TOOLS TO SUPPORT FEDERATION OPERATORS

Mr. Terry Smith, Australian Access Federation
THE MAIN OUTPUT OF THE OPERATION OF AN IDENTIFY IS TRUSTED METADATA. THERE ARE A NUMBER OF OPEN-SOURCE TOOLS THAT WILL SIMPLIFY THE CURATION OF FEDERATION ENTITIES AND THE CREATION OF SIGNED FEDERATION METADATA. WE WILL DISCUSS AVAILABLE OPTIONS AND THE CHOICES THAT HAVE BEEN MADE BY FEDERATION OPERATORS IN THE APAN REGION.
Web Site

Provides your federation with its own Identity

- May be part of your NREN’s web presence. Is your federation part of a larger service offering of the NREN?

Important information about your federation.

- Who will use it?
- What sort of information is being looked for?
- How easy is it to find?
Links to Federation web sites found on the REFEDs web site: https://refeds.org/federations

- Make sure your federation is listed here!
- Ensure your federation details are up to date!
  - No Policy – China, Indonesia, Singapore
  - No Metadata – Indonesia
- Participate in the REFEDs Surveys...
Web Site – minimal requirements

- What is the federation, overview (video), benefits, etc
- Who can subscribe / join and how to do so
- The rules of the federation, compliance requirements
- Current news and information from the federation
  - Good news stories
  - Security alerts
  - Maintenance announcements
- How to get support, ask a question, etc
- Who are your members
- What services you provide
Service Catalogue

- At some point you will be asked what services does your federation provide?
- Even a simple service catalogue will provide the answer to this question.
- Difficult to maintain – really require input from the SP owners...

Have a look at oktas – [find-your-apps](#)
Document Repository

Your federation will collect many documents over time

- Signed subscription forms
- Policies, procedures, plans, guidelines, rules, forms
- Presentations, photos, newsletters, reports, videos

The list goes on...

You don’t want to loose any of this stuff – The AAF uses Dropbox so we know it’s backed up, secure and able to be shared within the team. We also use Google Docs to collaboratively create documents. Other options are being considered by the AAF.

Google’s [G Suite for Nonprofits](https://gsuite.google.com/nonprofits) or [Google for Education](https://education.google.com) are free.
Federation Registry

- Simple to install and use
- Recommended for new federations

Alternatives:
- AAF Federation registry
  - In use by the AAF, SGAF, HKAF and Tuikiri
  - End-of-life technology stack – complete rebuild from group up to begin soon
- Jisc – Managed Federation - A cloud-based federation service for NRENs
- Janus - Fully featured metadata registration administration module built on top of simpleSAMLphp.
  - Maintained by SURFnet
- SWITCHaai Resource Registry (Not open source)
- InCommon Federation Manager (Not open source)

High level requirements
- Manager federation metadata
- Self service – reduce management overheads
- Validations
- Approval workflows
- Simple CRM
- Optionally manages multiple federations
Metadata Signing and distribution

Federation registry tools generate a federation metadata that is consumed by Identity providers and Service providers in the federation.

The technical trust in the federation come from the signature applied to the metadata by the federation operator.

- Publish end-points where signed metadata is available
- Publish the public key used to verify the signature
- Publish the function of and target audience of the metadata

See: https://md.aaf.edu.au
Metadata signing

There are a number of tools available for metadata signing

- Shibboleth xmlsectool V2 – Java command line tool
- pyFF - a simple but reasonably complete SAML metadata processor

Securing your signing key

Using a hardware-based security module (HSM)
  - NitroKey HSM – Ask Sifulan!
  - Using AWS tooling (expensive option, but nice fit if AWS infrastructure in use)

Most new federations will have their key stored securely on the file system where the metadata is generated and distributed.
Metadata Signing key

From the [eduGAIN Policy Framework Metadata Profile](#) 15.2.2013
- For signing its metadata, a metadata producer **MUST** use an RSA private key of at least 2048 bits

From the [eduGAIN Policy Framework v.0.5](#)
SAML Metadata Producers **MUST** ensure that their SAML Metadata signature meets the following requirements:

Public keys used for signing are at least 2048 bits in length. At least 3072 bits is **RECOMMENDED** for new deployments.
- EC public keys are at least 256 bits in length.
- The signature is made using an explicit ID reference, not an empty reference.
- The signature reference refers to the document element.
- The signature's digest algorithm is at least as strong as SHA-256, and does not use MD5 or SHA-1.
- The signature's signature method is RSA with an associated digest at least as strong as SHA-256 and does not use MD5 or SHA-1.
- The signature's transforms contain only these permissible values:
  - *Enveloped signature*.
  - *Exclusive canonicalisation with or without comments.*
SAML Metadata key rollover

AVOID at all costs!

The AAF recently rolled over from a 1024bits key to a 2048bits key
- Completed 10am AEST 22 July 2019
- Started some time in 2016

Aim to meet the highest level of signing requirements.
Use the same key for all metadata signing.
**MDQ (Metadata Query)**

**UK Federation**

“The size of the UK federation metadata aggregate has grown sufficiently large that scaling issues are appearing for some metadata consumers. We are piloting another approach where entities can request metadata for individual entities as required from our MDQ (Metadata Query) service, instead of periodically downloading a single aggregate file that contains metadata for all the entities in the world.”

MDQ is a mechanism that allows entities to request only the metadata they need, as they need it.

The [MDQ protocol](#)

The [InCommon per-entity Metadata Working Group final report](#) details much more about the operational aspects of an MDQ server.

What will happen when ASIAPac brings all its IdP into eduGAIN?
New tool under development by the Shibboleth Consortium...
  - Developer preview release available

Use Cases include
  - A command line tool that can read in a bunch of SAML entity descriptors, schema validate them, check certain policy constraints, filter out entities based on given rules, assemble the entities into multiple different SAML metadata documents, and sign them all.
  - A command line tool and web service that can perform the technical work of inter-federation. This essentially means doing everything in the previous use case but operating on whole metadata documents from various federations.
  - A web service that can operate as a metadata "oracle" for IdPs and SPs and hide the complexity of fetching, validating, and munging (potentially many) metadata sources. This service could be deployed within an organization and the organization's IdPs and SPs could delegate most of the hard work of dealing with metadata to the oracle, making their configuration simpler, decreasing network load, and potentially increasing resiliency in cases where external metadata may go offline.

These use cases are SAML-focused but the general aggregator product is not SAML-focused
Attribute Validator

- This service will validate the attributes provided about you from your identity provider ensuring they are provided in a format that is suitable for consumption by connected services.

Great tool to have to help diagnose attribute issues between IdPs and SPs and involves the user!
Virtual Home

Service Providers (SPs) often find that the population they want to serve includes individuals who are not represented by campus-based or other institutional Identity Providers (IdPs). In other cases, the individual's organizational IdP can not (or will not) release attributes necessary for the operation of the SP.

- Allow IdP subscribers to add users who are visitors
- Allow SP subscribers to add users for testing
- Allow small organizations to use as their home IdP
- Allow researchers to try federation!
Support Desk

- Respond to issues in the federation
- Knowledge base
- Assisting with installing, configuring and testing of IdPs and SPs
- Monitoring the federation status
- Setting up accounts (Virtual Home)
- Support involves everyone across the federation
  - Need to know the technical contacts of your subscribers
  - Involve IdP and SP admins
  - Be a conduit. e.g. direct simple password issues to the users home org
- Plenty of software options – Keep it Simple...
Federation Status

Knowing when some thing is down

- be proactive
- Minimal Red – in particular Core services and IdPs!

Check for...

- Service availability (HTTP Responding)
- SSL Status (Certificate current)
- Time Status (Time in sync)

Optionally...

- Send notifications
- Provide an API
Source Code Repository

- If you develop any software, configuration, etc for your federation...

Plenty of options out there...
Certificate Authority

For your web servers – everything thing HTTPS:

- **Let’s Encrypt** – free, automated and open
- Other free options available 30 to 90 days
- Paid options longer life, other uses

- Test your site with [SSL Labs’ Server Test](https://www.ssllabs.com/ssltest/)
  - *Aim for A or A+*
Email Server

Free Hosted email options are available particularly for
- *Not for profit*
- *Education related*

- Supports your domain name
- Email groups
- Secure email
- Virus and SPAM scanning
Video conferencing tools

Many virtual meetings as the federation operator
Many options

- Keep it simple and cheap
  - *For you and your meeting attendees*

- Be flexible
Customer Relationship Management

Know who your customers are
Know how to contact your customers
  - Individually
  - In bulk – newsletters, events, notifications, etc

Initially the federation register can address some of the CRM needs
  - Will need a better solution!