eduGAIN Information Pack

International connectivity for Tuakiri subscribers who want to connect their Identity Provider (IdP) or Service Providers (SP) to eduGAIN

What is eduGAIN?

eduGAIN (Education Global Authentication Infrastructure) enables researchers, educators and students in one country to collaborate with their colleagues and access applications, tools and datasets in other countries.

eduGAIN is a global initiative to connect federations around the world. For more information, go to https://edugain.org/

Tuakiri is now connected to eduGAIN. Subscribers can access international services or open their services to international researchers if desired. This information pack outlines the steps your organisation must take to connect to eduGAIN.

Why should my organisation connect to eduGAIN?

By connecting to eduGAIN, your organisation will benefit from:

- end-users gaining access to a growing number of services connected to international federations
- your researchers can share their applications, tools and data sets with their international colleagues international research collaboration
- furthering New Zealand research opportunities
- simple and secure access for researchers, removing the need for direct integration with applications in other federations.

What does my organisation need to do to connect to eduGAIN?

Requirements to connect to eduGAIN (connecting to eduGAIN is optional)

	SAML **Software implementation**	**Technical** **Connection requirements**	**R&S** **Research & Scholarship Entity Category**	**SIRTFI** **Security Incident Response Trust Framework for Federated Identity**

IdP	Run the latest version of software	Consume Metadata Release attributes	Mandatory	Mandatory
SP	Run the latest version of software	Consume Metadata Discovery Service Request Attributes	Recommende for qualifying services	Recommended

How to connect

- Step 1: Complete the **Connect to eduGAIN form** (linked here) to indicate your organisation's intent to connect to eduGAIN.
  - The Primary Representative for your organisation's Tuakiri Subscription must complete this form.
- Step 2: Complete the requirements to connect to eduGAIN.
  - Refer to the **Requirements to connect to eduGAIN** table above
- Step 3: Notify Tuakiri Support that you have completed the necessary requirements.
  - Email: tuakiri@reannz.co.nz
  - Complete the template (refer to Request to join eduGAIN).

Things to consider when connecting to eduGAIN

Tuakiri recommends reviewing relevant legislation before connecting to eduGAIN.

New Zealand Privacy Act

The New Zealand Privacy Act (1993) consists of 12 Principles (see a quick tour of the privacy principles).

These principles set the rules for collecting, storing, correcting, and disclosing personal information.

New Zealand Identity Providers may disclose personal information to overseas Service Providers, but must satisfy themselves that international Service Providers have taken steps to protect personal information to a similar standard.
Key privacy principles subscribers should consider:

For Identity Providers	For Service Providers
Principle 2 - Collection / Consent	Principle 1 - Purpose of Collection
	Principle 2 - Collection
	Principle 9 - Retention Period
	Principle 10 - Limits on use / Original Purpose
	Principle 11 - Disclosure

Tuakiri Subscribers should review their obligations as they prepare to connect to eduGAIN. Tuakiri Subscribers should also consider other regulation that may apply to them.

SAML software implementation

What does my organisation need to do with its SAML software implementation?

All Tuakiri Subscribers are required to observe good practice in relation to the configuration, operation and security of their connections to the federation. In order to achieve this you will need to make sure that the Service Provider software connecting to eduGAIN is running the latest version.

Technical connection requirements

There are a number of technical requirements your organisation's IdP and SPs must follow to connect to eduGAIN. Requirements cover metadata consumption, attribute release for IdPs, attribute consumption and discovery for SPs. Specific information about the technical requirements to connect to eduGAIN is available in the Tuakiri Documentation or by contacting tuakiri@reannz.co.nz.

eduGAIN metadata

Tuakiri supplies a new metadata source for eduGAIN that provides the technical trust for the international connection. Whether you run an IdP or an SP, you must consume this new metadata to connect to eduGAIN. This will require some minor configuration changes to your IdP or SP.

Attributes release (for IdPs)

Your IdP will already release the Tuakiri Core Attributes to services in Tuakiri. Attributes required by services in eduGAIN will generally be a subset of these Core Attributes. For eduGAIN services qualifying for inclusion in the Research & Scholarship Entity Category, Tuakiri provides attribute release configuration for your IdP. For all other services, you will need to determine the attribute requirements either directly from the SP or from the eduGAIN metadata. We recommend installing attribute release configuration to automatically release attributes that are requested in the metadata received from eduGAIN.

Attribute consumption (for SPs)

Service Providers must ensure their attribute requirements are recorded in the Tuakiri Federation Registry. These requirements will be made available to IdPs in eduGAIN via metadata.

Discovery mechanism (for SPs)

Tuakiri and international federations rely on the Discovery Service (also referred to as the 'Where Are You From' service) to help end-users identify which IdP to login to. The Tuakiri Discovery Service has been extended to include all eduGAIN IdPs. A simple change to the discovery URL in your Shibboleth SP configuration will enable the eduGAIN IdPs.
Your service can provide its own discovery mechanism rather than using the Tuakiri Discovery Service. The eduGAIN metadata that your service consumes will include all of the Metadata Extensions for Login and Discovery User Interface (MDUI) information that your service's discovery mechanism will require.

Research and Scholarship (R&S) Entity Category

What is R&S?

The Research and Scholarship (R&S) Entity Category establishes a baseline attribute set that all research-related IdPs and SPs agree to exchange. The R&S Entity Category is an initiative of the international Research and Education Federations (REFEDS) community.

Why does my organisation need to assert R&S?

To connect an IdP to eduGAIN, it is mandatory for Tuakiri Subscribers to assert R&S. R&S establishes a set of attributes that services can expect to receive from IdPs. This simplifies integration, improves interoperability, and creates a smoother experience for researchers. Service Providers can also trust they will receive the attributes they need to authorise access. R&S reduces the likelihood of technical connection issues between federations.

How do I assert R&S?

Asserting R&S

For Identity Providers	For Service Providers
Asserting R&S means	
"I support R&S and release the attributes defined in the R&S specification to Service Providers that meet the R&S specification requirements."	"I meet the requirements of the R&S category. I expect to receive attributes defined in the R&S specification from IdPs indicating they support R&S"
To connect to eduGAIN all IdPs need to assert the R&S Attribute Bundle.	**If an SP meets the R&S Registration Criteria (refeds.org/category/research-and-scholarship) then you can expect to receive these attributes from an IdP asserting R&S.**

R&S Attribute Bundle

The R&S attribute bundle consists of the following required data elements:

- shared user identifier
- person name
- email address

and one optional data element:

- affiliation

The shared user identifier is a persistent, non-reassigned, non-targeted identifier defined to be either of the following:

1. eduPersonPrincipalName (if non-reassigned)
2. eduPersonPrincipalName + eduPersonTargetedID

Person name is defined as either (or both) of the following:

1. displayName
2. givenName + sn

Email address is defined as the mail attribute. Affiliation is defined as the eduPersonScopedAffiliation attribute.

SPs asserting R&S will also have to provide an InformationURL - a URL to a page providing further information about the service (the page should provide more complete information than the Description of the SP in the Federation Registry provides).

For more information about the R&S Entity Category, go to refeds.org/category/research-and-scholarship

SIRTFI

Security Incident Response Trust Framework for Federated Identity (SIRTIFI).

What is SIRTFI?

SIRTFI (Security Incident Response Trust Framework for Federated Identity) provides a lightweight framework to request and provide security incident response assistance, publish security incident contact information and review your service's security incident capability.

Why does my organisation need to use SIRTFI?

SIRTFI is an important global framework covering good practice for communicating about security incidents in an effective and timely manner. SIRTFI helps security contacts know who to contact in other organisations and the best channels to use. The SIRTFI framework is an initiative of REFEDS.

How does my organisation assert SIRTFI?

Assert SIRTFI

Step 1: Read and understand the SIRTFI framework requirements.

- Go to refeds.org/sirtfi
- View the SIRTFI Framework (refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf)

Step 2: Self-assess your organisational capability against the SIRTFI requirements.

Step 3: Provide your security contact information to Tuakiri to share with security contacts in other federations.

- Update your contact details in Federation Registry (as contact type `security`) or contact Tuakiri Support at tuakiri@reannz.co.nz
- Notify Tuakiri Support that you have met the SIRTFI requirements.

Step 4: Notify Tuakiri Support when contact details change.

SIRTFI Framework

The SIRTFI framework (refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf) requires organisations to self-assess against the following areas:

Operational Security (OS)	Incident Response (IR)	Traceability (TR)	Participant Responsibilities (PR)
Security patches	IR assistance	Retaining records	Acceptable Use Policy (AUP)
Vulnerability management	SIRTFI IR assistance	Audit trails	User acknowledgement of AUP
Threat detection	Collaboration		
User access rights	IR procedures		
Contact information	User privacy		
Security incident response	Traffic Light Protocol		

Traffic Light Protocol

Organisations within the SIRTFI community agree to provide a coordinated response to security incidents, including assisting other organisations as required. SIRTFI requires organisations to understand and use the Traffic Light Protocol (TLP) for security incident communications. For more information about TLP, go to www.us-cert.gov/tlp

Logos

Both IdPs and SPs can provide logos that get embedded in their metadata - and can be used to provide users a visual clue in various parts of the user experience - an IdP logo can help identifying the right IdP at the Discovery Service, an SP logo displayed on the IdP login page can confirm to the user which service the user is logging into. And eduGAIN strongly encourages both IdPs and SPs to provide logos.

To provide a logo, please include an **HTTPS** link to your logo together in your request to join eduGAIN (below). The Tuakiri team will take care of including the logo in the metadata sent to eduGAIN.

Information URL

The registration data for an IdP or SP in the Federation Registry include a (human readable) name and a description - which get included in the generate metadata.

For a Service Provider, it is highly recommended to provide a URL to page with further information about the service, which will be published into the eduGAIN metadata as `InformationURL`.

Request to join eduGAIN

Join eduGAIN email template

For Identity Providers (IdP)

When your IdP is ready to be connected to eduGAIN, email tuakiri@reannz.co.nz using the following template.

```
Dear Tuakiri Support,

We request that the Identity Provider for “____SUBSCRIBER/ORGANISATION NAME____” be added to eduGAIN.

We have completed and tested the following technical requirements:
  * Running the latest version of SAML software
  * Consuming the Tuakiri eduGAIN metadata
  * Verified the IdP can resolve R&S attributes
  * Configure attribute release for R&S attributes.

Our IdP is R&S compliant.

Our organisation is self-asserting SIRTFI.

A logo representing our organisation is available at __URL__.

Additional Security Contacts for your Identity Provider:
    “___NAME___”
    “___EMAIL___”
    “___PHONE___”
```

For Service Providers (SP)

When your SP is ready to be connected to eduGAIN, email tuakiri@reannz.co.nz using the following template.

```
Dear Tuakiri Support,

We request that the service “____SERVICE NAME____” operated by “___ORGANISATION NAME___ “ be added to eduGAIN.

We have completed and tested the following technical configuration changes:
  * Loading the Tuakiri eduGAIN metadata
  * An eduGAIN enabled Discovery Service

We (do / do not) require this service to assert compliance with SIRTFI.

We (do / do not) require this service to assert Research and Scholarly to enable access to R&S attributes.

A logo representing this service is available at __URL__.

A page with further information about the service is available at __URL__.

Additional Security Contacts for your service:
    “___NAME___”
    “___EMAIL___”
    “___PHONE___”
```

Acknowledgements

With document has been adopted from original AAF documentation at https://aaf.edu.au/edugain/resources.html - with thanks to AAF for granting the permission for this reuse.