Request for tender templates

Request for tender of a service or an application often requires definitions for ensuring Haka compatibility. This page is a template for some possible requirements. Proper consideration is needed by a requestor.

Authentication protocol

Haka is a federated authentication infrastructure based on SAML2-protocol. In addition to general SAML2 standards Haka has certain Haka specific requirements. Haka aims to be as compatible as possible with international identity federations but in some cases it is not possible due to local requirements.

> User authentication must utilize Haka identity federation: In English. The service must include a SAML2 Service Provider component configured to support Haka SAML2-profile: Haka SAML 2.0 -profile 2.0

In some cases it is required that the application allows local user accounts in addition to federated identities.

> The service must support the use of local user accounts. The capability must be available concurrently with Haka.

User attributes

Haka user authentication enables transfer of user attributes to a service. User attributes in Haka are defined in FunetEduPerson attribute schema: FunetEduPerson schema

Application of personal data received as federated attributes and linking that data to local user accounts must always be evaluated per service. In general when using Haka, services should minimise the amount of locally created user attributes and rely on federated attributes.

> Storing and updating user information in the service must rely on attributes received through Haka.

Users in Haka are identified using one of the available identifiers specified in the attribute schema: FunetEduPerson schema. The most common identifier used is eduPersonPrincipalName-attribute. In some cases it is desirable that existing user accounts are linked to federated identifiers.

> User's Haka identifier must be linked to an existing user accounts in the service.

Authorisation

Based on the use case, authorisation can done based on attributes such as user name, role, organization or some other user attribute. Similarly more fine grained rights within the service may be based on user attributes.

> Only users from a specific identity providers are allowed to access the service.

> Authorisation must be based on federated attributes of the user.

> User roles of the service must be based on federated attributes.

Identity provider discovery

Each organization in Haka has their own identity provider. This requires Haka services to have means of directing users to authenticate at their respective identity providers. There are several options to handle identity provider discovery.

> Discovery must be done in service user interface.

> Discovery must be done using URL address

Centralized Haka Discovery Service must be used for identity provider selection.

The service redirects user to a specified single identity provider for authentication

User provisioning

User accounts may be provisioned prior to user accessing the service. Usually this means importing users' Haka identifiers to the service.

User accounts are created through management console based on Haka user identifiers. Service is accessible on first federated login for configured users.

Users may be provisioned as they access the service for the first time. After the user account exists additional rights can be granted to a user.

User account is provisioned on first federated access.

Access rights are granted through service management console.