


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>



A large, stylized tree logo with a circular base and a trunk, rendered in a light blue and grey color. It is positioned on the left side of the slide, partially overlapping the title text.

HOW TO PROTECT SERVER2SERVER(S) EXCHANGES WITH LemonLDAP::NG WEBSSO

Christophe Maudoux

June 8, 2023



OPEN SOURCE WEBSO

AUTHENTICATION, AUTHORIZATION & ACCOUNTING



I. LEMONLDAP::NG

II. ACCESS MANAGEMENT & ARCHITECTURE

III. SERVICE TOKEN HANDLER





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





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



Win – Win partnership → Bugs fix & New features



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



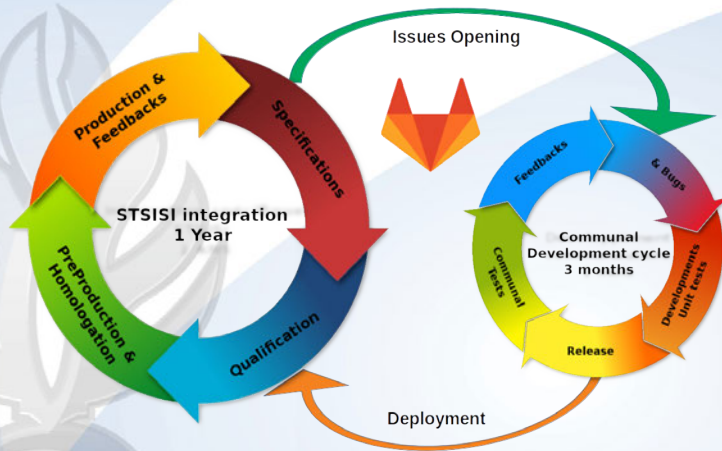
- Xavier Guimard (Yadd) → creator
- Christophe Maudoux → maintainer



Win – Win partnership → Bugs fix & New features



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



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

ACCESS MANAGEMENT & PLATFORMS

APPLICATION PROTECTION

CW2

server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

christophe.maudoux
ST(SI)²

LemonLDAP: :NG

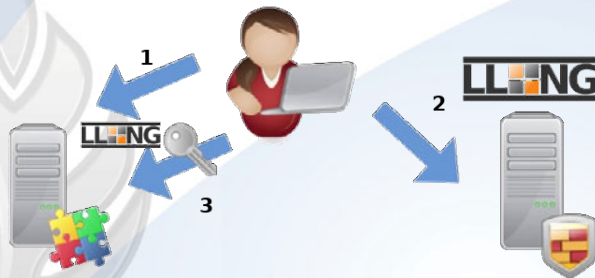
Access & Architecture

Application protection

Architecture

Handlers

ServiceToken Handler



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

LL::NG

ACCESS MANAGEMENT & PLATFORMS

LEMONLDAP::NG ARCHITECTURE OVERVIEW



server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

christophe.maudou
ST(SI)²

LemonLDAP::NG

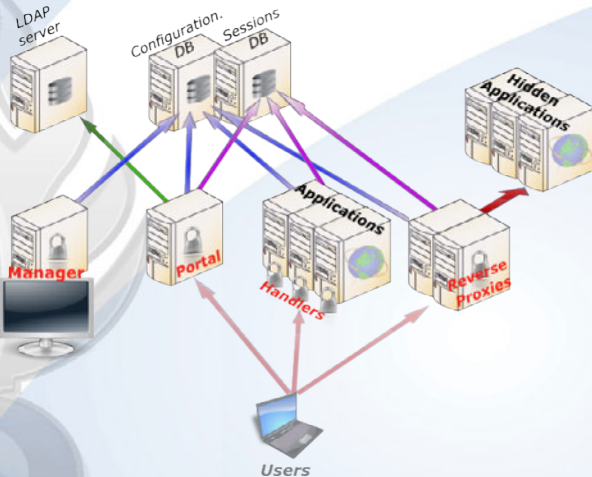
Access & Architecture

Application protection

Architecture

Handlers

ServiceToken Handler



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



ACCESS MANAGEMENT & PLATFORMS



server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

 christophe.maudoux
ST(SI)²

LemonLDAP::NG

Access & Architecture

Application protection

Architecture

Handlers

ServiceToken Handler



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 *ciphred* cookie
- SERVICETOKEN A *X-LLNG-TOKEN* header with the ServiceToken


SERVICETOKEN HANDLER

SERVER2SERVER(S) EXCHANGES PROTECTION



server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

 christophe.maudoux
ST(SI)²

LemonLDAP: :NG

Access & Architecture

ServiceToken Handler

s2s exchanges protection

How it works?

Configuration



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



SERVICE TOKEN HANDLER

SERVER2SERVER(S) EXCHANGES PROTECTION



server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

christophe.maudoux
ST(SI)²

LemonLDAP:::NG

Access & Architecture

ServiceToken Handler

s2s exchanges protection

How it works?

Configuration



THE BAD

Provide the SSO cookie to protected app → **security issue!!!**

THE UGLY

SecureToken handler → **deprecated**

THE GOOD

The ServiceToken mechanism!!!



SERVICE TOKEN HANDLER



HOW IT WORKS?

server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

christophe.maudoux
ST(SI)²

LemonLDAP:::NG

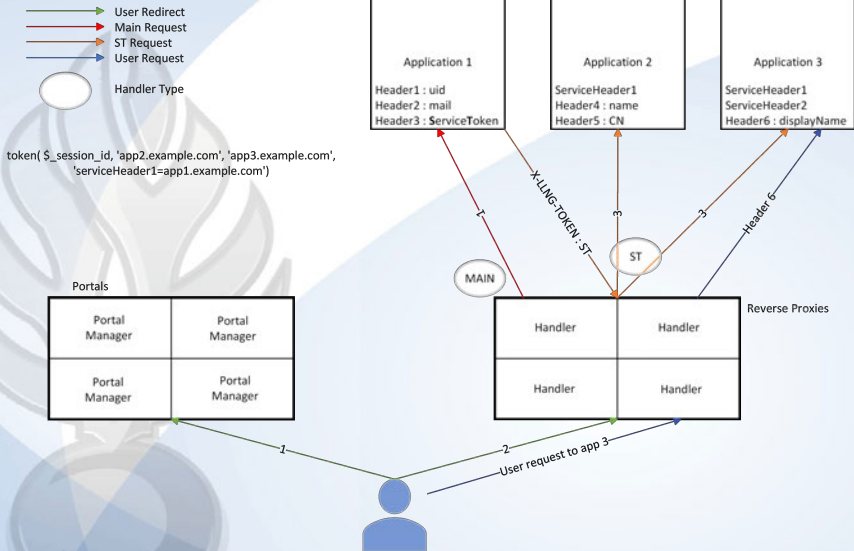
Access & Architecture

ServiceToken Handler

s2s exchanges protection

How it works?

Configuration



▶ ServiceHeaders can be used for tracking calling servers

SERVICETOKEN HANDLER

CONFIGURATION



server2servers
exchanges protection
with
▶ LL::NG ◀

2023/06

christophe.maudoux
ST(SI)²

LemonLDAP: : NG

Access & Architecture

ServiceToken Handler

s2s exchanges protection

How it works?

Configuration



foves.sso.gendarmerie.fr

- Access rules
- Exported headers
- Codeunite
- X-LLNG-TOKEN**
- cipherId

Home Save Browse Hide help New entry Delete

X-LLNG-TOKEN

Key X-LLNG-TOKEN

Value token(\$_session_id, 'siv1-ws.sso.gendarmerie.fr siv2-ws.sso.gendarmerie.fr')

siv-ws.sso.gendarmerie.fr

- Access rules
- Exported headers
- Form replay
- Options**
- Port
- HTTPS
- Maintenance mode
- Aliases

Options

Port -1

HTTPS On Off Default

Maintenance mode On Off

Aliases

Access to trace

Type ServiceToken

▶ *ServiceToken* handler **inherits** from *Main* handler
⇒ Applications protected by ST handler
can be requested by servers & users... This is Magic!!!

SERVICE TOKEN HANDLER

CONFIGURATION



server2servers
exchanges protection
with
▶ LL:NG ◀

2023/06

christophe.maudoux
ST(SI)²

LemonLDAP: : NG

Access & Architecture

ServiceToken Handler

s2s exchanges protection

How it works?

Configuration



foves.sso.gendarmerie.fr

- Access rules
- Exported headers
- Codeunite
- X-LLNG-TOKEN**
- cipherId

Save Browse Hide help New entry Delete

X-LLNG-TOKEN

Key X-LLNG-TOKEN

Value token(\$_session_id, 'siv1-ws.sso.gendarmerie.fr siv2-ws.sso.gendarmerie.fr')

siv-ws.sso.gendarmerie.fr

- Access rules
- Exported headers
- Form replay
- Options
 - Port
 - HTTPS
 - Maintenance mode
 - Aliases

Options

Port -1

HTTPS On Off Default

Maintenance mode On Off

Aliases

Access to trace

Type ServiceToken

▶ *ServiceToken* handler **inherits** from *Main* handler
⇒ Applications protected by ST handler
can be requested by servers & users... This is Magic!!!

THANKS FOR YOUR ATTENTION!

OW2

☺ KEEP IN TOUCH... ☺

admin-sso@gendarmerie.interieur.gouv.fr

christophe.maudoux@gendarmerie.interieur.gouv.fr

LLING

OFFICIAL WEB SITE ► <https://lemonldap-ng.org>

REPOSITORY ► <https://gitlab.ow2.org/lemonldap-ng>

RELEASES ► <https://releases.ow2.org/lemonldap/>

