Intégration OIDC dans la Fédération Éducation-Recherche

Guillaume Rousse

7 novembre 2024

Scénarios

Plusieurs possibilités

- fédération native OIDC
- passerelles dédiées
- passerelle centralisée

Fédération native OIDC

Principe

Échange direct de messages OIDC entre fournisseurs d'identité et application

Fonctionnement

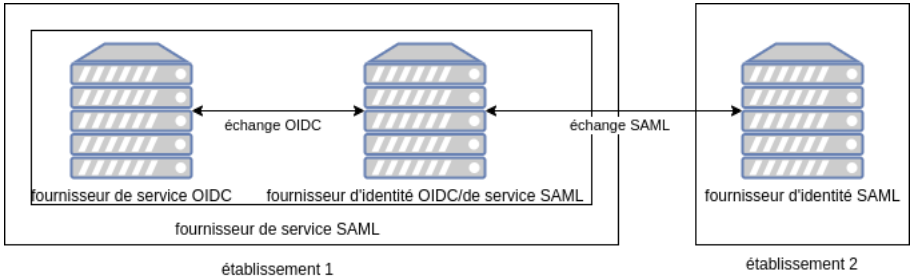
- déléguer à un tiers la mise en place des relations de confiance
- vérification dynamique d'une chaine de confiance

Faisabilité

Complexe :

- nécessite une évolution de tous les fournisseurs d'identité actuels
- nécessite une évolution de nos procédures d'enregistrement

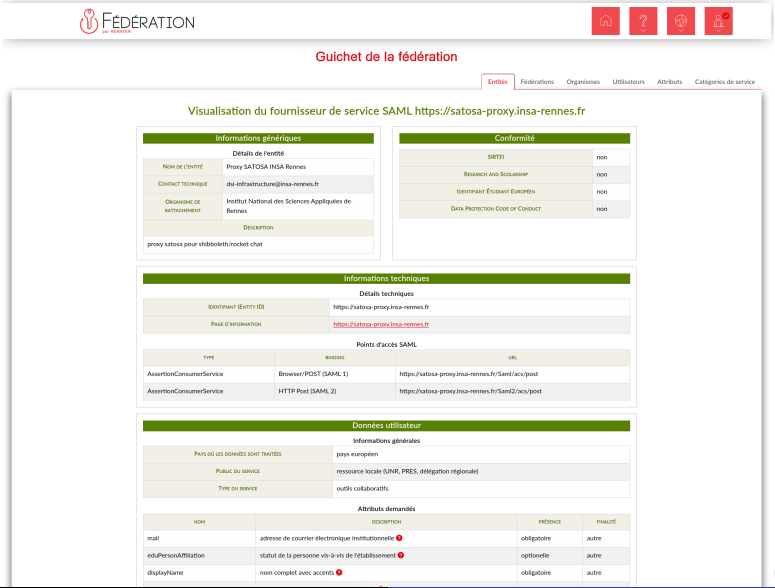
Passerelles dédiées



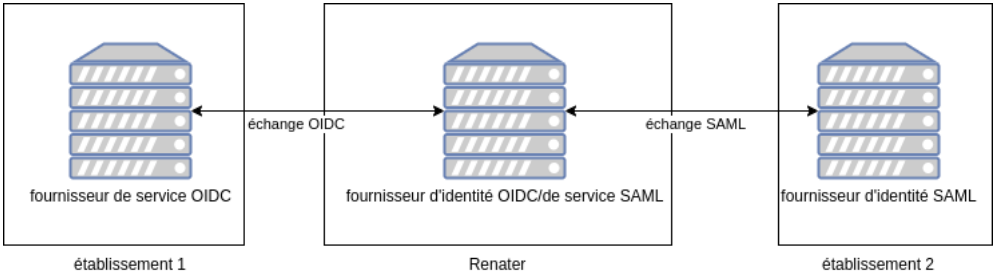
Faisabilité

- nécessite une double compétence SAML/OIDC
- au moins une dizaine d'instances déjà déclarées sur le guichet de la fédération

Déclaration d'un SP SAML sur le guichet



Passerelle centralisée



Faisabilité

- nécessite la mise en place d'un service centralisé dédié
- nécessite une évolution de nos procédures d'enregistrement

Déclaration d'un RP OIDC sur le guichet