Progress and Challenges In Introducing Eduroam and Federated Identity under Asi@Connect/Geant

Terry Smith – Australian Access Federtion (AAF)

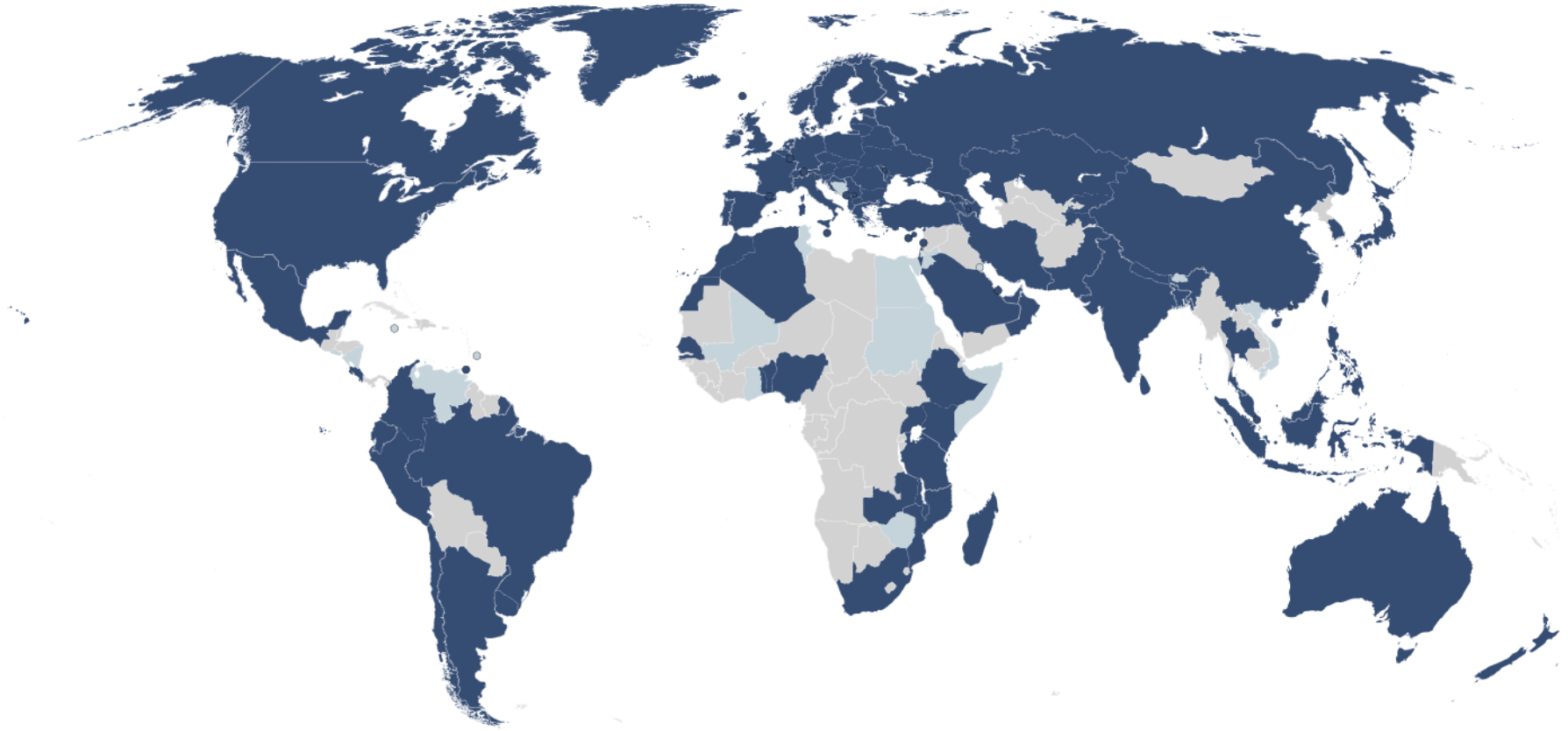
AUSTRALIAN ACCESS FEDERATION

eduroam is now available in 101 countries and has more than 4.3 billion authentications at educational and research institutions around the world. There are more than 400 million national and over 100 million international roaming authentications per month, together with nearly 30,000 hotspots around the world.

The service is a global success story offering secure, easy-to-use, WiFi roaming for students, staff and research teams and helping people work together wherever they are.

There is still a long way to go…

Coverage - Global



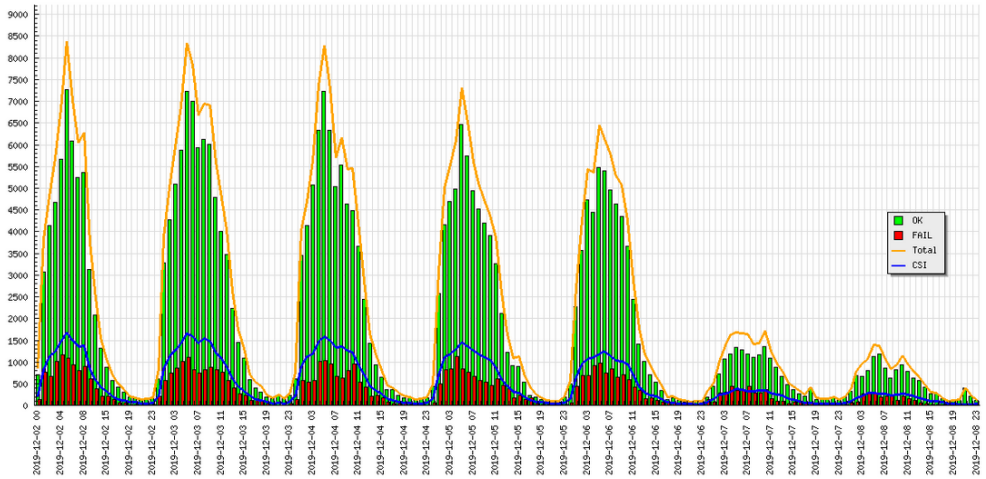
Coverage – Asia Pacific

Country	NREN/NRO	Number of service locations	Number of IdPs	Number of SPs
Australia	AARNet	410	74	93
Bangladesh	BdREN	N/A	N/A	N/A
China, Mainland	CSTNET	3	3	3
Hong Kong	JUCC	N/A	N/A	N/A
India	ERNET	N/A	N/A	N/A
Indonesia	UII	20	11	13
Iran	IRANet/IPM	N/A	N/A	N/A
Japan	NII	1413	172	175
Korea	KREONET	920	66	66
Lebanon	AUB	N/A	N/A	N/A
Macau	University of Macau	N/A	N/A	N/A
Malaysia	MYREN	55	21	21
Nepal	NREN	N/A	N/A	N/A
New Zealand	REANNZ	183	26	27
Oman	OMREN	16	15	16
Pakistan	PERN	52	52	52
Republica of China (Taiwan)	Moe	N/A	N/A	N/A
Singapore	SingAREN		12	12
Sri Lanka	LEARN	22	19	19
Thailand	UniNet	424	18	18
The Philippines	ASTI	3	3	3

Authentication Statistics

Nation	National	International (visitors from other countries)
Singapore	75573	247348
India	0	1699
Others	Unknown	Unknown

** Data from last week*



- Data is being collected
- Not been sent to central eduroam site / or sent in old format
- NRENs may generate their own stats

➔ Unable to determine the benefits

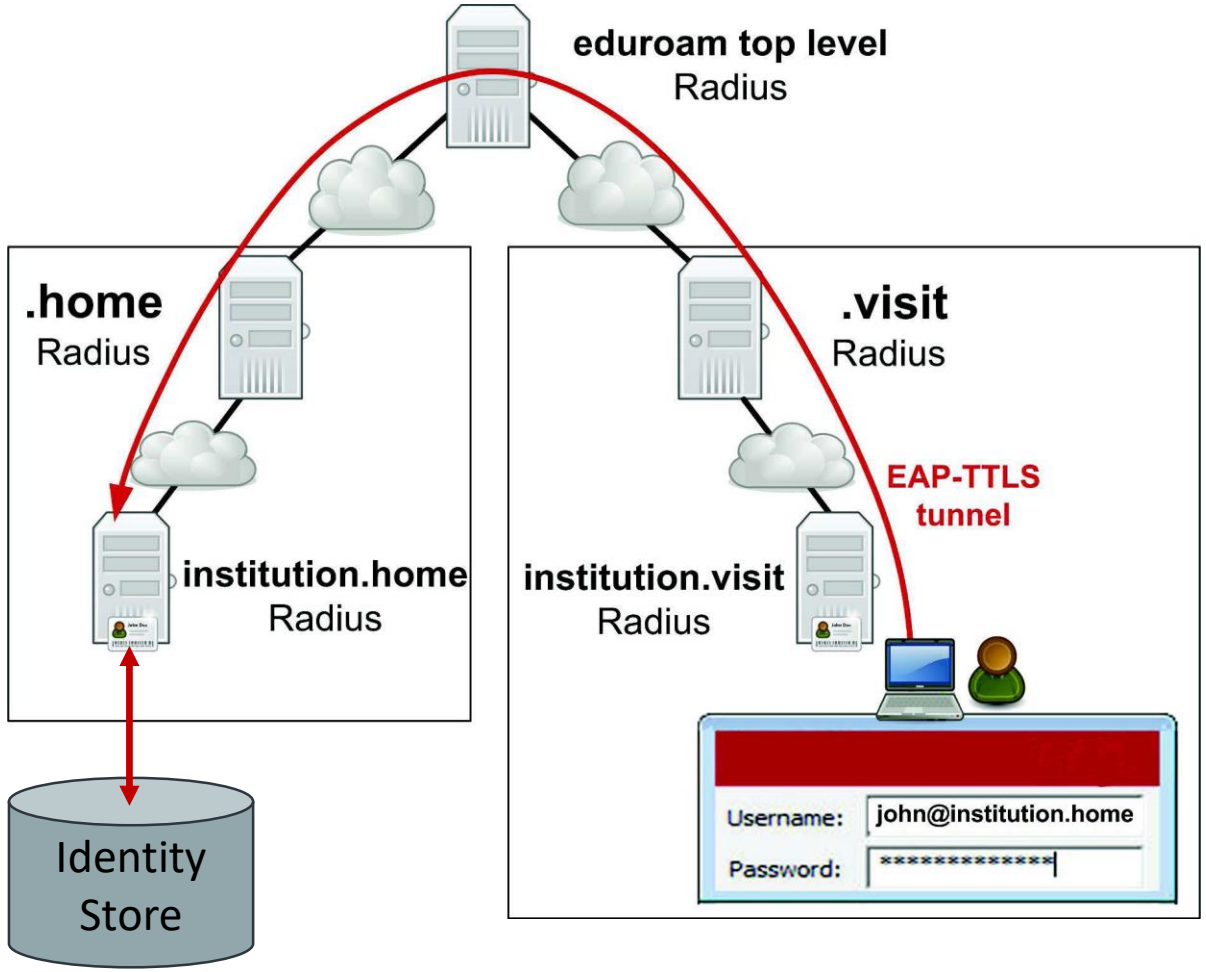
➔ Thus needs to be address by the region (APAN49)

Architecture

eduroam is based on 802.1X* and a linked hierarchy of RADIUS servers containing users' data (usernames and passwords). Participating institutions must have operating RADIUS infrastructure and agree to the terms of use. eduroam can be set up in three easy steps:

- Set up a RADIUS server connected to your institutional identity server (LDAP).
- Connect your access points to your RADIUS server.
- Federate your RADIUS server.

Requires a managed identity store at each institution (LDAP or AD)



Management

- Global eduroam Governance committee (GeGC)
  - Asia Pacific – 3 members (Hideaki Goto, Tohoku University, Japan: Neil Witheridge, AARNET,Australia: Deokjai Choi, Chonnam National University, Korea)
- Compliance Statement - outlines the minimum technical and organizational standards for…
  - roaming confederations (RC)
    - APAC Confederation?
  - national roaming operators (NRO)
  - roaming operators (RO)
  - Identity Providers (IdPs)
  - Service Providers (SPs)

Security

- eduroam does NOT use a Web Portal, Captive Portal or Splash-Screen based authentication mechanisms.
- eduroam requires the use of 802.1x which provides end-to-end encryption
  - private user credentials are only available to your home institution
  - Only required to trust certificate of your home institution

eduroam designed to be secure: https://www.eduroam.org/eduroam-security/

Security

- The RADIUS hierarchy forwards user credentials securely to the users' home institutions, where they are verified and validated.
- To protect the privacy of the traffic from the user's device over the wireless network, the latest up-to-date data encryption standards are used.
- The user's home institution is responsible for maintaining and monitoring user information, even when the user is at a guest campus. Thus, this data is not shared with other connected institutions.

Future Plan and Roadmap

- Continued growth
- govroam
- eduroam and Passpoint - City Wi-Fi Roaming
  - Investigations underway in Japan lead by Hideaki Goto and his team

More information

- eduroam
- AARNets eduroam
- How to....' (deploy, promote and support) eduroam (Géant wiki)

Presentation

- Intro To eduroam by Deokjai Choi at APAN46
- eduroam and Passpoint/NGH Updatesand the City Wi-Fi Roaming 2019 by Hideaki Goto at APAN48

Identity Federation

Federated identity is a secure way for disparate systems to get access to your identity information. Your information may only exist in one system. But, with federated identity, other systems can also have access this information.

The key to federated identity is trust.

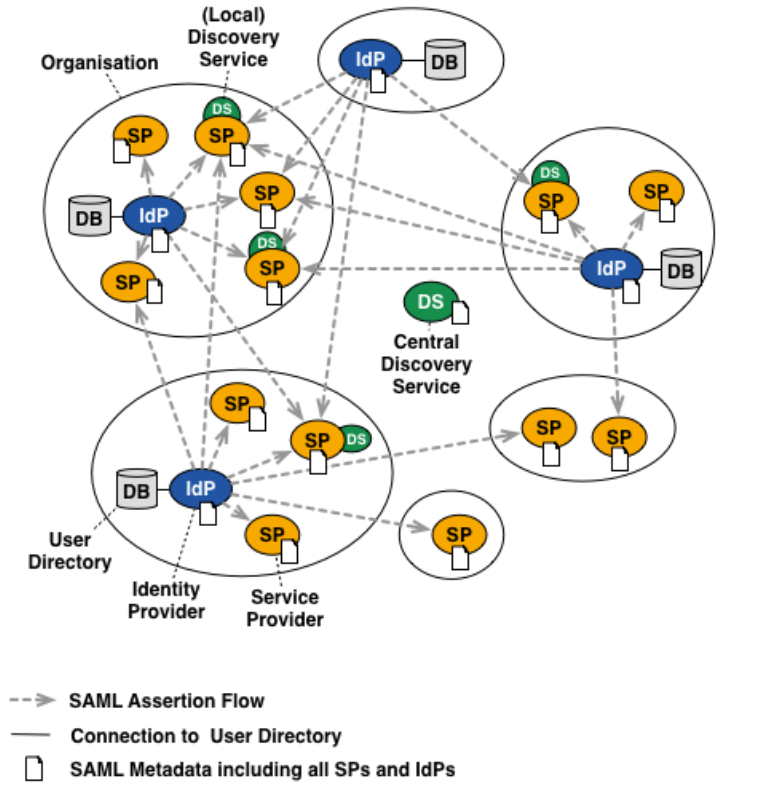
The system that holds your information and the system that is requesting your information must trust each other.

- To make sure your information is being transmitted to a trusted place, the system that holds the information must trust the system that is requesting the information.
- The system requesting the information has to trust the sender to ensure they are getting accurate and trustworthy information.

FIM – Existing / Proposed Architectures

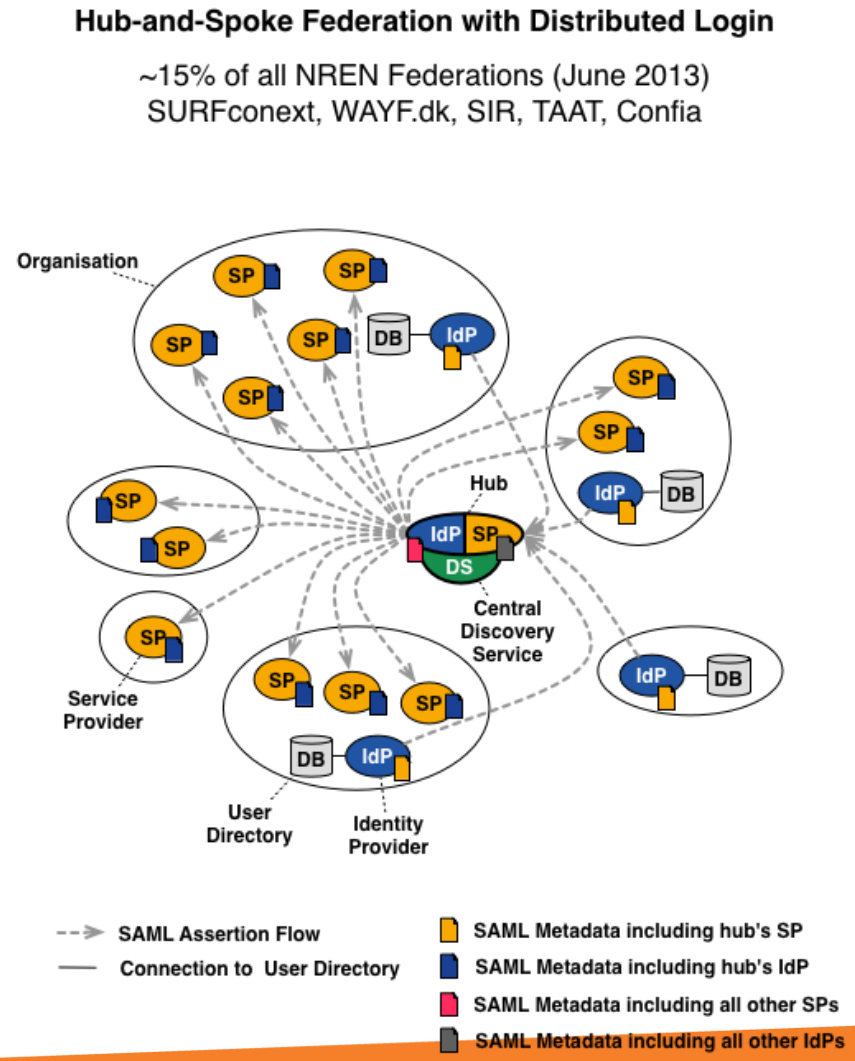
Full Mesh Federation

~80% of all NREN Federations (June 2013)
E.g InCommon, UKAMF, SWITCHaai, SWAMID, HAKA, AAF



- Common model, particularly for new federation
- Simple to deploy and maintain
  - Federation registry tool
  - One Federation metadata feed
  - Centralized discovery service
- Very resilient
- eduGAIN integration is straight forward
- Difficult to capture utilization information
- Slightly more work for IdPs and SPs

FIM – Existing / Proposed Architectures



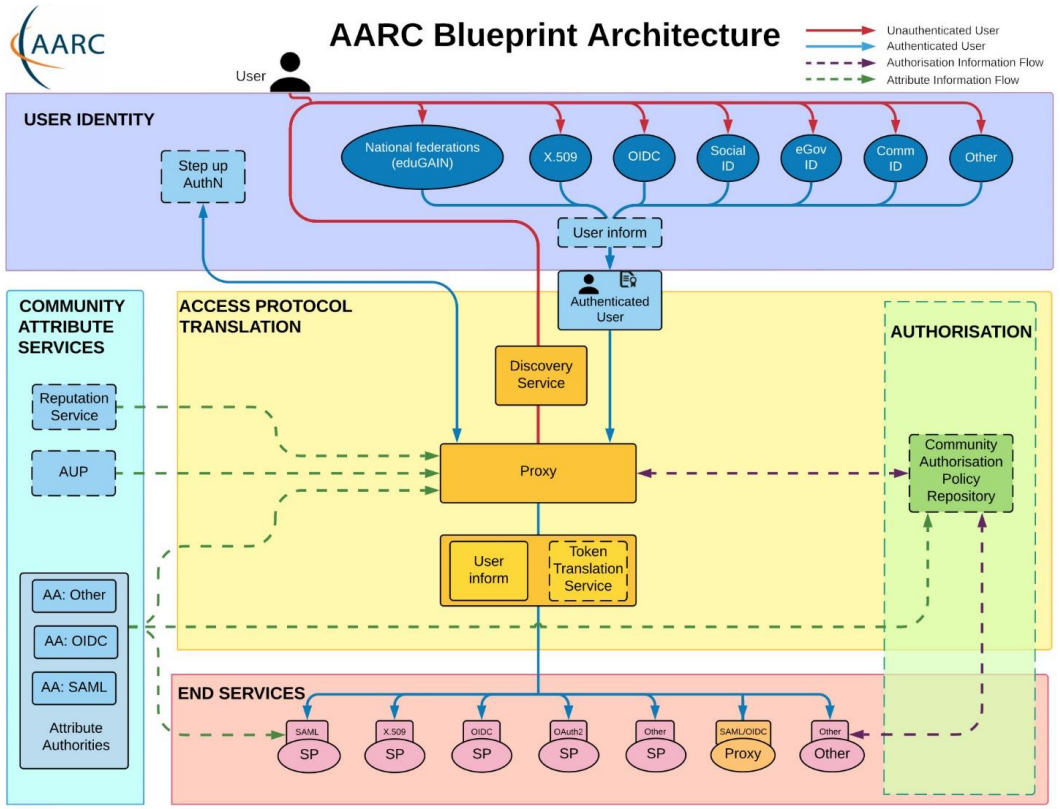
- More complex – all traffic passed through the hub. Needs to be highly available!
- Separate Metadata for IdPs and SPs
- Easier to obtain utilization information
- Centralized functions can be added with greater ease
- More difficult to integrate with eduGIAN
- Slightly easier for IdPs and SPs

FIM – Existing / Proposed Architectures

Hybrd

- Generally starts as a Mesh federation
- Small hubs of services start appearing
  - Authentication Proxies / Bridges
  - Services start to pool around these proxies / bridges
    - Protocol translation
    - Shared unique Identifiers
    - Additional attributes added at the hub
    - MFA at the hub
    - Social logins
- Can be operated by the federation or service provider

FIM – Existing / Proposed Architectures



Community focused

- Hybrid on steroids
- Hubs of activity based on the AARC Blueprint
- Services a community is interested in access or collaborating around
- Users can be identified as being part of the community from the wider federation.

FIM – Attributes

- Define a core set of attributes
  - *“A set of Attributes selected by the Federation that all Identity Providers are required to support”*
- A super set of the REFEDS Research and Scholarship Entity Category
    - shared user identifier
    - person name
    - email address
    - Affiliation
- The AAF currently has 16 CORE attributes defined

FIM – Challenges in Implementation

Making a start … Developing a Business case…

1. The technology required (in this case, the tools and platforms around identity and access management),
2. The policy required (including federation policies, organizational policies, and security policies),
3. A business model regarding the operations of the federation; and,
4. A Service Delivery system to support the use of the service

FIM – Challenges - Technology

The technology required

- Federation Registry
- Metadata distribution
- Centralized discovery service
- Virtual home IdP (for the homeless)
- Attribute validator
- Federation status
- Support desk
- Web site

Options

- Open Source
- SAS
- Avoid in-house developed!

Costs

- On-going cost in running and maintaining these components
- Providing for your nation – High avilibilty

FIM – Challenges - Policies

The policy required

- Federation Rules
- Metadata registration practice statement
- Privacy statement
- Security policies
- Change management
- Disaster Recovery and Business Continuity
- Logo usage policy
- Data breach policy
- Etc, etc, etc…

Policy life cycle

- Development
- Approval
- Maintenance

Policy Compliance by customers

- Self asserted
- Regular review

FIM – Challenges – Business model

A business model regarding the operations of the federation

- Funding
  - User pays – subscription model
    - IdP pay
    - SP pay
  - Government funded
  - Commoditizing identity information
  - Project funding

What are the costs?

- Staff (How many?)
- Running / Maintaining Infrastructure
- Marketing
- Innovation
- Support and Education
- Travel and Conferences

FIM – Challenges – Business model

VerifID Global is integrated with universities and research organisations, enabling verification of customers associated with their institution.

- Services that just want to know if their customer is a student or staff member
  - Offer discounts
  - Commercial in nature
  - Yes or No – no identity information provided
- Charge per verification – supplements your income

- Developed and run by the AAF
- Used by UKFed

- Service providers are looking for quality data
- Opportunity

FIM – Challenges – Service Delivery

A Service Delivery system to support the use of the service

- web content
- a knowledge base for help desk support
- training
- communication
- outreach
- marketing

Customer education

- A complex product
- Requires users to change change their existing behavior, processes, or workflows
- A diverse user base in terms of needs and roles
- Products that are updated regularly with new features and functionality
- Products that require extensive support

A strong customer education program can have a huge impact on the business including increasing customer satisfaction scores, reducing support ticket volume, improving product adoption, driving lead generation, generating services revenue, and increasing renewals.

FIM – Challenges – Innovation

Innovation must be a part of your business plan, not just for the initial discovery of what is required, but to provide information on how to make these services relevant as best practice and community requirements change.

By making innovation part of your future service delivery, you provide a stronger and more attractive area for the campus or other funding source(s) to continue to invest in identity services.

FIM – Planned services under federation

There is no viral/killer federated application!

- Each federation will identify its own key services

Australia – Shared storage (AARNets CloudStor), data sets and mash ups (AURIN), Cloud Infrastructure (NecTAR), and others. Research focused.

Sri Lanka – Video conferences, eduVPN, eduGAIN services

Korea – Shared storage, video conferencing, Jupyter Notebooks, GitLAB

FIM – Planned services under federation

Market Research

- Who is your target market, student, faculty, researchers, academics?
- How do they collaborate, could this be improved?
- Has it been done in other federations? (reuse)
- Are researchers from other federations wanting to collaborate

FIM – How many per country?

Generally one or two federations per country…

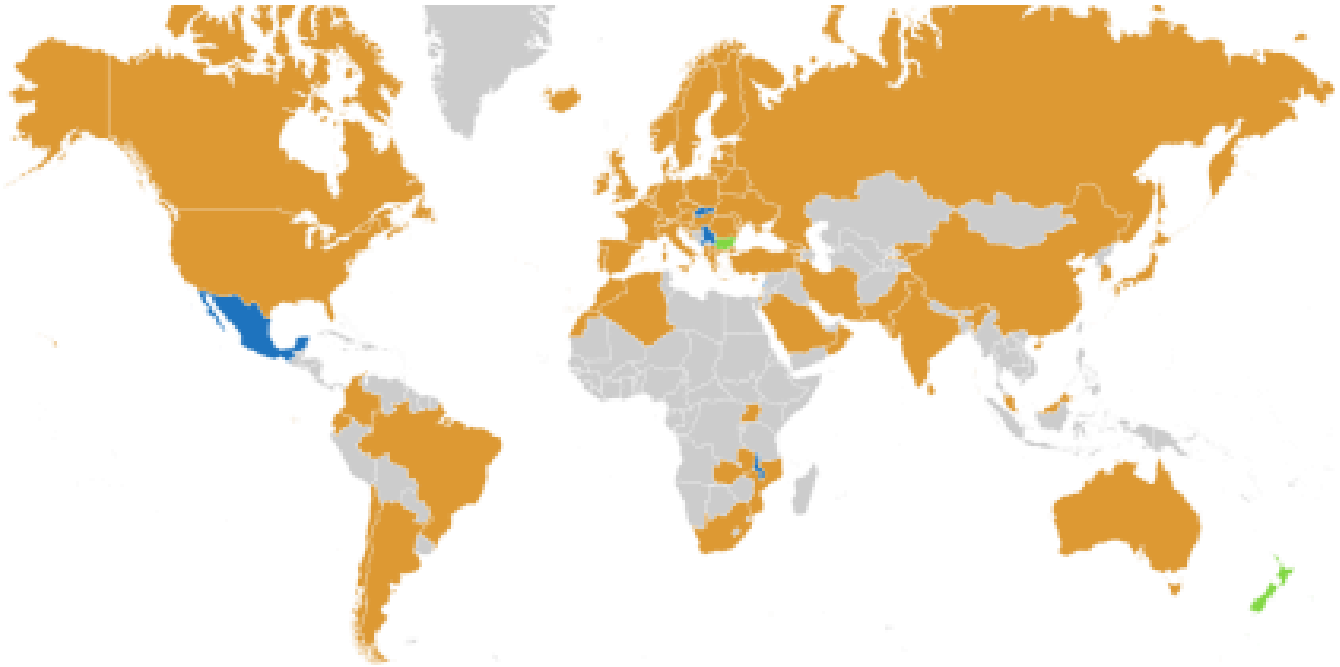
- Number of institutions
- Groupings of institutions
- Number of NRENs

Who runs the Identity Federation

- Mostly NRENs
- Other organisations trusted by the institutions (AAF, InfLibNet, JUCC, etc)

eduGAIN Inter-federation

- 68 Federations participating (and growing)
- 3168 Identity providers
- 2667 Service providers



eduGAIN Challenges

- No real service catalogue yet!
  - Entity Database Explorer is a good starting point
  - Is limited to data available in the SPs metadata

- Will all services work?
  - Many services are federation specific and may not be configured for eduGAIN
  - Attribute release will be a problem
    - Just determining which attributes a service want may not be easy
  - Some will run their own WAYF
  - Documentation may be limited or non-existant

eduGAIN Opportunities

- Many services on offer
- Build a simple catalogue for your researchers (See KAFE Applications page)
- Improve quality of your IdPs (Gold standard)
  - eduGAIN baseline
  - Configured for Research and Scholarship and SIRTFI
- Opt in for both IdPs and SPs
  - They need to know what it means to join eduGAIN
  - The Good, the Bad and the Ugly!

eduGAIN Outcomes

- Reduce the risk that will have issues with an eduGAIN SP
- Focus on quality services for our users

More Information

- REFEDS
- The Value Proposition for Identity Federations
- Research And Scholarship Entity Category
- SIRTFI
- Baseline Expectations
- VerifID Global

Conclusion and Recommendations

- It’s worth the effort – for your researchers!
- It’s not a project, it’s a life style – ongoing and rewarding commitment
- Start now
  - Build a pilot federation
  - Engage with REFEDS and APANs IAM-Task Force
  - Engage now with IT folk, training, webinars, demonstrations, etc
  - Engage now with IT leadership, sell the benefits, cost savings, etc
  - Identify the willing organisations and work with them, the rest will follow
  - Ensure people know the difference between eduroam, federation and eduGAIN
  - Use others tools, do NOT build new tools!


Time for
Questions