A History of IdP deployments in Australia

Mr. Terry Smith, Australian Access Federation
The Australian Access Federation (AAF) has been operating for over 10 years superseding an earlier pilot federation that tun for about three years. Over this time organisations have been deploying and maintaining their Identity provider software, primarily Shibboleth. This has required an investment by each organisation to develop technical staff skills and federation operators to assist with supporting this infrastructure as an integral part of the federation. Many approaches have been taken to ensure the delivery of these services and thus the continual operation of the identity federation. This discussion will review the history of IdP deployments in Australia, the approaches taken, the influences at the time and the level of success of each. The federation operator MUST support their organisation that provide identities, as without identities there will be no federation.
The MAMS project

- A pilot federation in Australia
On the road training

- Training IT staff at each institution
  - What is a federation
  - Federation rules and requirements
  - How to install and maintain Shibboleth IdP
- Shibboleth 1.3 + Autograph (A plugin for Shibboleth for Attr release)
- auEduPersonSharedToken plugin
  - Token created and stored locally
  - Token created and stored centrally
  - Requirement – token be able to follow its owner
- Many different setups resulted across the sector
- IT staff availability high, available time low
Step-by-Step guides

- Installation and configuration guides created
  - Long and complex, many steps to follow
  - Failure to complete a step correctly may impact on a successful outcome
  - Difficult to debug
  - Limited support
  - Requires maintenance of the document set
- Started to move towards more consistent setups
Pre-build ISO

- Complete operating system
  - Shibboleth and support packages pre-installed and configured
  - Local branding and integration required

- Difficult to maintain / upgrade
- Minimal uptake – restricted to the OS provided
MAMS Project folds

- No new funding MAMS
- New AAF project lead by CAUDIT and a number of institutions
- Migration of existing MAMS IdP to the AAF
- Shibboleth V2 arrives
- Migration for MAMS to AAF
- Migration from V1.3 to V2
Shibboleth V2 install guides

- AAF develops install and configuration guides for V2
  - Based on SWITCHaai documents
  - New versions of documentation for each IdP upgrade
- New installs starting be become more consistent
  - Eases support
  - Start to simplify upgrades
- Upgrades from v1.3 take a long time
  - Three IdPs still retain their entityId from MAMS
Infrastructure management tools

- Puppet, Chef, Ansible etc usage increasing across the sector
- Some IdPs roll their own configurations for their IdP
  - Generally based on the AAF install guides
  - Mostly Puppet
    - Lots of overheads running a puppet environment
- Shibboleth V3 being developed
Shibboleth V3

- Version 3 announced
- 1 year before EOL for Version 2
- Major migration of the AAF fleet required
- Significant effort required to re-write the AAF install guides
- AAF decides to develop and Installer using and infrastructure management tool
  - Ansible choosen
  - Lower overheads and system requirement
  - Simple to run on a single instance
The AAF Installer

- Released with version 3.1.0 of the Shibboleth IdP
  - No-one ever uses the first version of a new release 😊
- Simplified installation notes created
- Simple upgrade videos created
  - Create a new instance of a V3 IdP
  - Migrate your existing configuration across
  - Test and re-test the new installation
  - Deploy in production
  - Support REDHAT and CENTOS
    - In use by majority of AU Universities
Most universities used the installer
  ▪ Reduced setup time down from weeks to days
  ▪ Reduced need to IdP admin to understand all of the complexities

Still some struggled to upgrade
  ▪ Last upgrade completed June 2019. We started in 2016!

Installed built with following requirements
  ▪ Simple to use
  ▪ Provides simple upgrade path
  ▪ Does a complete install
    ▪ Shibboleth, Jetty, Apache, etc…
  ▪ Allows for new federation requirements
    ▪ Changes to CORE attributes
    ▪ eduGAIN
    ▪ Migration to RapidIDP
Commercial offering / Cloud

- Many AU universities now have an enterprise SSO in place
  - OKTA
  - ADFS
  - MS Azure
  - Ping Federate
  - WSO2
- Most universities want to move to the cloud
- Remove or move the Shibboleth IdP
AAF RapidIdP

- AAF now offer a fully managed, highly available cloud based IdP
  - Loss of technical skills in the sector
  - Move to the cloud and SAS solutions
- 3 years of development work
  - Very automated system
  - Simple migration from on-prem IdP
  - Eases compliance
- Cost involved in run the service
  - Cost recovered service
  - Setting the right price point has been difficult
  - Slow up-take but increasing
Some push back from technical folk – loss of their domain

In the end it’s a business decision

Always improving

- eduGAIN integration with a single button click
- Simplifying branding – going for Web Accessibility rather than full corporate branding
- Proxying to enterprise SSO (OKTA, AZURE, etc)
  - SSO for everything from the Users perspective
  - The right horse for the course from the technical perspective
- Integration into future BI systems
All new IdP to be offered a federation membership package that include RapidIDP in the subscription
- Can OPT out if they already have a Shibboleth IdP

Attempting to migration most of the federation to RapidIDP
- Some will never move – SPNEGO and other local configuration
- Easier to heard cats if they are all in your own back yard.
Disrupters

- Commercial IAM Vendors
  - Very focused on an enterprise model
  - Don't work well with federations
  - Work with them – Proxy to and IdP that works will in the federation space

- WebAUTHn
  - New standard published by W3C
  - Learning and understanding what it is, its impact and how it will fit in the federation space
How will you rollout your fleet of IdPs?

REVIEW #5