



20 octobre 2026
PARIS

Reprendre le contrôle de son authentification avec les solutions SSO libres

David COUTADEUR
Clément OUDOT





David COUTADEUR

Architecte en gestion d'identité

Contributeur LemonLDAP::NG, LTB, LSC,
FusionIAM

Clément OUDOT

Identity Solutions Manager

Contributeur LemonLDAP::NG, LDAP Tool
Box, LSC et FusionIAM

Ordre du jour

- **SSO et contrôle d'accès**
- **Protocoles CAS, SAML et OIDC**
- **Le logiciel Keycloak**
- **Le logiciel LemonLDAP::NG**
- **Conclusion**



Worteks

Société d'expertise, d'édition et d'hébergement Open Source
Centre de formation certifié Qualiopi

Contribue activement à de nombreux logiciels libres comme LSC,
LemonLDAP::NG, LDAP Tool Box, FusionIAM et OpenStack

Partenaires



Worteks

Une offre Open Source globale.

Solution de déploiement d'infrastructure complexe

 **V'Opla**

Suite collaborative globale

 **V'Sweet**

Intégration, support et expertise

 **V'ise**

Hébergement souverain

 **V'aaS**

Solution de gestion des identités et des accès

 **V'IDaaS**



SSO et contrôle d'accès



Imagine SSOng

Imagine there are no passwords
Or maybe just only one
A single secured form
To access our applications
Imagine all the users
Loving security

Imagine some protocols
Made by clever people
CAS, OpenID or SAML
Even WS Federation
Imagine authentication
Interoperability

Imagine applications
No more storing passwords
Relying on a token
Even for authorizations
Imagine all developers
Loving security

You may say
I'm a hacker
But I'm not the only one
I hope one day
You will log in
Using the Single Sign On



© John Lennon

Identification, authentification, autorisation

Identification

Définir quelle personne réalise une action

Authentification

S'assurer qu'une personne est bien qui elle prétend être

Autorisation

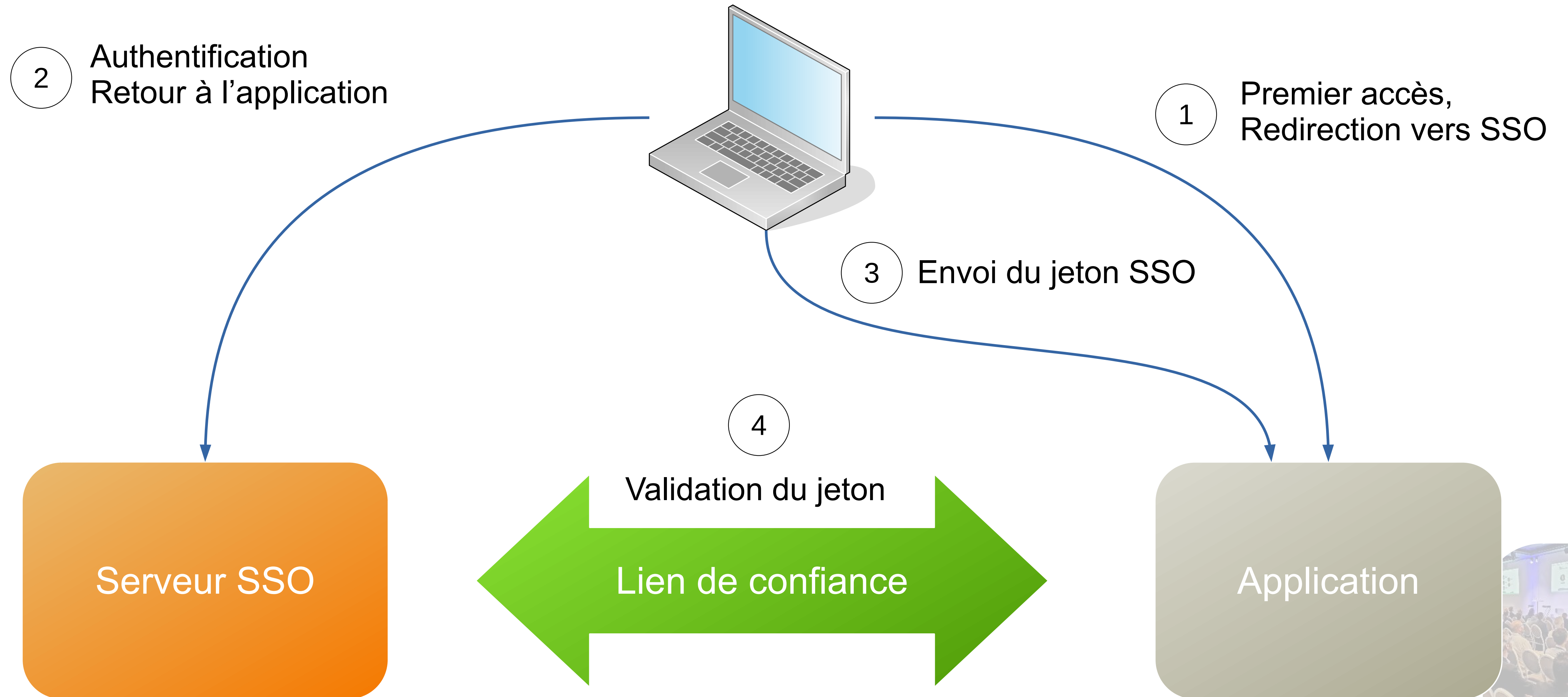
Processus par lequel on s'assure qu'une entité n'accède qu'à un ensemble de ressources donné

SSO : "Single Sign On"

Authentification unique pour l'accès à plusieurs ressources



Principe du SSO



Protocoles CAS, SAML et OIDC



Le protocole CAS

Central Authentication Service

Documentation du protocole pour les versions 1.0, 2.0 et 3.0 : <https://apereo.github.io/cas/5.2.x/protocol/CAS-Protocol-Specification.html>

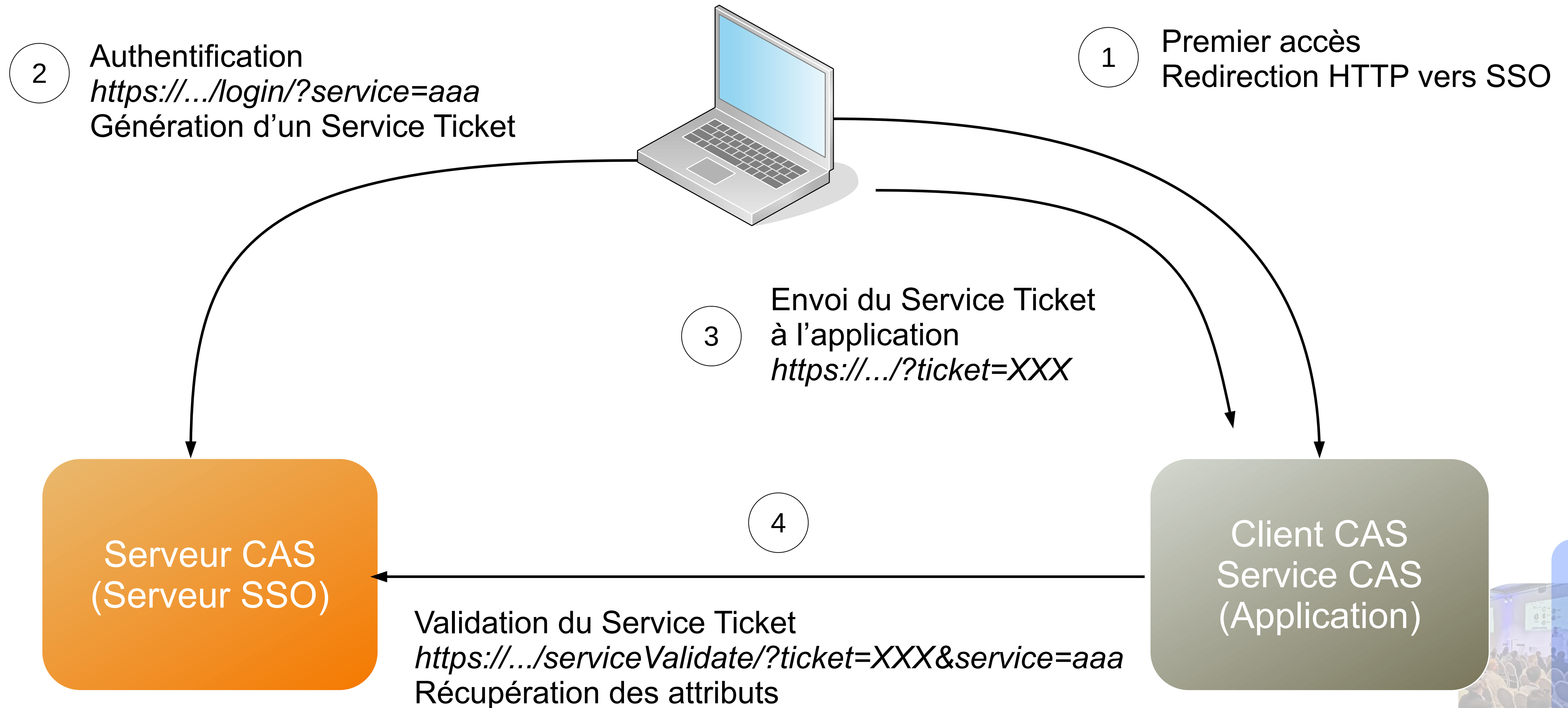
Utilisation de tickets de service dans l'URL, validés auprès du serveur CAS

Necessite que l'application puisse joindre le serveur CAS

Possibilité de tickets proxy depuis la version 2.0

Publication d'attributs depuis la version 3.0

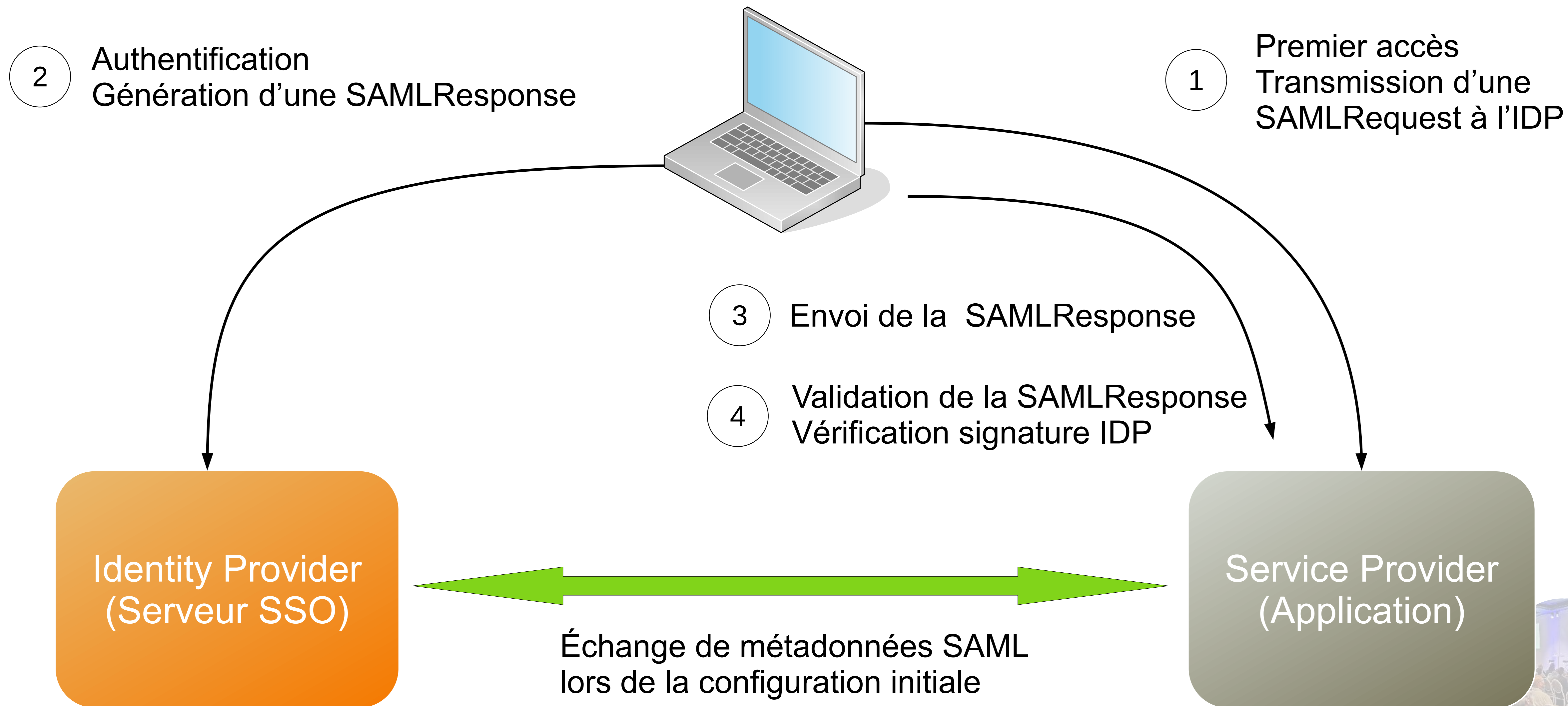




Le protocole SAML

- Security Assertion Markup Language
- Basé sur XML, XML Security, SOAP
- Choix des méthodes HTTP (GET ou POST)
- Possibilité d'utilisation d'un artefact pour transmettre les messages via SOAP (Artefact GET ou Artefact POST)
- Publication des informations de configuration (metadonnées) au format XML
- Les messages peuvent être signés et chiffrés

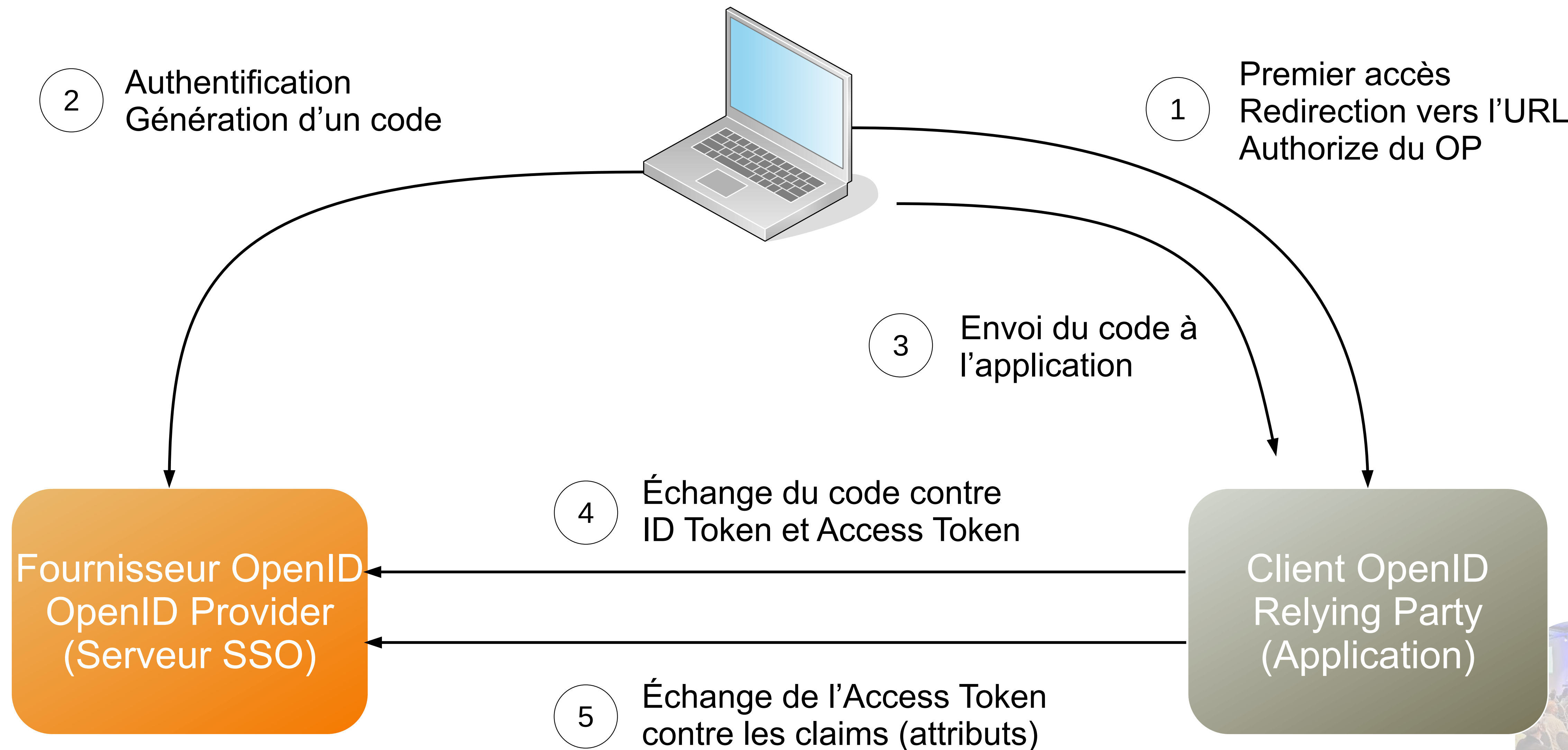




Le protocole OpenID Connect

- Basé sur OAuth2, REST, JSON
- Connexion nécessaire entre le client (application) et le serveur OIDC
- Publication des informations de configuration (métadonnées) au format JSON
- Les jetons JWT peuvent être signés et chiffrés





Le logiciel Keycloak



Le projet Keycloak

- Initialement un projet interne de Red Hat, démarré en 2013
- Donné à la CNCF (Cloud Native Computing Foundation) en Avril 2023
- CNCF : Kubernetes, Prometheus,...
- Open Source (Apache License 2.0)
- 600 000 SLOCs ! (dont 1/3 de tests)
- Mais encore principalement maintenu par des employés RH
- Basé sur Quarkus
 - framework d'application Java, avec faible empreinte mémoire et temps de démarrage réduit
 - lui-même basé sur Vert.x (framework événementiel inspiré de Node.js)



Activité du projet

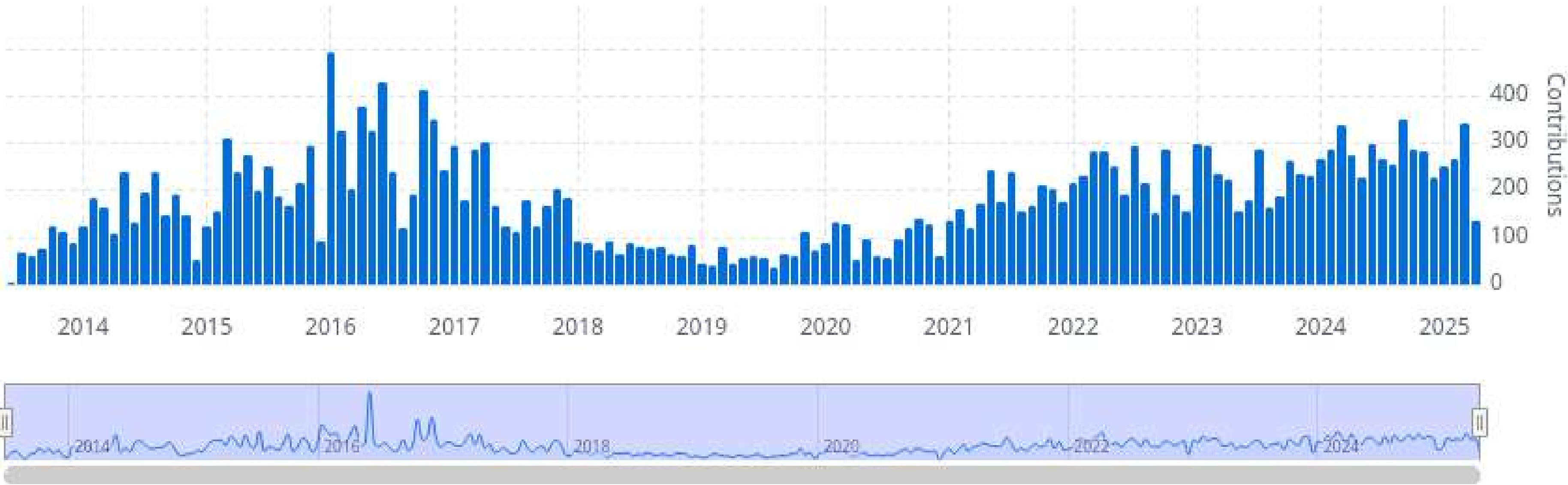
Contributors

Period: All ▾

Contributions per week to main, line counts have been omitted because commit count exceeds 10,000.

Commits over time

Weekly from Jun 30, 2013 to Apr 20, 2025



Fonctionnalités

- Single Sign On/Out
- Fournisseur OIDC / SAML
- Multi-tenant
- Login via un IdP externe
- Login via les RS (Google, FB,...)
- Fédération d'utilisateurs (LDAP, AD)
- Bridge Kerberos
- 2FA (TOTP, Webauthn)
- Parcours d'authentification
- Gestion des attributs utilisateurs
- Interface d'administration
- Gestion des comptes
- Gestion des sessions
- Supports de thèmes
- Personnalisation par SPI



worteks

Current realm

Manage realms

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Users > Create user

Create user

Required user actions

Select action

?

Email verified

Off

?

General

Username *

test

Email

test@worteks.com

First name

test

Last name

test

Groups

Join Groups

Jump to section

General



KEYCLOAK

Personal info

Account security

Signing in

Device activity

Applications

Signing in

Configure ways to sign in.

Basic authentication

Password

Sign in by entering your password.

My password

Created

April 22, 2025 at 8:30 AM.

Update



Avantages

- Solide: Basé sur **Quarkus**
- Facile à déployer
- Très configurable et extensible
- Beaucoup de documentation
- Monitoring étendu
- Très utilisé, grosse communauté d'utilisateurs
- Interface d'administration très complète



Mais...

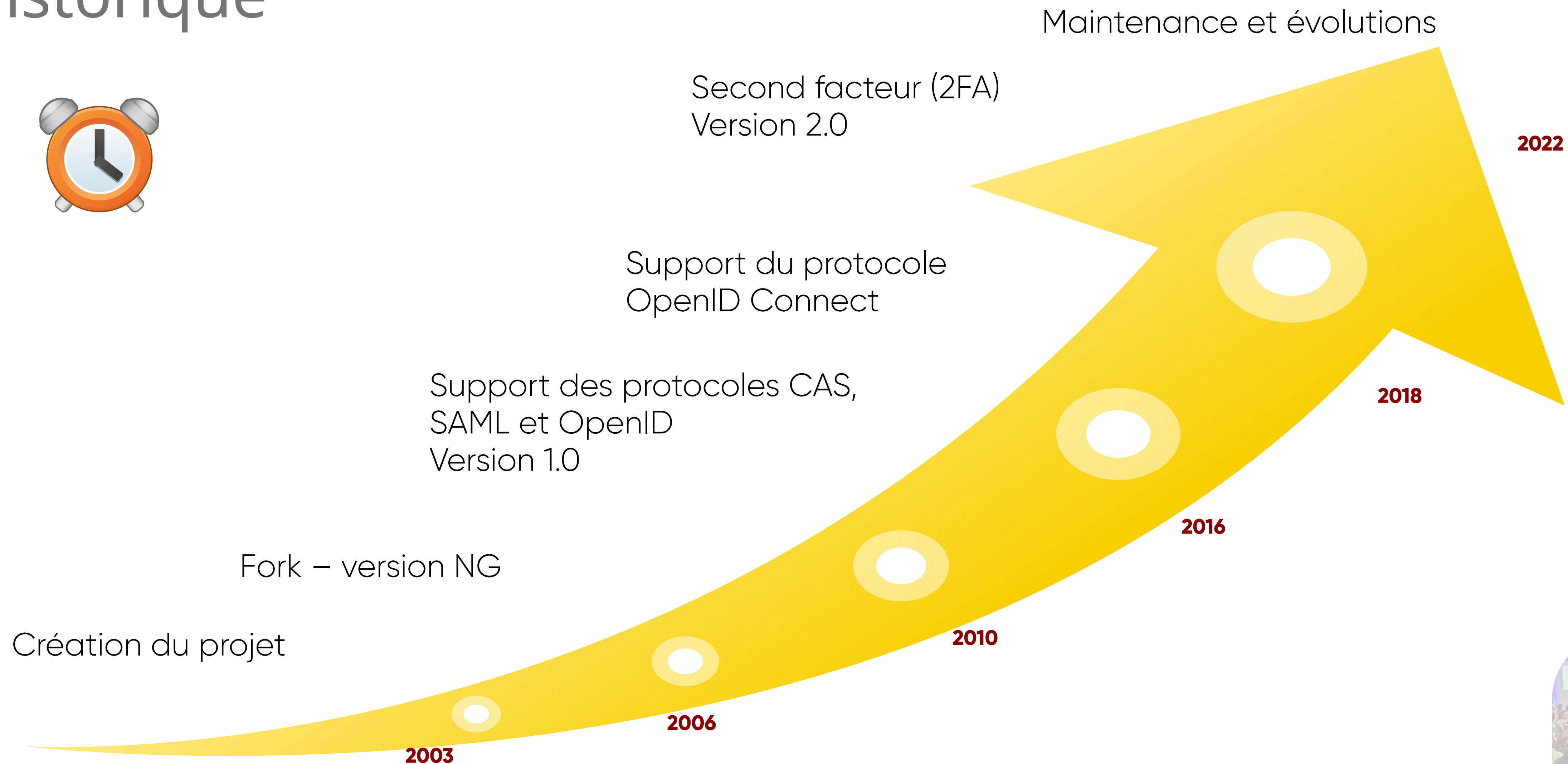
- Terminologie pas toujours intuitive
- Rythme de sortie des versions très élevée
- Pas de LTS gratuite, une LTS payante de courte durée (2 ans)
- Nécessite un suivi important
- Les développeurs principaux dépendent de Red Hat (pour l'instant)



Le logiciel LemonLDAP::NG



Historique



Principales fonctionnalités

- Authentification unique (WebSSO)
- Contrôle d'accès
- Portail d'applications
- Chaînage et choix des modules d'authentification
- Gestion du mot de passe, création de compte
- Authentification multi-facteurs
- Protection des applications Web et des API/WebServices
- Personnalisation graphique
- Paquets Debian/Ubuntu/RHEL/CentOS





Authentication required



Login



Password



Check my last logins



Connect



Reset my password



Create an account

Your applications

Password

Login history

Logout

Connected as **dw**ho ▾

Sample applications

Application Test 1
A simple application

Application Test 2
The same simple application

Administration

WebSSO Manager
Configure LemonLDAP:NG

Notifications explorer
Explore WebSSO notifications

Sessions explorer
Explore WebSSO sessions

2FA Sessions explorer
Explore WebSSO 2FA

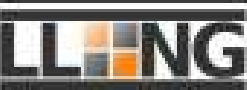
Documentation

Local documentation
Documentation supplied with

Official Website
Official LemonLDAP:NG

Service provided by **LemonLDAP:NG** free software covered by the GPL license.





- > General Parameters
- > Variables
- > Virtual Hosts
- > SAML2 Service
- > SAML Identity Providers
- > SAML Service Providers
- > OpenID Connect Service
- > OpenID Connect Providers
- > OpenID Connect Relying Parties
- > CAS Service
- > CAS Servers
- > CAS Applications

[Home](#) [Save](#) [Browse](#) [Show help](#) [Download it](#) [Restore](#)

Current configuration

Number	1
Author	The LemonLDAP::NG team
Author IP address	127.0.0.1
Date	04/04/2015 à 11:13:28
Configuration version	2.0.0
Resume	Default configuration provided by LemonLDAP::NG team

Command Line Interface

```
root@developpement-lemonldap:~# /usr/local/lemonldap-ng/bin/lemonldap-ng-cli help
Usage:
  Usage: lemonldap-ng-cli [options] ACTION [parameters ...]

  Available actions:

  help           : print the full documentation
  info           : get currentconfiguration info
  update-cache   : force configuration cache to be updated
  test-email DESTINATION : send a test email
  get KEY        : get values of parameters
  set KEY VALUE  : set parameter(s) value(s)
  del KEY        : delete parameters
  addKey KEY SUBKEY VALUE : add or set a subkey in a parameter
  delKey KEY SUBKEY : delete subkey of a parameter
  addPostVars HOST URI KEY VALUE : add post vars for form replay
  delPostVars HOST URI KEY : delete post vars for form replay
  merge FILE [FILE ...] : merge JSON/YAML files with existing configuration
  save           : export configuration to STDOUT
  restore -      : import configuration from STDIN
  restore FILE   : import configuration from file
  rollback       : restore previous configuration
```

```
root@developpement-lemonldap:~# /usr/local/lemonldap-ng/bin/lemonldap-ng-cli info
Num      : 135
Author   :
Author IP: 10.0.3.1
Date     : Thu Jul 11 15:04:12 2024
Version  : 2.19.0
Log      : disable hibp
```

```
root@developpement-lemonldap:~# /usr/local/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
Proposed changes:
Key           | Old value          | New value
ldapServer    | ldap://10.0.3.1    | ldap://ldap.example.com
Confirm (N/y)? █
```

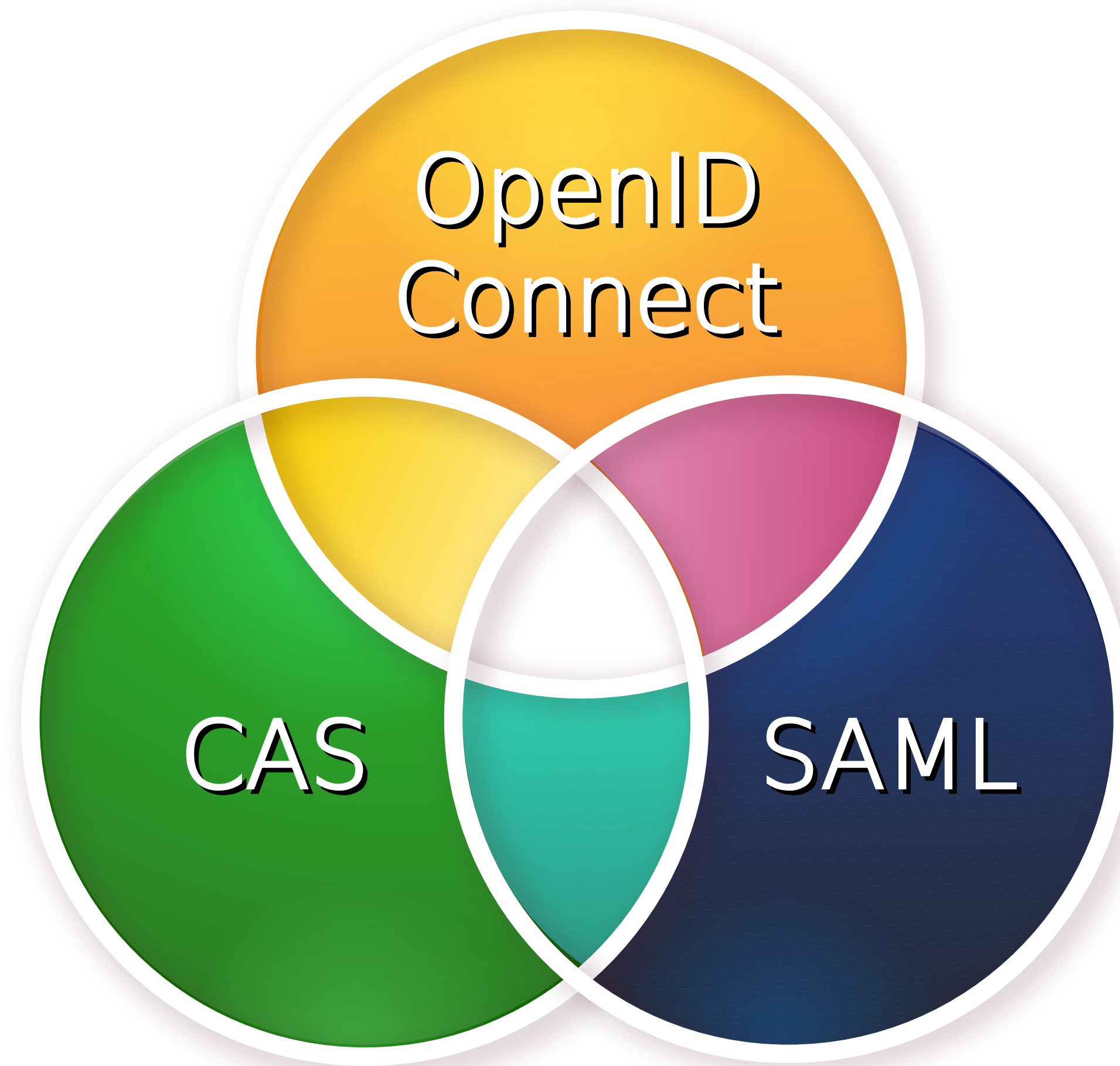


Logiciel Libre

- Licence GPL
- Projet OW2
- Forge : <https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng>
- Site : <https://lemonldap-ng.org>
- OW2 Community Award en 2014
- Composant SSO du projet FusionIAM : <https://fusioniam.org/>



Passerelle multi-protocoles



Fonctions « self service »



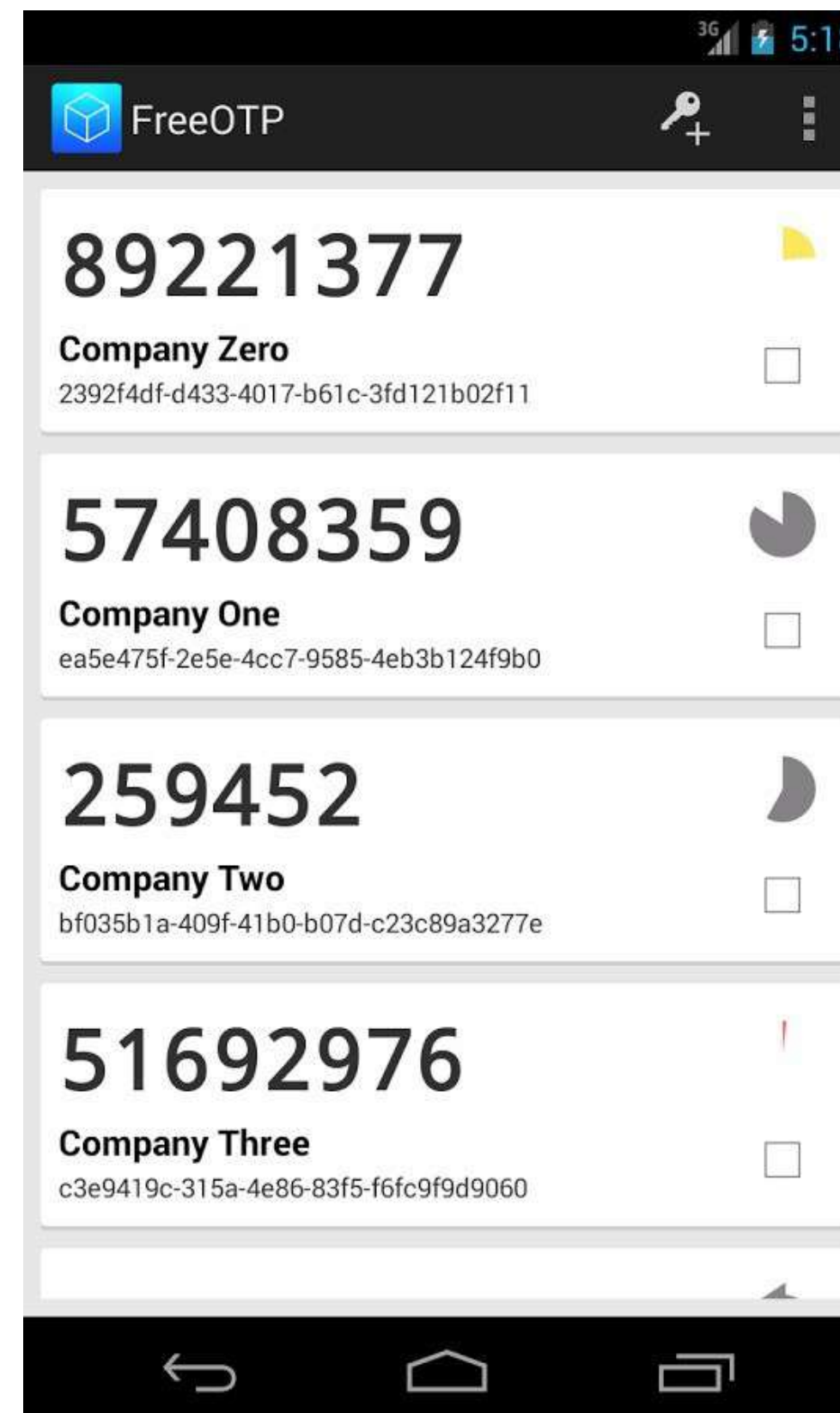
Gestion du mot de passe
(changement, réinitialisation)
Création de compte
Gestion des seconds facteurs
Réinitialisation de certificat



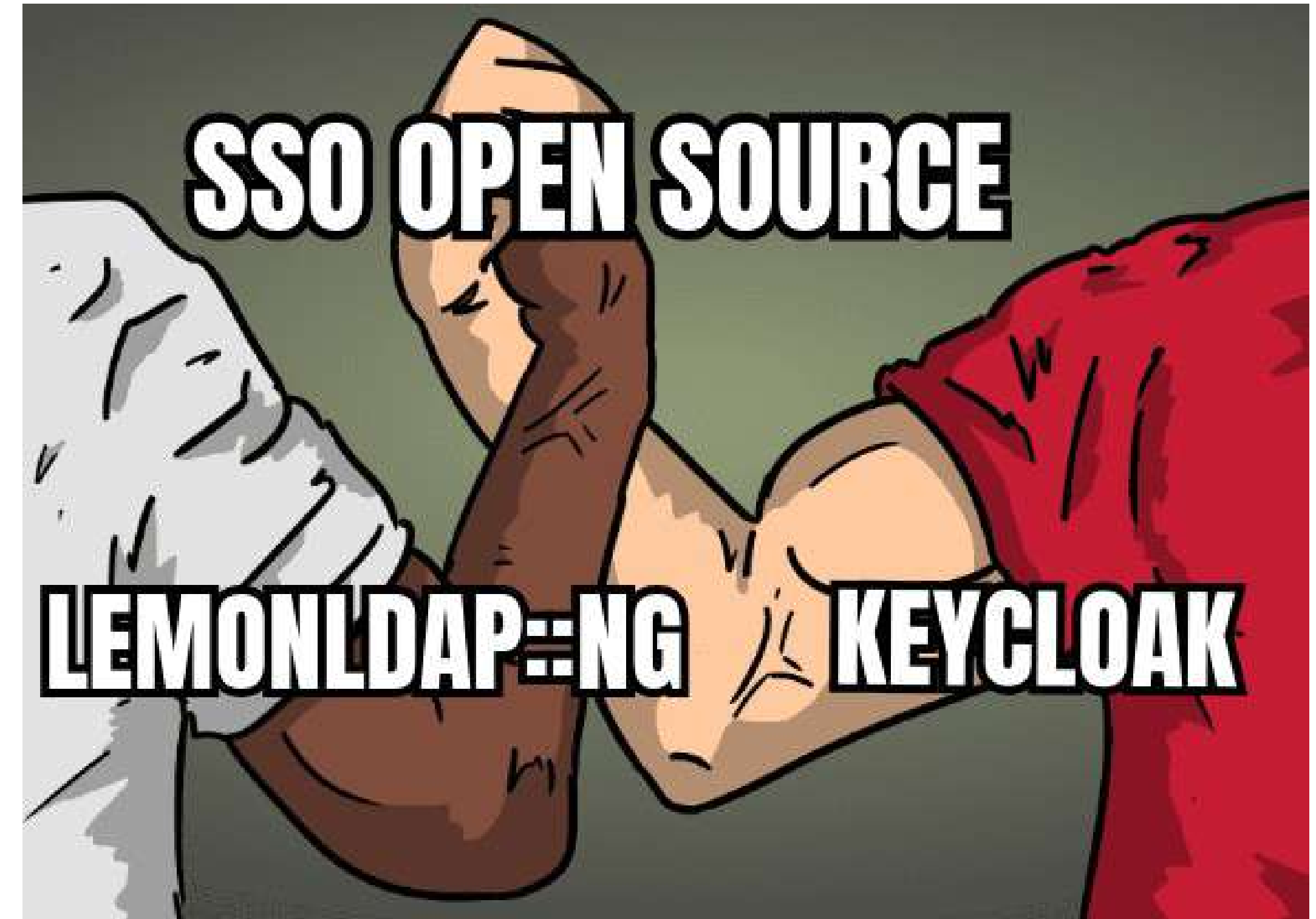
2FA/MFA

LemonLDAP::NG supporte nativement les MFA suivants :

- TOTP
- WebAuthn
- Externe
- Mail
- REST
- Okta
- Yubikey
- Radius



Conclusion



Conclusion

- 2 logiciels très complets et matures
- font référence par rapport à la concurrence payante
- Le choix entre les 2 dépend du contexte projet et de la ligne politique

Keycloak

LemonLDAP::NG

équipe Red-Hat dédiée

 souveraineté, équipe communautaire

Très apprécié des **développeurs / testeurs**

logiciel orienté **infrastructure**

base utilisateur prête à l'emploi, avec synchro possible depuis / vers un annuaire LDAP

grande capacité d'adaptation à l'infra actuelle

multi-tenant avec les **realms**

serveur / client **CAS** natif

très bon support d'**OIDC**

handler pour les vieilles applications



Conclusion

Keycloak

support de notion de **groupes / rôles**

personnalisation des **flux** : connexion, enregistrement de compte, réinitialisation de mot de passe,...

développement de fonctionnalités supplémentaires avec les **SPI**

LemonLDAP::NG

moteur de **règles d'accès** avancé... mais complexe

nombreux modules **MFA** nativement supportés : TOTP, Webauthn, mail, SMS, Radius, REST, External

développement de fonctionnalités supplémentaires par des **modules perl**

Fédération RENATER nativement supportée



The logo consists of four stylized human figures of varying heights. The second figure from the left is green, while the others are white. A small green circle is positioned above the tallest figure.

IDENTITY DAYS

@IdentityDays

#identitydays2025