth**

The ASMIMA project is a JISC Core Middleware Early Adopter project undertaken by CU where the main aim of the project was to explore the implementation of Shibboleth as a next generation method of access management to remote resources.

CU is a major user of the JISC funded Athens Access Management System (AMS), which controls access to web-based subscription services, with over a million CU logins to the Athens service each year. The current Classic Athens service is a centralised repository of user accounts and credentials which is managed at a local level, and management of these accounts is a substantial administrative workload. In an effort to solve this problem, CU became an early adopter of the next generation of AMS – Shibboleth. This is especially important as JISC are going to stop funding the Classic Athens service as of July 2008. To continue to use the service, educational institutions will have to pay up to £0.50 per user – this would cost CU approximately £13,500 per year.

Implementing Shibboleth as an early adopter has been very useful to CU. We have implemented a pilot Shibboleth Identity Provider and are moving to turn this into a production service in time for the next academic session (September 2006). Allowing our users to access resources through Shibboleth rather than the Classic Athens service will considerably ease the administrative burden which is currently placed on CU. Also, Shibboleth will make access remote resources easier for our users, as they will have one less username and password to remember. Easier access will also increase awareness of the range of resources available to them.

## Appendix 2 – Quote provided to CU Dental School

# Improved Access Management possibilities for joint Cardiff University/NHS members of the Dental School.

### *Executive Summary*

*This document explores the possibilities for improved access management for joint Cardiff University (CU) and NHS staff and students of the Dental School. Several options are discussed, with various levels of complexity, price, and value.*

*Our final recommendation is that the solution that offers the most benefit for the least cost would be to implement a secure proxy server on the Cardiff & Value Trust network that allows specific personnel to access specific Dental School resources. The estimated cost for this solution would be £11,247 for three years (exc. VAT, including all setup, recurring and support costs over the three year period), and would allow joint CU/NHS Dental School personnel using a computer on the CU network to achieve access to specified internal Dental School services that can currently only be accessed from a machine on the Cardiff & Vale Trust network (note that those services that require a further authentication step (e.g. logging into the PACS2 application with PACS2 username/password) will still require that extra step).*

## **1. Introduction**

This document aims to outline the current Access Management Systems (AMS) in use in the Dental School, and provide advice on the possibilities available to improve access for members of the Dental School who are members of both Cardiff University (CU) and the National Health Service (NHS) by allowing these members to access NHS resources using their CU credentials.

The intended audience for this document are members of the Dental School and members of Information Services (INSRV).

Please note that all quotes given in this document are exclusive of VAT, and are estimates. Full and final quotes for specific solutions described can be provided upon request.

## **2. Background**

CU has a strong connection with the NHS via its University Hospital of Wales site and elsewhere. Some members of staff in the University Hospital of Wales are members of both CU and the NHS, and are therefore entitled to access both CU and NHS resources: CU resources usually sitting on the CU network and internet, and NHS resources usually sitting on NHSnet and the internet.

The initial method used which allowed these joint members to access both types of resources was simply to have two computers on their desk, one connected to a CU network outlet and one connected to a NHS network outlet. This is obviously an inelegant solution to the problem.

In an attempt to improve this situation, the All Wales Citrix Service was implemented, using technology from Citrix Systems Inc. This service allows CU members to gain access to the CU network from off-campus, using their CU credentials, and therefore to resources that are restricted to users on the CU network.

However, a solution for access the other way – i.e. to access NHS resources from off the NHS

network has not yet been implemented. The only way to access these resources currently is to use a computer directly on the NHS network.

One particular group of users who find this situation less than satisfactory are the members of the Dental School – 24 of 34 members of staff are members of both CU and the NHS, and understandably would like the access management to be easier to use and more consistent.

### **3. Summary of resources available to joint CU/NHS members**

The following are a selection of NHS resources available to authorised users:

The Dental School Clinical Portal (*note this is not HOWIS*): a portal, in the form of an interactive website, containing information useful to members of the Dental School. Parts of the portal have access to patient records. This is hosted on the Cardiff & Vale Trust network.

PACS2: an application provided by AGFA, in the form of a Java Applet accessed through a web browser, that allows the user to view patient X-rays. To gain access to this, users must login to the application in the applet window using a username and password provided to them.

### **4. Summary of current Access Management to resources**

Firstly to gain access to any NHS resources, including the two resources detailed above, a user must first be connected on the Cardiff & Vale Trust network. To gain access to this network, users must currently log into a machine on the network. Management of usernames and passwords used to log in to computers directly on this network is currently undertaken by the Cardiff & Vale Trust IT staff and is implemented in the form of integrated Windows Domain Authentication;

Dental School Clinical Portal: certain aspects of the clinical portal are password protected. To gain access, users must login to the portal using a username and password provided to them. These passwords are held in an Oracle database.

PACS2: users must login to the application in the applet window using a username and password provided to them.

### **5. Possibilities for Improved Access Management for joint CU/NHS members**

There are several possibilities for improvement of Access Management for joint CU/NHS members, ranging from the technologically simple to the complex. We shall now describe these possibilities, reviewing them as we go along.

#### **5.1 Gaining access to the NHS network using CU credentials**

The aim here would be to allow joint CU/NHS members to gain access to the Cardiff & Value Trust network using their CU credentials. This could be done in a few different ways, described below.

##### **5.1.1 Integrating Authentication Mechanisms**

*Description:* This solution would involve integrating the CU eDirectory authentication mechanism and the C&V Trust Windows Domain Authentication in some way.

*Technical Difficulty:* Extremely high - this would be technically difficult to implement, if at all possible.

*Political will:* Very high - a great deal of political will would be required as it would involve integrating authentication mechanisms – a fundamental aspect of network security - or at least providing a bridge between the two.

*Potential costs:* High – could potentially be quite a costly solution due to the technical work involved. Actual estimation of cost is hard to produce without further information.

### **5.1.2 Implementing a Citrix solution to access the NHS network**

*Description:* This solution would involve implementing a Citrix Service similar to the existing CU Citrix Service on the NHS network.

*Technical Difficulty:* Medium-High - this would require a lot of technical effort to set up, but CU has experience doing this.

*Political Will:* Low - no political agreements would be required, as the agreements for a reverse Citrix service are already in place.

*Potential Costs:* High. Estimating costs and resources required on figures from our current Citrix service, a pilot service would require:

- Minimum of 4 servers. Each server:
  - Initial installation and setup - £5,947. This includes:
    - Cardiff University Server (3yr platinum warranty);
    - Server racking, UPS, network connection;
    - Security setup;
    - Backup Setup and configuration;
    - Admin.
  - Support & Maintenance for 3 years - £4,286. This includes:
    - Backup charges;
    - Security Management;
    - Admin;
    - Hardware fault reporting;
    - Server footprint, power, environment;
    - Backup monitoring.
- Total for 4 servers for 3 years: £40,932
- Citrix licensing for 1 server farm @ estimated £25,000/year (current licensing is approx £50,000 for 2 server farms);
- Centralis support for 1 server farm @ estimated £25,000/year (current support for 2 server farms is approx £50,000/year);
- Relevant Microsoft licensing (cannot estimate without further info – this depends on the OS' used on the machines accessing the Citrix Service);
- CU staff effort @ £250/day + expenses, approx 10 days setup of Citrix;
- NHS staff effort.

This totals to a minimum of approx £190,932 plus staff effort costs plus Microsoft licensing. This is for three years, including all support costs. (This breaks down to a minimum initial setup and configuration cost of approx £23,788 plus staff effort, and a yearly recurring support cost of £55,715 plus Microsoft licensing).

If this was to move to production status for many users, more servers would undoubtedly be needed, and the cost would rise accordingly. (*As a point of reference, the current production All*

*Wales Citrix service consists of 17 servers).*

### **5.1.3 Implementing a secure proxy server to access the Cardiff & Vale Trust network**

*Description:* This solution would involve implementing a proxy server on the Cardiff & Value Trust network connected to the CU network via some link (there are a few possible options in how to set up this link). This would allow a user to gain access to the Cardiff & Vale Trust network by providing the proxy server with their CU credentials, which would verify them with CU and allow the user through if the credentials were valid.

*Technical Difficulty:* Medium – A proxy server is fairly simple to set up; a great deal of care would have to be taken however with the security of the system as it would allow access to the Cardiff & Value Trust network - a very secure network containing a lot of sensitive material.

*Political Will:* Medium – this would likely require some political agreement; however, it is fairly similar in idea to the Citrix Service for which an agreement is already in place.

*Potential Costs:* Low-medium – the technical effort required is only a medium amount; however, dedicated hardware would be required. Thus, the corresponding costs would be low to medium. This would consist of:

- Constancy to set up and configure the solution (3 days @ £250/day) = £750
- Cost of the proxy server:
  - Initial installation and setup - £5,947. This includes:
    - Cardiff University Server (3yr platinum warranty);
    - Server racking, UPS, network connection;
    - Security setup;
    - Backup Setup and configuration;
    - Admin.
  - Support & Maintenance for 3 years - £4,286. This includes:
    - Backup charges;
    - Security Management;
    - Admin;
    - Hardware fault reporting;
    - Server footprint, power, environment;
    - Backup monitoring.
- Proxy server licensing (Ezproxy) @ £264

This totals to £11,247 for three years. (This breaks down to £6,961 initial setup, configuration and consultancy costs, and three yearly recurring support costs of £1,429).

*(Note that there are several options of how to set up the link between the CU network and the Cardiff & Vale Trust network, each requiring different amounts of work. Full details would be provided upon request of a full quote of this option).*

## **5.2 Access to the Dental School Clinical Portal Restricted areas**

The aim here would be to allow joint CU/NHS members to gain access to the restricted areas of the

Dental School Clinical Portal on the Cardiff & Vale Trust network using their CU credentials. A prerequisite of this is that the user has authenticated themselves onto the Cardiff & Value Trust network in order to access the basic Dental School Clinical Portal first, either by current methods or by using one of the options presented in Section 5.1.

### **5.2.1 Changing the Dental School Clinical Portal to become a Shibboleth Service Provider**

*Description:* This would involve adding code to the Dental School Clinical Portal back-end, which would allow the portal to use the Shibboleth technology for authentication and authorisation of joint CU/NHS users through a federated identity agreement.

*Technical Difficulty:* Medium – changing the portal's back-end authentication systems could be tricky, but definitely not impossible, as it is a standard web portal.

*Political will:* High – a formal agreement would be needed as it would require the NHS to trust CU to authenticate and authorise users, and as the restricted areas of the Clinical Portal contain patient details, this could be an agreement that could be hard to get.

*Potential costs:* Low-medium – as the technical effort required would be medium, but no additional hardware would be required, the cost would likely be low to medium. This would be charged *pro rata* of our standard internal consultancy rate of £250/day + expenses.

## **5.3 Access to PACS2**

The aim here would be to allow joint CU/NHS members to gain access to the PACS2 application on the Cardiff & Value Trust network using their CU credentials. A prerequisite of this is that the user has authenticated themselves onto the Cardiff & Vale Trust network in order to access the PACS2 application, either by current methods or by using one of the options presented in Section 5.1.

### **5.3.1 Changing the PACS2 application to become a Shibboleth Service Provider**

*Description:* This would involve adding code to the PACS2 application which would allow the portal to use the Shibboleth technology for authentication and authorisation of joint CU/NHS users through a federated identity agreement.

*Technical Difficulty:* Very high – changing the PACS2 authentication systems would have to be done by the providers of the software - AGFA.

*Political will:* High – a formal agreement would be needed as it would require the NHS trust and CU to authenticate and authorise users, and as the restricted areas of the Clinical Portal contain patient details, this could be an agreement that could be hard to get.

*Potential costs:* Medium – as the technical effort required would be high, but no additional hardware would be required, the cost would likely be medium, depending on what AGFA would charge!

## **6. Recommendations for improving Access Management for joint CU/NHS members**

We recommend implementing the solution described in Section 5.1.3 – implementing a proxy server to enable access to the NHS network for joint CU/NHS staff – as the most cost effective method of allowing joint CU/NHS members access to the NHS network, and therefore the clinical portal and the PACS2 application.