APAN Task Force proposal

for

Federation Deployment in the Asia Pacific Region

Version 1.0

Prepared by Terry Smith

Australian Access Federation

November 2014

1. Acknowledgements

2. Contributors

This document has been produced by Australian Access Federation Inc. in conjunction with the collaborating partner editors, with input and comments from individuals selected for their expertise in the subject area, including eduroam, research and education federation service development and operating it as a national service.

The views expressed in this publication are those of the editors, unless stated otherwise, and do not necessarily reflect the opinion of the participating experts.

Contributors	Role	Organisation
Sat Mandri	Service Manager	Tuakiri, New Zealand Access Federation Inc.

3. Document References

This section contains a list of links and documents that have been referenced or are related to eduroam and identity federation services mentioned in the document.

Links	Information
TERENA	Trans-European and Education Networking Association
SCHAC v1.4.1	Schema for Academia (Schac), developed by TERENA
REFEDs	Research and Education Identity Federation Global Working-group
eduGAIN	eduGAIN interfederation service
Internet2 Middleware	Trust, identity and middleware consortium

NIST Special Publication 800-63-2	NIST Electronic Authentication Guideline
auEduPerson Schema	auEduPerson Definition and Attribute Vocabulary developed by CAUDIT
eduroam	Secure access to internet connectivity and world-wide roaming
elecira	Europe Latin America Collaborative e-Infrastructure for Research Activities

4. Title

The task force will have the title "***Federation Deployment in the Asia Pacific Region***".

5. Objective

A coordinated approach by the taskforce to support the development and establishment of research and education identity federation and eduroam service in the Asia Pacific region.

6. Goals

This taskforce committee will maintain focus on three primary goals:

1) Develop and establish national identity federation service within participating/member countries in the Asia Pacific region
2) Enable participating/member countries national identity federation services to join eduGAIN
3) Enable participating/member countries to deploy eduroam

7. Joint Collaboration

This initiative will be jointly led by APAN, and the appointed Taskforce Committee in collaboration with the participating/member countries in the Asia Pacific region who are willing and demonstrate commitment to establish and operate national identity federation and eduroam service in their respective country.

7.1 Taskforce committee responsibilities

- Lead, plan, organise, and jointly execute project deliverables
- Subject-matter-expertise and knowledge share
- Coordinate training workshops and present at events and conferences
- Report back to APAN Board

7.2 Participating/member country responsibilities

- Create a national initiative and gather support from your respective country's tertiary and research sector
- Liaise with your country's respective Ministry responsible for Tertiary Education and Research sector and the National Research and Education Network (NREN), and get their buy-in.
- Establish project governance committee, and funding arrangement
- Setup project, plan, organise and implement
- Carryout outreach and communication
- Establish Project Space/Wiki/Document Store and Service website

8. Meeting Proceedings and Reporting

Members of the Task force will meet monthly (virtually) to ensure steady progress. An invitation will be made to an APAN Board director or the General Manager to join the meetings as an observer.

All meeting minutes will be recorded and published on the APAN website.

Meeting agendas and minutes from the previous meeting will be distributed to members of the Taskforce no later the 1 week prior to each meeting.

The Taskforce will report briefly at each APAN meeting to the Council on plans, progress and any proposed changes, and any requests to extend their terms.

9. Federated Identity Management

Any reference to **Federated Identity Management (FIM), Identity Federation, Identity Access Federation** and **Web Single-sign-on/SAML Federations** mean the same thing.

Federated identity, and its management, refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources.

In other words, rather than having separate credentials for each system, federated identity management allows users to use a single digital identity (i.e. username and password) to access all resources to which the users are entitled.

Federated Identity Management constitutes of three key components: **Users, Identity Providers** and **Service Providers**.

9.1 Users

Each user (sometimes called a subject or principal) is associated with a person. A user is characterised by an identity, a collection of attributes that represent properties about the user. The attributes are classified into categories to give a general indication of how they are normally used:

- Personal characteristics

- Contact/location information
- Student/staff information
- Employee information
- Unique identifiers
- Entry metadata/administration information
- Security attributes and keys
- Confidentiality/attribute release (visibility)
- Authorisation and entitlements
- Group-related attributes
- Other attributes

9.2 Identity Providers

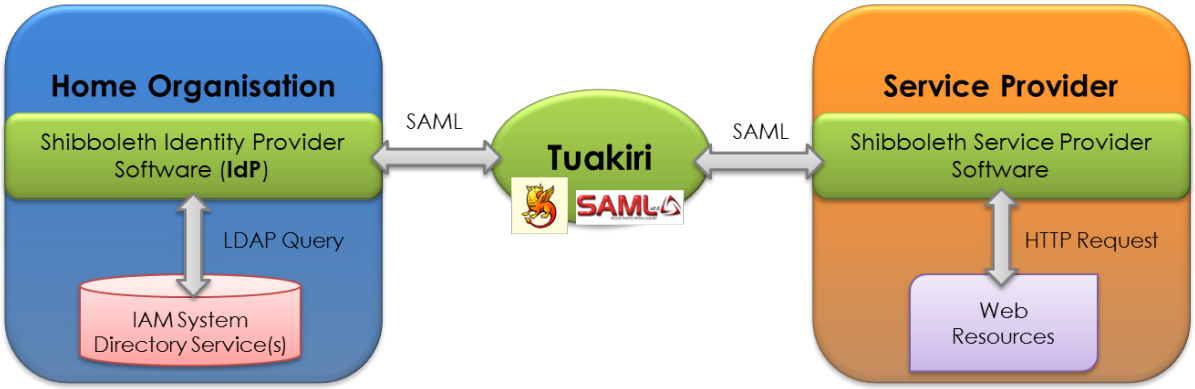
Federated Identity Management enhances security and convenience by introducing an identity provider that must be trusted to perform certain functions. User authentication and identity management are delegated to this identity provider, which implements mechanisms that let administrators control attribute release and mechanisms that issue authentication assertions (statements about user attributes). A service provider may decide whether to authorise the user on the basis of their authentication assertions.

The principal responsibility of the identity provider is creating, updating, releasing, and deleting attributes and identities, and complying with relevant privacy laws (such as the Privacy Act 1993).

9.3 Service Providers

Service providers authorise users on the basis of authentication assertions. The authorisation decision depends on the attributes received, and the core attributes mandated by a Federation Service. Service providers depend on receiving authentication assertions that contain up to date attributes. An identity provider is responsible for validating attributes initially, verifying their value in connection to a real world identity, and maintaining currency of those attributes.

Illustration 1: How it works



1) An institution deploys an Identity Provider (IdP), a Service Provider (SP), or both.
2) The IdP connects to the existing Identity and Access Management System (IAM).
    - The institution creates and administers user credentials in its IAM system.
    - Some configuration is done to map the organisation's attributes to attributes in the schema used by a national identity federation service (Tuakiri in this example).
    - The IdP is configured to release a set of core attributes specified by the national identity federation service.
3) The national identity federation service provides public metadata about IdPs and SPs.
4) The SP consumes the attributes and grants access based on those attributes.

9.4 Benefits

Through the use of Federated Identity Management at a national level, the Universities, Technical Institutes, Research Institutes, Government Agencies and including the higher education sector can remain competitive in an increasingly competitive world of teaching and learning, academia and research. Federated Identity Management will aid effective, interactive collaboration between users and contribute positively to future tertiary students.

A national identity federation service provides many benefits for **Identity Providers**, **Service Providers**, **End Users**, and **Educational and Research Sectors.**

- ➢ Easier to comply with regulatory requirements *(Respective Countries Privacy Act)*
- ➢ Conformance to authentication standards
- ➢ Ease of use when accessing services and better service offered to users
- ➢ Can integrate with existing access management systems
- ➢ No need to create local accounts and maintain multiple user databases

- ❖ Authentication is performed by the Identity Provider
- ❖ Can authorise per institution, role, and /or entitlement

➢ Reduced user support requirements

➢ Timely provisioning and de-provisioning of services, leading to user license savings

➢ ePublishers can tailor services based on usage and preference

➢ Facilitate sharing of resources and collaboration across sectors

➢ Ultimately improve the user experience

10. Guiding Principles for a National Identity Federation Service

Guiding Principles

✓ **Policy driven, centrally led, collaboratively delivered**

Top down approach: The national identity federations initiative will be led jointly by the country's Universities, Research Institution and the sectors R&E support organisations, and delivered in collaboration with the Ministry responsible for higher Education and Research sector.

Bottom up approach: Identified organisations willing to contribute resources, expertise and knowledge work together to develop and deploy pilot federations highlighting the successes and benefits to other Universities, Research Institution and the sectors R&E support organisations developing a groundswell of interest and activity in growing them into national federations and gaining the support of the Ministry responsible for higher Education and Research sector.

✓ **Customer ease of use, seamless experience**

A service oriented approach to provide the customer with a seamless experience when accessing services for teaching and learning, research, industry and Government agency collaboration.

✓ **Fabric of trust, assurance, confidence**

To provide a platform for fabric of trust, assurance and confidence in accessing digital assets, while maintaining privacy and security of information.

✓ **Shared capability, benefits all parties**

Sharing resources by default reduces duplication, re-engineering, complexity and cost, and benefits all parties.

✓ **Efficient, Effective and Excellence**

A national federated identity management service that is efficient, cost effective and excellent serving wider sector needs.

11. eduGAIN

eduGAIN is a service developed within the GÉANT project. eduGAIN connects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.

11.1 Benefits

eduGAIN will serve as a platform for universities, research institutes and government agencies to develop solutions to challenges and to foster cross-border collaboration and connect at a global scale level. Federated Identity Management together with eduGAIN will bring simplicity when collaborating across borders whilst adapting to the multiple needs of the research community.

12. eduroam

eduroam (**edu**cation **roam**ing) is the secure, world-wide roaming access service developed for the international research and education community. For more information see: eduroam policy service definition_ver28_26072012

12.1 Benefits

eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.

13. Proposed Chair

Terry Smith, Technical Manager, Australian Access Federation

14. Proposed Taskforce Committee

The following list of participants is currently unconfirmed, will need confirmation for each regarding their willingness to participate. Members of the Taskforce Committee are expected to volunteer equal contributions.

Organisation	Name	Person
AAF	Australian Access Federation	Terry Smith
AARNet	Australia's Academic and Research Network	Neil Witheridge

GakuNin	Academic Access Management Federation in Japan	Hideaki Goto Kazu Yamaji Motonori Nakamura
SIFULAN	Malaysia Academic Access Federation	Suhaimi Napis
Tuakiri	New Zealand Access Federation	Sat Mandri
TERENA	The Trans-European Research and Education Networking Association	Brook Schofield
APAN-KR	Asia Pacific Advanced Network-Korea	Deokjai Choi

15. Terms of reference

Stimulate the development of national identity federations across the APAN/TIEN members and non-member countries in the Asia Pacific region.

Using a top down approach and working with each of the Asia Pacific countries identify an appropriate organisation to be the initial operator of identify federations within each nation providing them with;

A policy and governance framework (based on previous work undertaken by TERENA in Latin America, and developments in Australia and New Zealand over the past 5 years)

A set of tools to streamline the implementation and operation of the federations

Training workshops and materials to enable the national federation operator organisation to develop and grow the federation usage across their respective countries.

The terms of reference includes;

1) Establish and operate a National Identity Federation as an-ongoing-concern and Customer Services
2) Federation Policy/Rules
3) Federation Technology
4) Federation Business Development, Value Proposition and Marketing

Based on experience of the TERENA project by introducing eduroam first will result in quick win where in some cases it has helped build enthusiasm before tackling the national identity federation service initiative. While both eduroam and federated identity management operate

on different technology stack, the benefits realised and experienced by the users are the same "secure and easy access".

The taskforce committee will work with participating/member countries identity federation service to enable them respectively join eduGAIN as this will provide the new federations with a number of research and scholarly services minimising the chicken and egg issue experienced by most of the earlier national federations. Experience from the Europe Latin America Collaboration e-infrastructure for Research Activitues (ELCIRA) program nations are join eduGAIN early to gain access to the many services leaving the creation of local services until later in the deployment.

Federation tools and best practices will be selected from best of bread tools from established national federation where there is clear evidence of continued maintenance and development of the tools and service utilisation/growth.

All training material will be made available to participating organisations via the APAN website. Translation of the material into local language will be encouraged to ensure the widest possible dissemination of knowledge.

15.1 Out of scope

15.1.1 Certificate Services

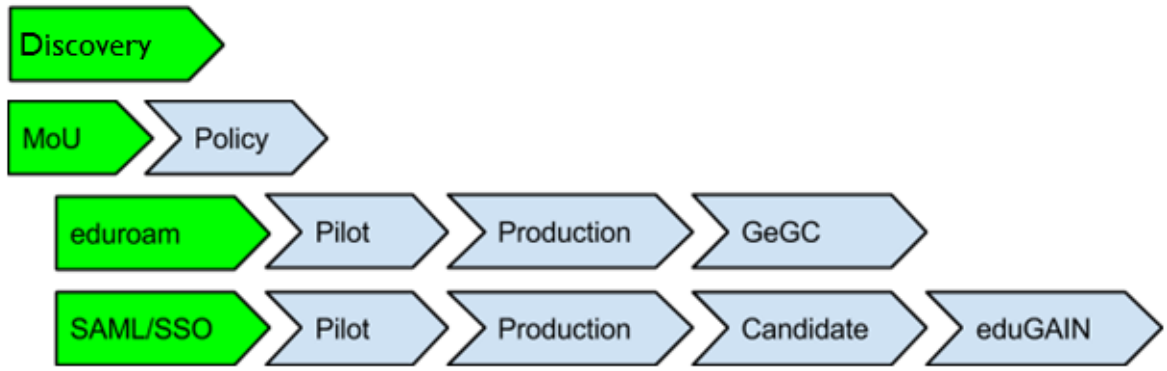
The offering or creation of a certificate service for the AP region is out of scope for this Task Force. There are number of commercial certificate providers that offer a range of certificate products including Grid certificates that can be used at a national level.

15.1.2 Service Provider Agreement and License Brokerage

Any requirement for service provider agreement and license brokerage will be the responsibility of the respective participating/member country, or its appointed national procurement agency.

16. Milestones and Expected Outcomes

16.1 Work Packages



Project Initiation

Task P.1 Develop a high level project plan as the Task Force Master plan

Work Package 0 (WP0) – Discovery

Task 0.1 Collection of information to understand the level of development of federations across the APAN/TIEN members and non-members countries in the Asia Pacific region;

- Existing deployments of eduroam and SAML/SSO federations
- Country's National Research and Education Network and/or National Research Organisations
- Size and make up of country's tertiary and research sectors
- Identify potential governance structures that could be used to initiate federation activities within each nation

Task 0.2 Report on each countries capacity to operate an eduroam and SAML/SSO federations identifying any gaps that need to be filled

Task 0.3 Identify a country that is capable and ready for federations that can be targeted for early adoption to produce a case study and federation launch templates. Malaysia has agreed to early adoption and to be used in a case study.

Work Package 1(WP1) – APAN Member Services

Task 1.1 Ensuring that the APAN Secretariat (and TEIN*CC) offer all their services via Federated Infrastructure.

Task 1.2 Write a Memorandum of Understanding / Letter of Intent for circulation between APAN/TEIN members.

Task 1.3 Promote the Memorandum of Understanding / Letter of Intent between APAN/TEIN members and get agreement on the adoption of record the progress.

Task 1.4 Ensure that APAN/TEIN meetings are supported by the necessary federated infrastructure to promote further deployment

Task 1.5 Record and report on progress of the other work packages to the APAN board

Task 1.6 Wrap up the taskforce at the end of its term and ensure all information is publicly available

Task 1.7 Provide guidance on the future direction of taskforces to support the development needs of the APAN community including investigation of additional Federated Infrastructure for Deployment/Adoption

Work Package 2 (WP2) – Federation Development

Task 2.1 Establishing a Policy Development Group for each Territorial Federation

Task 2.2 Adapting the REFEDS Federation Policy Template to support Federation Goals

Task 2.3 Advice Guidance on Technical Profiles, Governance and Business Processes

Task 2.4 Federation Operation Practice Statement Development for Federations

Work Package 3 (WP3) – Federated RADIUS Deployment

Task 3.1 Deployment of a Federation Level RADIUS infrastructure in each Federation ensuring they meet the specifications and operational requirements for eduroam

Task 3.2 Deployment of eduroam at the institutional level

Task 3.3 Recognition of each deployment by the Global eduroam Governance Committee (GeGC)

Work Package 4 (WP4) – Federated SAML Deployment

Task 4.1 Establish Test/Staging SAML Federation with institutions who are willing to participate

Task 4.2 Establish Pilot SAML Federation with Name, Website and Metadata Aggregate

Tack 4.3 Deployment of a Virtual Home Identity Provider by the Federation Operator in each country for users who are not directly associated with any subscriber

Task 4.4 Adoption + Participation in a SAML Interfederation Service for each Federation

17. Project deliverables

The Taskforce will operate for approximately two year (four APAN meetings) in which time it will deliver on its objectives along a series of milestones. These deliverables and milestones will be identified and schedules in the project plan that will be presented to the Joint Session of Identity and Access Management (IAM) WG and REFEDS at the APAN 39 meeting.

ID	Deliverables	Due Date	Presented at
M0	D1 Taskforce proposal accepted by APAN Council	Dec 2014	
M1	High level project plan	Jan 2014	APAN39

18. Participating places in the Asia Pacific Region

The following places have been identified that may be beneficiaries of the activities of this task force. This table will be used as starting point for Work Package 0 – Discovery identifying places of interest to the Task Force.

	Affiliations	Federation Operator	NREN
Afghanistan	TEIN*CC		
Australia	APAN TEIN*CC	**SAML/SSO:** AAF - Australian Access Federation **eduroam:** AARNet	AARNet
Bangladesh	TEIN*CC		BDREN
Bhutan	TEIN*CC		
Brunei Darussalam			
Cambodia	TEIN*CC		
China	APAN TEIN*CC		CSTNET, CERNET, NSFCNET
Fiji			
Hong Kong	APAN TEIN*CC		HARNET
India	APAN TEIN*CC		ERNET
Indonesia	APAN TEIN*CC		INHERENT
Japan	APAN TEIN*CC	GakuNin - Academic Access Management Federation in Japan	SINET
Laos	TEIN*CC		
Malaysia	APAN TEIN*CC	SIFULAN - Malaysia Academic Access Federation	MYREN
Marshall Islands			

Federated States of Micronesia			
Mongolia	TEIN*CC		
Myanmar			
Nauru			
Nepal	APAN TEIN*CC		NREN
New Zealand	APAN	**SAML/SSO:** Tuakiri – New Zealand Access Federation **eduroam:** REANNZ	REANNZ
Pakistan	APAN TEIN*CC		PERN
Palau			
Papua New Guinea			
Philippines	APAN TEIN*CC		PREGINET
Republic of Korea	APAN TEIN*CC		KOREN, KREONET
Samoa			
Singapore	APAN TEIN*CC		SingAREN
Solomon Islands			
Sri Lanka	APAN TEIN*CC		LEARN
Taiwan	APAN		TWAREN
Tajikistan			
Thailand	APAN TEIN*CC		UniNet
Timor-Leste			
Tonga			
Tuvalu			
Vanuatu			
Vietnam	APAN TEIN*CC		VinaRen