Federated Identity Management

AKA, Identity Federation or just Federation

Siju Mammen

SANReN

26th June 2013

What is Federation? Part 1

'When you hear the word "Federation" what do you think about?'

What is Federation? Part 1

'When you hear the word "Federation" what do you think about?'

Control

Purpose **Union**

Trust

Political System **Autonomy**

Centralised?

What is Federation? Part 2

Federation can be defined as:

- The formation of a purpose focused association/centralised unit where each member keeps internal autonomy. *(Paraphrased from an online dictionary)*

What is Federation? Part 2

Federation can be defined as:

- The formation of a purpose focused association/centralised unit where each member keeps internal autonomy. *(Paraphrased from an online dictionary)*

So, together, let us together define a purpose for a Fedearation.

Time for some roleplaying!

Volunteers?

Everyone wants everything?

Conflicting requirements?

The following are very important to an organisation's ICT team

- Legislation
- Security
- Control

Everyone wants everything?

Conflicting requirements?

The following are very important to an organisation's ICT team

- Legislation
- Security
- Control

But users do not care about any of that and they want:

- Convenience
- Ease of use
- Freedom
- Privacy? *(maybe)*

Everyone wants everything?

Conflicting requirements?

The following are very important to an organisation's ICT team

- Legislation
- Security
- Control

But users do not care about any of that and they want:

- Convenience
- Ease of use
- Freedom
- Privacy? *(maybe)*

And Service providers want

- Access control
- User information
- Compensation *(maybe)*

RECAP

Where are we now?

- A Federation is a group coming together for a purpose
- Institutions want easy access to services
- Services want some level of assurance that the user can have access to that service
- Services want to talk the same language to all the institutions
- Users want freedom and privacy

Bringing it all together!

We can finally define our Federation?

- Entities coming together to allow identities to be authenticated between one other, to provide users access to services without divulging unnecessary information to the service, while at the same time providing services seamless access to identities between institutions.

How do we implement this?

This part is not very important for this discussion.
Come talk to me privately.

How do we implement this?

This part is not very important for this discussion.
Come talk to me privately.

But the most important aspects are:

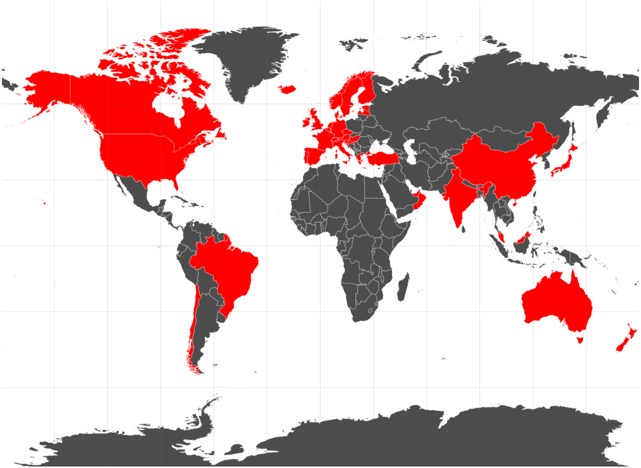
1. Trust
2. Common Language (SAML)

Research and education identity federations

The concept of Federation is not new and especially in the Research & education sphere, it is quite widely deployed in developed nations as shown in the following diagram:

Research and education identity federations

The concept of Federation is not new and especially in the Research & education sphere, it is quite widely deployed in developed nations as shown in the following diagram:



Federation in South Africa

'Could we assume that everyone is friendly to the idea?'
The SA environment had the following challenges (not unique to us though):

- Culture - SA's IT environment is very conservative
- Legal aspects - Legislation to deal with digital identities and information privacy are still being hashed out
- Funding - At least to get the Federation started.
- Knowledge - what/who/why/when?

The Plan - Part 1

'How we tried to overcome the challenges we faced'

Our approach was to:

- Following a top-down approach
- Get the CIO's of identity providers in a room together
- Have the community take ownership of the Federation moving forward

The Plan - Part 2

This was accomplished by holding a Workshop

The Plan - Part 3

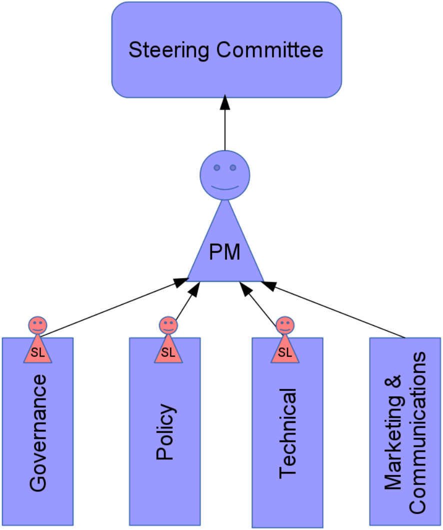
With a few international speakers

The Plan - Part 4

And lots of the participants from the community

The Outcome - The goal

'What we set out to achieve'



How to get involved

Contact me: smammen@csir.co.za

Get in touch with the various working groups that are working on different aspects of the Federation.

Tell Others about it.

Questions

Thank you

Supplementary Slides - Roleplayers in the Federation stage

'All the world's a stage - but who are the actors?'

Identity Provider - IdP

- The organisation that provides the user credentials

Service Provider - SP

- Whoever provides the web service that you want to access

Discovery Service

- Allows you to find your home institution

Federation Agent/Operator

- An optional entity that manages the Federation

Supplementary Slides - Technology part 1: Protocol

'We need to standardise our grammar!'

In the entire sphere of Federated Identity Management we have 3 or 4 protocols to choose from

- SAML 2.0
- WS-Federation
- OpenID Connect
- Information Card based identities

Practically we only have one choice: SAML 2.0. However we do have a choice of implementations of SAML 2.0 including:

- simpleSAMLphp
- Shibboleth

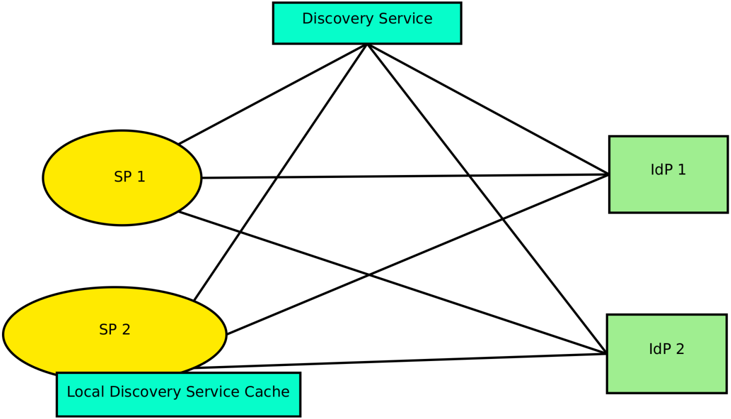
Supplementary Slides - Technology part 2: Attributes

'Let's make sure we are all speaking the same language'

Very Important - but I'll let the other speakers elaborate.

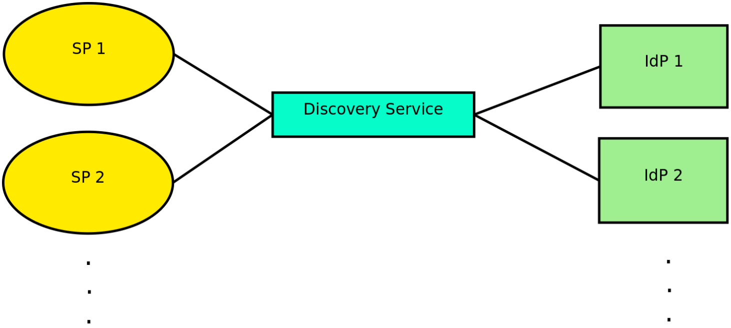
Supplementary Slides - Technology part 3.1: Mesh Architecture

'Maybe everyone should connect to everyone'



Supplementary Slides - Technology part 3.2: Hub-and-spoke architecture

'Or maybe central management is useful'



Supplementary Slides - Services

'Why should anyone go through all this effort?'

The simple answer to this question is Services.
Service providers want access to verified identities. To personalise and target their products better.

Examples of services include:

- Library services
- Grid services
- Video conferencing
- Cloud Services
- Certification Services
- Other Commercial Services

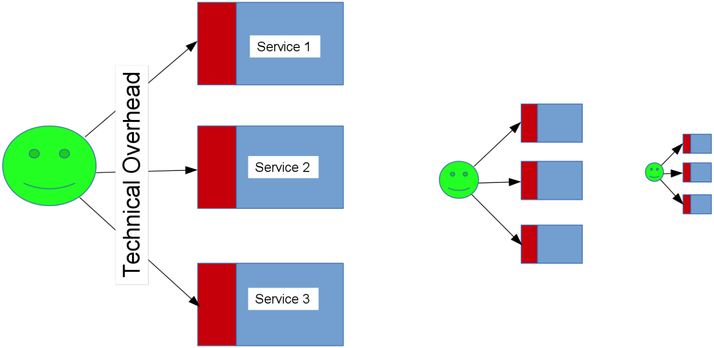
Supplementary Slides - Why bother? Part 1

Many of you will be thinking now:

- IdPs already connect to these services individually anyway.
- What incentive is there to be part of a Federation?

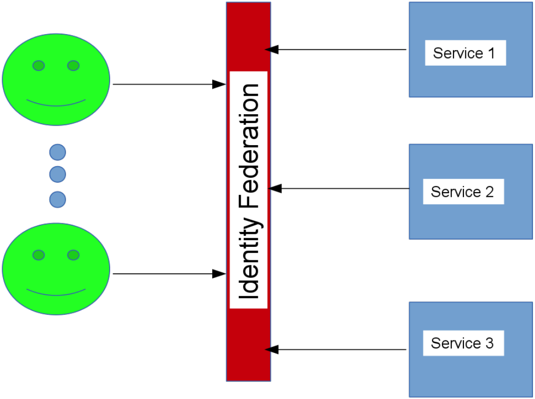
Supplementary Slides - Why bother? Part 2

Lets expand this idea a bit



Supplementary Slides - Why bother? Part 3

So whats different in a Federation?
IdPs and SPs, in a way, share the overhead of connecting between all services that they are connected to.



Supplementary Slides - Why bother? Part 4

The most important take home message for you:

1. You will need to expend the effort to connect to one another anyway. But in a federation, the effort you expend will be shared by all your services, including future ones.

Supplementary Slides - Decisions needed to be made

'What needs to be done, and who needs to do it?'

While there is no set procedure to implement a federation, the following aspects will always have to be decided on (my opinion is provided in brackets):

- Identify the scope of the Federation *(R&E institutes and related services)*
- Choose a protocol to use within the Federation *(SAML 2.0)*
- Identify a schema or set of attributes to be used within the Federation *(eduPerson as a Starting point)*
- Decide on the architecture of the Federation *(pilot both out)*
- Define the policies of the Federation *(build on the policies of other Federations)*

Supplementary Slides - Responsibilites of the Project Manager

'Making sure that things are done right?'

Tasked with:

- Manage streams
- Report progress to the steering committee
- Draw up a proposal for taking the Federation into production

Supplementary Slides - Responsibilites of the Governance stream

The Governance stream will provide recommendations on the following:

- Business Model and Strategy
- Funding of the Federation
- Scope/Boundaries of the Federation

Supplementary Slides - Responsibilites of the Policy stream

The Policy stream's has been tasked to:

- Draft a policy (based on our friends' policies)
- Decide on the attributes/attribute release policy needed for the Federation
- Level of assurance needed from institutions
- Decide how consent will be handled
- Define the roles and responsibilities of each member institution.
- To inter-federate or not to inter-federate?

Supplementary Slides - Responsibilites of the Technical stream

The Technical stream has been tasked to familiarise themselves with the available technologies in rolling out Federation and make recommendations on:

- Protocol for the Federation.
- Architecture for the Federation.
- Implementing a pilot of willing institutions.
- Identify potential use cases for the Federation.
- Interfederation?
- eduPerson Schema?

Supplementary Slides - Responsibilites of the Marketing and Communications stream

Very important stream that will:

- Define the Vision/Mission
- Draw up official communications with stakeholders
- Help sell the Federation at the right level

Supplementary Slides - Responsibilites of the Steering Committee

They are officially responsible for taking the Federation forward in South Africa. Specifically, they need to:

- Guide the PM and streams to move federation from a conceptual phase through a pilot phase and eventually into a production system.
- Ratify the proposal that can be submitted to member institutions regarding Federation.