Welcome to OW2con'23

Christophe Maudoux

Networks & Systems Engineer
PhD Student in Cybersecurity at Cnam Paris
Part-time Professor at Cnam & ESIEE Paris
LemonLDAP::NG WebSSO Maintainer

IAM infrastructure Architect
& SSO platforms Administrator

https://fr.linkedin.com/in/christophe-maudoux-iam

How to protect server2server(s) exchanges with LemonLDAP::NG WebSSO

Christophe Maudoux

June 8, 2023

Main dates & Features

- Created in 2004 by Gendarmerie nationale
- First stable version in 2010 → `Apache` only with `Mod_Perl`
- 1.4 in 2014 → Responsive Portal with `Bootstrap`
- 1.9 in 2016 → OIDC & `Nginx` support – `AngularJS` Manager
- 2.0.1 in 2018 → MFA & Plugins system
- 2.16.2 in 05/2023 → Last stable version (new MFA,...)
- 3.0 planned 2024 → `ReactJS` Manager & New plugins system

2014 & 2018 OW2 Community Award

christophe.maudoux
ST(SI)^2

- Xavier Guimard (Yadd) → creator
- Christophe Maudoux → maintainer

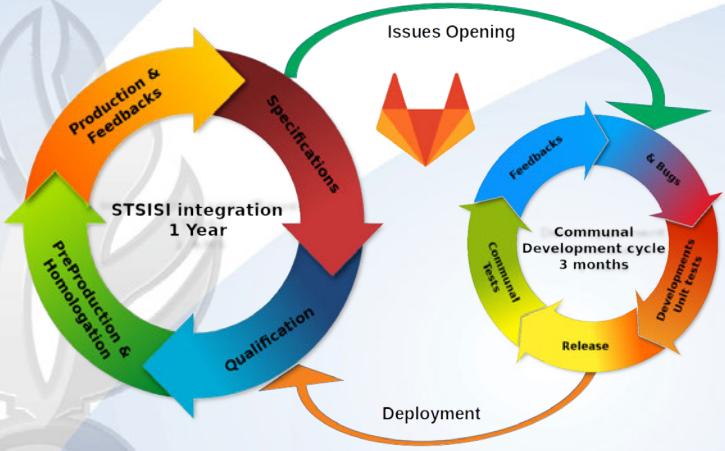
Win – Win partnership → Bugs fix & New features

- Clement Oudot (KPT) → project leader
- Maxime Besson → maintainer
- David Coutadeur → developper

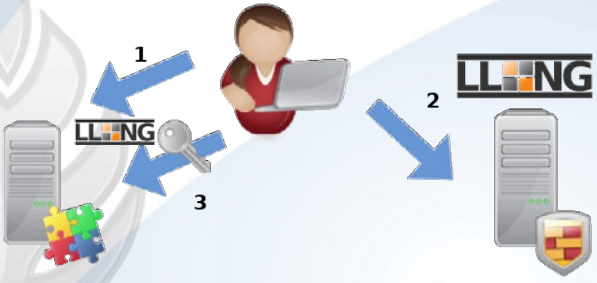
- Xavier Guimard (Yadd) → creator
- Christophe Maudoux → maintainer

Win – Win partnership → Bugs fix & New features

- Clement Oudot (KPT) → project leader
- Maxime Besson → maintainer
- David Coutadeur → developper



STSISI *Internal* validation cycle – OW2 *Internet* GitLab cycle

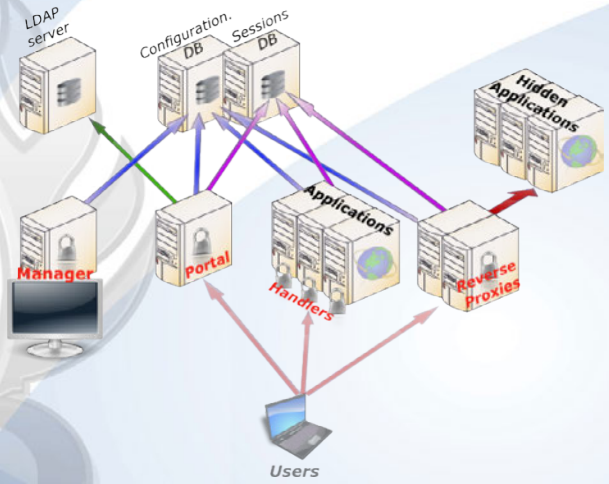


1. Not authenticated – Try to access to a protected app
2. Redirect by `LemonLDAP::NG` (Handler) to the Portal to log in
3. Portal provides a SSO token (cookie) &
   redirects user to original requested app. with a SSO cookie

christophe.maudoux
ST(SI)^2

Access Management & Platforms

LemonLDAP::NG architecture overview



- **Handler** can be embedded by applications themselves or by ReverseProxies

Access Management & Platforms

LemonLDAP::NG provides different handler types

Each handler looks for a specific token

Main	A *Cookie* header
AuthBasic	An *Authorization* "Basic XXXX" header
OAuth2	An *Authorization* "Bearer `AccessToken`" header
DevOps	A *rules.json* file to retrieve access rules & headers to sent to protected app
SecureToken	A *ciphered* cookie
ServiceToken	A *X-LLNG-TOKEN* header with the ServiceToken

- How to protect servers2servers(s) exchanges?

  ⇒ Three different ways can be employed...

- How to protect servers2servers(s) exchanges?
  ⇒ Three different ways can be employed...

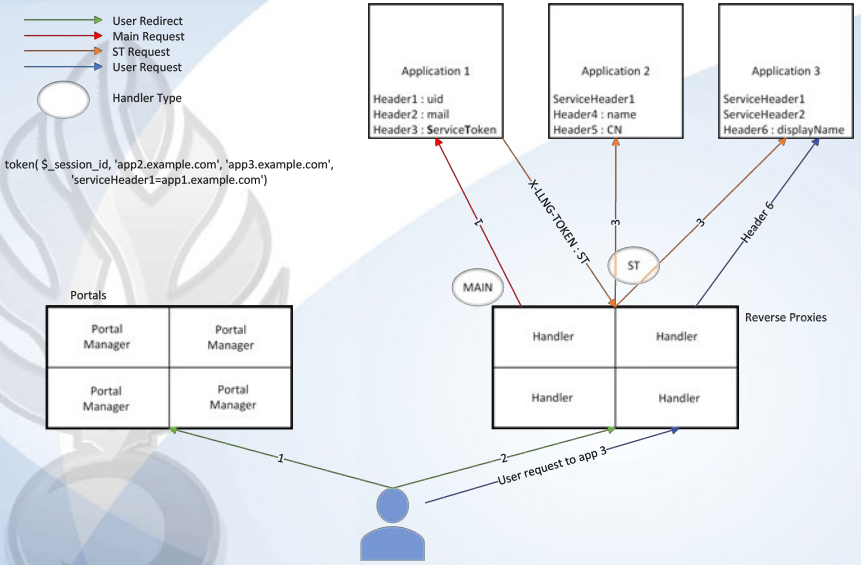
ServiceToken Handler

server2server(s) exchanges protection

The Bad	Provide the SSO cookie to protected app → security issue!!!
the Ugly	SecureToken handler → **deprecated**
The Good	The ServiceToken mechanism!!!

ServiceToken Handler

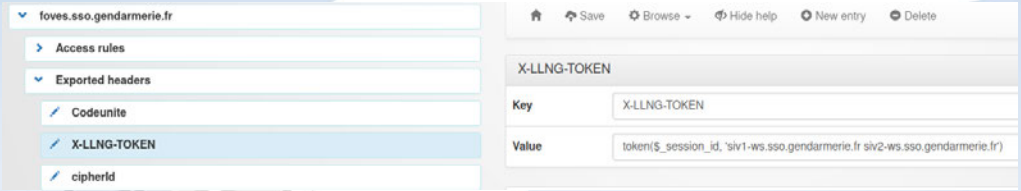
How it works?

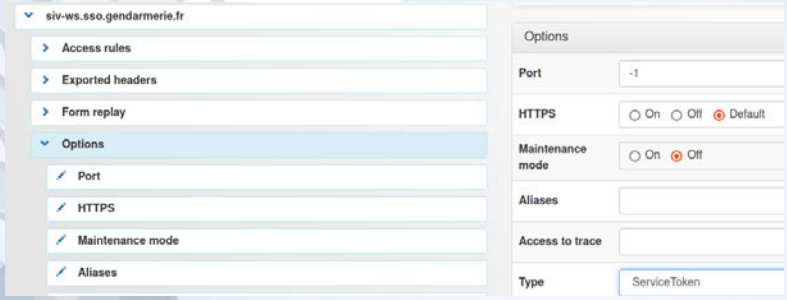


- *ServiceHeaders* can be used for tracking calling servers

ServiceToken Handler

Configuration



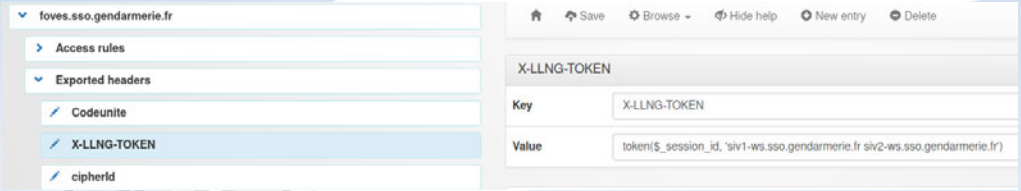


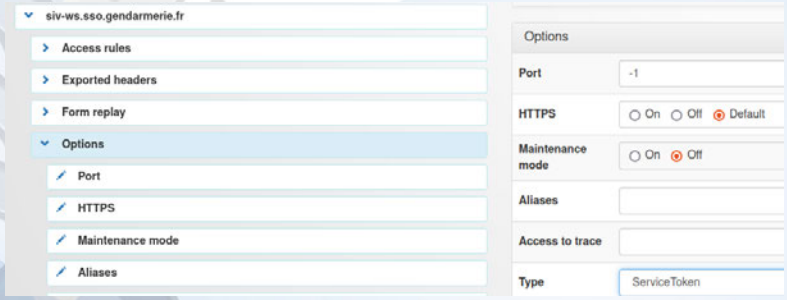
- *ServiceToken* hanlder **inherits** from *Main* handler

=> Applications protected by ST handler can be requested by servers & users... This is Magic!!!

ServiceToken Handler

Configuration





- *ServiceToken* hanlder **inherits** from *Main* handler

⇒ Applications protected by ST handler

can be requested by servers & users... This is Magic!!!

Thanks for your attention!

☺ Keep in touch... ☺

admin-sso@gendarmerie.interieur.gouv.fr
christophe.maudoux@gendarmerie.interieur.gouv.fr

Official Web Site ▶ https://lemonldap-ng.org
Repository ▶ https://gitlab.ow2.org/lemonldap-ng
Releases ▶ https://releases.ow2.org/lemonldap/