AUSTRALIAN TECHNOLOGY NETWORK OF UNIVERSITIES

Federated AAA middleware and the QUT SSO environment

Bradley Beddoes

Senior Network Programmer

AAA Review Project Manager

b.beddoes@qut.edu.au

Shaun Mangelsdorf

Network Programmer

s.mangelsdorf@qut.edu.au

Presentation Overview

- Introduction to Federation concepts and why we think its so important
- Discuss our current ATN AAA implementation and our work with Shibboleth to provide next generation ATN services.
- Describe the QUT single sign on service and our proposed future architecture.
- Finish up with some upcoming projects that will impact the education sector with regards to AAA
- Feel free to ask questions at any point, no need to wait for the end
- Try our best to keep you all awake!

Federation and AAA Introduction

- **Federated AAA** - Also called cross-domain AAA. Federated identity allows for information about users in one security domain to be provided to other organizations in a common federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain authentication credentials.
- **Shibboleth** - An Internet2 middleware Initiative project that has created an architecture and open-source implementation for federated AAA based on SAML
- **SAML** - "Security Assertion Markup Language", An XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider and a service provider in a federation.
- **IdP** - "Identity Provider", Organization who maintains registry of authentication credentials and associated data for individuals whom they have identified personally and trust.
- **SP** - “Service Provider”, a resource provided within a federation. Consumes assertion statements from IdP's to make authorization decisions about users and provide access to the protected resource.
- **WAYF** - “Where Are You From”, server allowing unauthenticated users to select their home institution.
- **AuthN / AuthZ**- AutheNtication / AuthoriZation

Participation Age

Welcome to the Participation Age. Advances in technology have made it possible for more and more people to connect with each other to participate and to share work flows, to compete for jobs, to purchase goods and services, to learn and create.

Information Age thinking says, ‘Control the creation and distribution of information and you dominate markets.’ Participation Age is the antithesis of that. It's all about access. That access allows for value to be created through networked human beings who share, interact and solve problems. Because of participation, meaningful content, connections, and relationships are created like never before.

In the Participation Age, there are no arbitrary distinctions between passengers and crew, actors and audience. Be one, be both, be everything in between. Welcome to the revolution.

Scott McNealy
CEO, Sun Microsystems

ATN

What it is and where we are coming from....

Curtin University of Technology

RMIT University

UniSA

QUT Queensland University of Technology Brisbane Australia

UNIVERSITY OF TECHNOLOGY SYDNEY

- Currently provides eLearning resource hosted at QUT called "ATN-LEAP", 5 learning modules for research students
- Limited to single QUT resource, hard to deploy additional resources at QUT, no ability to deploy resources at other institutions
- Access uses local institution credentials over QUT/ATN developed protocol, several major issues with this model

ATN Operation

ATN Operation Log

Jul 10 09:32:23 olt-atn httpsauth[24492]: set the data pointer for curl callback

Jul 10 09:32:24 olt-atn httpsauth[24492]: call curl_easy_perform

Jul 10 09:32:25 olt-atn httpsauth[24492]: RECIEVED: SUCCESS: FULLNAME: Student Name EMAIL: s9999999@student.rmit.edu.au ROLES: CRSTYP03 STUDENT: s9999999

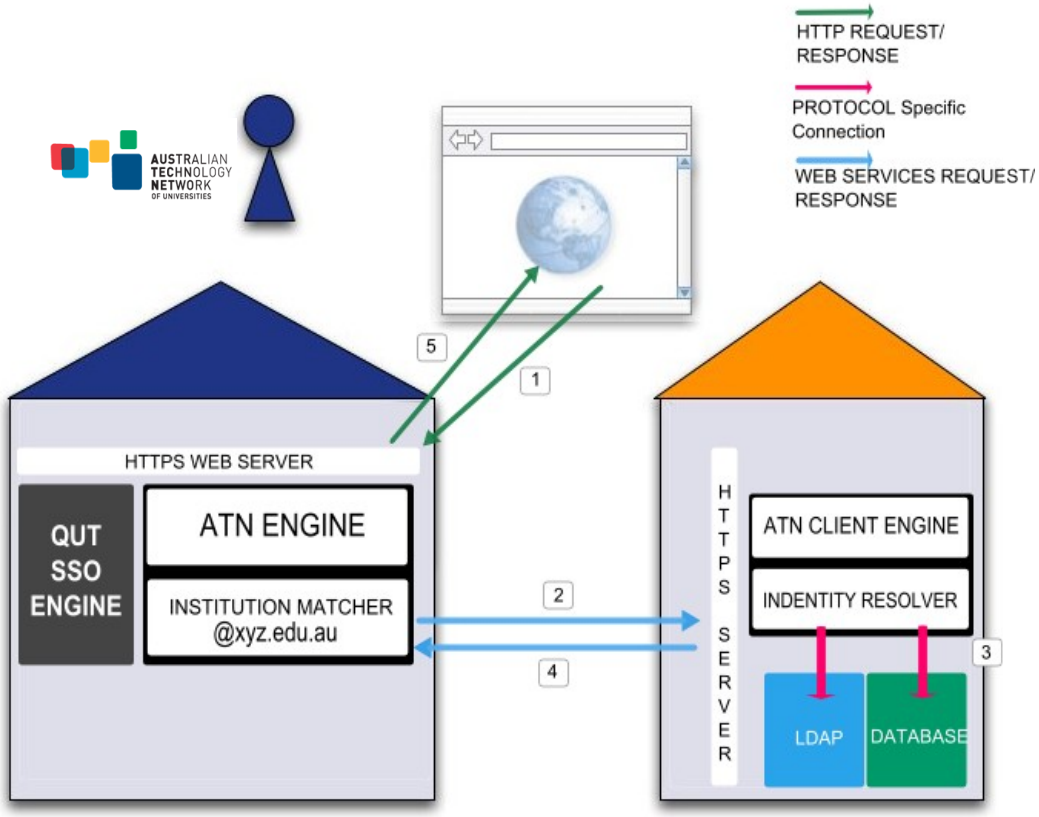
Jul 10 09:32:25 olt-atn httpsauth[24492]: sending good reply for s999999@rmit

Jul 10 09:32:25 olt-atn httpsauth[24492]: result is a success

Jul 10 09:32:25 olt-atn httpsauth[24492]: cli = '-4' stud = 's9999999' staff = '00000000'

Jul 10 09:32:25 olt-atn httpsauth[24492]: result is '60Y -4 s9999999 00000000 N 1 0 s9999999@student.rmit.edu.au Y N|N||| Student Name|131.181.117.130|RMIT+CRSTYP03'

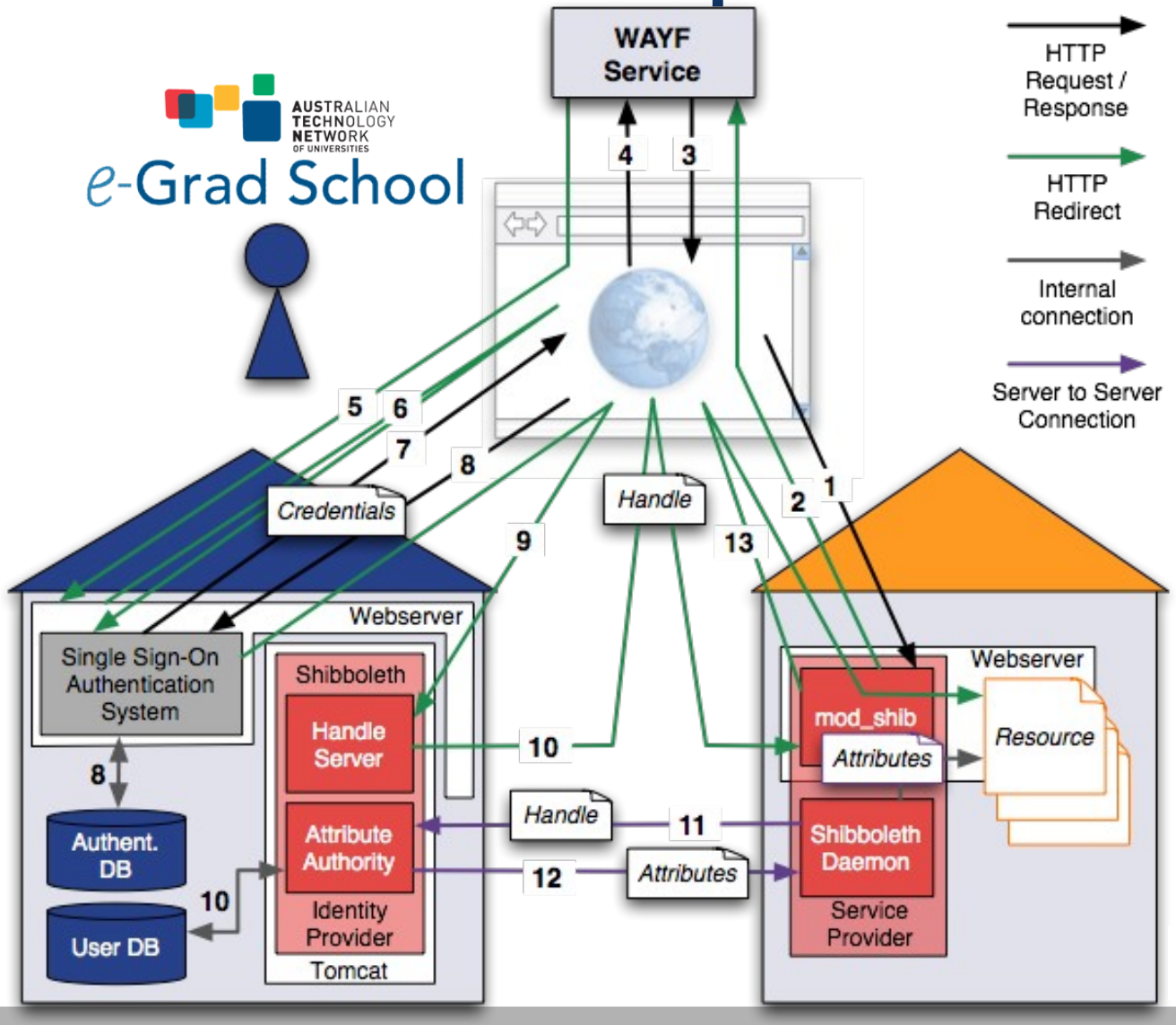
Jul 10 09:32:25 olt-atn httpsauth[24492]: SUCCESS: Authentication successfull. [CLIENT: s9999999 | INSTITUTION: RMIT]



ATN eGrad School

- eGrad school is the next generation of ATN services to enhance the ATN-LEAP system
  - http://www.egradschool.edu.au/
- MAMS grant provided to setup ATN universities as identity providers with QUT providing technical guidance and initial service provider
  - As shibboleth is open source and open standards based it supports currently deployed campus identity stores and SSO services, no steep costs to join the federation
  - Currently the 5 ATN universities have exposed some 190,000+ staff and student identities to the AARNet federation
  - QUT is continuing to assist more universities to join the federation with up to 7 new Australian and New Zealand universities slated to become identity providers and consumers of eGrad services

Shibboleth Operation



Shibboleth Demonstration

- Complete federation provided on Virtual Machines
  - Fedora Core 4 Linux (Java 1.5 (r07), Tomcat 5.5, Apache 2.0.54)
  - Latest Shibboleth 1.3e code base
  - Two example organizations QUT and BusinessPartner with IdP's
  - Example Mediawiki SP
  - Runs entirely on free VMWare server product
    - http://www.vmware.com/products/server/
- Originally created for this QuestNet presentation, now to be incorporated into world wide shibboleth project!
- We are offering this as a download to allow institutions to learn shibboleth without initially needing to go through all the complex setup
  - Grab it from https://egrad.qut.edu.au/vm/ or watch the shibboleth wiki for future announcements
- On to the 'thrilling' demonstration.....

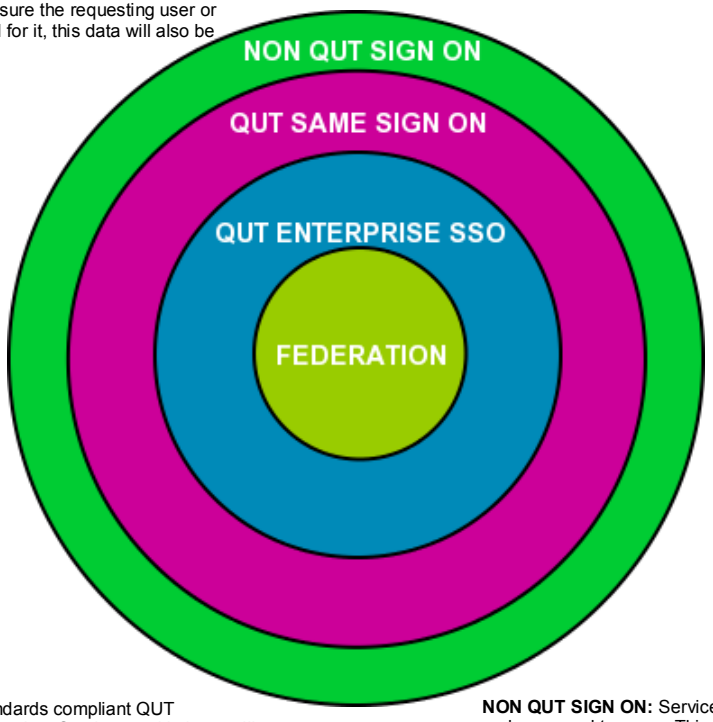
QUT SSO and AAA

- QUT has had campus wide Same Sign On and Web Tier SSO for around 10 years, 'QUT Access'
  - Extremely good position to be in with majority of clients having to only remember one username and password
  - Some very clever forward thinking helped put QUT in a strong position when very little other work was happening in this area, all of our AAA protocols were completely developed in house
  - QUT developers in the Web Tier now simply expect to have available drop in solutions for AAA that are easy to deploy and provide attribute based authorization services
- Some changes have been made over the years but with several new systems on the way we have the best opportunity to re-evaluate the design and collate our various business area requirements
  - Windows users want IE --> Web Tier SSO, Linux and Mac users want Firefox --> Web Tier SSO
  - Windows, Macintosh desktops and servers authenticate to AD, what about *nix desktops and servers?
  - More fine grained identity information about clients accessing services to make better AuthZ decisions
  - Introduce ability to make AuthZ decisions at web tier based on AD group memberships
  - Easy support for Federation without need to learn and manage shibboleth or other such technologies
  - Currently only support Apache 1.3.x, 2.x (all platforms) and Java well, our developers want support for everything going around and they want it yesterday!
    - VB.NET, C#, IIS, Coldfusion, Apache 1.3.x, 2.x, 2.2.x, C, C++, Java, Tomcat, JBoss the list goes on.....
  - Easier integration support to our Vendor supplied products such as Oracle Portal our new Student Management System and our new Learning Management Systems
    - We can only do this with Vendor support, pluggable/extensible AAA systems please guys!!

QUT Environment Breakdown

FEDERATION: The core of the model and the newest feature set. Resources within this layer are able to provide services not only to QUT users and machines but to users and machines of other institutions with whom QUT has entered an agreement of trust. Within this Federation external institutions will assert the validity of the user or machine requesting access to a QUT resource using their local account details and our federated policy enforement points will trust this assertion. For QUT staff and students accessing federated content at other institutions creation of these assertions will be handled in the enterprise SSO layer. Authorization will be carried out at all resources in this layer to ensure the requesting user or machine meets all additional policy assertions which have been defined for it, this data will also be transmitted the trusted institution.

QUT ENTERPRISE SSO: All corporate services with large QUT user bases should be deployed at this layer. Services adhering to the requirements of this layer will provide Single Sign On to QUT users and machines for QUT resources. Authorization will be carried out at all resources in this layer to ensure the requesting user or machine meets all policy assertions which have been defined for it.

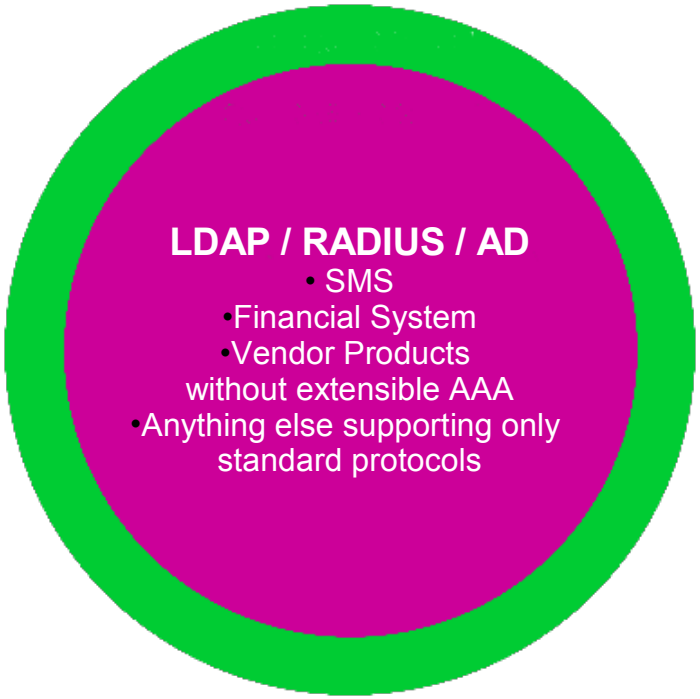


QUT SAME SIGN ON: Services deployed at this layer will utilise standards compliant QUT authentication protocols to allow users and machines to access the service. Services at this layer will require users and machines to enter their authentication credentials each time they access the service. Where the service being deployed is purchased from an external vendor the product will need to be able to utilise one of the available standard authentication protocols as deployed at QUT. Ideally the available protocols should be written into RFO's. Where authorisation is required for services at this layer this will be limited to queries that can be natively made to the utilised protocol. Outside this these services will be responsible for provisioning of their own data to make authorisation decisions. All transmission of credentials at this layer must be secure.

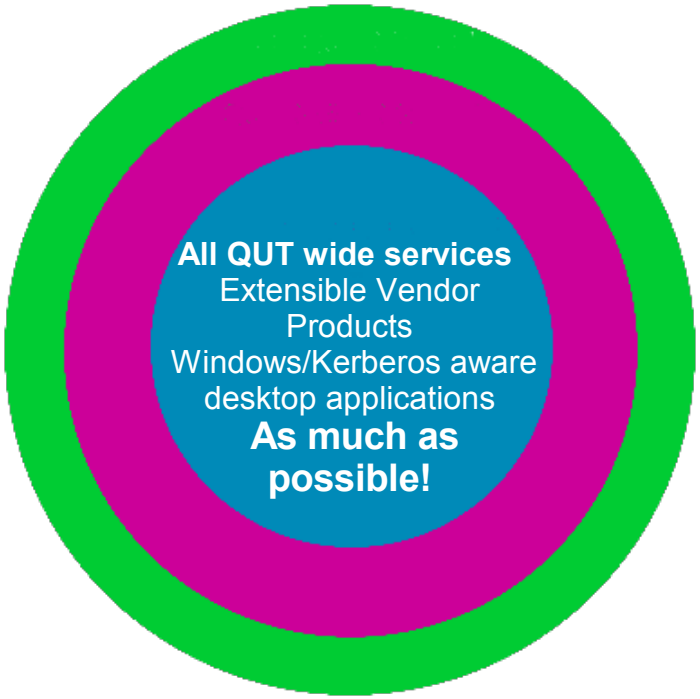
NON QUT SIGN ON: Services deploed at this layer will provide their own effectively one-time username and password to users. This should be avoided so users aren't having to remember duplicate identities. Solutions such as Federation should be looked at here especially when the applications are hosted offsite.

QUT Environment Breakdown

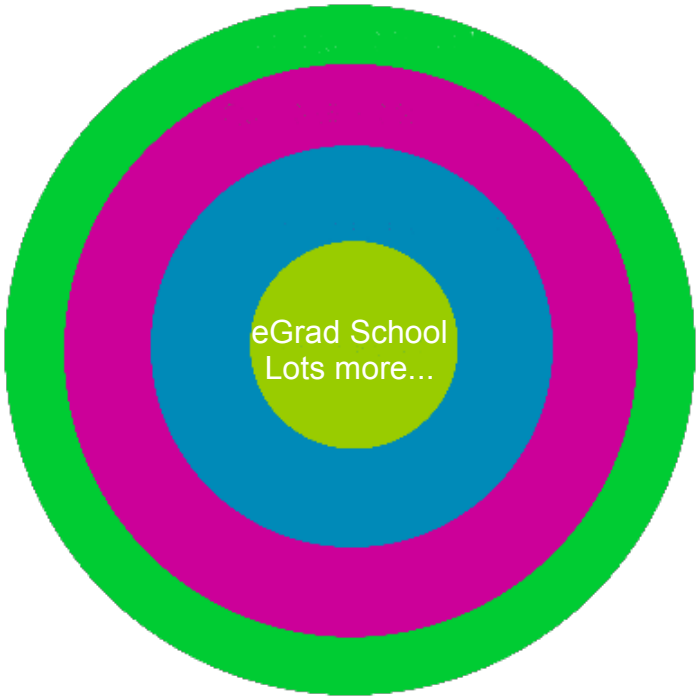
QUT Environment Breakdown



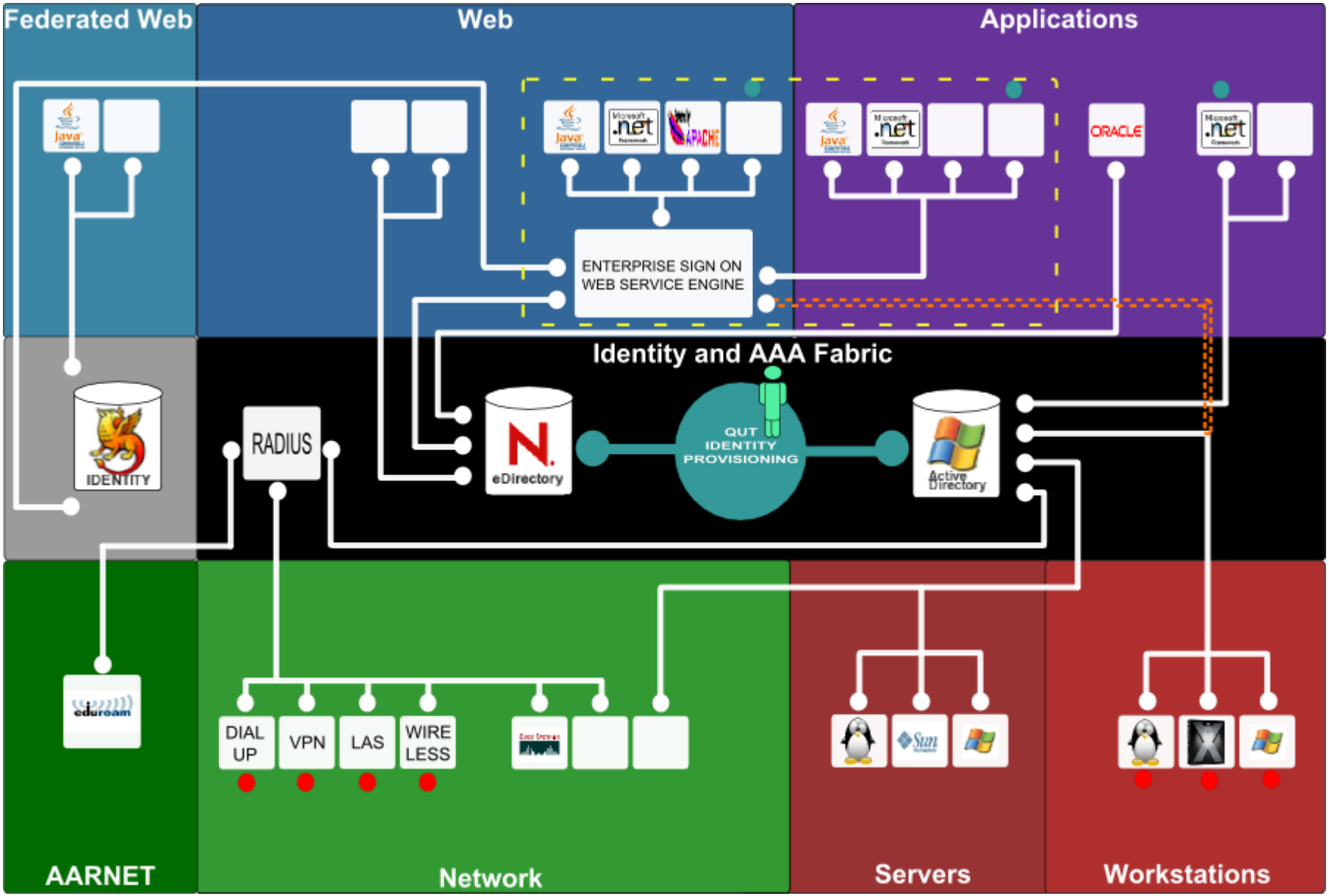
QUT Environment Breakdown



QUT Environment Breakdown



Future QUT AAA Architecture



Upcoming AAA projects

- ## Higgins Project
  http://www.eclipse.org/higgins/ - Higgins is a framework that will enable users and enterprises to integrate identity, profile, and relationship information across multiple systems. Using context providers, existing and new systems such as directories, collaboration spaces, and communications technologies.

- ## Bandit
  http://www.bandit-project.org/index.php/Welcome_to_Bandit - Bandit is a system of loosely-coupled components that provide consistent identity services and creates a community that organizes and standardizes identity-related technologies in an open way, promoting both interoperability and collaboration.

- ## Infocard / Windows CardSpace
  http://msdn.microsoft.com/winfx/reference/infocard/default.aspx - Collates different digital identities users may have at different locations, will provide support for many differing standards. It also presents a GUI that allows a user to choose among several digital identities, each of which is represented visually as a card.

- ## OSIS (Identity Commons 2)
  http://osis.netmesh.org/wiki/Main_Page - OSIS is a project committed to the development and distribution of non-Microsoft implementations of Microsoft's "InfoCard" technology. OSIS stands for "Open Source Identity Selector", and is a collection of interested parties including Red Hat, Novell, IBM, VeriSign, XDI and Microsoft. The goal of the community to develop a common, open source code base and software practice for implementing "InfoCard" technology on disparate operating platforms.

- ## XRI and implementations of iName and iNumber
  http://www.oasis-open.org/committees/download.php/15694 - http://en.wikipedia.org/wiki/I-number - http://en.wikipedia.org/wiki/I-name

Question Time and References

- Shibboleth
  - http://shibboleth.internet2.edu
- MAMS Project
  - http://www.federation.org.au
  - https://mams.melcoe.mq.edu.au/zope/mams
- Shibboleth interaction digram by Switch AAI
  - http://www.switch.ch/aai/shibboleth/
- eGrad School
  - http://www.egradschool.edu.au/