February 9th, 2022, eResearch NZ 2022

Bridging the Connectivity Gap: Tuakiri Hosted IdP connects Small Research Organisations into R&E Identity Federations

Vlad Mencl

REANNZ

What is this about?

Tuakiri Hosted IdP is a new service provided by REANNZ

- Allows organisations to join Tuakiri without having to run an IdP server
  - this has been long seen as obstacle to joining Tuakiri
- REANNZ runs the Tuakiri IdP on behalf of the member
  - on scalable REANNZ infrastructure
- Member-run cloud-based identity store authenticates the user
  - Google Apps / GSuite or Office 365 / Azure AD
- Tuakiri Hosted IdP acts as a bridge between the identity store and Tuakiri (and possibly also eduGAIN)
- Target audience: small research organisations (~100 FTE)

Why Tuakiri Hosted IdP

- Small research organisations have been unable to use Tuakiri
  - everyday routine work gets more difficult: accessing
    - journal subscriptions
    - collaboration tools
    - research repositories
  - yet, they typically already have an IdMS - such as:
    - Google Apps / GSuite
    - Office 365 / AzureAD
  - but running an IdP server to connect into Tuakiri has been too difficult.
    - specialised expertise require
  - Just need to bridge the gap...

Tuakiri Hosted IdP: How it Works

Tuakiri Hosted IdP acts as a proxy in the authentication exchange

- Typically SAML-to-SAML
  - other upstream protocols (such as OIDC) are possible
- Services in Tuakiri (and eduGAIN) authenticate against the Tuakiri Hosted IdP
  - which in turn delegates authentication upstream to the cloud-based system
    - browser redirect: user interacts directly with the upstream cloud-based IdP
    - authentication strength MFA as required by the cloud-based system
- Tuakiri Hosted IdP constructs the response expected by the Service Provider
- Can also easily connect to eduGAIN

Tuakiri Hosted IdP - What is involved to get going

- The Tuakiri Hosted IdP is registered as a Service Provider with the member-run cloud based system
  - this is the only configuration to be done by the member
- REANNZ will create configuration for the Tuakiri Hosted IdP instance based on information provided by the member.
  - REANNZ-managed automation tools will deploy and manage the Tuakiri Hosted IdP instance
- What about costs
  - The service is included in REANNZ membership
  - No extra cost

Why Tuakiri Hosted IdP

If upstream IdP already speaks SAML, why use Tuakiri Hosted IdP?

- cloud-based IdPs (Google, Azure AD) integrate well with a single SP
- and provide a limited set of attributes

Tuakiri Hosted IdP

- acts as a hub for connecting to all of Tuakiri - and eduGAIN
- translates the attributes received from upstream IdP into what R&E federations expect
- constructs missing attributes (based on member-specific configuration)

What Tuakiri Hosted IdP is NOT ?

Tuakiri Hosted IdP is not an Identity Management System (IdMS) replacement

- Member organisation is still responsible for managing the user identity lifecycle
- And this happens in a system upstream from the Tuakiri Hosted IdP

Tuakiri Hosted IdP - under the hood

What is under the hood?

- Shibboleth IdP
  - same as what existing members run on-prem
  - but with SAML proxying (new in 4.x)
  - and kept up-to-date via our automation
- Shared infrastructure (VM) with per-member IdP instance (distinct entityID)
- HA geographically distributed (WLG/HLZ)

Tuakiri Hosted IdP

How to get started

- Talk to a friendly REANNZ staff member
- Or just email engagement@reannz.co.nz

Where to find more information

https://tuakiri.ac.nz/confluence/display/Tuakiri/Tuakiri+Hosted+IdP
or get redirected from https://hosted-login.tuakiri.ac.nz/

February 9th, 2022, eResearch NZ 2022, Bridging the Connectivity Gap: Tuakiri Hosted IdP connects Small Research Organisations into R&E Identity Federations

Thank you!

Questions?

Vlad Mencl

REANNZ