worteks

make IT work, make IT free

# LEMONLDAP::NG SUCCESS STORIES

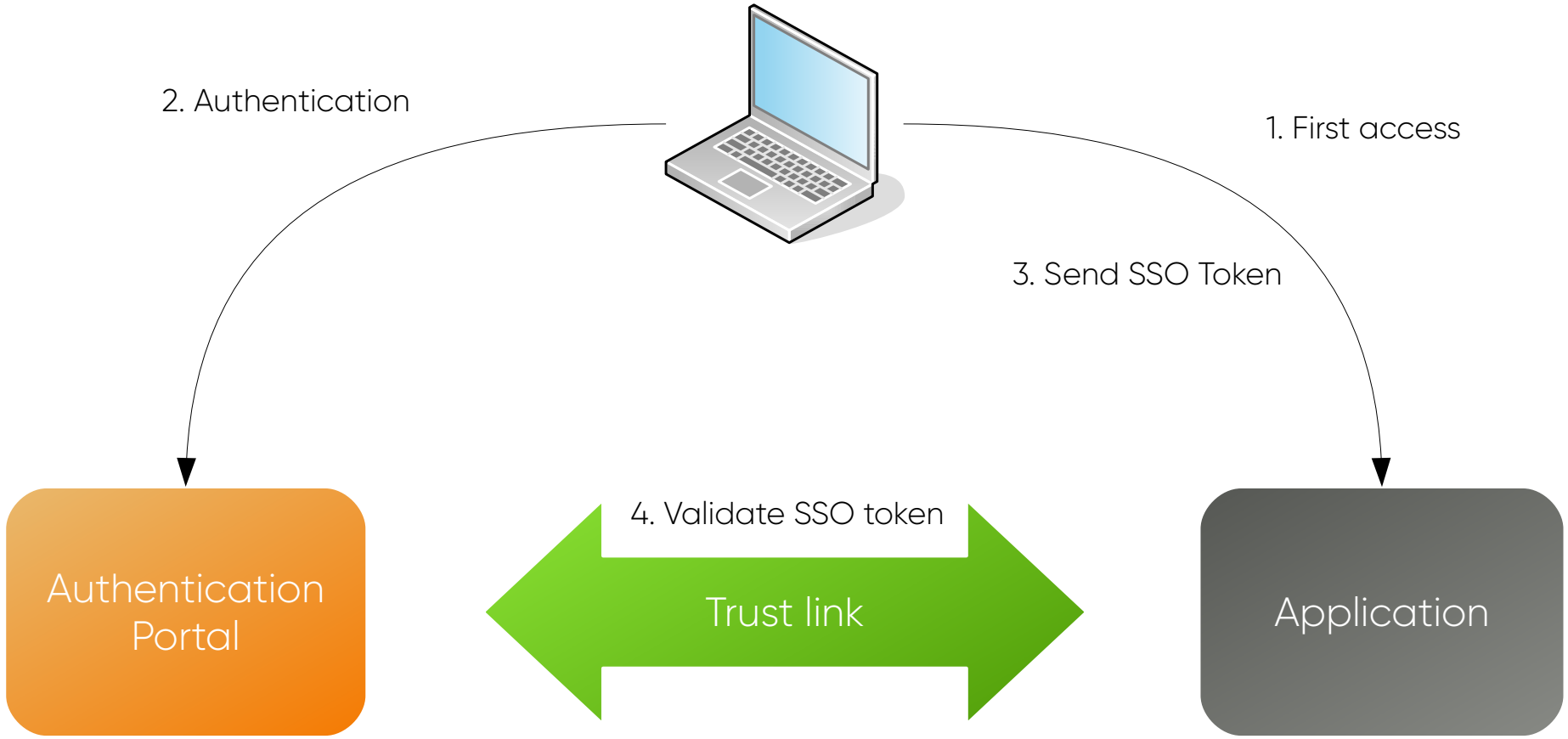
Gendarmerie nationale

Une force humaine

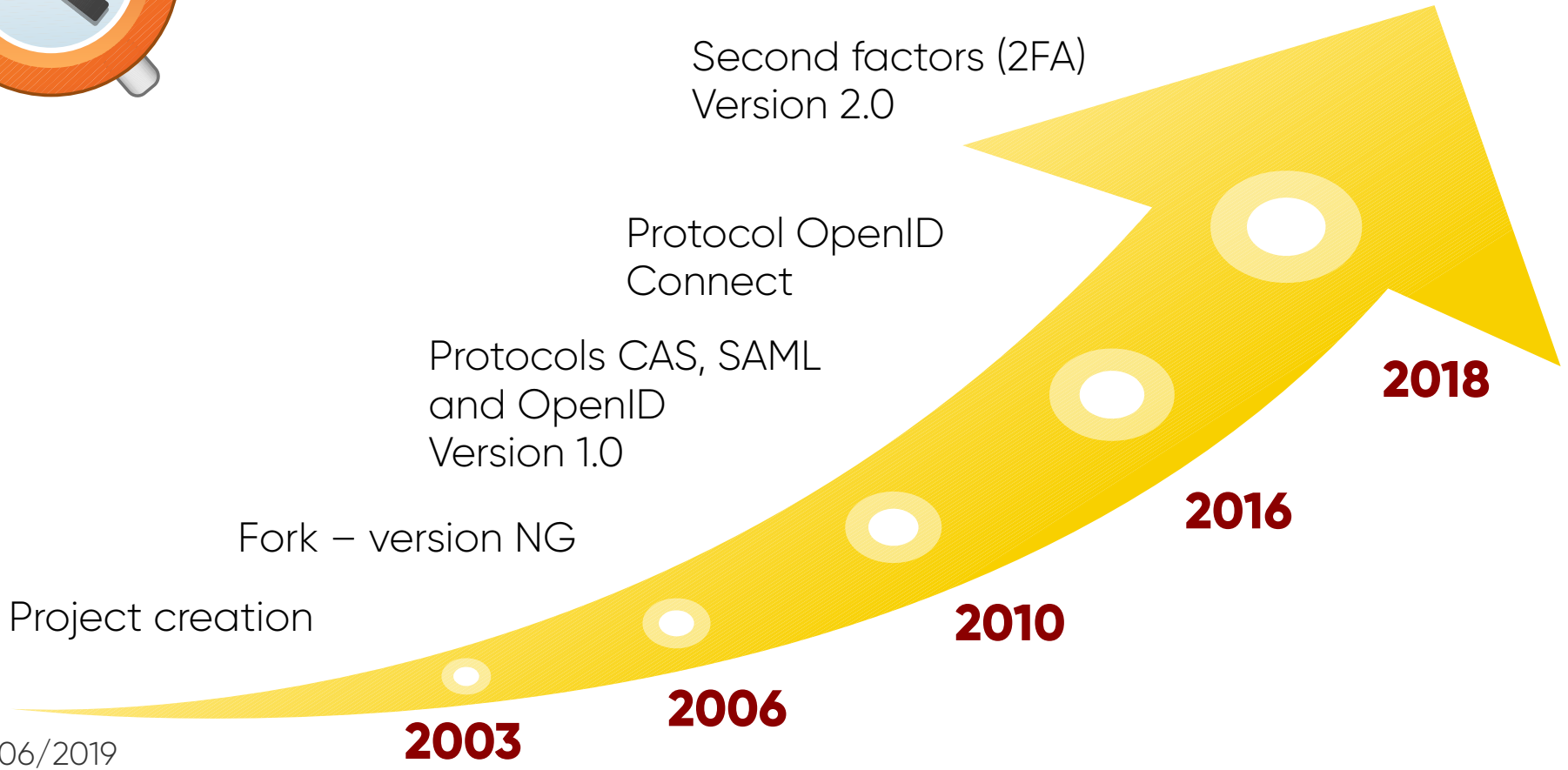
orange™

# LemonLDAP::NG Software

# SSO Workflow



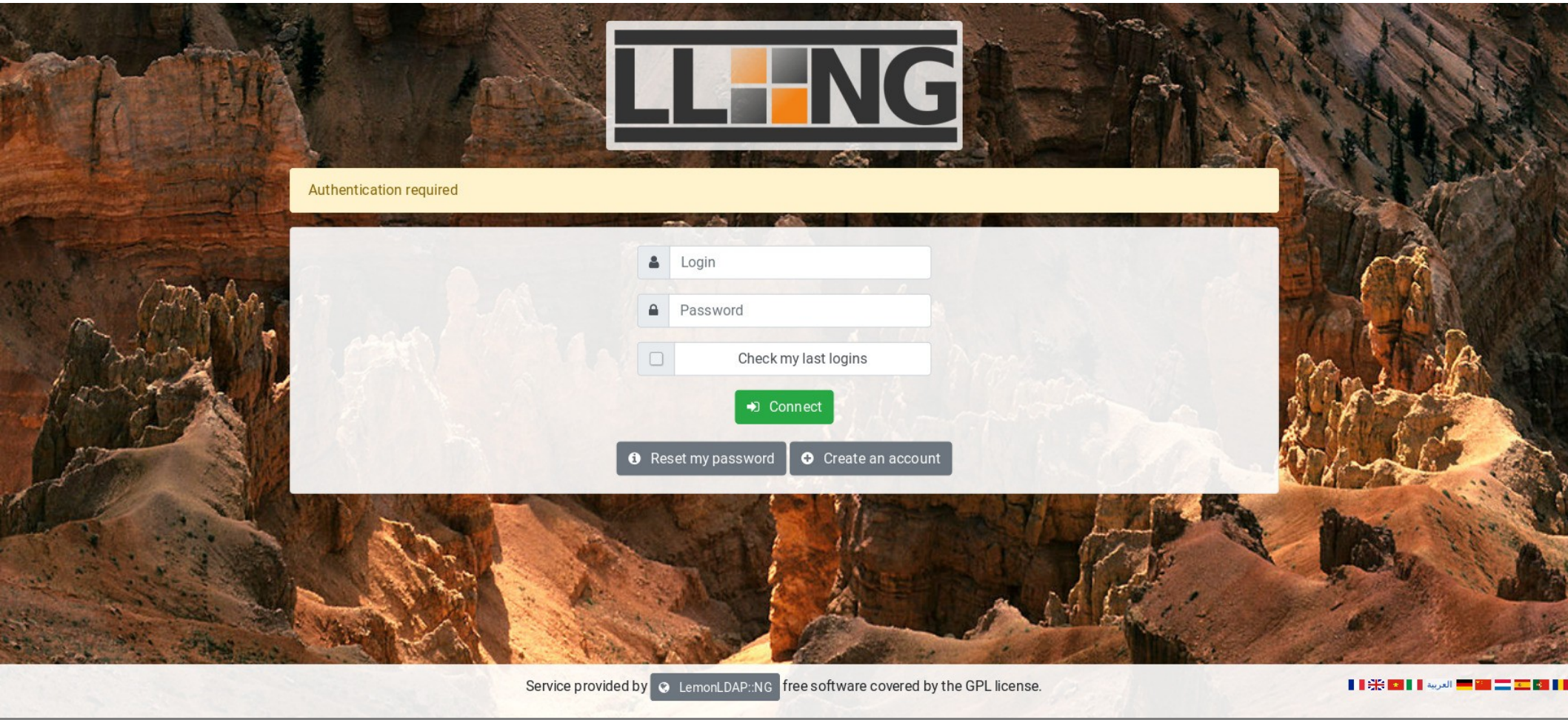
# History


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

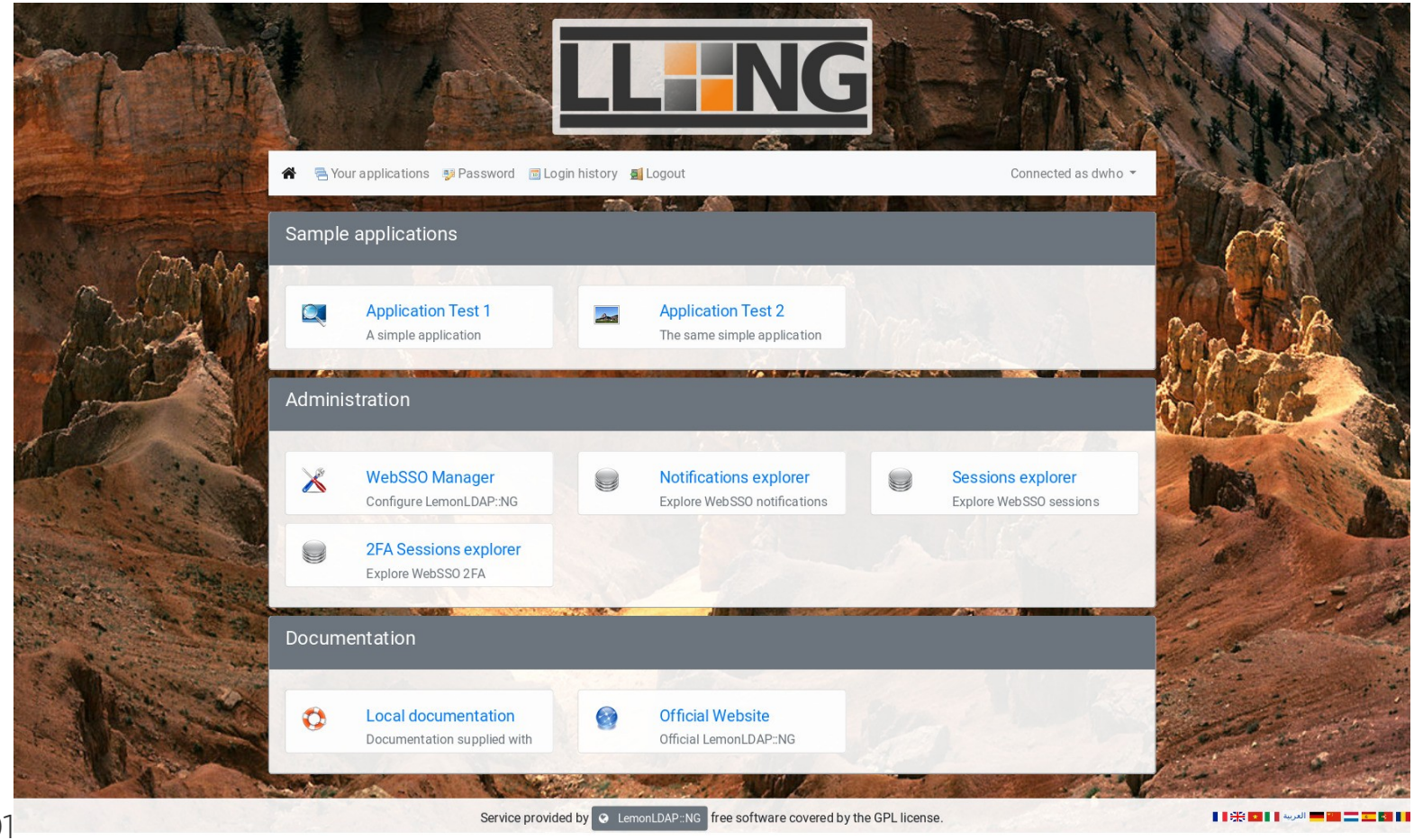
# Main features

- Web Single Sign On
- Access control
- Applications portal
- Authentication modules choice and chain
- Password management, account creation
- Multi-factor authentication (MFA)
- Protection of Web applications and API/WebServices
- Graphical customisation
- Packages for Debian/Ubuntu/RHEL/CentOS

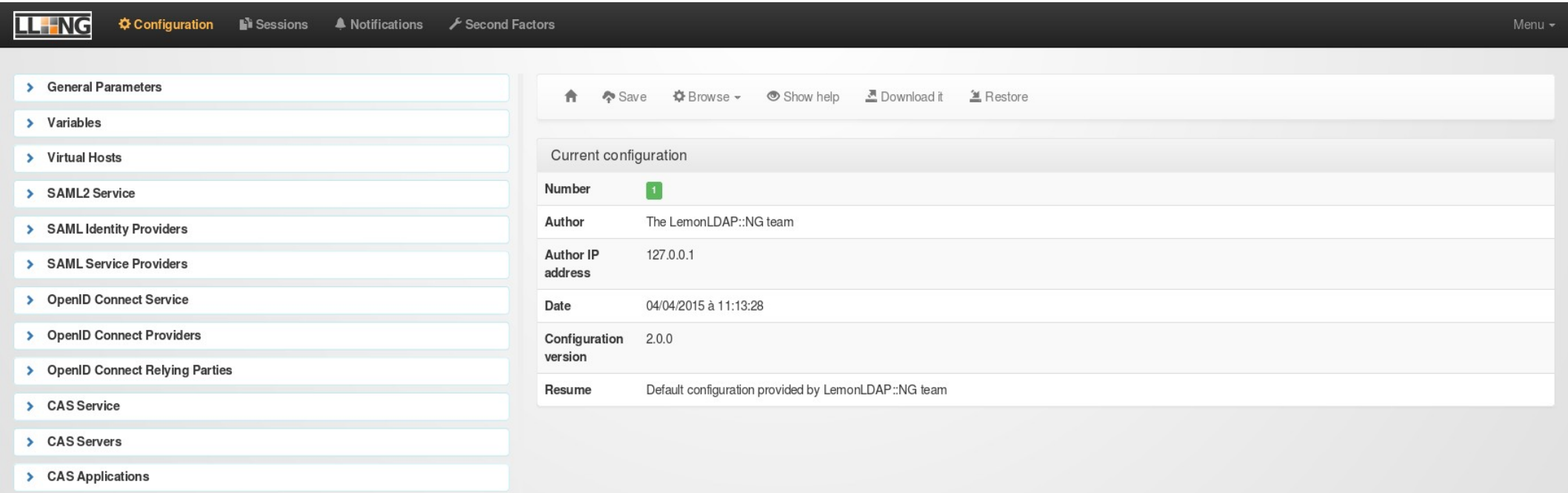
# Login page


LL NG
Authentication required
Login
Password
Check my last logins
Connect
Reset my password
Create an account
Service provided by LemonLDAP::NG free software covered by the GPL license.

# Portal with application menu



# Web 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

Portal

Application menu

CAS
SAML
OpenID Connect

Self Services

SOAP/REST server

Session management

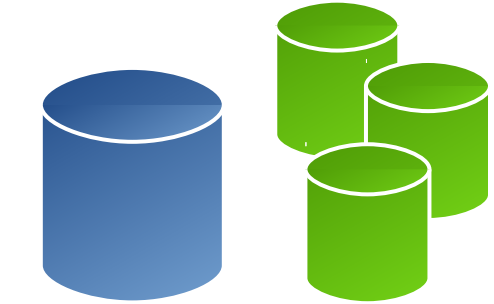
Manager

Configurations

Sessions

Notifications

Second factors



Configurations

Sessions

Handler

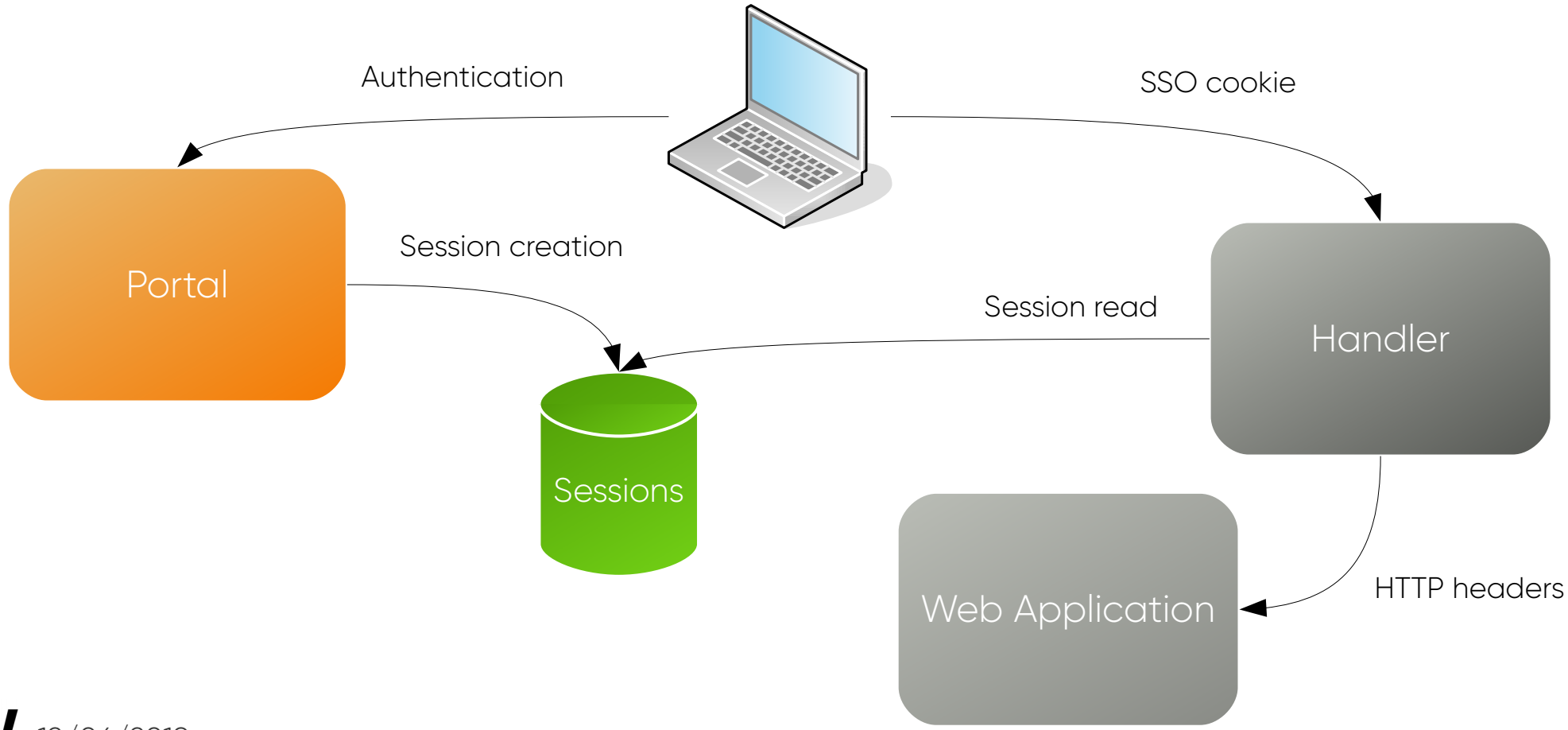
Access Control

SSOaaS

Web Service Token

Custom

# Web application



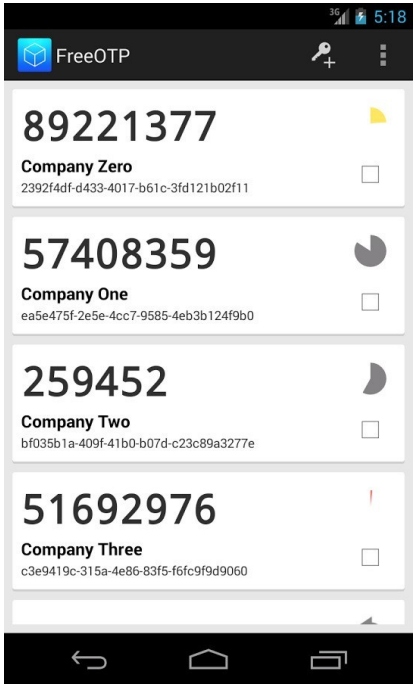
# CAS, SAML and OpenID Connect

- LL::NG can act as client and as server
- Attributes sharing
- Manage authentication contexts and levels
- Autogeneration of public/private keys
- Access control per services
- Publication of configuration data (metadata)
- Multi-protocols gateway
- Single logout



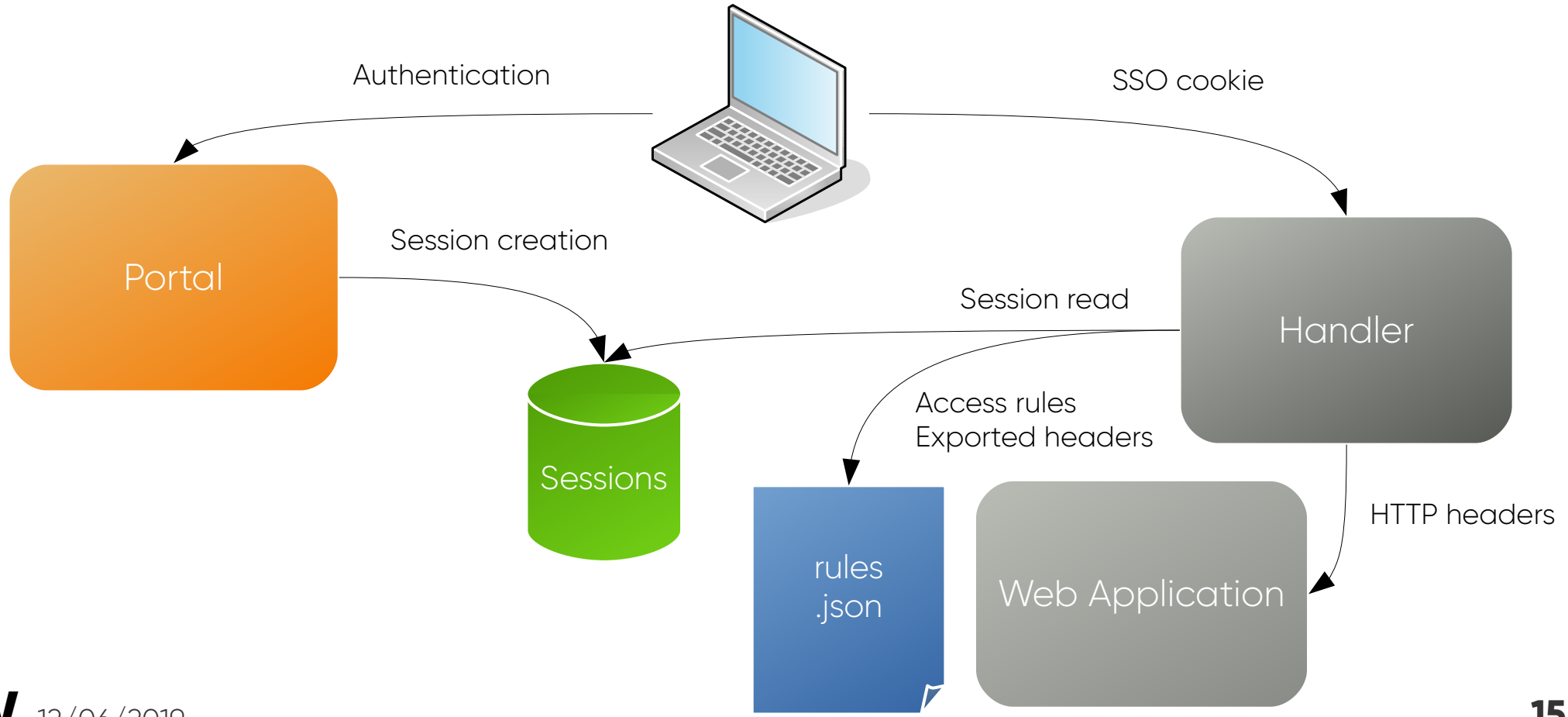
# Second Factor Authentication (2FA)

- LemonLDAP::NG can use the following 2FA:
  - TOTP
  - U2F
  - TOTP or U2F
  - Mail
  - External
  - REST
  - Yubikey

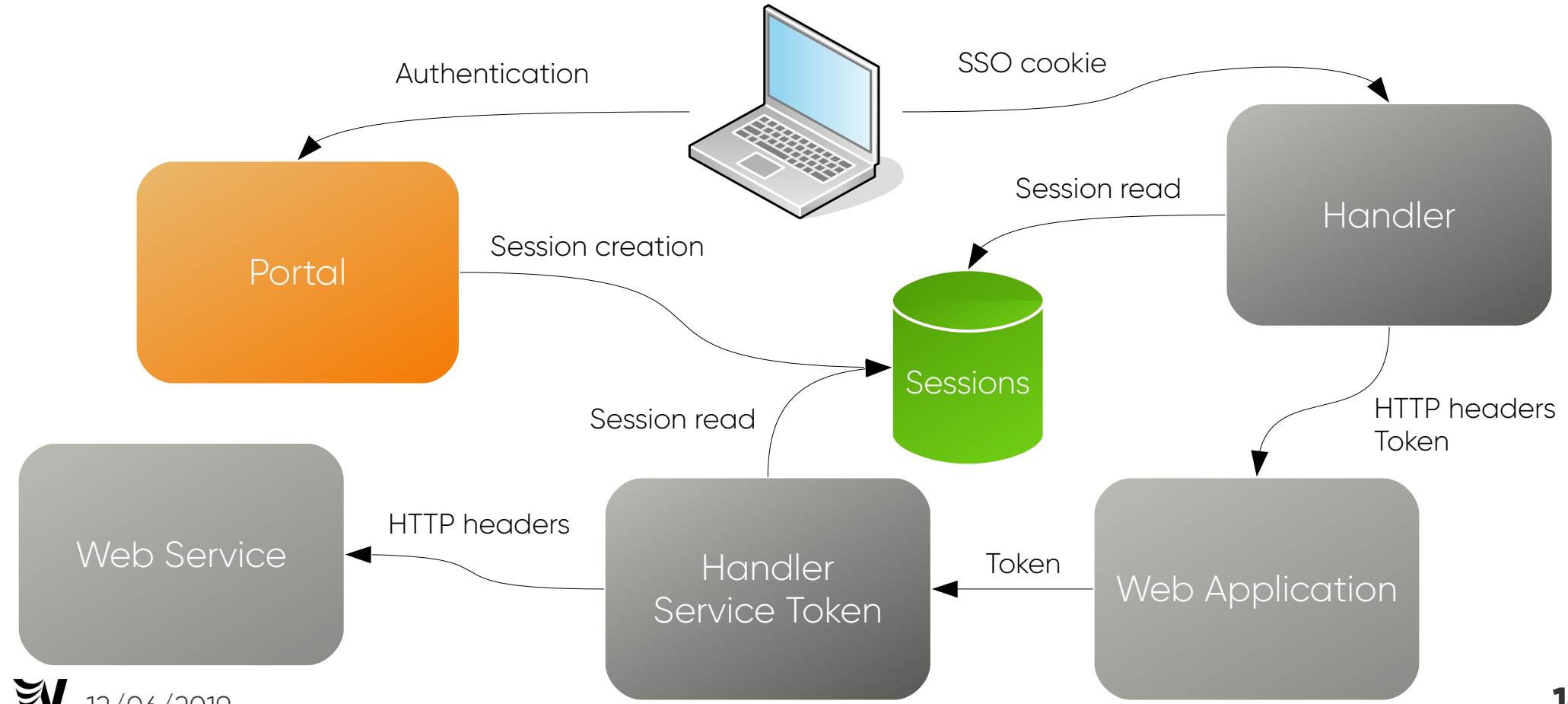



fido ALLIANCE

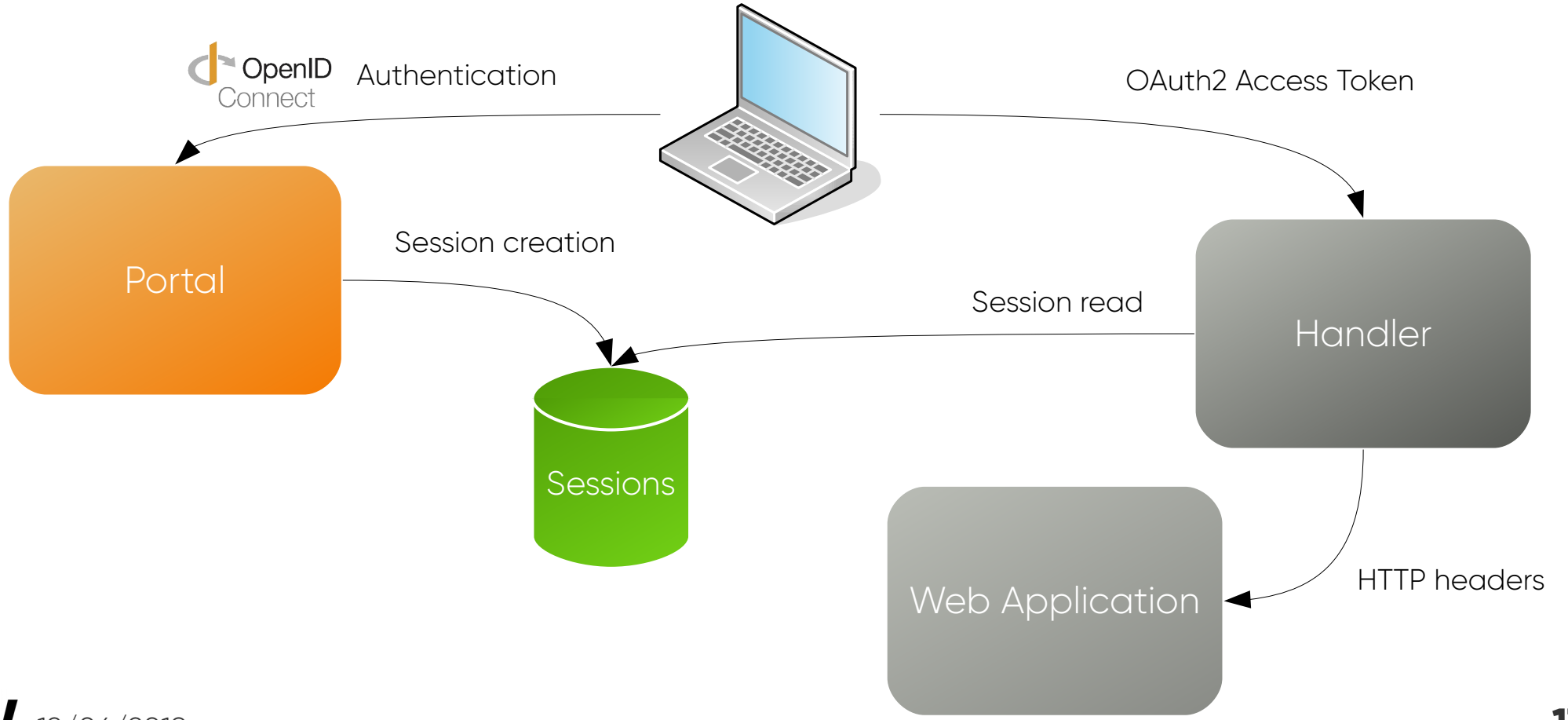
# DevOps (SSO as a Service)



# API – Service Token



# OpenID Connect / OAuth2



# 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

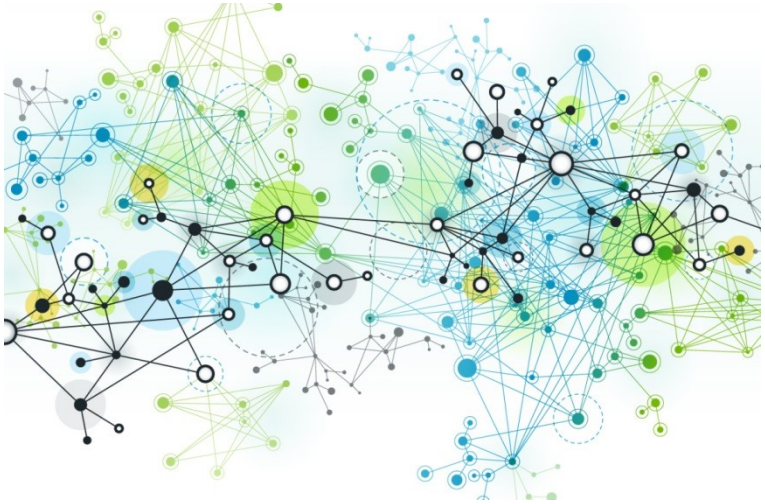
- Portal code was fully rewritten, and it now allows to write plugins
- Plugin examples, provided by default:
  - Auto Signin: direct authentication for some IP
  - Brute Force: protect against brute-force attacks
  - Stay Connected: "remember me" button
  - Public Pages: create static pages using portal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


# The beginning of the journey

# Orange is a complex environment…

***With many people and kind of skills***


***With thousands applications***



***In a full motion environment***

# Orange is a complex environment in complex world…

***With many people and kind of skills***

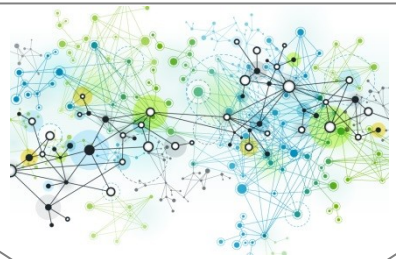

**Long time parthnerships**

- § Orange people
- § Contractors
- § Partners
- § Universities

**On demand relationships**

- § Freelances with few days contracts

***With thousands applications***

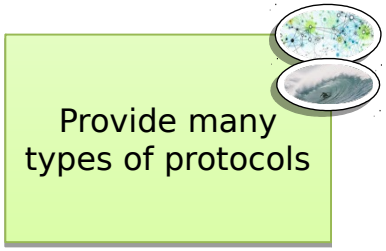


- § Orange made or bought.
- § Including SSO compatibility or not.
- § Accessible from Internet or Intranet.
- § Security access level specific for each.
- § Each application has its own livecyle.

***In a full motion environment***

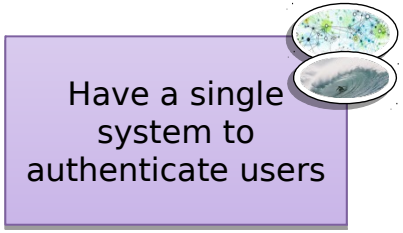
- § Our users want the same quality on work tools than on the personnal offer on Internet.
- § Rise of « fashion tool ».

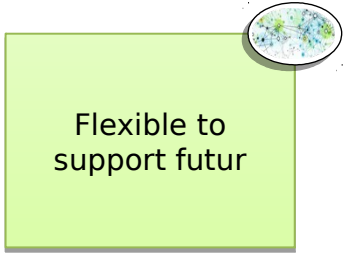
# …With the constraints and needs than others…

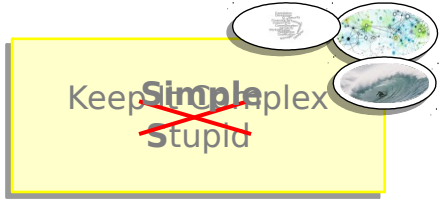




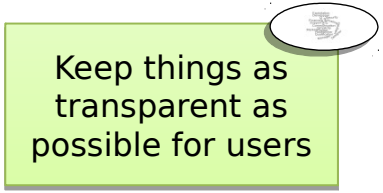


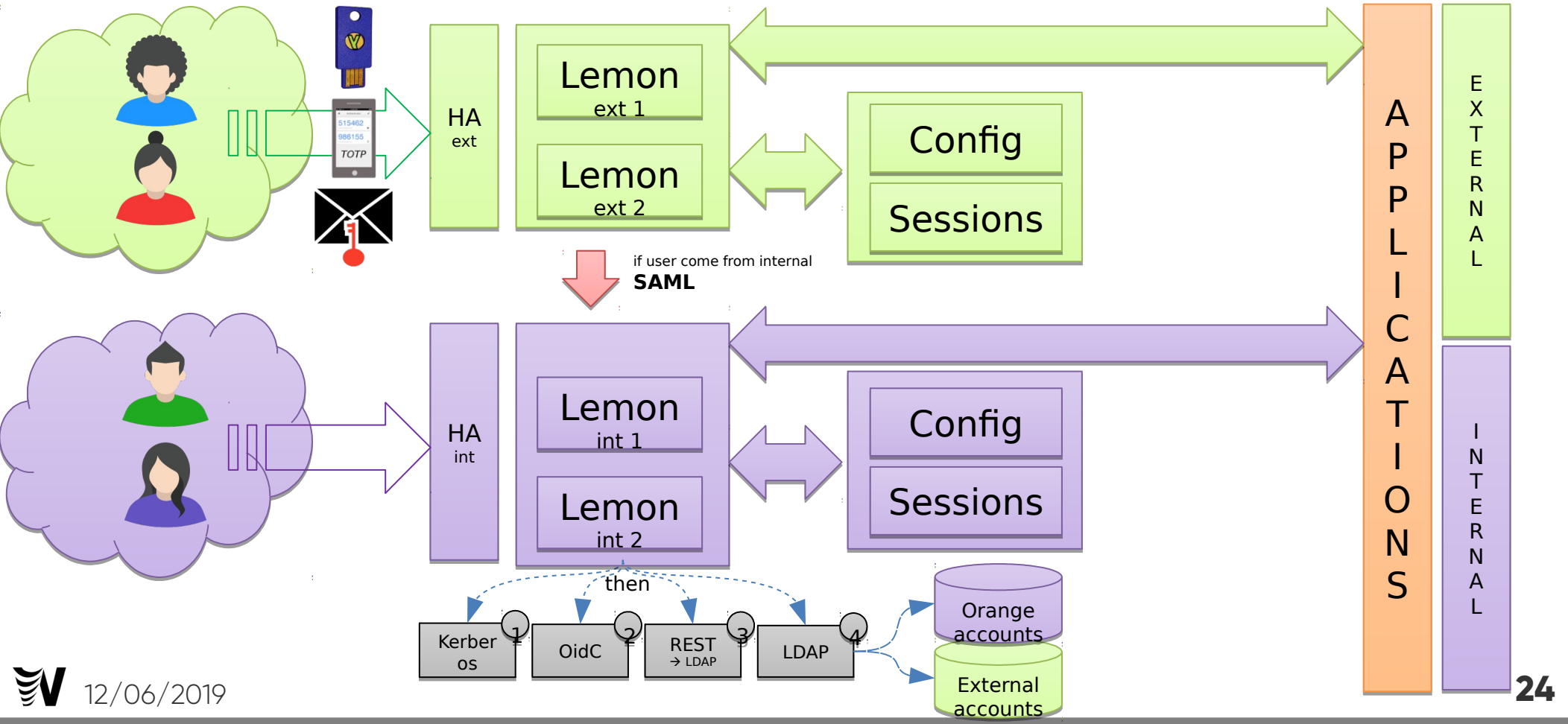







# ...So we are building a scalable LemonLDAP::NG infrastructure...



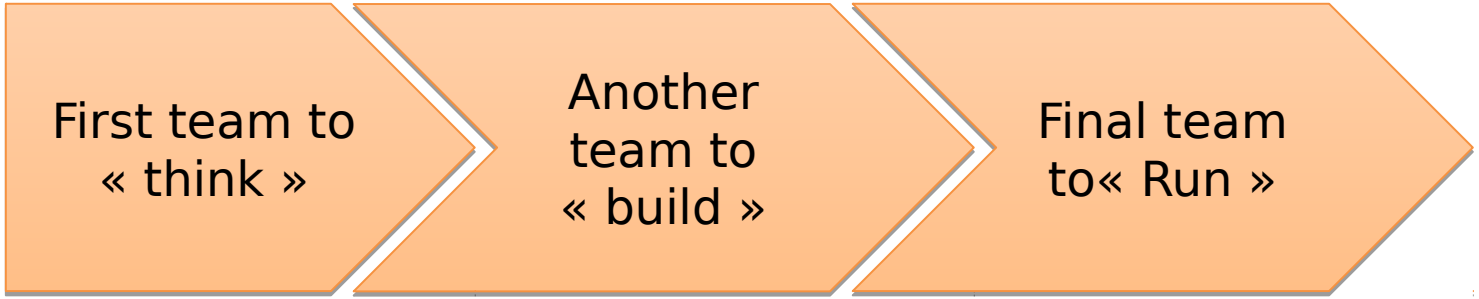
# ...And we are at the beginning of the journey...

We have tested LemonLdap in real conditions on many applications used by innovation people:





# …Under industrialisation by a specialized team.




- Test LemonLdap and try to get its limits
- Test the potential architectures
- Test intégration with about 20 applications (gitlab, nextcloud, jira & confluence, Dokuwiki, Apache 2, Flexible Engine, Grafana, WebCom, WordPress, OpenStack…).
- Test authentication protocols and ways (OTP, …)

- Get the results of the previous level to create an « industrial solution » able to support millions people.

# Orange-Worteks Partnership

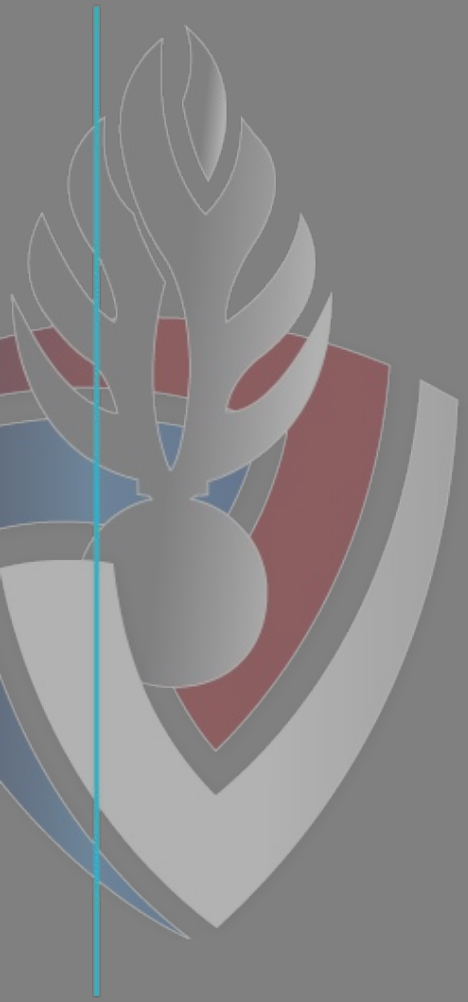
- Worteks offers a framework contract for support around LemonLDAP::NG and other free softwares, with two parts:
  - Incident management: a ticket can be opened to solve any fault on a production or development system (business hours)
  - Evolutions: a request can be done to fix bugs or code new features in the software
- Any Orange Business Unit can request a contract, prices are already defined
- It can then contribute to LemonLDAP::NG roadmap by requesting evolutions

# Thanks to all the contributors

Thank you to all the contributors to this project, for their competence, their good humor and their motivation that are overcoming all the problems that veinly tried to stand up against us:

- **The LemonLDAP::NG Team** (Clément, Xavier and all the others).
- **Worteks** for the support.
- **Orange internal contributors :** Christian P., Laurence T. , Daniel V., David M., Ronan H.B., Aurelien P., Alexandre L., Jean-Louis F.
- **All others** success keys in this project:





# Gendarmerie Nationale
# ST(SI)²

# History

- 2002: First WebSSO GN (SiteMinder)
- Licencing cost : 90 k€/year for 5000 users (target ~1 M€/year)

→ Take LemonLDAP over from the Ministry of finance

- 2005: Development of LL::NG (fork), SSO now used by (almost) all civil services

# Budget

- Project build (excluding machine cost) :
  - Between 2005 and 2015: ~ 150 k€
  - 2015 :  100 K€
  - 2016 & 2017: 0 €
  - 2018 : 25 k€
  - 2019 : 0 €

# Technical team for all ST(SI)² SSO

- X. Guimard : Lead developer LL::NG
- S. Marcq : Project manager
- A. Rosier & C.Maudoux : developers and administrators

# Platforms

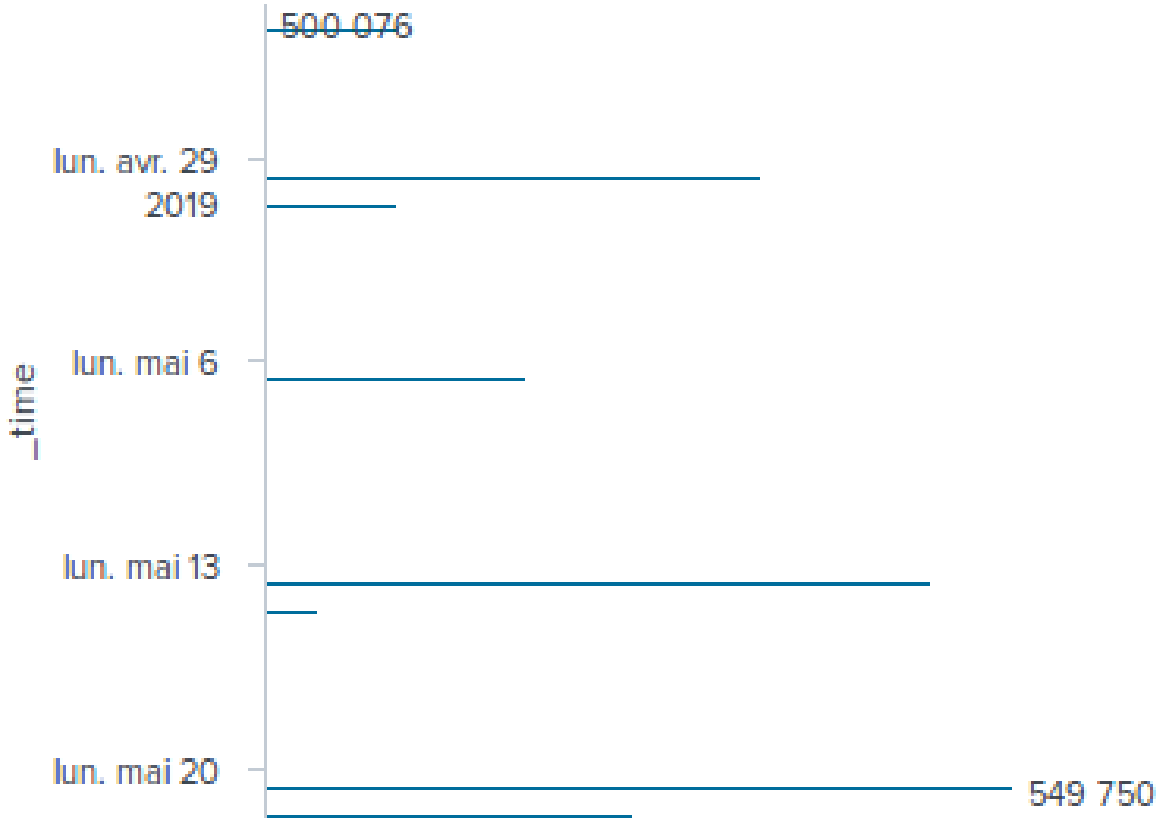
- Proxyma → GN
- CheopsNG → PN
- PSI → SP (SAML with interior security services)
- Judiweb → SP RIE (government network)
- Curasso & Espresso → internet SSO
- SAML with 12 civil services

# Proxyma : SSO GN

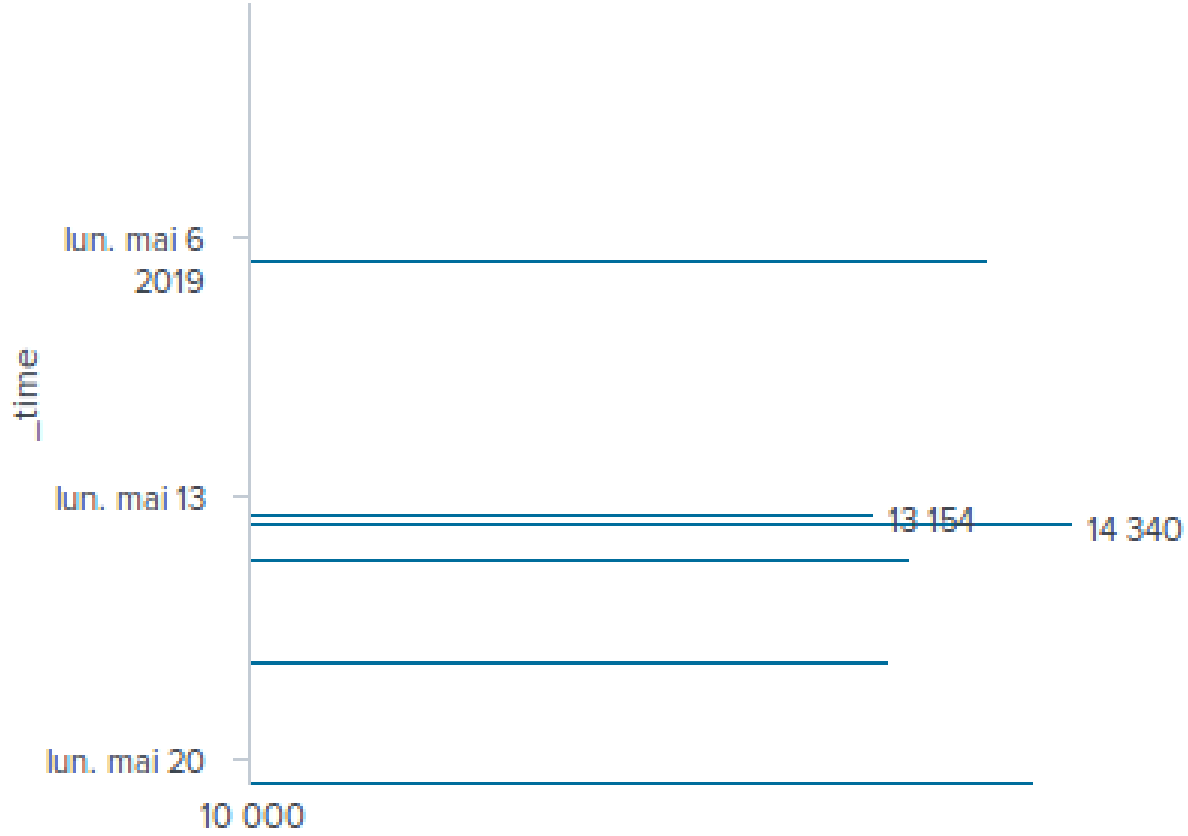
- ~ 22 millions requests / day
- ~ 65 000 unique users / day
- 253 different applications used / day
- 12 reverse proxies
- 7 LDAP servers
- 4 portals

# Top 10 connection's peak during 10 min

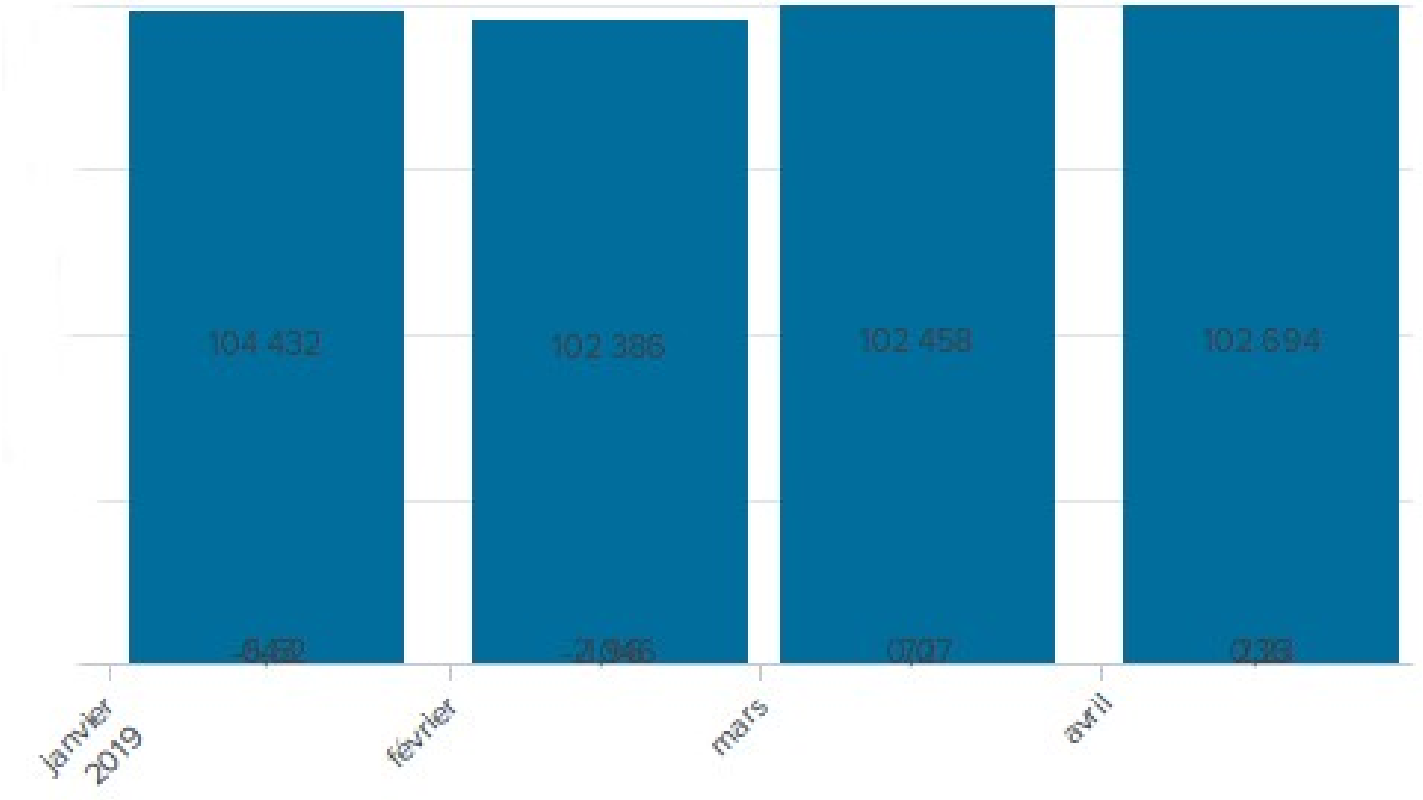
# Top 10 event's peak during 10 min



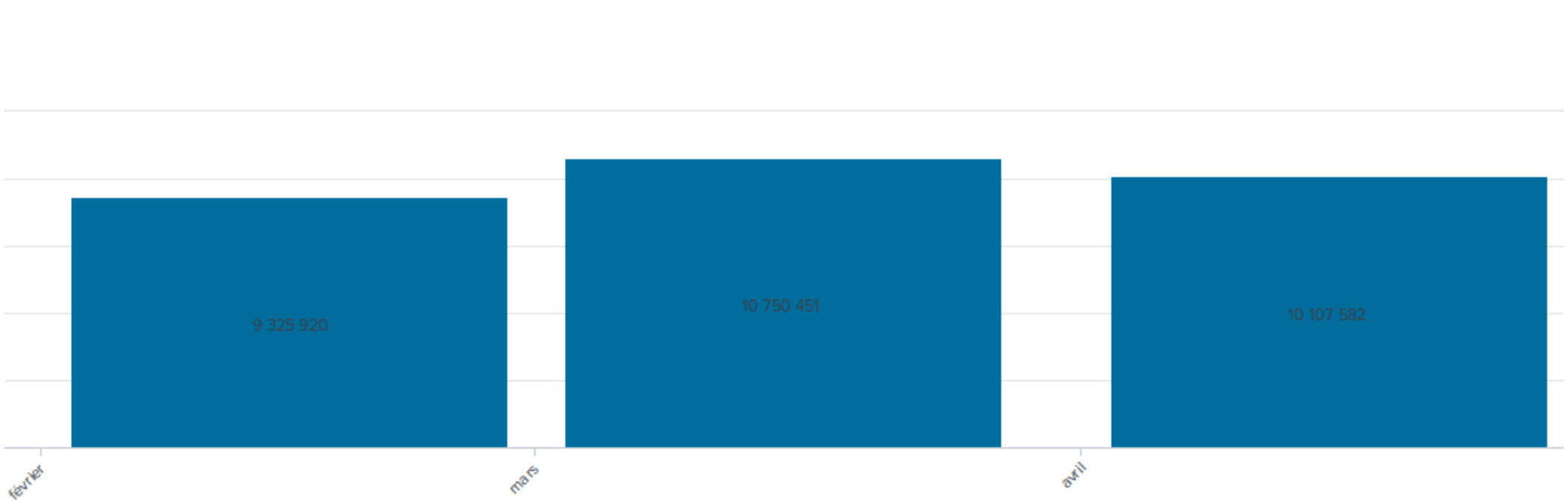
# Top 10 unique user's peak during 10 min



# Unique users / month



# « good authentification » / month



# 2019/2020 Evolution

- Upgrade all platform → LL::NG 2.0
- Connect Agent implementation
- 2FA implementation
- Cloud : SSO as a service (handler devops + scalability)

worteks

*make IT work, make IT free*

# THANKS

**Pour plus d'informations :**

**info@worteks.com**

**@worteks_com**

**linkedin.com/company/worteks**