worteks

make IT work, make IT free

LEMONLDAP::NG 2.0

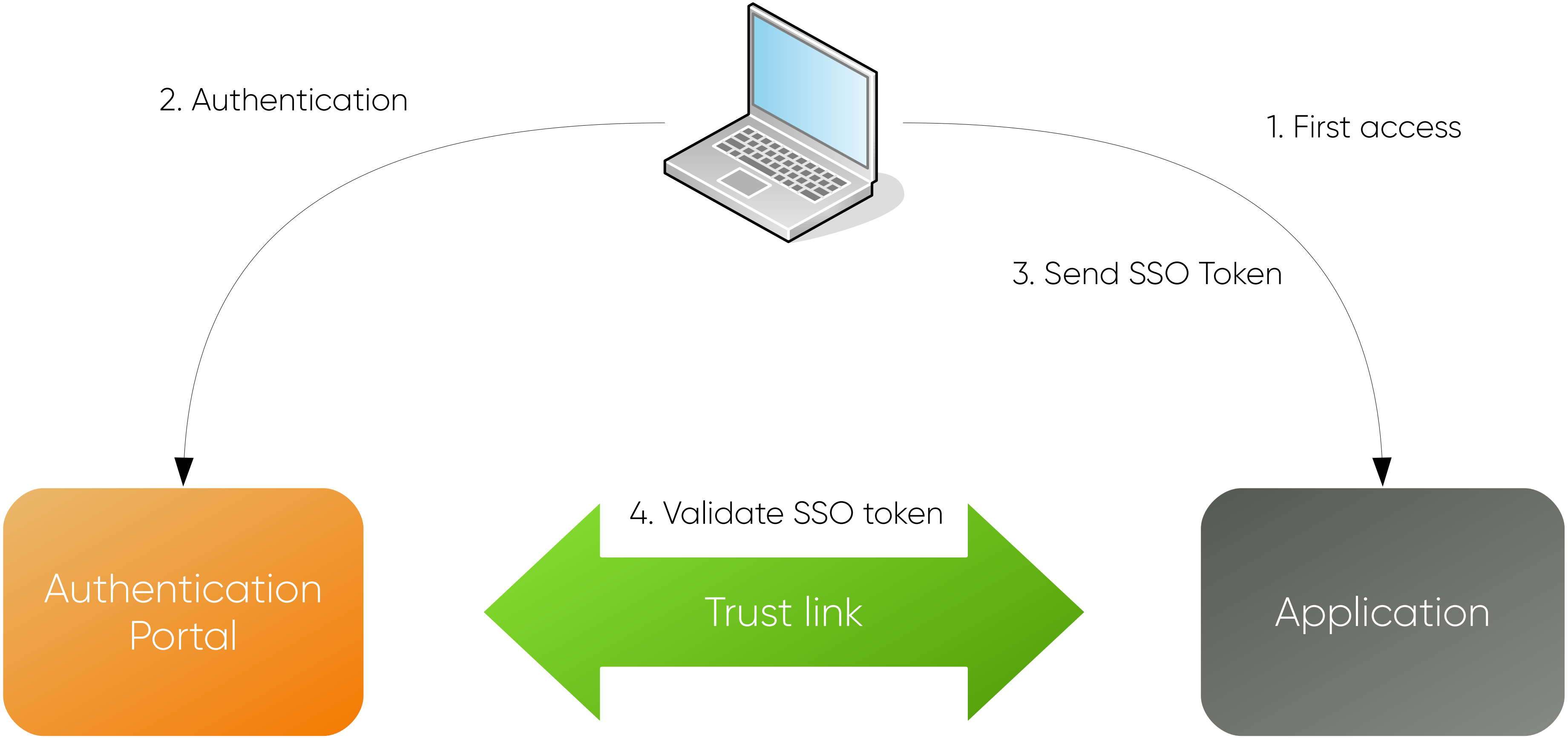
LL::NG

info@worteks.com

FOSDEM 2019

LemonLDAP::NG Software

SSO Workflow



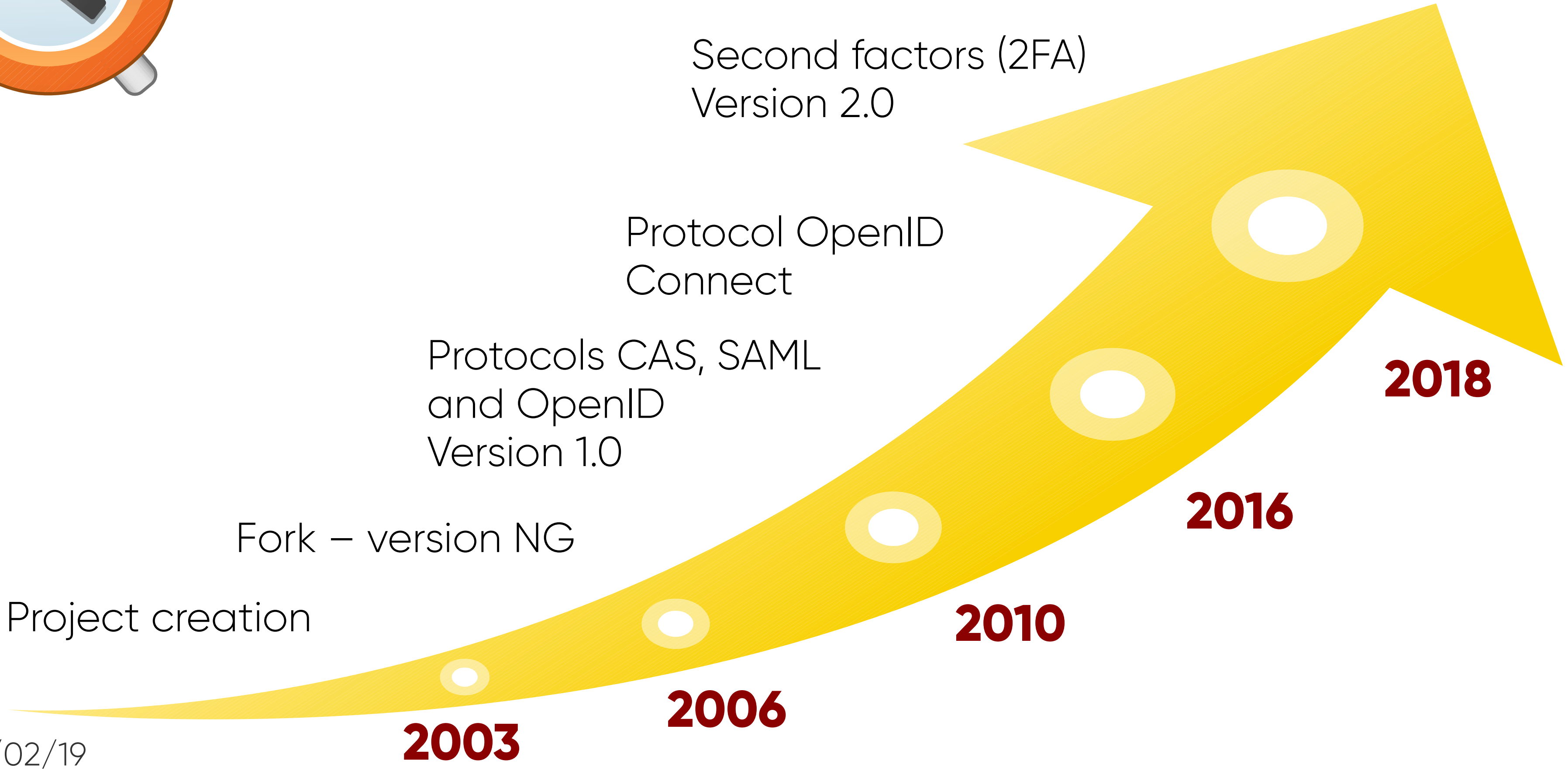
2. Authentication

1. First access

3. Send SSO Token

4. Validate SSO token

History



2003

Project creation

2006

Fork – version NG

2010

Protocols CAS, SAML
and OpenID
Version 1.0

2016

Protocol OpenID
Connect

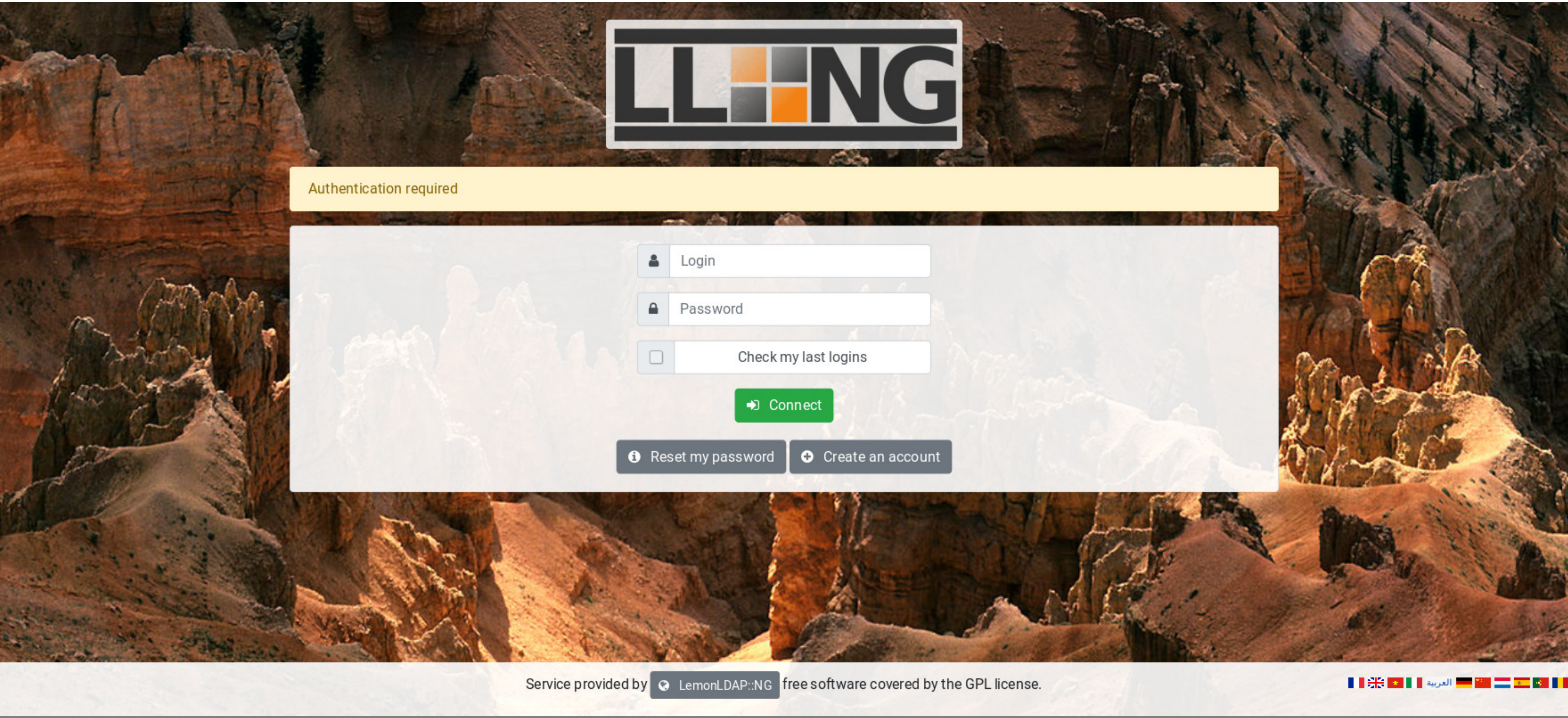
2018

Second factors (2FA)
Version 2.0

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

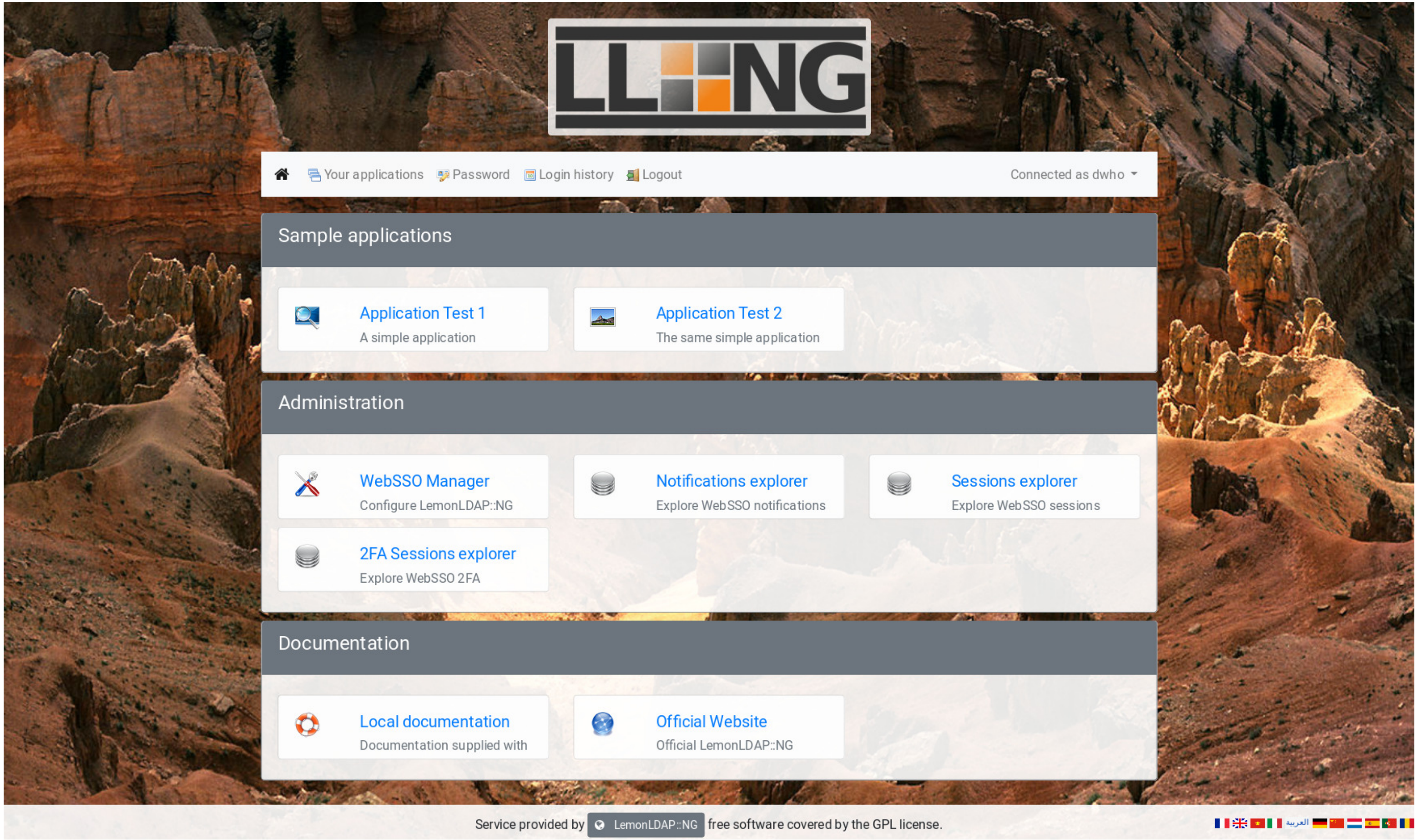
Login page



Authentication required

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

Portal with application menu



Your applications | Password | Login history | Logout | Connected as dwho

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

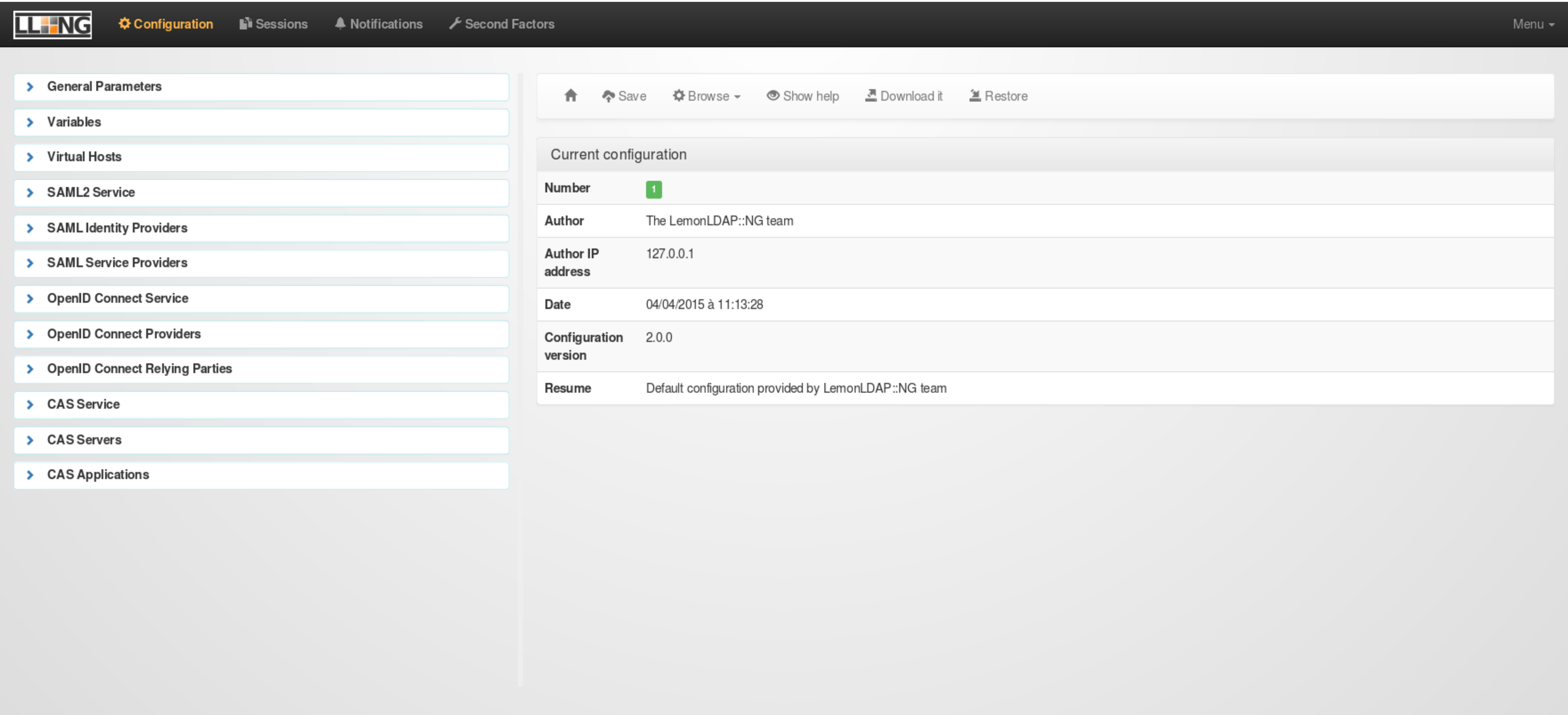
Documentation

Local documentation
Documentation supplied with

Official Website
Official LemonLDAP::NG

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

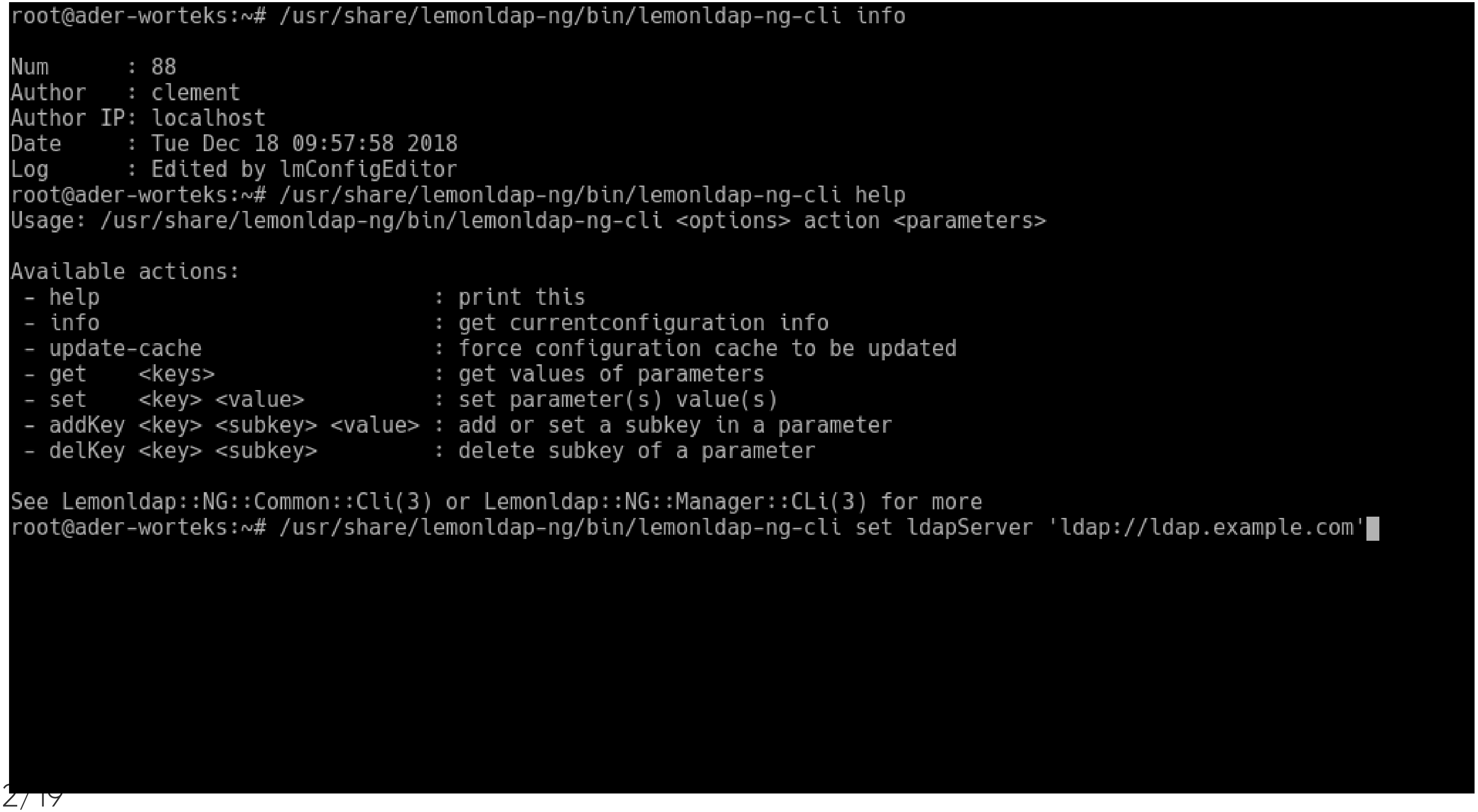
Web Administration interface



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

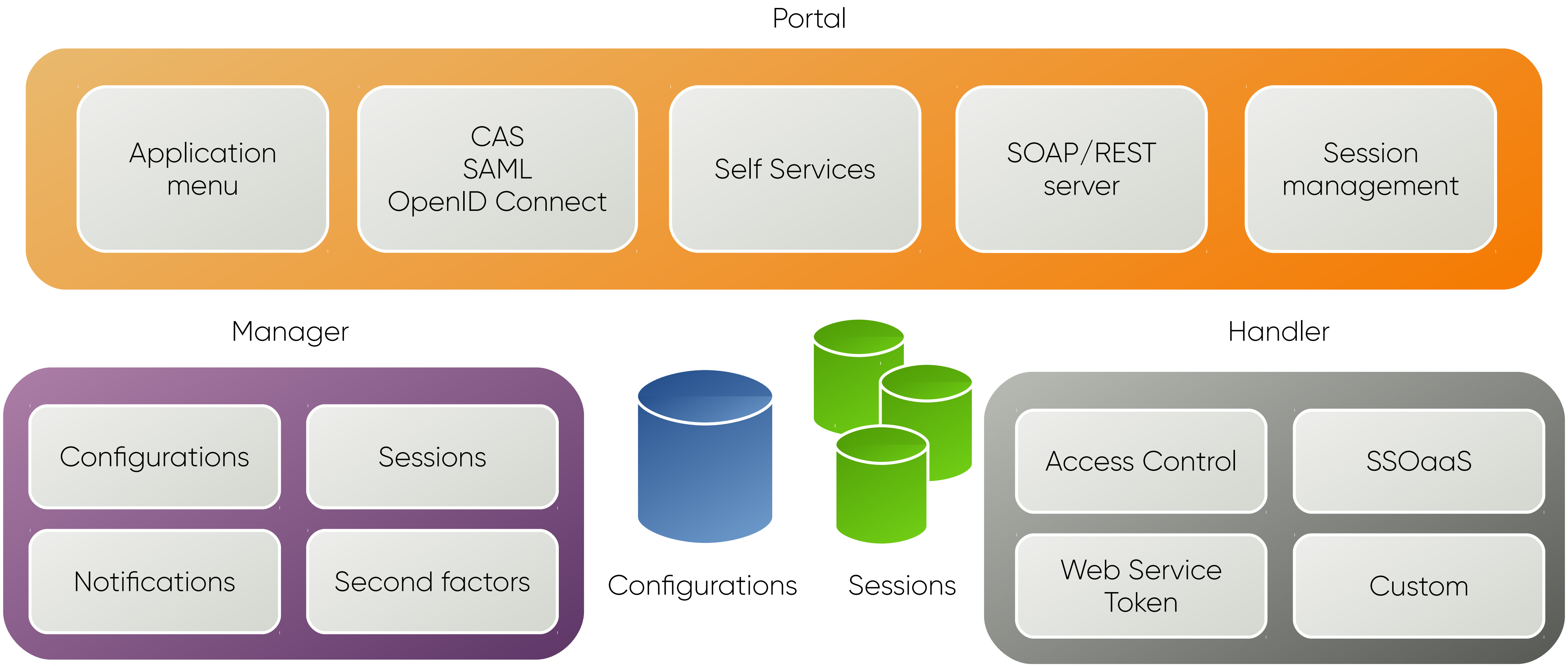


```
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

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

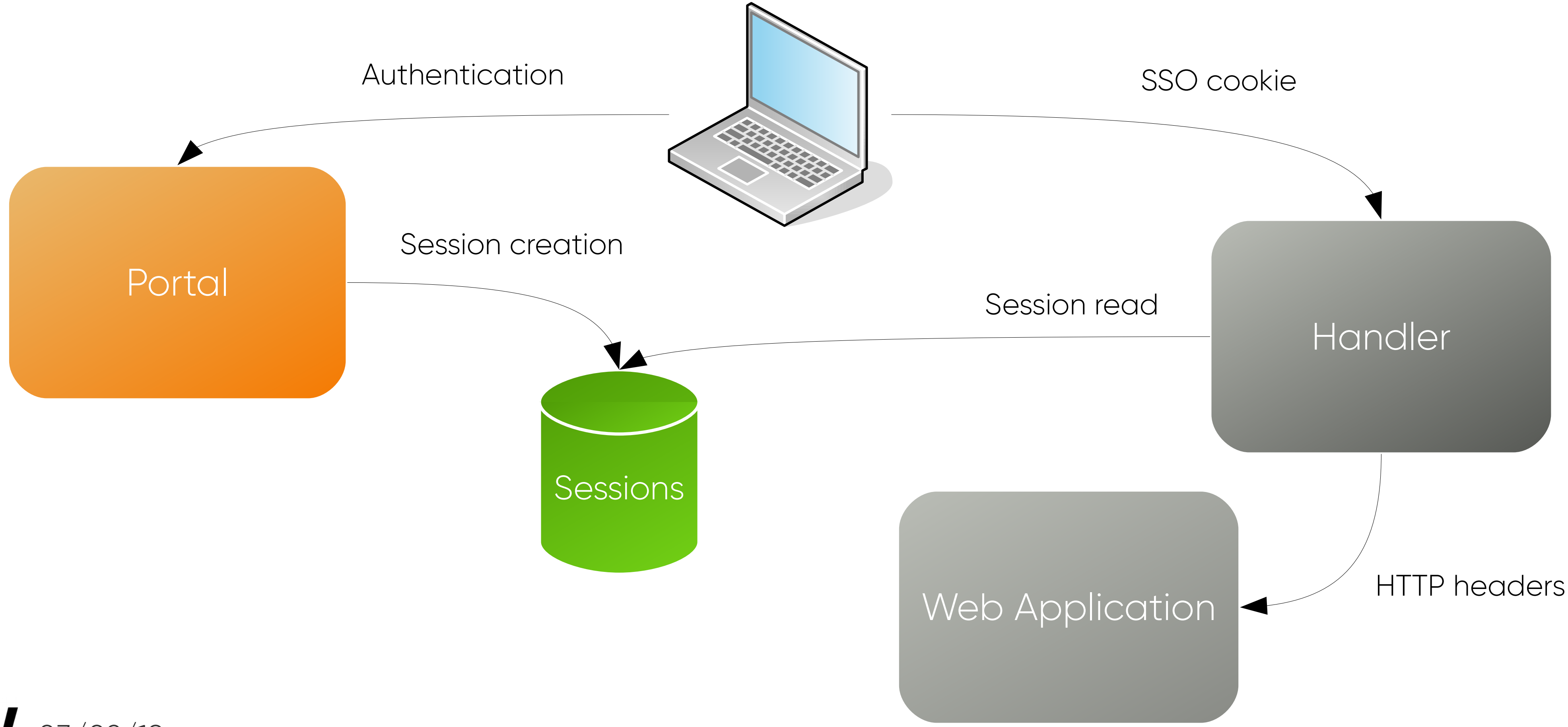
SSOaaS

Web Service Token

Custom

How works the agent (Handler)

Web application



Authentication

SSO cookie

Portal

Session creation

Session read

Handler

Sessions

Web Application

HTTP headers

03/02/19

Protocols CAS, SAML and OpenID Connect

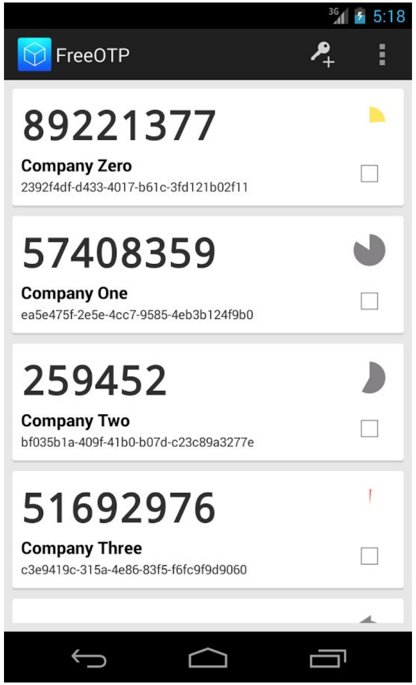
Main features

- 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

New in LemonLDAP::NG 2.0

Second Factor Authentication (2FA)

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



89221377
Company Zero □
2392f4df-d433-4017-b61c-3fd121b02f11

57408359
Company One □
ea5e475f-2e5e-4cc7-9585-4eb3b124f9b0

259452
Company Two □
bf035b1a-409f-41b0-b07d-c23c89a3277e

51692976
Company Three □
c3e9419c-315a-4e86-83f5-f6fc9f9d9060

Configuration backends

- Already existing backends:
  - JSON file
  - Database
  - LDAP
  - NoSQL (MongoDB)
  - SOAP
- New backends:
  - YAML file
  - REST
  - Local (no backend, only lemonldap-ng.ini file)

NodeJS Handler

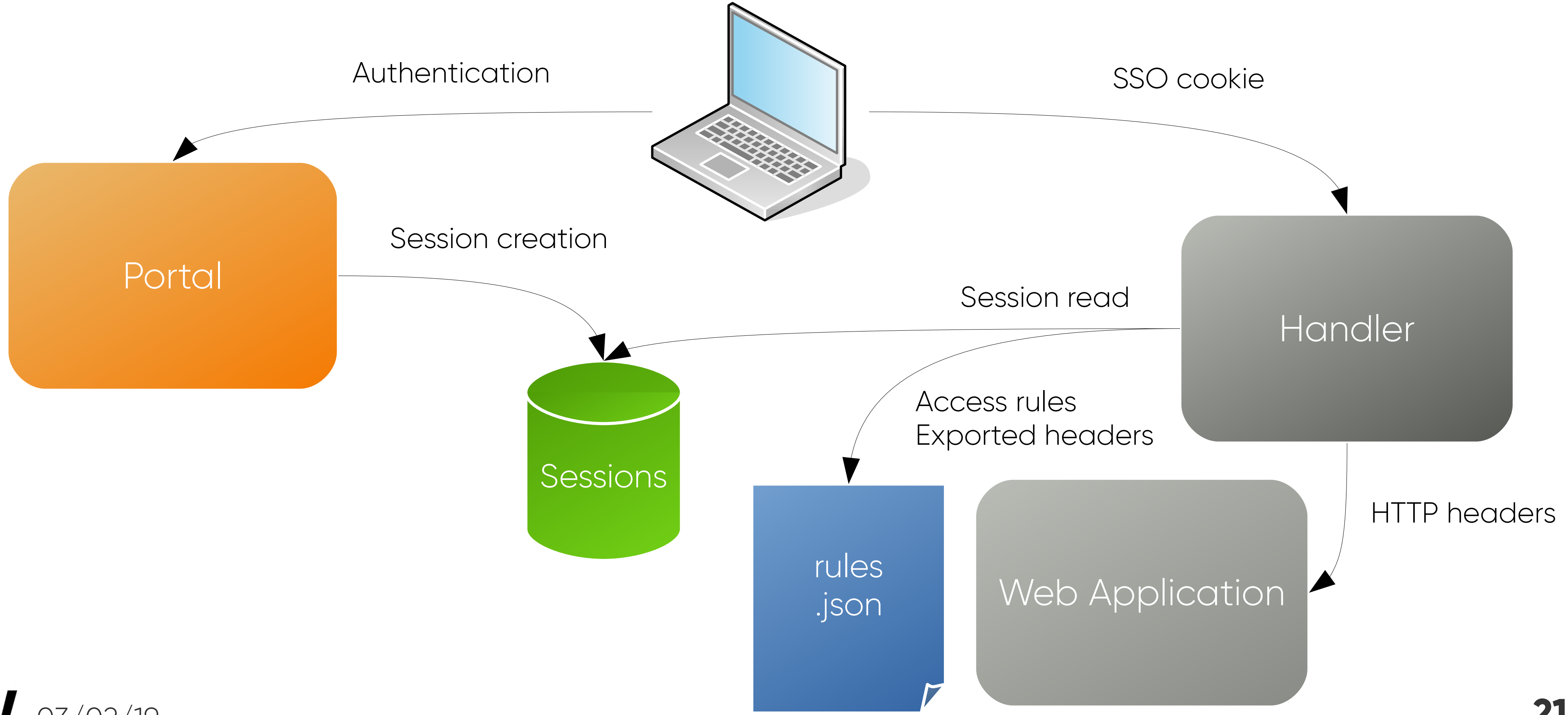
- Native integration in Express application
- Rules and headers configured in Javascript
- https://github.com/LemonLDAPNG/node-lemonldap-ng-handler

```
npm install node-lemonldap-ng-handler
```

DevOps (SSO as a Service)

- Authentication managed by portal
- Access control and HTTP headers configuration set in a local JSON file
- Allow quick applications deployement without need to edit main SSO configuration

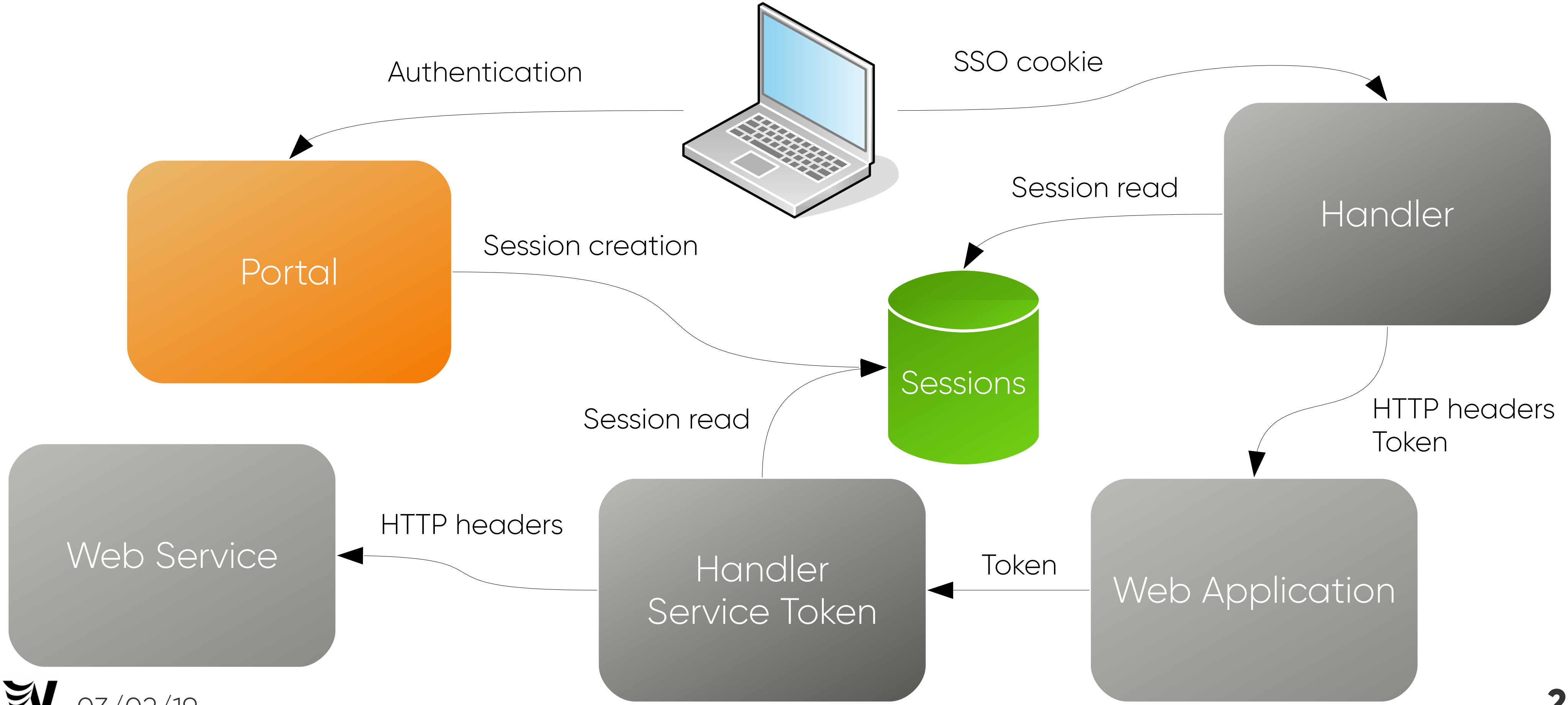
DevOps (SSO as a Service)



API / WebService protection

- New Handler "Service Token" installed between application and WebService
- Main Handler generates a token based on time session_id and virtual hosts
- The token is sent by application to WebService
- The Handler "Service Token" intercepts the token, validates it and apply access rules, and sent HTTP headers to WebService

API – Service Token



Authentification modules

- New modules:
  - PAM
  - REST
  - Kerberos (GSSAPI)
  - CAS (attributes reading)
- Multi is replaced by Combination
- Custom module

Administration interface

- Configurations comparator: differences between two configurations are displayed in a tree
- Second factors administration (search, revoke)
- Sort sessions by creation date or modification date

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

Other new features

- A user can refresh rights without disconnect/reconnect
- REST services for configurations and sessions
- Select language before authentication
- New graphical theme built with Bootstrap 4
- Logo customization (used in graphical theme and sent mails)
- Log system choice (syslog, Apache, Log4Perl, Sentry...)

worteks

make IT work, make IT free

THANKS

Pour plus d'informations :

✉ info@worteks.com

@worteks_com

in linkedin.com/company/worteks