

# eduGAIN Access Check

Guillaume Rousse

GIP RENATER

12 april 2022



# Plan

- 1 Overview
- 2 Implementation
- 3 Demonstration

# Plan

- 1 Overview
- 2 Implementation
- 3 Demonstration

# Objectives

## Purpose

federated application testing

# Objectives

## Purpose

federated application testing

## Features

- no additional trust relationship needed : ready to use
- usable in production federation : no account with public credentials

# Fonctionning

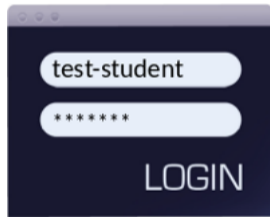


create service-specific test  
accounts with different profiles

# Fonctionning



create service-specific test accounts with different profiles

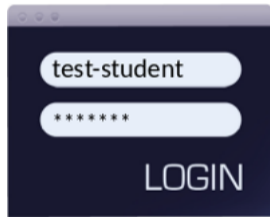


use them for login on own service only

# Fonctionning



create service-specific test accounts with different profiles



use them for login on own service only



Check if access works and attributes are available



# Account details

## Diversity

- multiple profiles with different attribute sets  
student, teacher, other, etc.
- realistic attribute values  
cn="Åsold Wahlstrøm"

# Account details

## Diversity

- multiple profiles with different attribute sets  
student, teacher, other, etc.
- realistic attribute values  
cn="Åsold Wahlstrøm"

## Security

- strong random passwords
- restricted to a single service provider  
IdP-enforced restriction
- lifetime limitation  
7 days by default

# Plan

- 1 Overview
- 2 Implementation
- 3 Demonstration

# Components

## Identity Provider

- SimpleSAMLphp
- restrictLogin plugin (internal development)

# Components

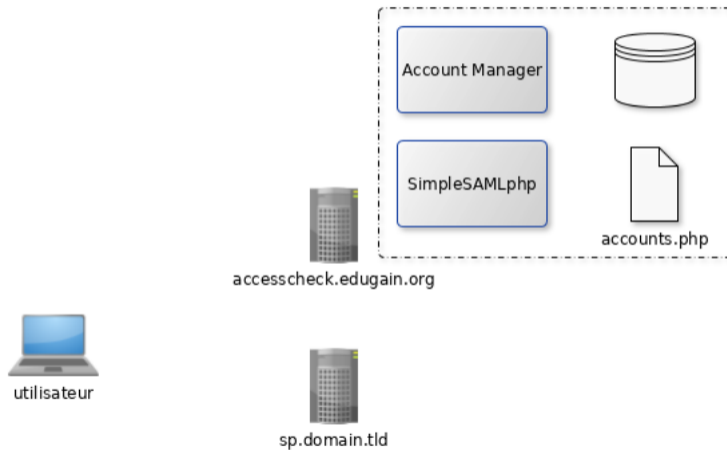
## Identity Provider

- SimpleSAMLphp
- restrictLogin plugin (internal development)

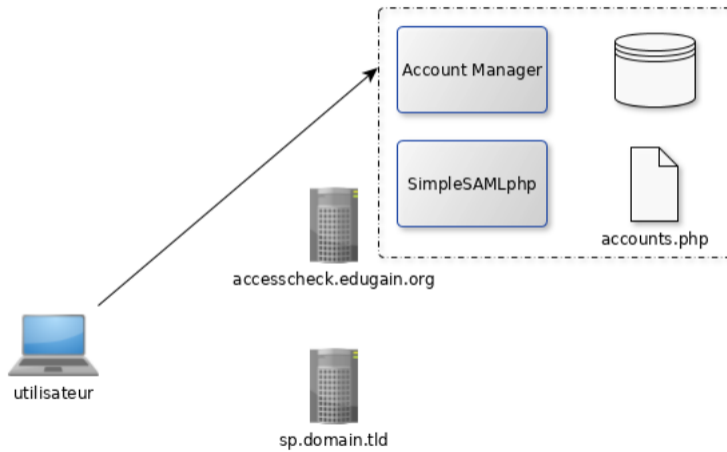
## Account management interface

- Perl web application (internal development)

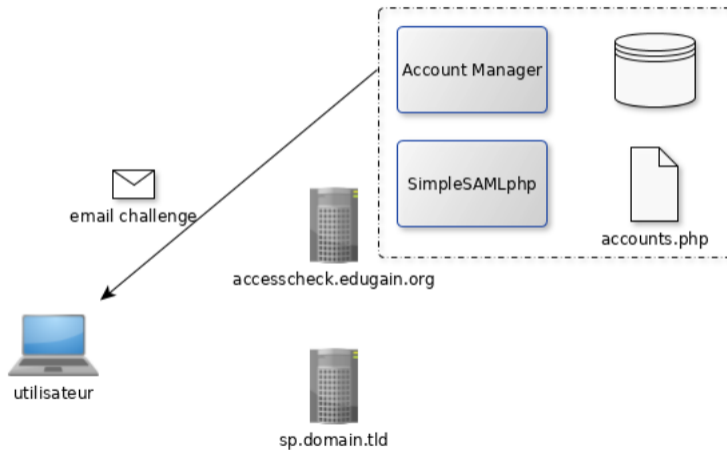
# Architecture



# Account creation

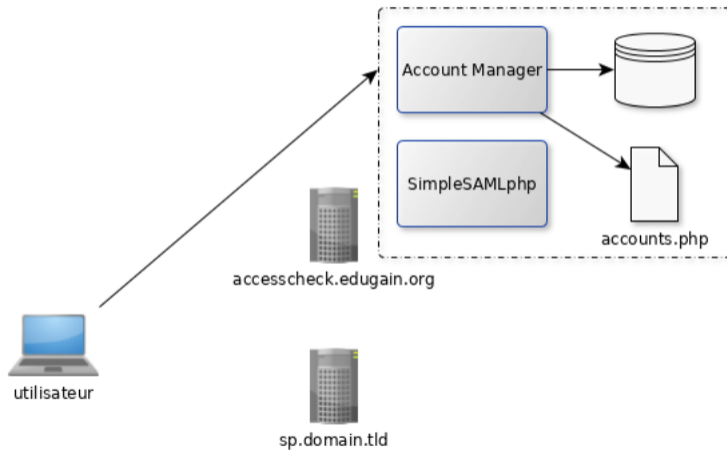


# Account creation

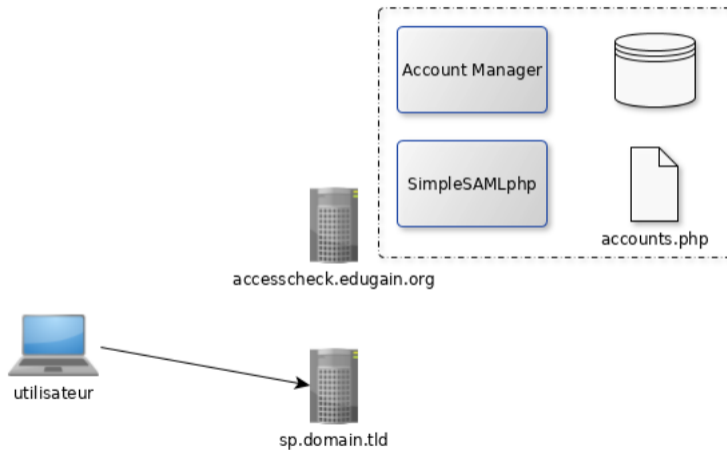




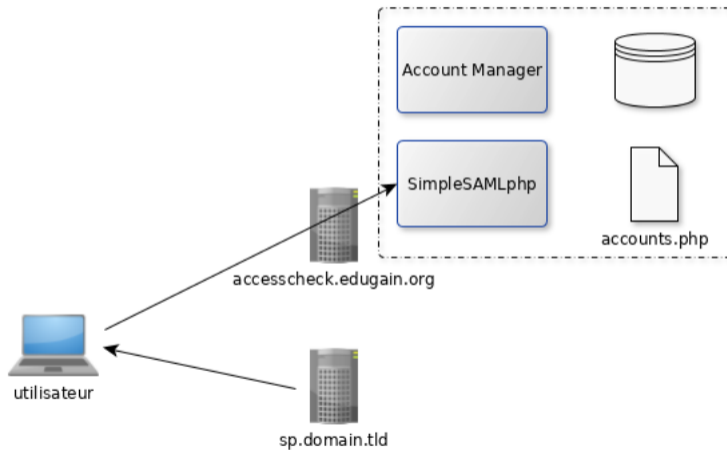
# Account creation



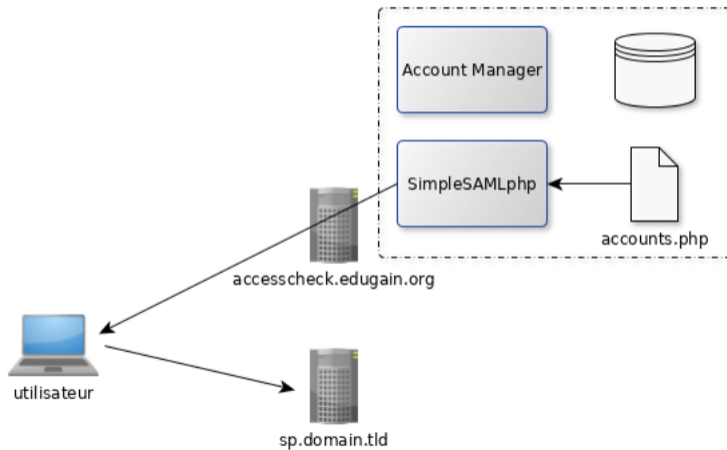
# Service provider access



# Service provider access



# Service provider access



# Security

## Proof of ownership

- EAC is an IdP trusted by all federation members
- accounts creation is restricted to legitimate SP admins
- achieved through an email challenge, based on SP metadata

# Security

## Proof of ownership

- EAC is an IdP trusted by all federation members
- accounts creation is restricted to legitimate SP admins
- achieved through an email challenge, based on SP metadata

## Password storage

- non-reversible format : hashed for SimpleSAML PHP usage
- reversible format : encrypted with transient key for CVS export

# Multi-tenant support

## Purpose

Same tool usage, in different contexts :

- eduGAIN instance ([access-check.edugain.org](https://access-check.edugain.org)) for international context
- RENATER instance ([access-check.renater.fr](https://access-check.renater.fr)) for national context

# Multi-tenant support

## Purpose

Same tool usage, in different contexts :

- eduGAIN instance ([access-check.edugain.org](https://access-check.edugain.org)) for international context
- RENATER instance ([access-check.renater.fr](https://access-check.renater.fr)) for national context

## Customization support

- multiple look'n'feel : eduGAIN and RENATER themes provided
- optional authentication : delegated to web server
- multiple entities sets : federations, custome aggregates



# Multiple deployment scenarios

## Do it yourself

Download source code, install and run your own instance yourself

## Multiple deployment scenarios

### Do it yourself

Download source code, install and run your own instance yourself

### Mutualized hosting

eduGAIN instance already supports eduGAIN and ACOnet federations

## Multiple deployment scenarios

### Do it yourself

Download source code, install and run your own instance yourself

### Mutualized hosting

eduGAIN instance already supports eduGAIN and ACOnet federations

### Dedicated hosting

No service offer available currently

# Roadmap

## Version 2.0

- user-controlled accounts lifetime
- user-controlled profiles selection
- profiles defined as templates, easier to customize
- switch from plain CGI to Mojolicious framework

# Roadmap

## Version 2.0

- user-controlled accounts lifetime
- user-controlled profiles selection
- profiles defined as templates, easier to customize
- switch from plain CGI to Mojolicious framework

## Desirable features

- user-controlled attribute sets
- user-controlled attribute values

# Plan

- 1 Overview
- 2 Implementation
- 3 Demonstration



🏠 Language

[eduGAIN Wiki](#)

[eduGAIN Site](#)

## eduGAIN Access Check

### Objectif

eduGAIN Access Check permet aux administrateurs d'un fournisseur de service (Service Provider) enregistré dans une fédération d'identité de créer des comptes de test avec différents profils, afin de tester l'authentification fédérée et de valider le comportement du service. Ces comptes de test ne peuvent être utilisés qu'avec ce service.

[Plus d'information](#)

### Fonctionnement



### Commencer

Pour commencer à tester vos propres services, commencez par en sélectionner un dont vous êtes l'administrateur.

[Commencer](#)

eduGAIN Access Check 1.1 - [contact us](#)



[Disclaimer](#) [Policies](#)

En tant que membre de l'accord GÉANT 2020 Framework Partnership Agreement (FPA), ce projet bénéficie d'un financement du programme de recherche de l'Union Européenne Horizon 2020 sous l'agrément No. 731122 (0N4-2).

