Tuakiri Hosted IdP

The requirement to run an Identity Provider (IdP) server has been a barrier to joining Tuakiri for some organisations. REANNZ has now removed this barrier by developing the Tuakiri Hosted IdP, a solution to make joining Tuakiri easier.

The Tuakiri Hosted IdP service is a scalable solution, where REANNZ hosts the Tuakiri IdP for the member.

The Hosted IdP instance connects to an Identity Management System (IdMs) run by the member - this can be a cloud identity store like Google Apps /GSuite or Office 365/Azure AD.

How does it work?

Users logging into a Tuakiri service first select their institution from the list of Tuakiri members.

For institutions using the Tuakiri Hosted IdP, the users would get redirected to their Tuakiri Hosted IdP instance.

The Tuakiri Hosted IdP would in turn redirect the users to their cloud-based Identity Management System to authenticate.

After authenticating, the user would be redirected back to the Tuakiri Hosted IdP, and from there back to the service the user was logging into.

TODO: diagram

Why Tuakiri Hosted IdP?

Tuakiri Hosted IdP is a scalable service - in multiple dimensions:

- REANNZ designed the service to make it easy to add new members to this service.
- When a new service gets added into Tuakiri, it becomes automatically visible to all Tuakiri IdPs.
  This would not work easily with cloud-based Identity Management Systems, where each service has to be configured manually.
- For institutions using the Tuakiri Hosted IdP service, it is also easy to join eduGAIN - as the platform meets all the technical requirements.
  And that means easy access to a much higher number of services available via eduGAIN.

How do I get started with a Tuakiri Hosted IdP?

Please get in touch with us first at tuakiri@reannz.co.nz

We will need to work with you to confirm:

- Membership details
- Cloud-based identity management system to be used

After the initial conversation, we will give you details of your Tuakiri Hosted IdP instance which you'll need to register as a Service Provider with your cloud-based IdMS - and in turn, we'll need the IdP metadata of your cloud-based IdMs.

Please see the specific details here:

- Registering Tuakiri Hosted IdP as a Service with Google Apps / GSuite
- Registering Tuakiri Hosted IdP as a Service with Office 365 / Azure AD

Alongside the registration steps linked above, you will need to provide us with the following information:

- Name of your organisation as it should be presented to users
- Domain name of your organisations
- Public website URL
- Logo to represent your organisation (provided as a file, with width and height to render to).
- Contact email addresses (ideally role-based): technical and security
- Details on the information sent by the cloud-based IdMS in SAML messages:
  - metadata of the cloud-based upstream IdP (IdP side of the IdMS) - will be retrieved as part of the registration
  - NameIDFormat used by the IdP (will likely be `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`)
  - List of attributes sent by the IdP

After testing (first deploying an instance in the Tuakiri-TEST environment), we should be in a position to turn your Production instance on.