Tuakiri OpenID Connect Bridge

The Tuakiri OpenID Connect Bridge allows to connect services using OpenID Connect to authenticate users into Tuakiri.

The bridge acts as an OpenID Connect Provider (OP) towards these services - and translates the OpenID Connect authentication request into a SAML authentication request, acting as a SAML SP towards Tuakiri.

The services is similar to Tuakiri RapidConnect, but is based on a proper standard (OpenID Connect) - which wasn't yet available at the time RapidConnect was developed. Eventually, this service will replace RapidConnect.

The bridge runs SATOSA, an identity proxy initially developed by SUNET.

The bridge allows configuring Tuakiri login for services that are not able to participate in SAML, but support OpenID Connect (as an RP - Relying Party). The bridge acts towards the service as a single OpenID Connect Provider (OP).

Same as with other Tuakiri services, besides a Production instance, there is also a member-facing TEST instance registered into the Tuakiri-TEST federation, suitable for testing OIDC integration for services being developed.

Connecting a service to the Tuakiri OpenIDConnect Bridge

All Tuakiri member organisations are welcome to connect an OpenIDConnect-compatible service with the bridge to use Tuakiri for authentication.

Initial registration

To provide a secure and trustworthy environment, the bridge does not allow self-registration and all registrations must be processed by REANNZ Tuakiri staff.

Please start the process by contacting us at tuakiri@reannz.co.nz - and in your initial request, please include the following information:

- A descriptive name of the service
- The redirect_uri the OpenIDConnect RP on the service will use
    - the redirect_uri must use HTTPS - and must use a host name properly registered in DNS; an IP address would not be accepted
- Which of the Tuakiri Attributes the service will need access to (and what scopes the service will be requesting - see below)
- Whether for authenticating to the service, a *targeted* (*pairwise*) subject identifier will be sufficient, or whether the service needs *public* (non-targeted) subject identifier.
  (The latter would only be the case when multiple services connected to the bridge independently need to receive matching subject identifiers).
- Name of the organisation operating the service
- A further (brief) description of the service (going beyond the service name) - for use in the Tuakiri Service Catalogue.
- A URL that can be used to link to the service from the Service Catalogue
- Which federation this registration is for - Tuakiri (Production) or Tuakiri-TEST.
- The deployment state of the service (Production, UAT, Testing, Development...)

We will respond with further instructions.

We will also need a way to communicate the clientID and secret to you in a secure way. For this, we use Keybase.io - so please also include your Keybase account ID in your registration request.

Service configuration

When configuring your service, you should be able to get most of the OpenIDConnect configuration URL served by the bridge.

The URLs are:

- Production: https://openidconnect.tuakiri.ac.nz/.well-known/openid-configuration
- TEST: https://openidconnect.test.tuakiri.ac.nz/.well-known/openid-configuration

You will receive the clientID and secret from us via a secure message.

You will also need to configure your service to request the correct scopes - this way, the bridge would know what claims (corresponding to attributes) to expose to your service. The scopes and the corresponding claims are:

Scopes	Claims	Notes
openid	sub	This scope must be always present in OpenID Connect
phone	phone_number	
email	email email_verified	

profile	name given_name family_name nickname	Correspond to SAML attributes (in the same order): commonName givenName surname
eduperson	eduperson_scoped_affiliation eduperson_affiliation eduperson_primary_affiliation eduperson_assurance eduperson_principal_name eduperson_orcid schac_home_organization schac_home_organization_type organization_name organizational_unit	
aueduperson	aueduperson_shared_token	
mobile	mobile_number	