AAF REFEDs MFA and RAF rollout

Terry Smith
Head of Support - AAF

Supporting services

Supporting researchers that access services that require REFEDs MFA

- National Institute of Health (NIF)
- Others will follow...

What MFA is good enough? Phishing-resistant MFA

Step improvement for the AAF

A national Trust & Identity program for research

We will work closely with the NCRIS community to identify six incubators – programs developed in collaboration with NCRIS facilities to demonstrate and implement exemplar T&I solutions.

- enhance cybersecurity
- enhance connectivity across NRI
- improve access to sensitive data
- enhance research translation.

Enhancing cybersecurity

Sector wide improvement in cybersecurity across the sector

- Major data breaches
  - OPTUS - 9.8 Million customers (names, birth dates, addresses, phone numbers and password and driver's license numbers [in some cases])
  - The Australian National University - 200,000 Students (name, addresses, phone numbers, birth dates, tax file numbers, bank details, student academic records)
  - Medibank - 3.9 million customers (personal data including health records)

Notifiable data breaches report January to June 2022

Most, if not all Universities are moving to MFA for all staff and students for all services including federation services (AAF and eduGAIN).

The task at hand - REFEDs MFA

55 Identity Providers (all but one is Shibboleth) connected to the AAF.

AAF's Rapid IdP - 26

- 4 Virtual mode - credentials held
  - Passwordless Auth
- 3 Delegated mode - Connects to on-prem LDAP
  - Passwordless Auth
- 19 Proxy mode - Authn off-loads to enterprise IdPS
  - Utilize enterprise MFA

On-Prem IdPs - 29

Two have already implemented REFEDS MFA

- DUO
- Passwordless Authentication using the Cipherise

A few have configured Shibboleth to proxy to their Enterprize IdP that provides MFA

- None do REFEDS MFA yet.

Some still running Shib IdPv3

- Priority in 2024 - preferably to RapidIdP

Signaling REFEDS MFA

Universities are implementing MFA at their enterprise IdP, but are not signaling that MFA occurred when requested by a service provider.

- AAF needs communicate the need to implement REFEDS MFA
- Provide conversions between how the enterprise IdPs signal MFA and REFEDS signals
  - Microsoft - Azure AD (done)
  - OKTA (via an attribute)
  - Google Authentication (nothing)
  - Pingfederate (SAML2AuthnContextClassRef)
  - F5 Access (TBD)
  - OpenAM (TDB)
  - ORACLE Access Manager (TBD)
- Ensure the selected MFA solution meets requirements - Move towards **Phishing-resistant MFA**
- Provide a tool to verify MFA is working

REFEDS Assurance Framework

Most of the work needs to be done at the Universities

To assist our customers the AAF will:

- Provide Communications - the requirements of RAF
- Provide Guidance
  - How to meet the requirements
  - Setting eduPersonAssurance correctly
- Update testing tools to verify RAF has been implemented correctly
- Deprecate our old assurance values

Giving our customers something to think about...

First, this will replace the existing AAF assurance values;

```
urn:mace:aaf.edu.au:iap:id:1
urn:mace:aaf.edu.au:iap:authn:1
```

This new framework splits assurance into the following orthogonal components:

- the identifier uniqueness;
- the identity assurance; and
- the attribute assurance.

Note: The assurance of authentication is not covered by this specification.

More to come...

With our customers we need to work through the requirements of RAFv2

- It’s been a moving target
- Consider including something in our yearly compliance process
  - Self asserting their compliance to RAFv2 requirements