eduGAIN Access Check

Guillaume Rousse

GIP RENATER

12 april 2022

RENATER
CONNECTEUR DE SAVOIRS

Plan

1. Overview
2. Implementation
3. Demonstration

RENATER
CONNECTEUR DE SAVOIRS

Plan

1 Overview

2 Implementation

3 Demonstration

RENATER
CONNECTEUR DE SAVOIRS

Objectives

Purpose

federated application testing

RENATER
CONNECTEUR DE SAVOIRS

Objectives

Purpose

federated application testing

Features

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

RENATER
CONNECTEUR DE SAVOIRS

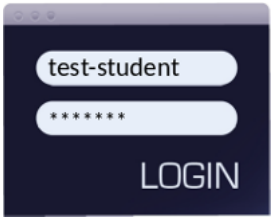
Fonctionning

create service-specific test accounts with different profiles

RENATER
CONNECTEUR DE SAVOIRS

Fonctionning

create service-specific test accounts with different profiles

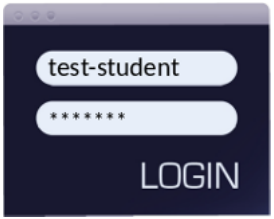


use them for login on own service only

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

Account details

Diversity

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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

Components

Identity Provider

- SimpleSAMLphp
- restrictLogin plugin (internal development)

RENATER
CONNECTEUR DE SAVOIRS

Components

Identity Provider

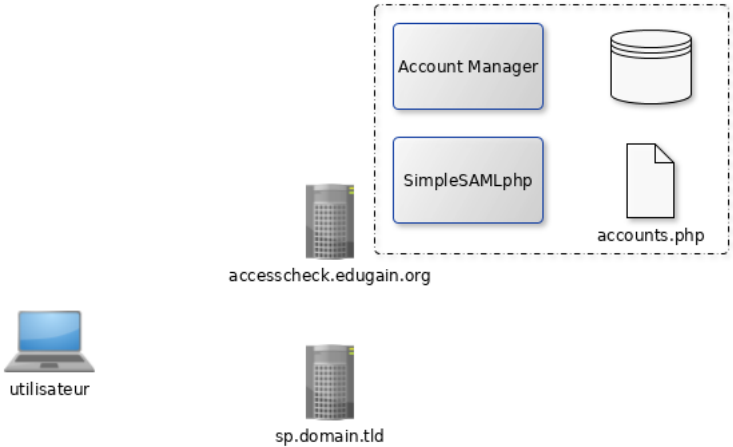
- SimpleSAMLphp
- restrictLogin plugin (internal development)

Account management interface

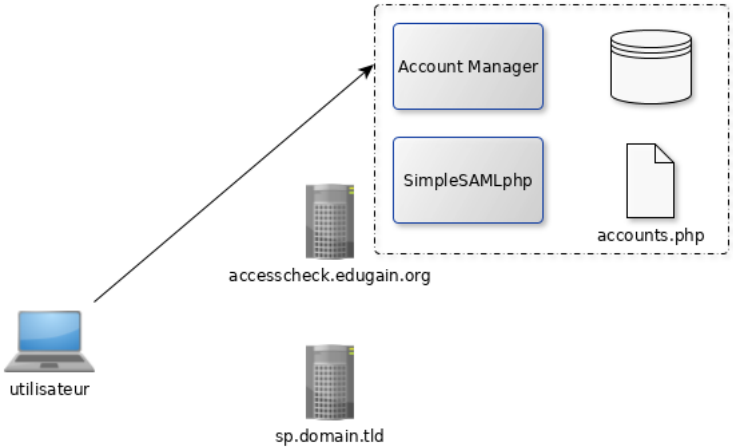
- Perl web application (internal development)

RENATER
CONNECTEUR DE SAVOIRS

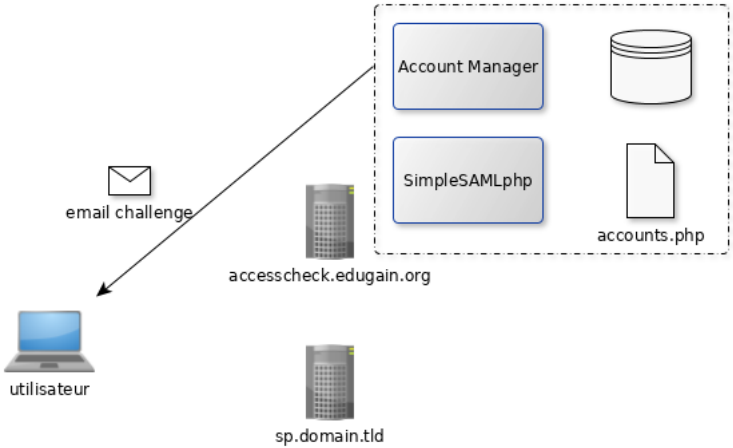
Architecture



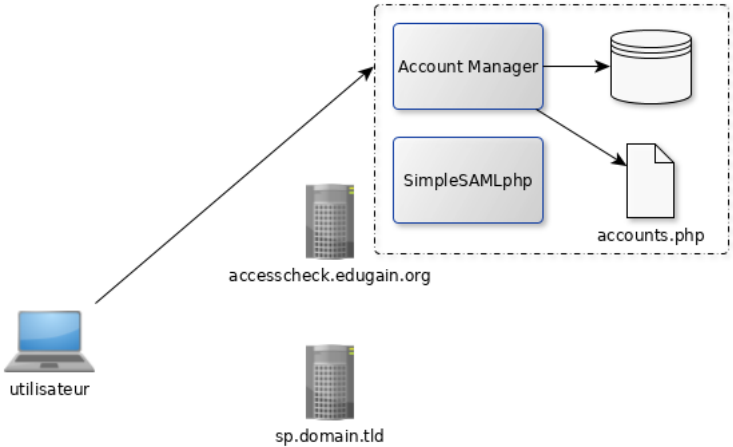
Account creation



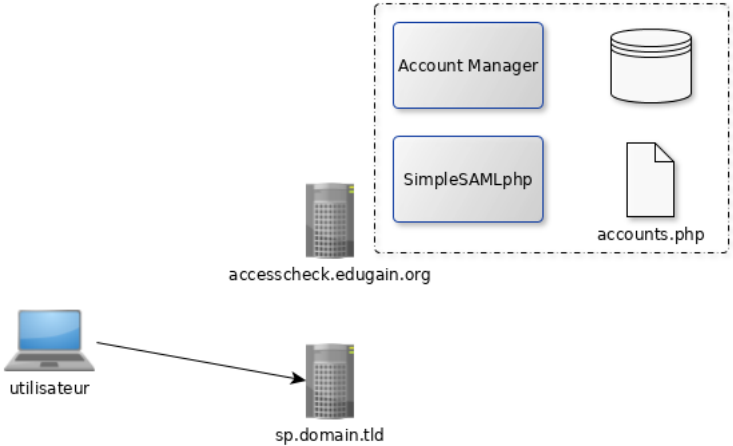
Account creation



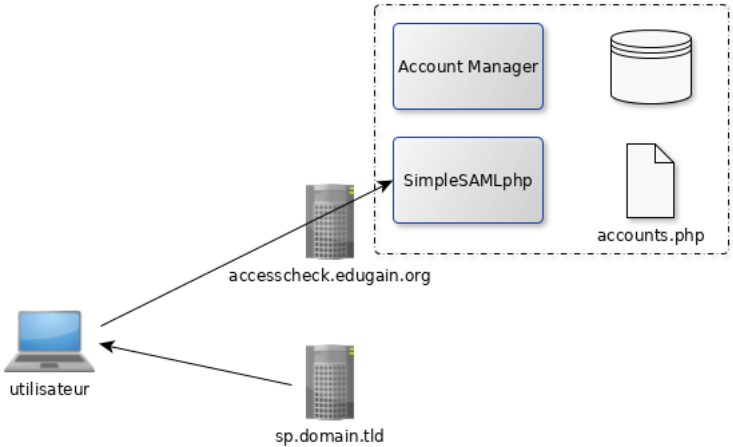
Account creation



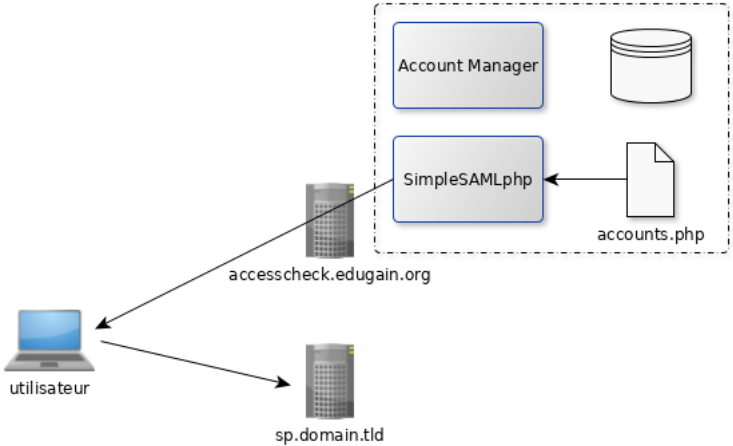
Service provider access



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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

Multi-tenant support

Purpose

Same tool usage, in different contexts :

- eduGAIN instance (access-check.edugain.org) for international context
- RENATER instance (access-check.renater.fr) for national contex

RENATER
CONNECTEUR DE SAVOIRS

Multi-tenant support

Purpose

Same tool usage, in different contexts :

- eduGAIN instance (access-check.edugain.org) for international context
- RENATER instance (access-check.renater.fr) for national contex

Customization support

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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

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

RENATER
CONNECTEUR DE SAVOIRS

Demonstration