

# Intégration OIDC dans la Fédération Éducation-Recherche

Guillaume Rouse

7 novembre 2024

## Plusieurs possibilités

- fédération native OIDC
- passerelles dédiées
- passerelle centralisée

## Principe

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

## Fonctionnement

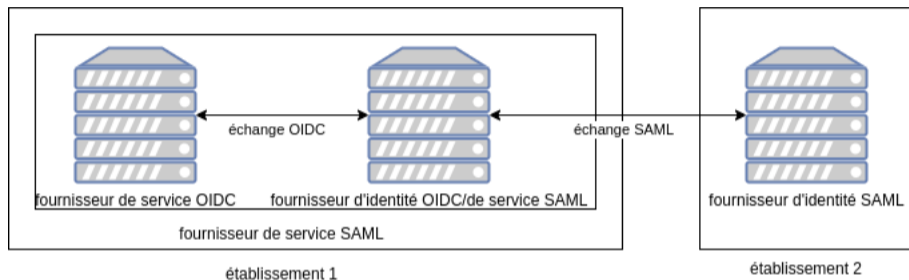
- déléguer à un tiers la mise en place des relations de confiance
- vérification dynamique d'une chaîne de confiance

## 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

## Guichet de la fédération

Entités | Fédérations | Organismes | Utilisateurs | Attributs | Catégories de service

### Visualisation du fournisseur de service SAML <https://satosa-proxy.insa-rennes.fr>

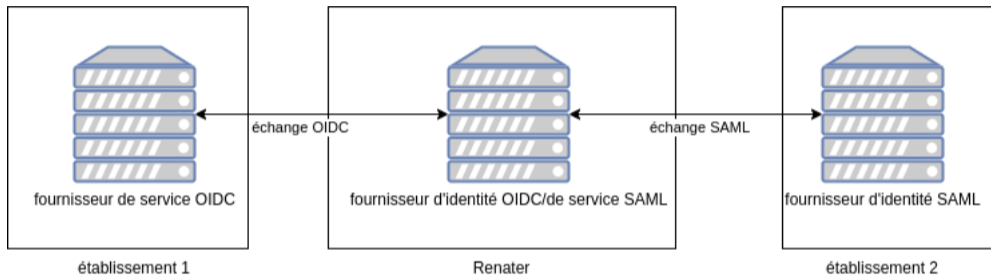
Informations générales	
Détails de l'entité	
NOM DE L'ENTITÉ	Proxy SATOSA INSA Rennes
CONTACT TECHNIQUE	di4-infrastructure@insa-rennes.fr
ORGANISME DE RATTACHEMENT	Institut National des Sciences Appliquées de Rennes
DESCRIPTION	
proxy satosa pour shibboleth/rocket chat	

Conformité	
SIRTFI	non
RESEARCH AND SCHOLARSHIP	non
IDENTIFIANT ÉTUDIANT EUROPÉEN	non
DATA PROTECTION CODE OF CONDUCT	non

Informations techniques		
Détails techniques		
IDENTIFIANT (ENTITY ID)	<a href="https://satosa-proxy.insa-rennes.fr">https://satosa-proxy.insa-rennes.fr</a>	
PAGE D'INFORMATION	<a href="https://satosa-proxy.insa-rennes.fr">https://satosa-proxy.insa-rennes.fr</a>	
Points d'accès SAML		
TYPE	BINDING	URL
AssertionConsumerService	Browser/POST (SAML 1)	<a href="https://satosa-proxy.insa-rennes.fr/Saml/acs/post">https://satosa-proxy.insa-rennes.fr/Saml/acs/post</a>
AssertionConsumerService	HTTP Post (SAML 2)	<a href="https://satosa-proxy.insa-rennes.fr/Saml2/acs/post">https://satosa-proxy.insa-rennes.fr/Saml2/acs/post</a>

Données utilisateur			
Informations générales			
PAIS OÙ LES DONNÉES SONT TRAITÉES	pays européen		
PUBLIC DU SERVICE	ressource locale (UNR, PRES, délégation régionale)		
TYPE DU SERVICE	outils collaboratifs		
Attributs demandés			
NOM	DESCRIPTION	PRÉSENCE	FINALITÉ
mail	adresse de courrier électronique institutionnelle	obligatoire	autre
eduPersonAffiliation	statut de la personne vis-à-vis de l'établissement	optionnelle	autre
displayName	nom complet avec accents	obligatoire	autre

# 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

## Guichet de la fédération

Entités | Fédérations | Organismes | Utilisateurs | Attributs | Catégories de service

### Visualisation du fournisseur de service OIDC dev-test-rp.federation.renater.fr

Informations générales	
Détails de l'entité	
NOM DE L'ENTITÉ	dev-test-rp
CONTACT TECHNIQUE	eq@pe-federation@renater.fr
ORGANISME DE RATTACHEMENT	GIP RENATER
DESCRIPTION	
GIP RENATER - RP de test (développement)	

Conformité	
SIRTFI	non
RESEARCH AND SCHOLARSHIP	non
IDENTIFIANT ÉTUDIANT EUROPÉEN	non
DATA PROTECTION CODE OF CONDUCT	non

Informations techniques	
Détails techniques	
IDENTIFIANT (CLIENT ID)	dev-test-rp.federation.renater.fr
PAGE D'INFORMATION	<a href="https://dev-test-rp.federation.renater.fr">https://dev-test-rp.federation.renater.fr</a>
URIs de redirection	
<a href="https://dev-test-rp.federation.renater.fr/redirect_uri">https://dev-test-rp.federation.renater.fr/redirect_uri</a>	

Données utilisateur	
Informations générales	
PAIS OÙ LES DONNÉES SONT TRAITÉES	pays européen
PUBLIC DU SERVICE	service à portée nationale
TYPE DU SERVICE	application métier
Portées demandées	
openid	
profile	
email	