

Creating a Central Directory for UK's National Health Service (NHS).

King's College Hospital 
NHS Trust

"Getting accurate identity data and keeping it accurate and synchronized - was a major hurdle. We were impressed how easy Imanami made managing identities."

*Damian Lewsley
Network Team Leader
King's College Hospital*

Problem

What do you do when you have to share key identity data with an external system? Especially when you have limited time, a very limited budget, and you're not sure if your data is accurate in the first place?

That was the problem facing Damian Lewsley, Network Team Leader at King's College Hospital, London, one of the largest and busiest hospitals in England. Like most hospitals in Great Britain, King's is part of the National Health Service (NHS), and connects into the national "NHSNet" IP backbone that connects the many hospitals, General Practice surgeries and other NHS locations together. Also, like most of the larger hospitals, King's has its own IT infrastructure to manage, serving 5000 users and based around Windows 2000 Server and Active Directory.

The NHS had recently awarded one of the largest ever public sector contracts to EDS to deliver an email and directory service to all 1.2 million NHS staff, and it was this initiative that was giving Damian (and his counterparts at many other hospitals), his headache.

"We had to allow the EDS central directory service to reach into our Active Directory and locate the users that were there, in order to give each of them an entry in the central email system," said Damian. "The problem was that we weren't sure the data we had in Active Directory was good enough for export."

There were two reasons for doubting the integrity of the data within Active Directory. First, it had been there a long time; King's College Hospital had originally used a Banyan Vines network operating system directory in the early 1990s and had ported the accounts from Vines into Windows NT4 and then to Active Directory without any major data cleansing operations. Secondly, a local initiative to allow users the ability to modify their own data in Active Directory via a home-grown web interface had not been as successful as had been hoped.

"The problem with the web interface was that we had allowed users to modify some attributes, such as role, that really should have been kept read-only," said Damian. "This meant some of the roles they gave themselves didn't match the official NHS roles."

So before he could allow the EDS directory to discover the user data within his Active Directory, Damian decided he had to get that data into better shape. What he needed was a reliable and authoritative data source that had up to date user data, and the correct role names. In most organizations this data can be found in the Human Resources (HR) system, and King's was no exception. An NHS HR and payroll system called PRISM contained exactly the information Damian needed: up to date user names and roles. However, even after identifying his trusted source of data, his problems hadn't been alleviated completely. PRISM was an old UNIX system, built specially for the NHS.

With help from colleague John Thornley, Personnel Systems Manager, Damian managed to get PRISM to export the user data to comma-separated file (.csv) format, but that only solved half the problem. There seemed to be no way to automatically merge the Active Directory data with the PRISM data, and keep that data in synch automatically.

Solution

Damian needed to do more than just update the Active Directory user accounts with the data from PRISM. He also wanted to manipulate that data as it moved between the two sources. In particular, he wanted to avoid non-NHS staff with accounts in Active Directory (such as external catering staff) from being exported into the EDS system, and he wanted to give each account that had been successfully synchronized a unique user ID, to indicate that the mapping of accounts between the two systems had been successful.

"I had been aware of metadirectory technology for sometime," said Damian. "And I knew that I needed some kind of metadirectory here, so I started out by considering Microsoft's Identity Integration Server (MIIS). Although this could have done what I needed, I just didn't have the time or the budget to deploy it. I needed something less costly and quicker to deploy."

MIIS could certainly have met Damian's functionality requirements, but at \$25,000 per CPU, and needing Windows 2003 Server and SQL Server Enterprise Edition, it came in over his budget. What's more, in order to meet his requirements for data transformation, MIIS would need to be extended from its basic capabilities by programming in one of the .NET languages. Damian wanted software that could do the necessary data transformation without having to employ external consultants to do the coding.

Damian turned to Google for help and typed "metadirectory" into the search engine, hoping that something might turn up. It did, in the form of Imanami's Directory Transformation Manager (DTM).

Imanami, a Microsoft® Gold Certified Partner, develops applications that facilitate and automate Microsoft directory management and DTM looked as if it might be the ideal solution to Damian's problem. DTM is designed to synchronize Active Directory with various other databases such as Lotus Notes, Oracle, SQL Server, PeopleSoft, iPlanet, SAP or LDAP and, importantly for Damian, CSV files or Excel spreadsheets. Also, unlike other metadirectories, DTM had a simple and intuitive interface and didn't require advanced coding skills to apply transformations to the data as it was synchronized. All synchronization jobs were configured via simple wizard interfaces with the familiar Windows look and feel. It seemed too good to be true, so Damian decided to put Imanami's claims to the test and downloaded DTM to run in his lab.

"I downloaded it, tried it and loved it!" said Damian. "I started out with one simple job. I wanted to join users in the spreadsheet to users in Active Directory, and then gradually increased the depth and breadth of the import. Once I was happy with this I started adding transformations to the imported data, including identifying which users could be exported to EDS, and which could not. I simply added a static field to be exported to Active Directory using DTM's data transformation tools, then told EDS that when they ran an LDAP search to our AD, if this field was absent, they should not export the user."

Following his download, Damian was contacted by Imanami's UK reseller, Infant Technology Ltd, to see if the trial had been successful. "We didn't try and convince King's College Hospital that DTM was the right solution for them," said Phil Kelly, Technical Director at Infant. "We didn't need to. Damian was on the same wavelength as us and supported the adoption of Imanami from the start. We had been attracted to Imanami after appraisal of their product range," Kelly continued. "They were a welcome breath of fresh air after dealing with other directory management products; we believe that their simplicity of implementation coupled with their extensive functionality represents a significant shift in this area."

"DTM had a simple and intuitive interface and didn't require advanced coding skills to apply transformations to the data as it was synchronized."

*Damian Lewsley
Network Team Leader
King's College Hospital*

*"Imanami is a welcome
alternative to heavy identity
management solutions.
Deployment is so simple and yet
the functionality is still powerful."*

*Phil Kelly
Technical Director*

Trial Software
30 Day Evaluation version at:
www.imanami.com/download



Looking Forward

Having solved one problem with DTM, Damian now has more ideas as to how DTM can help with ensuring that identity data at King's remains accurate. He is planning to extend the system to synchronize data between Active Directory and the internal telephone exchange, by exporting telephone number and user name combinations from Active Directory, via DTM, to the telephone exchange database. But the possibilities don't end there.

"As far as I know, we are one of the first hospitals to successfully open up our directory for EDS to use," Damian said. "It may be that other NHS users could benefit from using DTM in the same way. At a meeting of other hospital administrators before the roll-out, we all agreed that we shouldn't re-invent the wheel in our solutions. Using DTM means that we can take an off-the-shelf solution and deploy it in only a day or two, without the need for costly software or external consultants."

Phil Kelly agrees. "We believe all organizations concerned with transferring and transforming their directory data should take a serious look at DTM and the full range of Imanami Identity management point solutions" Kelly said. "I'm convinced it would be the most cost-effective solution for them."

Contact Imanami for a free demonstration at: 1-800-684-8515
or visit our website at: <http://www.imanami.com>

