Vorteks

make IT work, make IT free

BIBLIOTHÈQUE MUNICIPALE DE LYON

# Déploiement de LemonLDAP::NG à la Bibliothèque Municipale de Lyon


RPLL

28 juin 2022

# Intervenants

Jean-Baptiste VICAIRE
Responsable Informatique
BM Lyon

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

# Worteks (\vɔʁ.tɛks\)

## Service

Complex infrastructures, cloud, mail, authentication, security

- Studies, audit & consulting
- Technical expertise
- Support
- Training
- R&D and innovation

## Edition

**V'Sweet** — Collaborative portal

**V'Opla** — Common developement platform

**V'IDaaS** — Identity and Access Management

## Partners

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

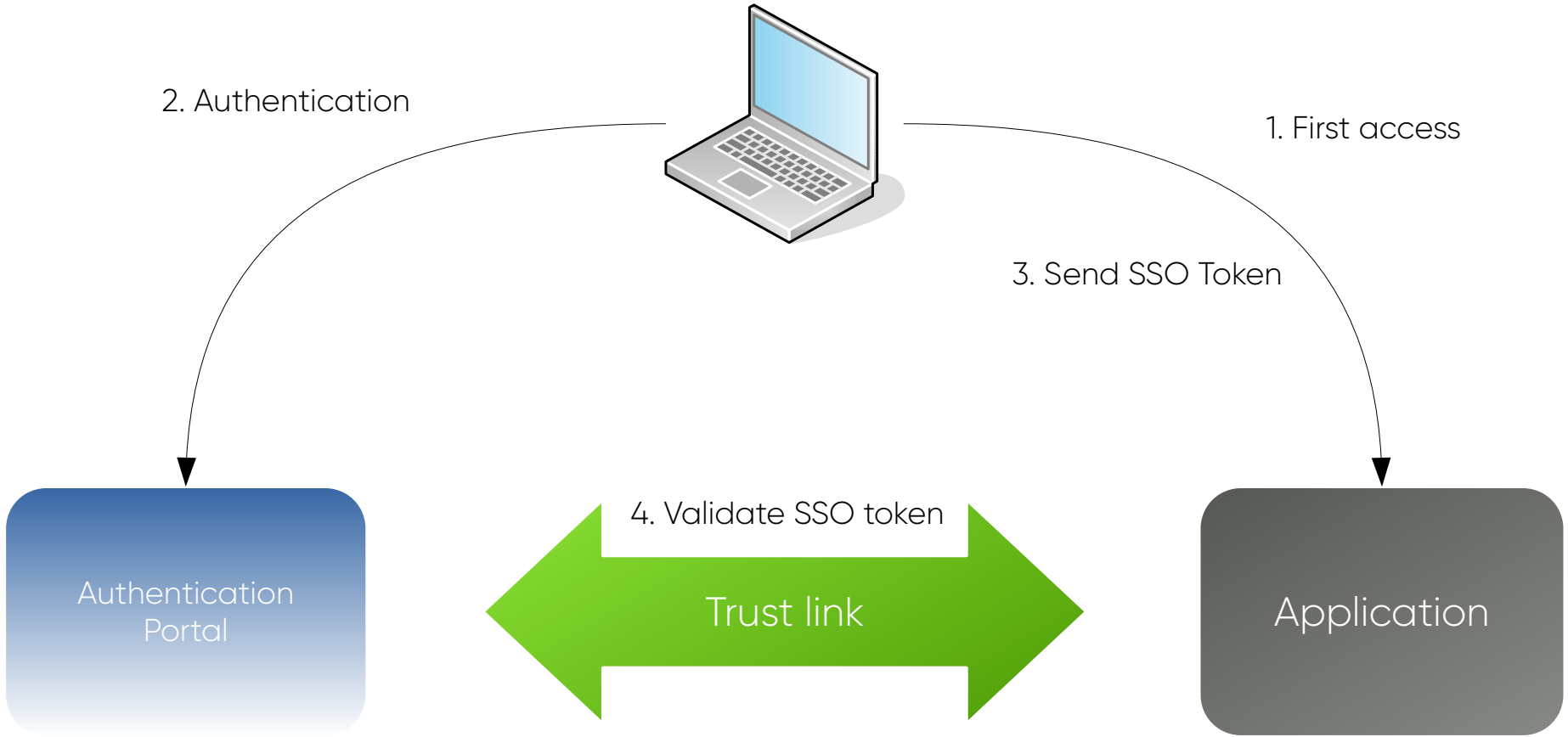
Collabora Online

# All we need is you!

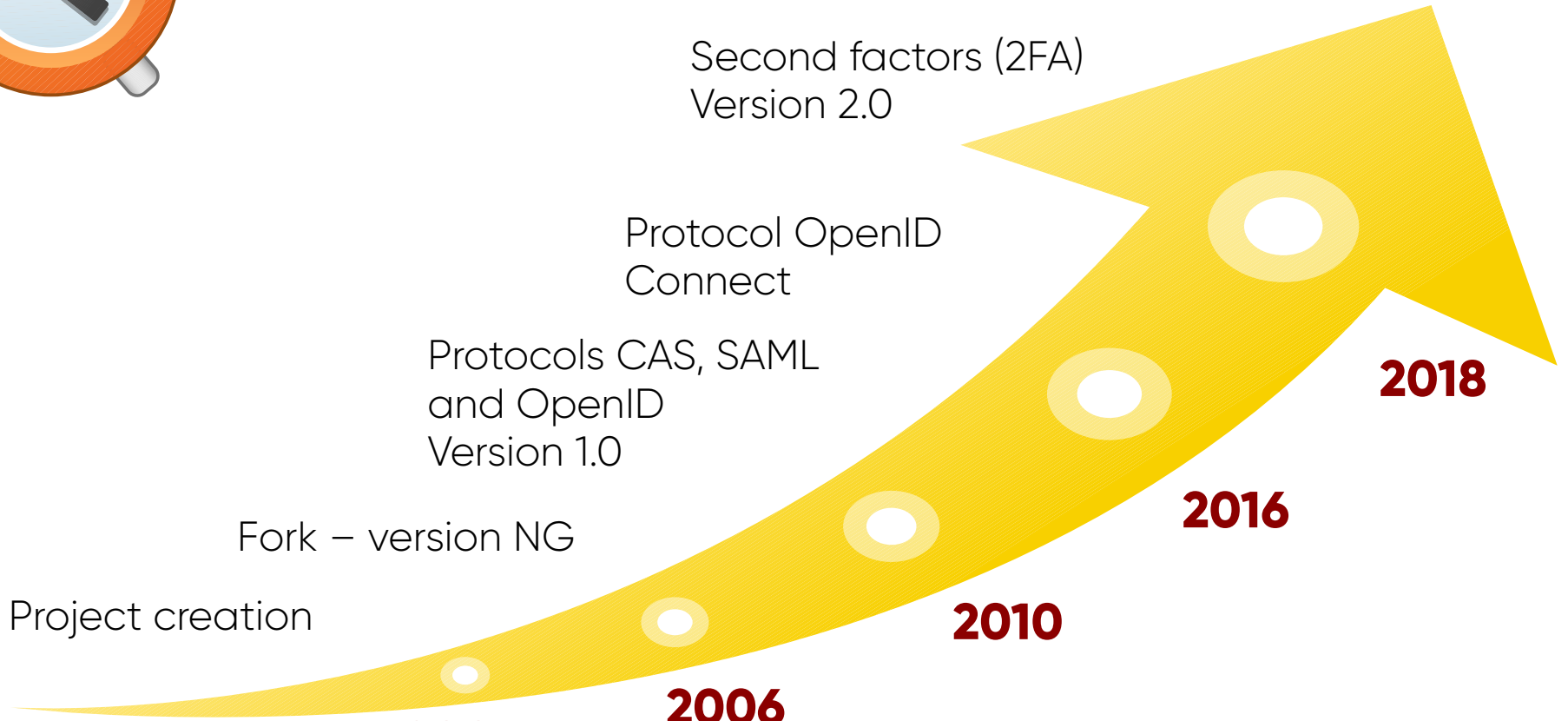
https://www.worteks.com/rejoindre/

# Présentation de LemonLDAP::NG

# SSO Workflow

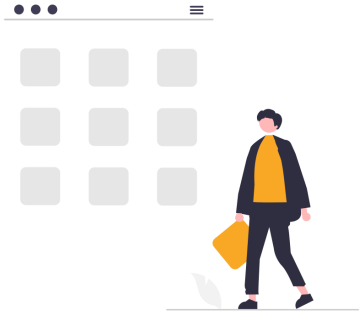


# History


Second factors (2FA)
Version 2.0
Protocol OpenID
Connect
Protocols CAS, SAML
and OpenID
Version 1.0
Fork – version NG
Project creation
2018
2016
2010
2006
2003

# Main features

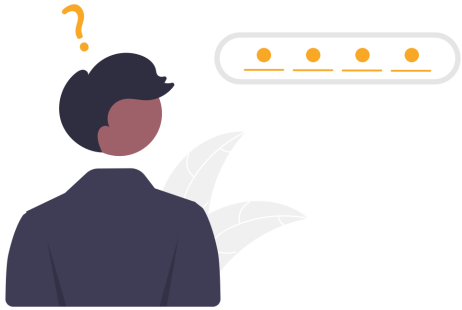
SSO & Access Control



Application menu

CAS / SAML / OIDC

Second Factor (2FA)

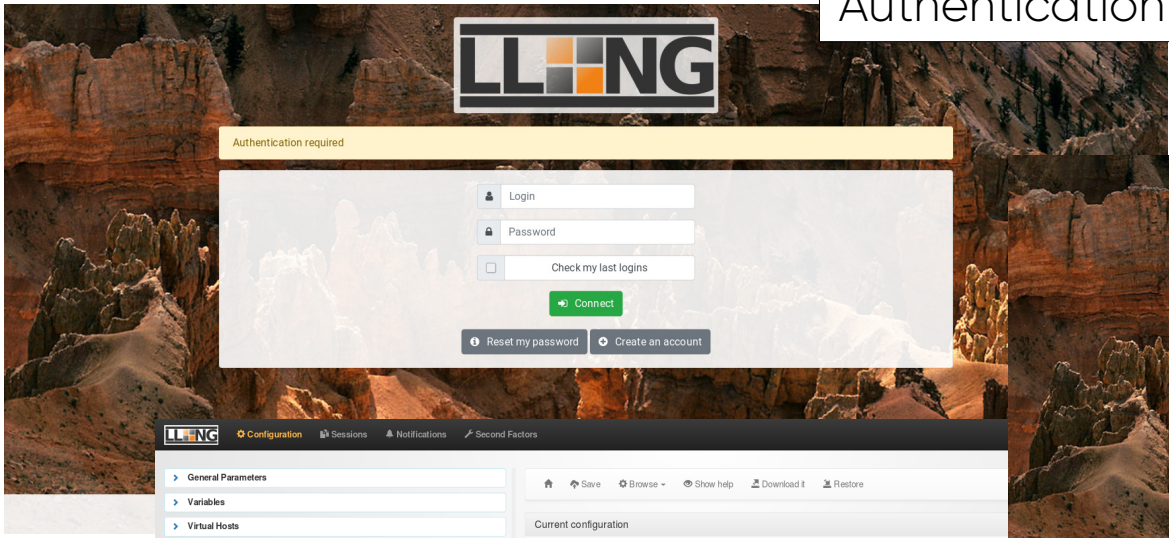


Password management

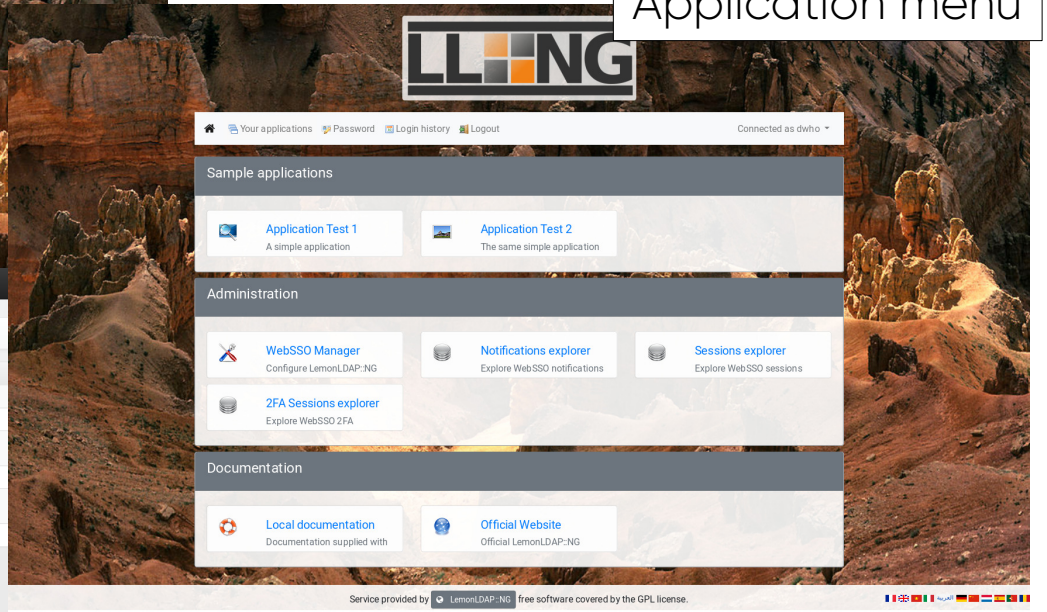
Graphical customization

# Screenshots

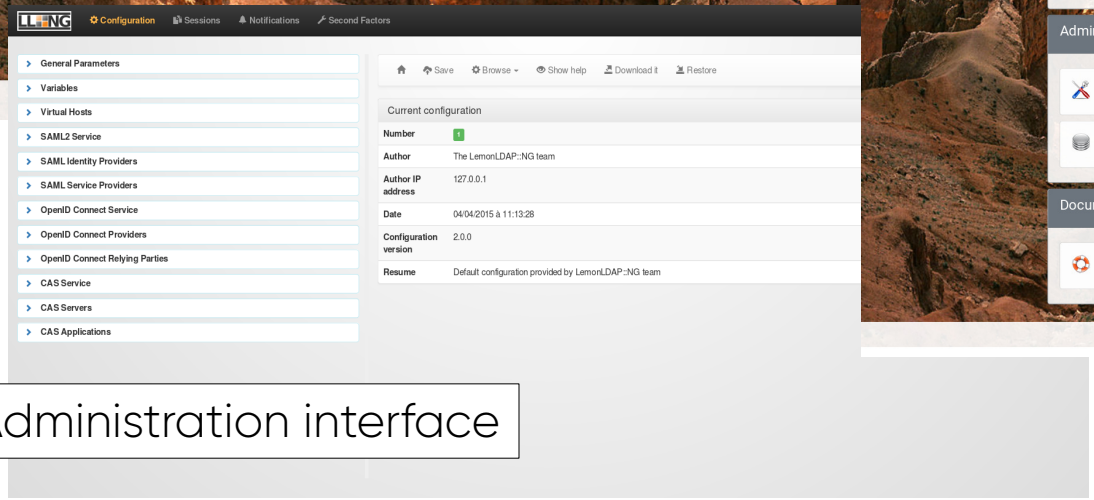
Authentication form




Application menu




Administration interface



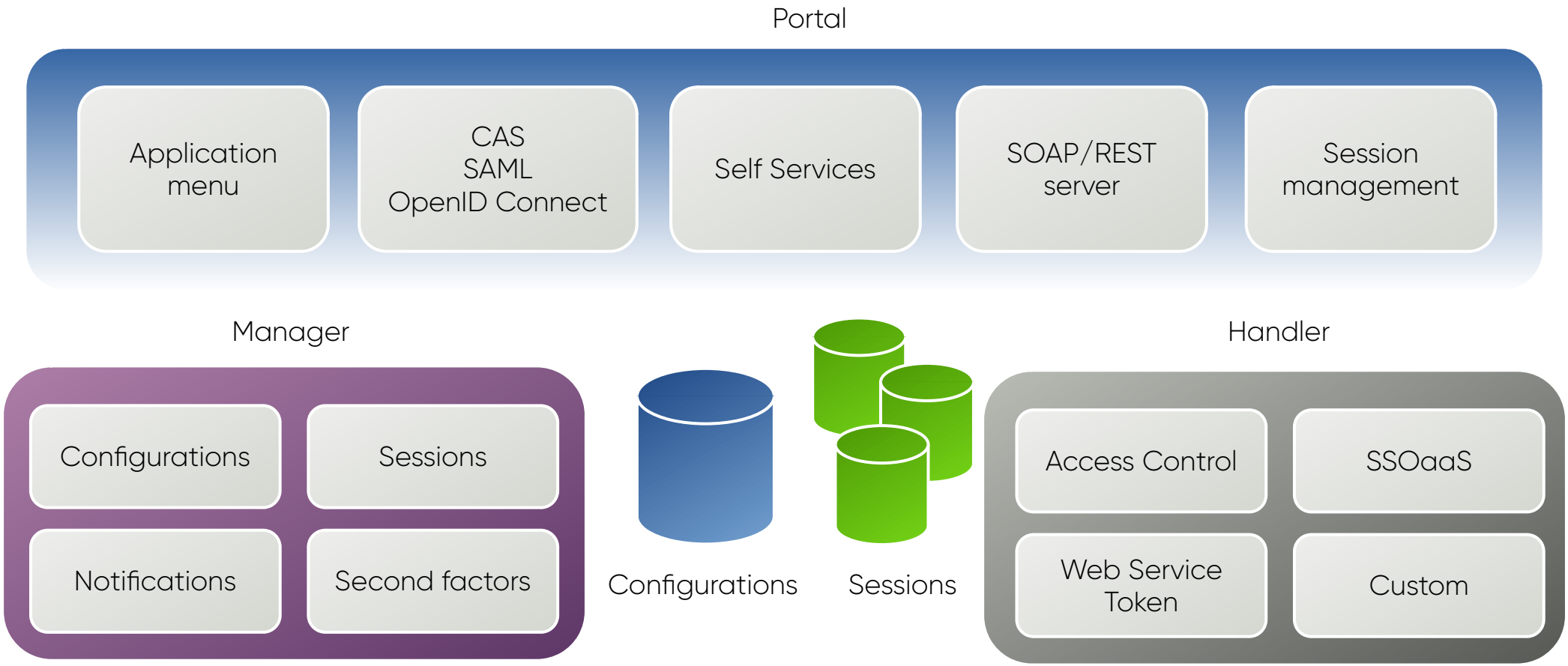
# Command Line Interface

```
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

Num      : 88
Author   : clement
Author IP: localhost
Date     : Tue Dec 18 09:57:58 2018
Log      : Edited by lmConfigEditor
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli help
Usage: /usr/share/lemonldap-ng/bin/lemonldap-ng-cli <options> action <parameters>

Available actions:
 - help                          : print this
 - info                          : get currentconfiguration info
 - update-cache                  : force configuration cache to be updated
 - get    <keys>                 : get values of parameters
 - set    <key> <value>          : set parameter(s) value(s)
 - addKey <key> <subkey> <value> : add or set a subkey in a parameter
 - delKey <key> <subkey>         : delete subkey of a parameter

See Lemonldap::NG::Common::Cli(3) or Lemonldap::NG::Manager::CLi(3) for more
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
```

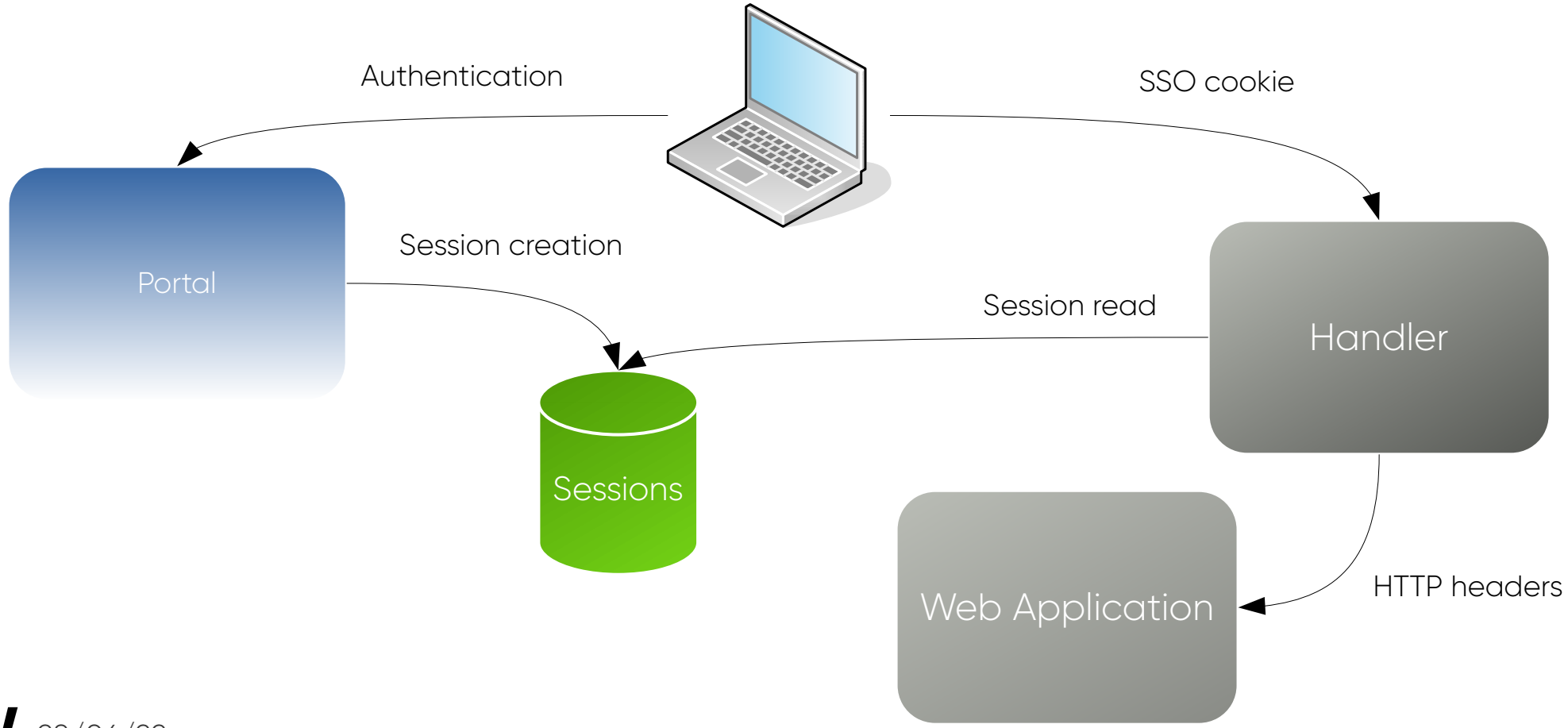
# Free Software

- License GPL
- OW2 project
- Forge: https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng
- Site: https://lemonldap-ng.org
- OW2 Community Award in 2014
- SSO component of FusionIAM project: https://fusioniam.org/

# Component roles



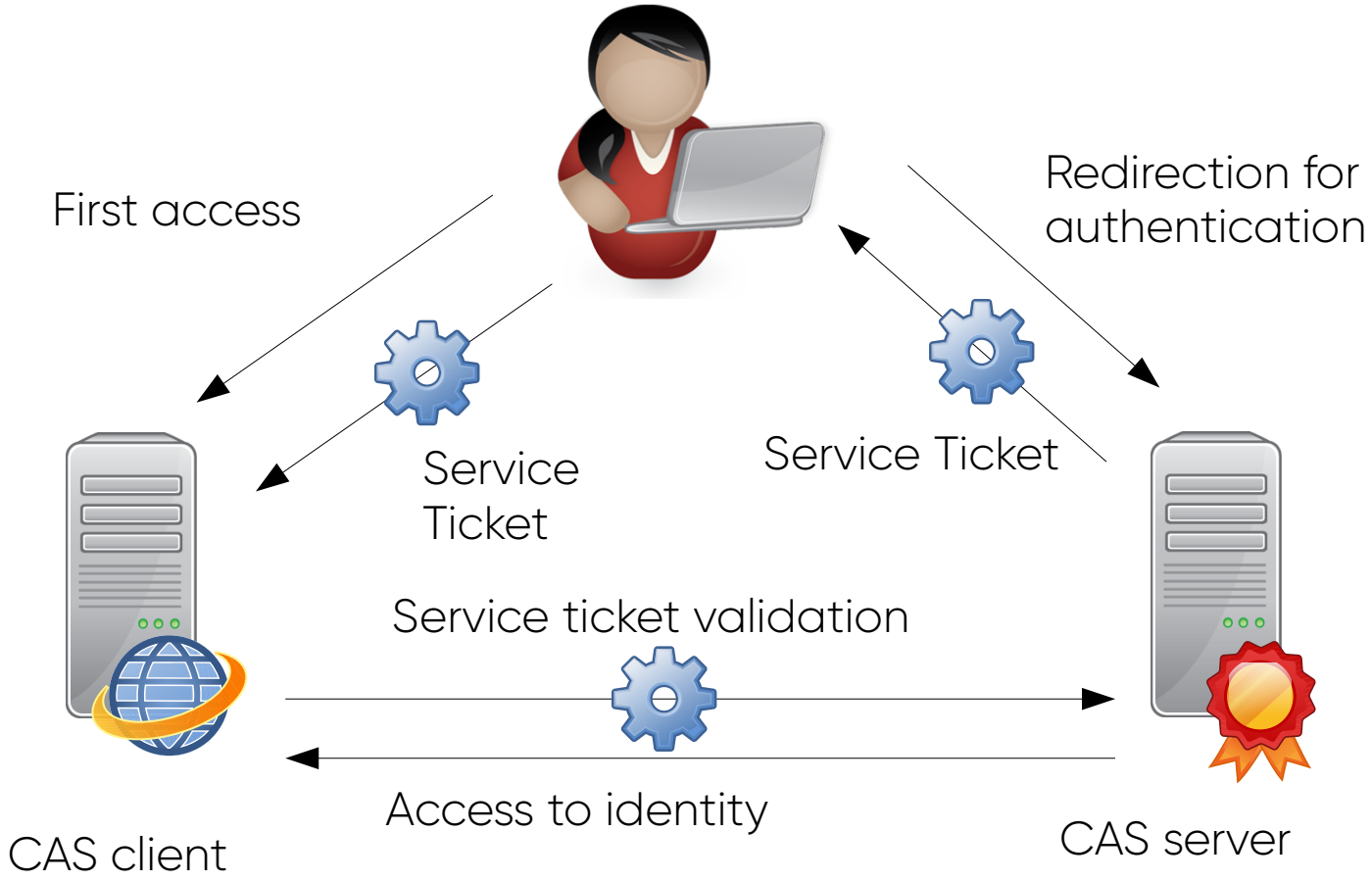
# Web application



# CAS

- Created by University of Yale
- Central Authentication Service
- Proxy mode since v2.0
- Attributes sharing since v3.0
- https://www.apereo.org/projects/cas

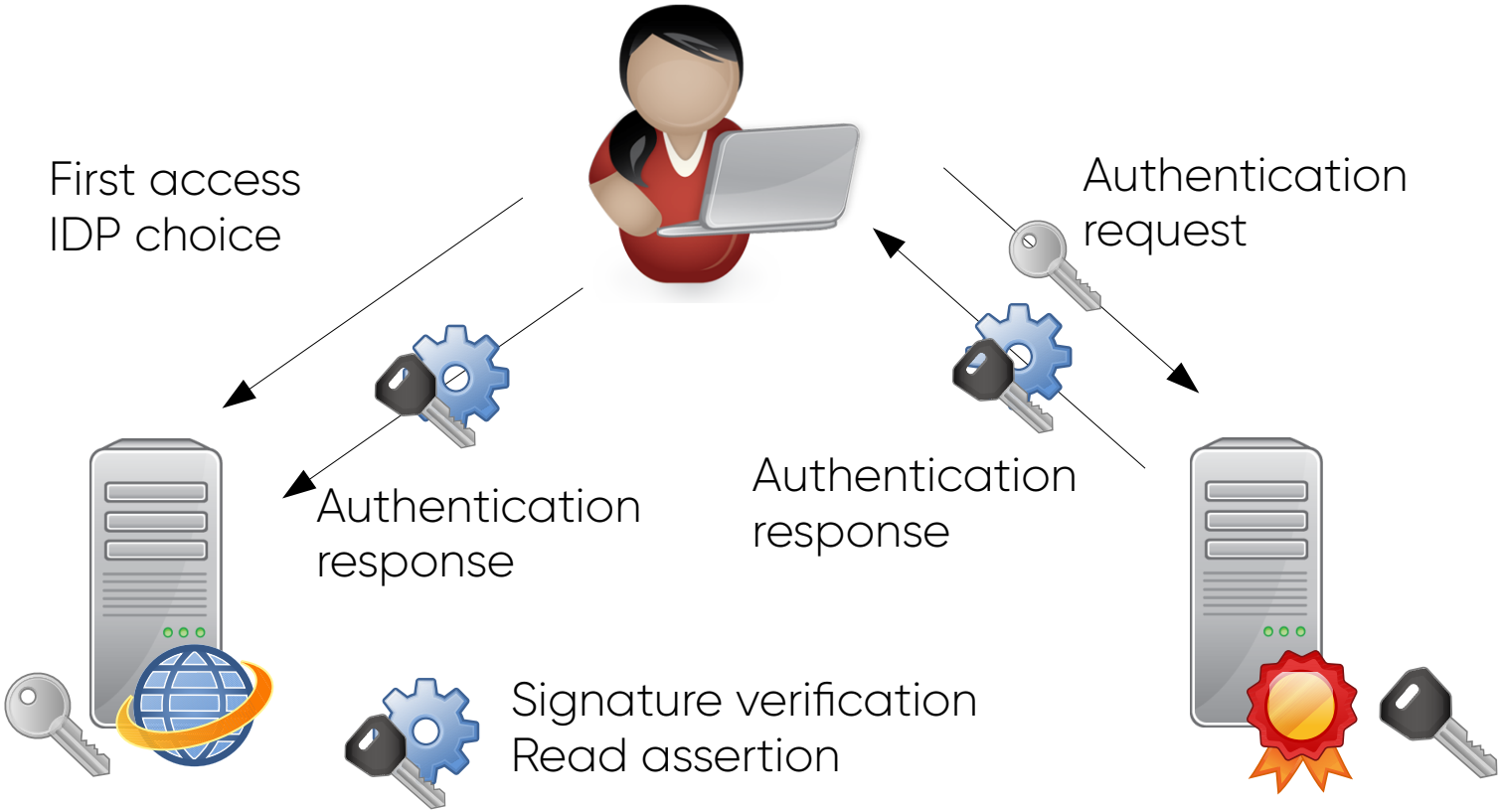
# CAS


First access
Redirection for authentication
Service Ticket
Service Ticket
Service ticket validation
Access to identity
CAS client
CAS server

# SAML

- Created by OASIS organization
- Security Assertion Markup Language
- Version 1.0 in 2002
- Version 1.1 in 2003
- Version 2.0 in 2005 merging SAML, Shibboleth and ID-FF (Liberty Alliance)

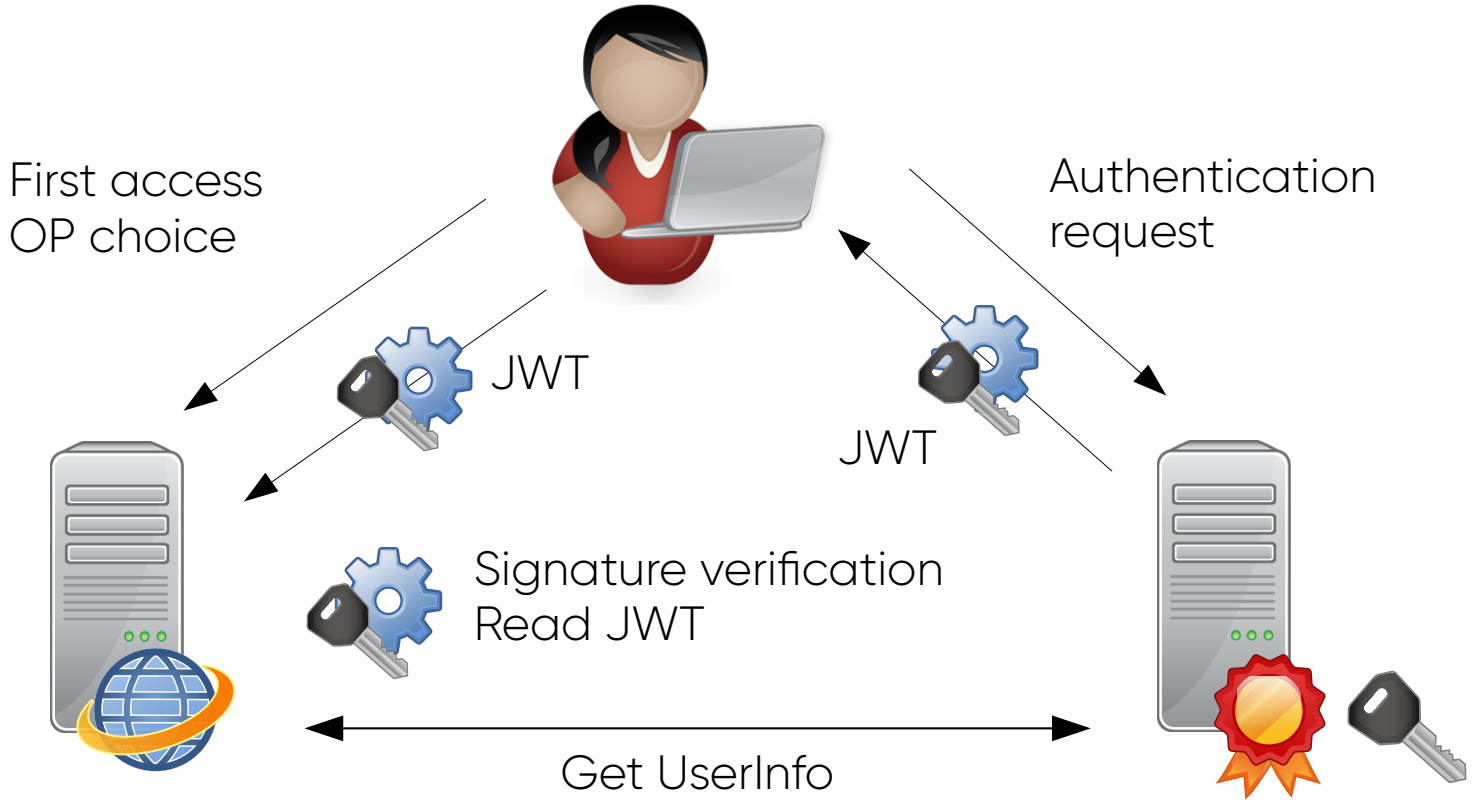
# SAML


First access
IDP choice
Authentication
request
Authentication
response
Authentication
response
Signature verification
Read assertion
Service Provider (SP)
Identity Provider (IDP)

# OpenID Connect

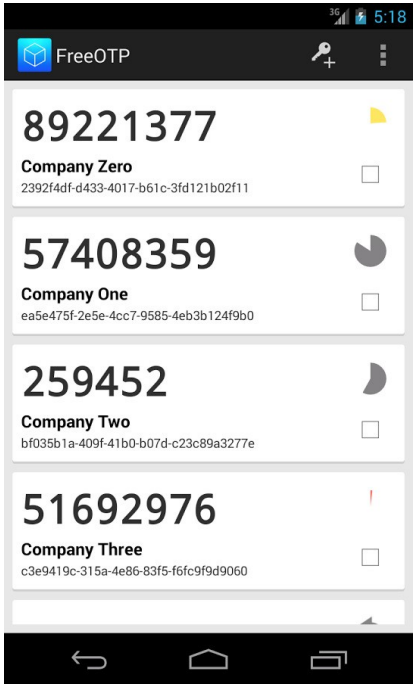
- Created in 2014
- Presented at RMLL in 2015
- Based on OAuth 2.0, REST, JSON, JWT, JOSE
- Adapted to web browser and native mobile applications
- Attributes sharing trough UserInfo endpoint

# OpenID Connect



# Second Factor Authentication (2FA)

- LemonLDAP::NG can use the following 2FA:
  - TOTP
  - WebAuthn
  - Mail
  - External (SMS)
  - REST
  - Yubikey
  - Radius




fido ALLIANCE

# RENATER / eduGAIN

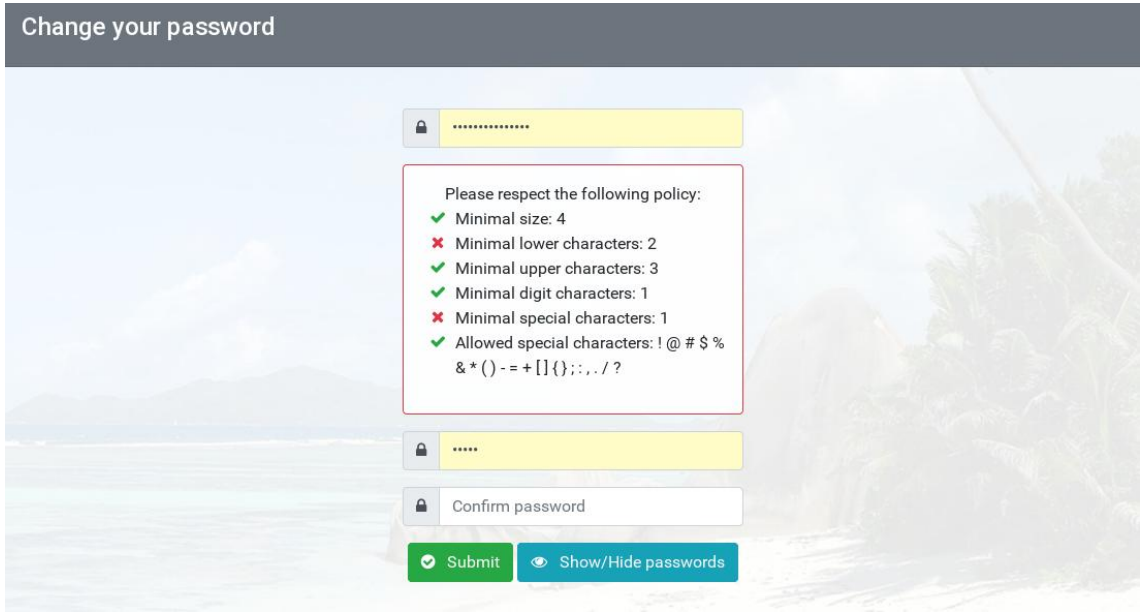
- Support of RENATER / eduGAIN via SAML2:
  - Service Provider
  - Identity Provider
- Call to Identity Provider selection page (WAYF) via SAML Discovery Protocol
- Metadata bulk import script


# Plugin engine

- Portal code was fully rewritten, and it now allows to write plugins
- Plugin examples, provided by default:
  - Auto Signin: direct authentication for some IP
  - Brute Force: protect against brute-force attacks
  - Stay Connected: "remember me" button
  - Public Pages: create static pages using portal skin
- Write a custom plugin: https://lemonldap-ng.org/documentation/latest/plugincustom

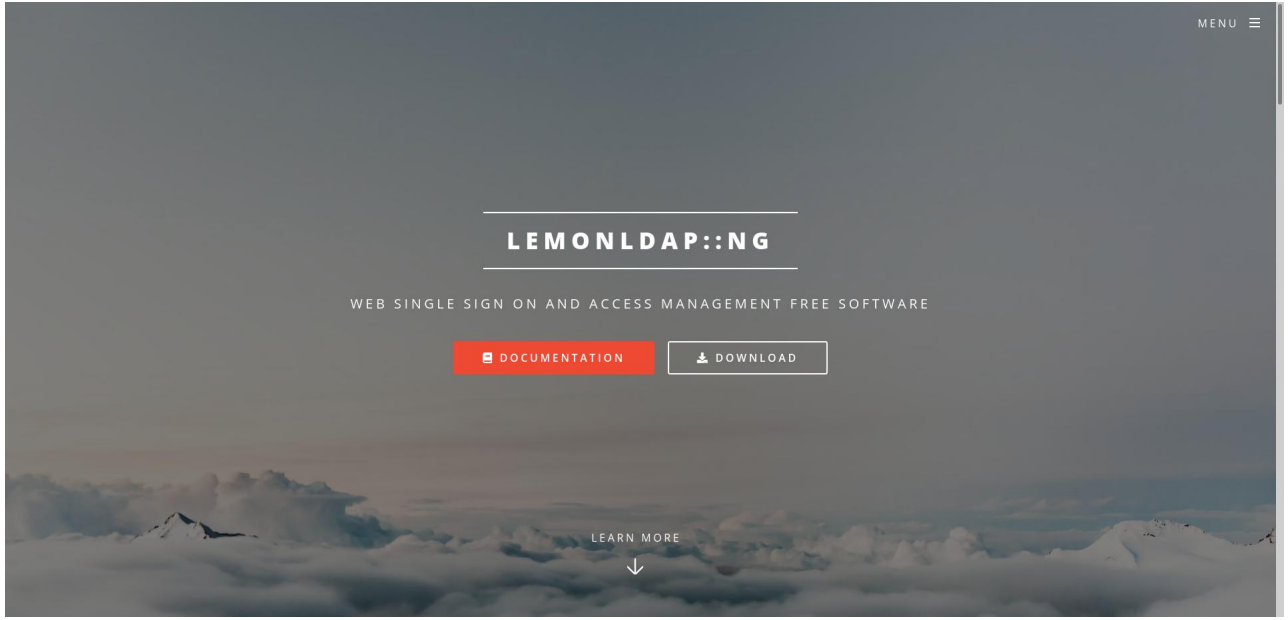
# Password Policy

- A local password policy can now be configured (minimal size, type of characters, ...)
- A graphical form shows which criteria are filled



# Documentation and Website

- Documentation was rewritten with Sphinx (reStructuredText)
- Website rebuilt as static pages with Templer



# Keep informed about LL::NG

- Register to lemonldap-ng-announces mailing list
  https://mail.ow2.org/wws/subscribe/lemonldap-ng-announces
- Follow project updates
  https://projects.ow2.org/bin/view/lemonldap-ng/
- Social networks:
  - Twitter: https://twitter.com/lemonldapng/
  - Facebook: https://www.facebook.com/lemonldapng/

# Mise en place à la BM Lyon

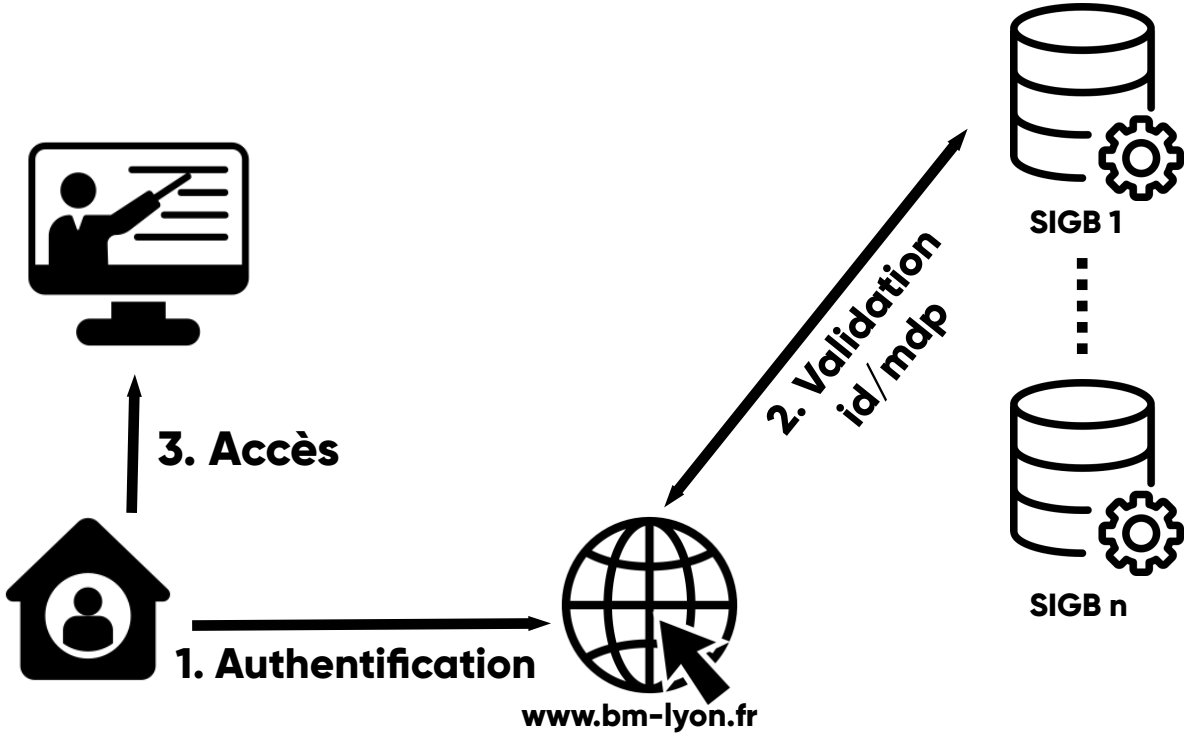
# Contexte

- Offre de ressource en ligne pour les usagers BML et partenaires


- Comptes usagers dans 38 logiciels métiers (SIGB) différents

# Etat des lieux 1

- Autorisation par HTTP referer



# Etat des lieux 2

- Autorisation par http referer non sécurisée
- Peu fiable
- Pas de SSO
- Statistiques déficientes

# Objectif

- SSO
- Protocole standard
- Autonomie
- Amélioration statistiques


# Solution

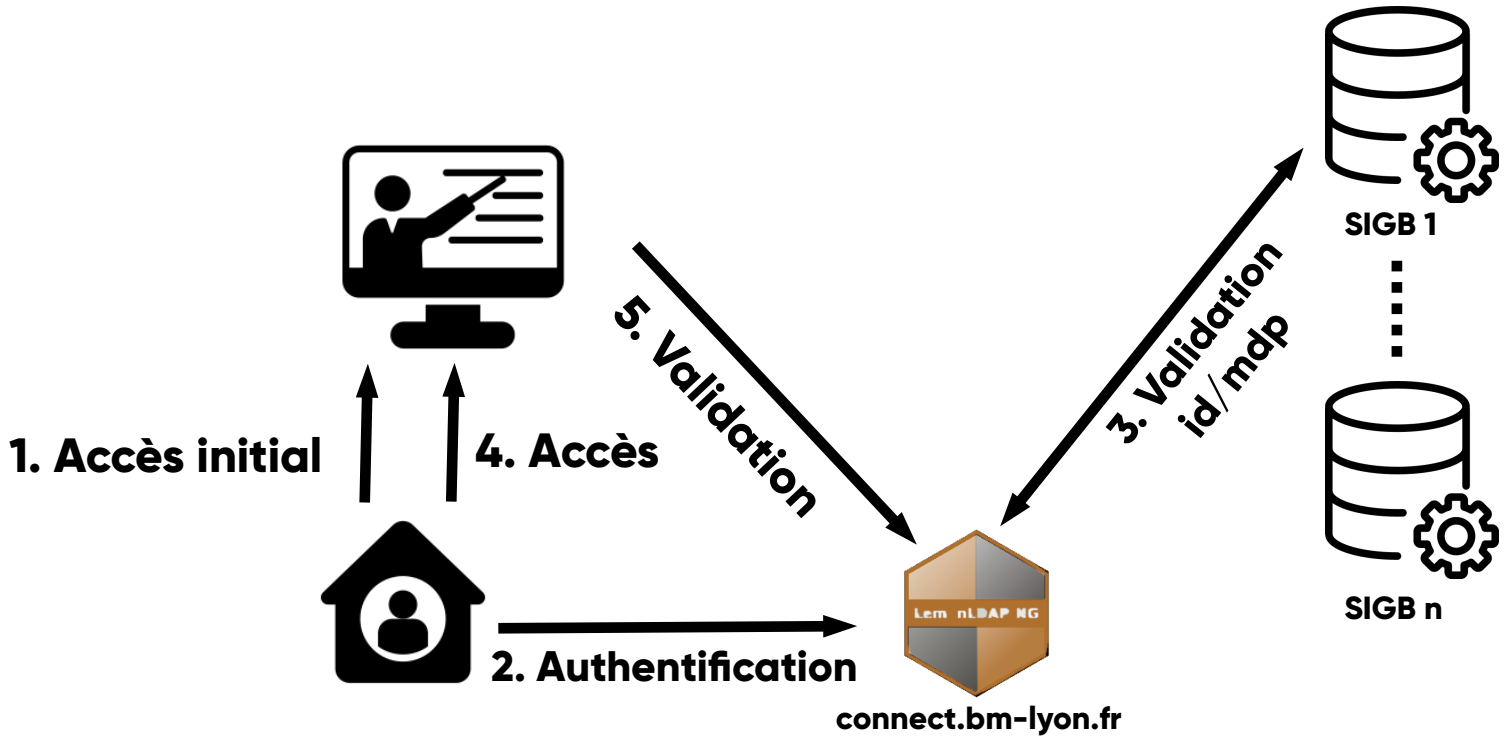

**SSO**


**Traitement log**

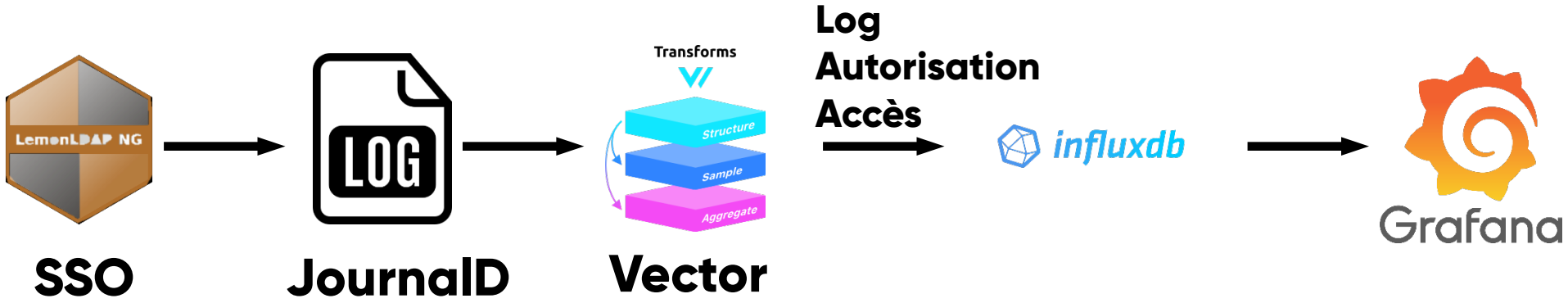

**Stockage TSDB**


**Visualisation**

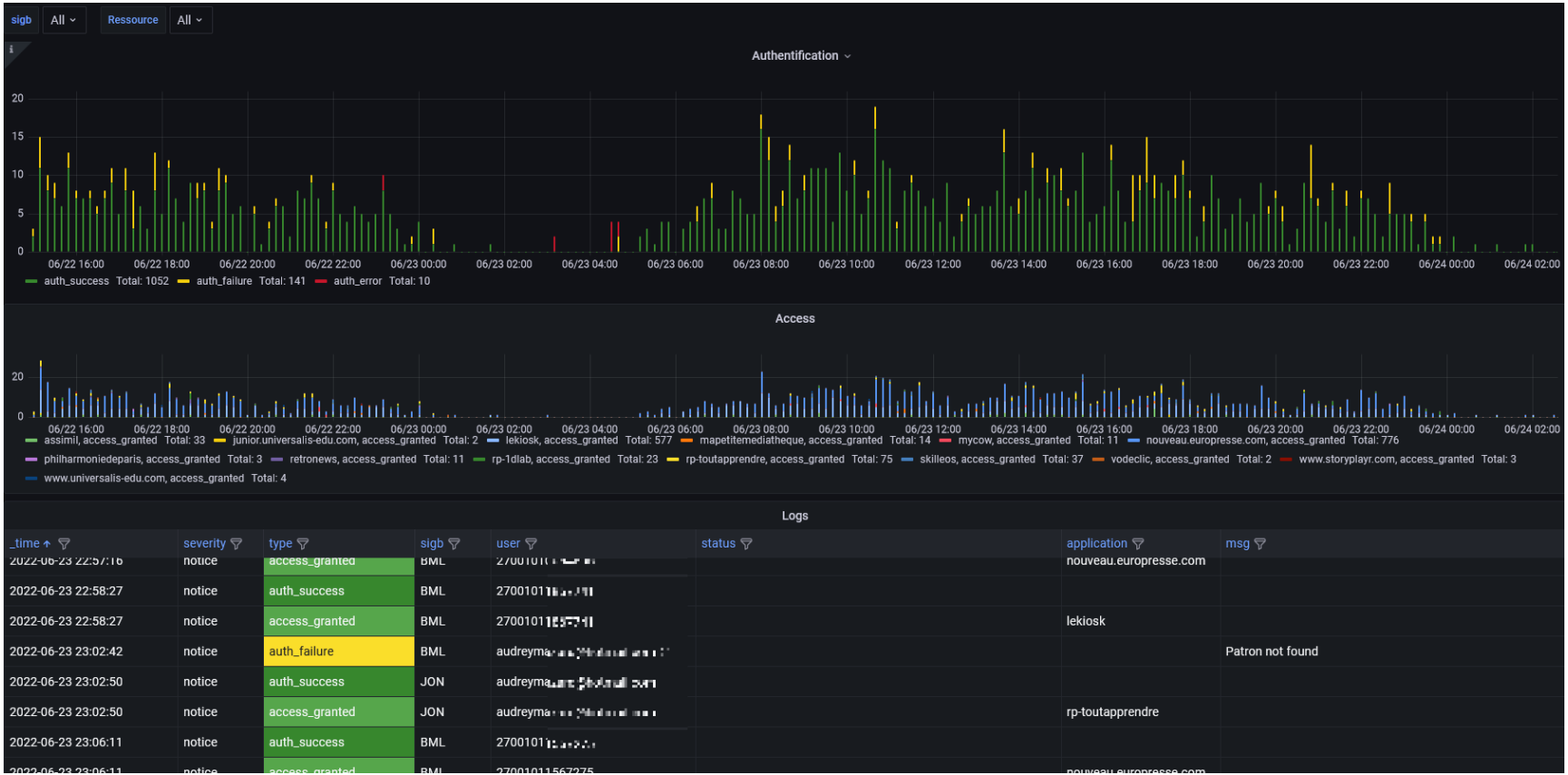
# Principe


1. Accès initial
4. Accès
5. Validation
3. Validation
id/mdp
2. Authentification
Lem nLDAP NG
connect.bm-lyon.fr
SIGB 1
SIGB n

# Statistiques



# Visualisation statistique



# Usage sur 1 an

# Bilan

Fiabilité

Coût

Autonomie

Worteks

*make IT work, make IT free*

BIBLIOTHÈQUE MUNICIPALE DE LYON

# Merci de votre attention


info@worteks.com

@worteks_com

linkedin.com/company/worteks