Identity Federation in South Africa

Sci-GaIA Final Event
CSIR International Convention Centre, March 2017
Introducing SAFIRE
The need for an identity federation was identified by the community in 2014

Took a long time to get going – apparently a common story :-)

Eventually a number of universities agreed to provide seed funding, which spurred some motion

Initially piloted as a full-mesh federation, later changed architecture to a hub-and-spoke
Current status of identity federation in South Africa

- Hub-and-spoke architecture deployed
- Transition from pilot underway, mostly completed
- Roadmap showing next phases
- Supported service with full time staff

- South Africa was accepted as a member of eduGAIN in February 2017...

... and published metadata the next day
The hub-and-spoke architecture was chosen to address two concerns:

1. Reducing the barriers to entry for identity providers
2. Increasing access to attributes for service providers
Current deployment

- web-cpt-01.safire.ac.za
- www.safire.ac.za
- testsp.safire.ac.za
- validator.safire.ac.za
- PHP, Shibboleth, WordPress

- md-cpt-01.safire.ac.za
- metadata.safire.ac.za
- php.safire.ac.za
- PHP, PHPH, OpenSC

- hub-cpt-01.safire.ac.za
- iziko.safire.ac.za
- proxy.safire.ac.za
- consentadmin.safire.ac.za
- PHP, SimpleSAMLphp, BIRK

- db-cpt-01.safire.ac.za
- syslog.safire.ac.za
- MySQL, rsyslogd

- AS2013

- SAFIRE
  SOUTH AFRICAN IDENTITY FEDERATION
Roadmap to a resilient, fully redundant architecture

- **web-cpt-01.safire.ac.za**
  - **www.safire.ac.za**
  - **testsp.safire.ac.za**
  - **validator.safire.ac.za**
  - PHP, Shibboleth WordPress

- **md-cpt-01.safire.ac.za**
  - **metadata.safire.ac.za**
  - **php.safire.ac.za**
  - **PHPH, OpenSC**

- **db-cpt-01.safire.ac.za**
  - **syslog.safire.ac.za**
  - **MySQL, rsyslogd**

- **hub-cpt-01.safire.ac.za**
  - **iziko.safire.ac.za**
  - **proxy.safire.ac.za**
  - **consentadmin.safire.ac.za**
  - **PHP, SimpleSAMLphp BIRK**

- **haproxy-cpt-01.safire.ac.za**
  - **iziko.safire.ac.za**
  - **proxy.safire.ac.za**
  - **metadata.safire.ac.za**
  - **haproxy, exabgp**

- **haproxy-jnb-01.safire.ac.za**
  - **iziko.safire.ac.za**
  - **proxy.safire.ac.za**
  - **metadata.safire.ac.za**
  - **haproxy, exabgp**

- **hub-jnb-01.safire.ac.za**
  - **iziko.safire.ac.za**
  - **proxy.safire.ac.za**
  - **consentadmin.safire.ac.za**
  - **PHP, SimpleSAMLphp BIRK**

- **md-jnb-01.safire.ac.za**
  - **metadata.safire.ac.za**
  - **php.safire.ac.za**
  - **PHP, PHPH, OpenSC**

- **db-jnb-01.safire.ac.za**
  - **syslog.safire.ac.za**
  - **MySQL, rsyslogd**
The technology is easy(ish)

The difficult part is getting the governance layer right – policies, contracts, lawyers, etc

However, that time wasn’t wasted – because that’s the bit that eduGAIN cared most about

And it’s also an area where REFEDS has done a lot of work
So what does this all mean for R&E?
One ring identity to rule them all
For identity providers

- Simplified integration = lower costs
- Reuse of existing identity information
- Standardised attribute release
  - The hub also helps add missing attributes
- Mandatory consent
  - Helps with POPI/privacy legislation

Things university management / IT departments care about, not researchers…
For service providers

- Access to existing, high quality identity information
- Reduced support costs
  - Password problems go to the IdP’s help desk
- Helps comply with privacy laws
- Less personal info = reduced risk
- Access is revoked when people leave
- Improved user experience – easier for people to get started using your service

Things CIOs / IT managers care about, not academics...
Provides a new approach to electronic resource management
Better control over who has access to your resources = better compliance with licensing agreements
Allows you to downsize/decommission reverse proxies
- Deals with the burgeoning SSL subject alternative name problem
Less confusing for your users
For academic & research staff

- Immediate access to a wide range of existing global services via eduGAIN
- One username and password to remember
- Better control over personal info
- Fosters (global) collaboration

But don’t take my word for it...

- Allows you to forget about identity and focus on teaching & research...
Federated technologies are good. Take advantage of them.

The infrastructure needs to be improved to take advantage of federated technologies. Do it.

Relying on older models of local account creation and IP-based ACLs is easier. This is a very limited view. Stop it.

If you can’t fix it all yourself (and you can’t), facilitate the efforts of groups that can. Build relationships, target your spending or funding to make the biggest impact.
Questions?
With your help, the RIPE NCC is building the largest Internet measurement network ever made. RIPE Atlas employs a global network of (>10,000) probes that measure Internet connectivity and reachability, providing an unprecedented understanding of the state of the Internet in real time.

https://atlas.ripe.net/