




## Christophe Maudoux

- Docteur en informatique
- Ingénieur réseaux & systèmes
- MCF associé au **Cnam Paris**
- Mainteneur **LemonLDAP::NG**
- Architecte & Administrateur plateformes SSO à l'**ANFSI**



 christophe-maudoux-iam

le **cnam**

I. WEBSO & **LemonLDAP::NG**

II. PLATEFORMES SSO FSI

III. INSTANCES CHEOPS

IV. INSTANCES PROXYMA

V. INSTANCES CURASSO & CALYPSSO

VI. SECOND FACTEUR D'AUTHENTIFICATION

**Christophe Maudoux**

# WebSSO & LemonLDAP :: NG

## Principes de base

Christophe Maudoux

# LemonLDAP : :NG<sup>1</sup>

AUTHENTIFICATION UNIQUE AAA



## SOLUTION COMPLÈTE AAA :

**AUTHENTICATION** Vérification d'identité ( $\neq$  identification)

**AUTHORIZATION** Contrôle d'accès (règles)

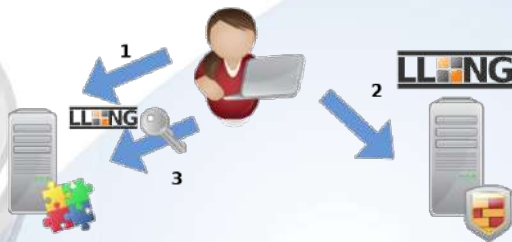
**ACCOUNTING** Traces & journaux d'activité (imputabilité des actions)

---

1. LemonLDAP : :NG - Web SSO and Access Management Free Software. URL : <https://lemonldap-ng.org/>.

# LemonLDAP::NG

CINÉMATIQUE SSO



1. Utilisateur *NON authentifié* essaye d'accéder à une ressource protégée
2. Redirigé par **LemonLDAP::NG** vers le *Portail unique d'authentification*  
→ **Authentification**
3. Portail fournit un *jeton SSO* (cookie) puis redirige utilisateur vers la ressource initialement demandée :  
→ **Authentifié** (dispose d'un cookie SSO)  
→ **Vérification** des règles d'accès

# LemonLDAP : :NG<sup>2</sup>

ÉQUIPE DE DÉVELOPPEMENT

- Xavier Guimard (Yadd)
- Christophe Maudoux

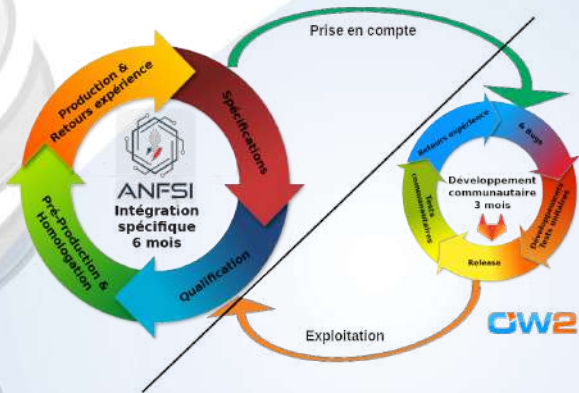


- Clément Oudot (KPT)
- Maxime Besson
- David Coutadeur

2. X. GUIMARD et al. "LemonLDAP : :NG". In : (déc. 2010). URL : <https://hal.inria.fr/hal-03776592>.

# LemonLDAP : :NG

CYCLE DE DÉVELOPPEMENT <sup>3</sup> (LE P'TIT VÉLO LemonLDAP : :NG...)




Cycle *interne* de validation / Cycle *communautaire* d'intégration continue

3. GitLab OW2 LemonLDAP : :NG. URL : <https://gitlab.ow2.org/lemonldap-ng>.



# **Plateformes SSO des Forces de Sécurité Intérieure**

Différents besoins



Christophe Maudoux

# PLATEFORMES SSO DES FSI

CLOISONNEMENT DES POPULATIONS & APPLICATIONS

Déclinées en Prod, PréProd, Form & Dév

## INTRANET

PROXYMA	SSO GN (≈ 350 app. / 130 000 users)
CHEOPS	SSO PN (≈ 150 app. / 150 000 users)
PSI	SSO fédéré → FS GN, PN, Préfectures
JUDIWEB	SSO DMZ → FS autres ministères

## INTERNET

CURASSO	SSO GN (formation continue)
CALYPSSO	SSO PN
ESPRESSO	SSO autres utilisateurs (recrutement)
EXTENSSO	SSO en DMZ (France Connect Agent)

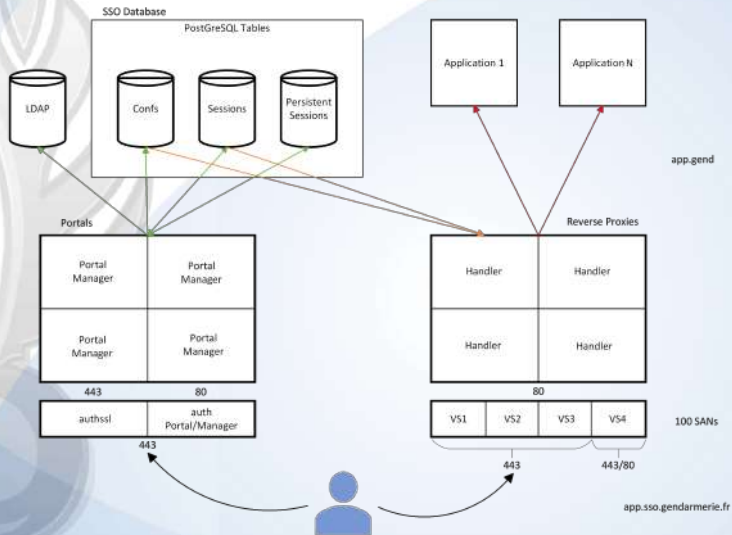
▶ Règles de gestion des utilisateurs & droits d'accès différents





# PLATEFORMES SSO DES FSI

## PRÉSENTATION ARCHITECTURE DE BASE



► LDAP multi-mâtres ou différents esclaves par instance SSO

# PLATEFORMES DES FSI

## INSTANCES CHEOPS – PORTAIL

**Police Nationale**  
Portail CHEOPS

- **NSIS**: Operation de maintenance du NSIS entrainant une interruption de service en alimentation et en consultation le lundi 14 octobre sur le creneau 09h00-04h30. (CNAU)
- **ACCUEIL** : Une perturbation touche l'application ACCUEIL. (Impossible de recuperer la liste des accueils). Les equipes support sont avisees. Merci de patienter. (CNAU)
- **VIDEOGAV** : le serveur de traces sera coupe le 24/09 a 16h30. Les rapports ne pourront plus etre transmis a celui-ci et les procedures "VideoGAV" ne pourront pas etre cloturees jusqu'a la mise en place de la version 3.8.3 de VideoGAV. (CNAU)

Veillez vous authentifier

par carte agent

par identifiant / mot de passe

Identifiant ou Matricule

Mot de passe

Se connecter

Voir mes dernières connexions

Des données nominatives vous concernant sont enregistrées pendant votre connexion. En vertu de l'article 105 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; vous disposez d'un droit d'accès, de rectification, de limitation et d'effacement de ces données. Vous pouvez exercer ce droit en adressant un courrier à l'ANFSI / DSA / D2S, 4 rue Claude Bernard - 92130 ISSY LES MOULINEAUX.

# PLATEFORMES DES FSI

## INSTANCES CHEOPS – MENU

Forçage du mot de passe

Admins nationaux

Profil SSO d'un utilisateur

iTop  
Gestion des demandes

**Plateforme SSO Internet**

Portail  
Calyppo

Manager  
Calyppo

CheckUser  
Calyppo

ServiceDesk  
Calyppo

**Documentation**

MdP CL  
MdP Client Lourd

WIKI PRETAJ

Site du CNAU  
Assistance utilisateur

LemonLDAP:NG  
Site officiel

**Aide à l'enquête**

ADOC  
Demandes de consultation

AEROPE  
Demandes de fiabilité

F2CO  
Comptabilité centralisée

▶ LL::NG ◀

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxyma

Instances Curasso &  
Calyppo

Instances Cheops  
& TOTP

**LLNG**

# PLATEFORMES DES FSI

INSTANCES CHEOPS – SECOND FACTEUR D'AUTHENTIFICATION (TOTP)

Plateformes	Prod.	Form.	PréProd.
LDAP maîtres	2	2	2
Portail	4	2	2
RVPRX	4	2	2
BDD SSO	PostGreSQL	PostGreSQL	PostGreSQL
Extension	ContextSwitching	—	—
	TOTP, CheckUser & Notifications		
<b>Gestion des comptes – droits décentralisée gérants habilitations</b>			

# TIME-BASED ONE TIME PASSWORD

PERTE CARTE PROFESSIONNELLE



Portail de la Police Nationale

Votre nouvelle clef TOTP. Testez-la et entrez le code

1 Scannez ce QR code dans votre application TOTP



2 Choisissez un nom pour votre périphérique TOTP

MyTOTP

3 Recopiez le code affiché par votre application

Si votre application n'accepte pas les QR codes, saisissez la clé suivante:

MEHC KV3D D0XS UZZ4 CBZL TF0C J0PW 0R0D

Enregistrer

Gestionnaire Zndf A Aller au portail



Portail Police de Pré-Production

Information

Expiration du TOTP (24 heures)

Votre second facteur (MyTOTP) a été supprimé !

Annuler Accepter

► LL::NG ◀

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxyma

Instances Curasso &  
Calyppo

Instances Cheops  
& TOTP

LLNG

# PLATEFORMES DES FSI

## INSTANCES PROXYMA – PORTAIL

**Portail Proxima**  
Gendarmerie Nationale

Connecté en tant que MAUDOUX Christophe ADC (SGI 025 ANFSI) -

[Vos applications](#)
[Mot de passe](#)
[Historique des connexions](#)
[Déconnexion](#)

**Administration**

- Manager
- Sessions
- Notif.
- Visionneur
- Droits & Attributs
- Splunk

**instances SSO Internet**

- Manager Espresso
- CheckUser Curasso
- ServiceDesk Curasso

**Opérationnel**

- BDSP
- Pulsar
- PVE
- IDICS
- Evengrave
- Ma Sécurité
- PSGN
- Neoparc
- Gecem
- Parc Informatique
- Portailfag
- Preflight

**Métier**

- Annuaire GN
- NATINF
- Cyber-side
- Infocentre BI
- GEAUDE2GMAT
- GEAUDE2GA
- Vulcan
- Reuni
- Partage-NG
- Memorial
- Wiki
- manLegement

LL::NG

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxima

Instances Curasso &  
Calyпсо

Instances Cheops  
& TOTP

LLNG

# PLATEFORMES DES FSI

## INSTANCES PROXYMA – MENU

**Portail Proxima**  
Gendarmerie Nationale

Connecté en tant que MAUDOUX Christophe ADC (SGI 025 ANFSI) -

**Administration**

- Manager
- Sessions
- Notif.
- Visionneur
- Droits & Attributs
- Splunk

**Opérationnel**

- BDSP
- Pulsar
- PVE
- IDICS
- Evengrave
- Ma Sécurité
- PSGN
- Neoparc
- Gecem
- Parc Informatique
- Portailfag
- Preflight

**Métier**

- Annuaire GN
- NATINF
- Cyber-side
- Infocentre BI
- GEAUDE2GMAT
- GEAUDE2GAI
- Vulcan
- Reuni
- Partage-NG
- Memorial
- Wiki
- manLegement

**instances SSO Internet**

- CheckUser Curasso
- ServiceDesk Curasso
- Manager Espresso

Menu contextuel sur Manager Espresso:

- Éprouvateur de notifications
- Décoder une valeur chiffrée
- Endosser l'identité d'un autre utilisateur
- Rafraîchir mes droits

LL::NG

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxima

Instances Curasso &  
Calyпсо

Instances Cheops  
& TOTP

LLNG

# PLATEFORMES SSO DES FSI

## INSTANCES PROXYMA – CARACTÉRISTIQUES & SPÉCIFICITÉS

Plateformes	Prod.	Form.	PréProd.	Dév.
LDAP esclaves	6	2	2	1
Portail	4	2	2	1
RVPRX	4	2	2	1
BDD SSO	PostGreSQL	PostGreSQL	PostGreSQL	PG & Redis
Extension	ContextSwitching	FindUser	Impersonation	GenericPwd
	CheckUser & Notifications			
<b>Gestion des comptes et droits centralisée &amp; automatisée</b>				

### CHAQUE INSTANCE ⇒ BESOINS SPÉCIFIQUES

- DÉV.** MdP identique pour tous les utilisateurs sauf *admins*
- PRÉPROD.** Simuler l'identité d'autres utilisateurs → test
- FORM.** Rechercher un compte à simuler → formation
- PROD.** Endosser l'identité d'un autre utilisateur → analyse
- TOUTES** Vérification règles d'accès, entêtes transmis, données de session → contrôle



# PLATEFORMES DES FSI

## INSTANCES PROXYMA – CHECKUSER

Check user SSO profile

christophe.maudoux

http://agenda.sso.gendarmerie.fr

Search

Access ALLOWED

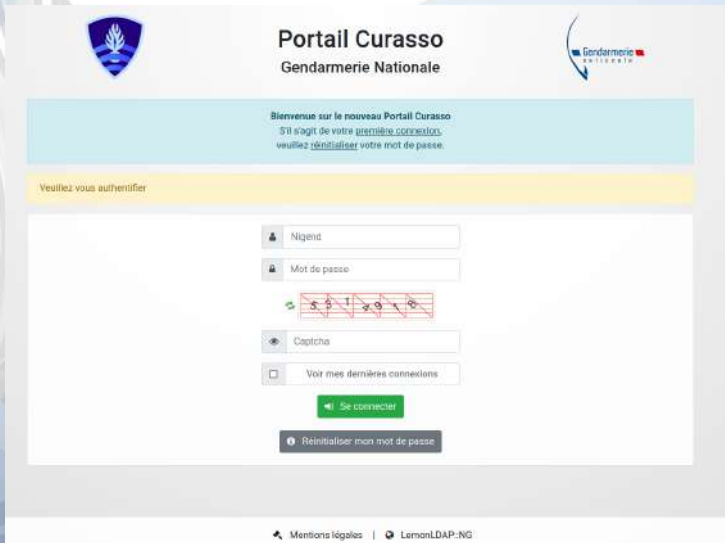
**HEADERS**

HTTP\_AUTH\_USER: christophe.maudoux  
HTTP\_OBM\_DISPLAYNAME: MAUDOUX Christophe ADC (SCT BICOF STSISI)  
HTTP\_OBM\_DOMAIN: gendarmerie.interieur.gouv.fr  
HTTP\_OBM\_MAIL: christophe.maudoux@gendarmerie.interieur.gouv.fr  
HTTP\_OBM\_NIGEND: 173668  
HTTP\_OBM\_UID: christophe.maudoux  
HTTP\_OBM\_WHOAMI: christophe.maudoux

SSO GROUPS	Key	Value
adm_bdd	accountStatus	active
admin-proxy	adresse	4 RUE CLAUDE BERNARD5CS 60003592136 ISSY LES MOULINEAUX CEDEX
admin-static	authenticationLevel	5
impressiondg	businesscategory	SECT ADM CENT
moncompte_midpccole	cn	MAUDOUX Christophe
pulsar_formules_pilgrage	codeServiceRd	3067658
scode_de_admin	codeUnite	67658
scode_de_cnis	codeUniteService	67625
scode_de_consld	deliveryMode	active
scode_de_gai	departmentUID	GEND NAT/DIR GEN GEND NAT/SERV TECHNO SYS INFO SECU INTERIEUR/SDIR APPLI CMDT/BUR CONTROL CPER FICH/SECT CONTROL TECH
scode_de_traces	departmentnumber	GEND/STSISI/BICOF/SCT
scode_de_vam		
sic		
sirboard_consult		
spunk_admin		
spunk_master		
tu		
wiki_cvtid11		

# PLATEFORMES DES FSI

## INSTANCES CURASSO & CALYPSO – PORTAIL



The screenshot shows the login interface for the Portail Curasso Gendarmerie Nationale. At the top, there are logos for the Gendarmerie Nationale and the Curacao government. The main heading reads "Portail Curasso Gendarmerie Nationale". Below this, a light blue box contains a welcome message: "Bienvenue sur le nouveau Portail Curasso. Si il s'agit de votre première connexion, veuillez réinitialiser votre mot de passe." A yellow bar below this says "Veuillez vous authentifier". The login form includes fields for "Nigend" (username), "Mot de passe" (password), and a "Captcha" field. There is also a checkbox for "Voir mes dernières connexions" and a green "Se connecter" button. A link for "Réinitialiser mon mot de passe" is located below the login button. At the bottom of the page, there are links for "Mentions légales" and "LemonLDAP:NG".

▶ LL::NG ◀

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>eme</sup>  
21 octobre 2024

 christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxyma

Instances Curasso &  
Calypso

Instances Cheops  
& TOTP

**LLNG**

# PLATEFORMES DES FSI

## INSTANCES CURASSO & CALYPSO – MENTIONS

### Mentions d'informations légales

#### Droits CNIL

Afin d'authentifier les personnels de la Gendarmerie Nationale depuis le réseau Internet, de permettre aux personnels de la Gendarmerie Nationale d'accéder aux applications professionnelles disponibles depuis Internet, de permettre aux personnels de la Gendarmerie Nationale d'accéder aux applications exposées par les autres ministères au travers d'**AgentConnect**, de gérer le contrôle d'accès des utilisateurs en fonction de leurs droits applicatifs, de transmettre les données utilisateurs aux applications afin que ces dernières identifient l'utilisateur accédant, l'Agence du Numérique des Forces de Sécurité Intérieures met en œuvre un traitement de données dénommé **Curasso**.

Des données professionnelles, de connexion et d'identité vous concernant sont traitées pour une durée de 3 ans. Seuls des personnels de la Gendarmerie Nationale en sont destinataires. Les données proviennent des traitements de gestion des ressources humaines de la Gendarmerie Nationale. Celles-ci ne sont pas accessibles au public.

En vertu de l'article 48 de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et de l'article 14 du RGPD, nous vous informons que la base légale du traitement est l'intérêt public. Vous disposez donc d'un droit d'accès, de rectification, de limitation et d'opposition. Vous pouvez exercer ces droits en adressant un courrier au responsable de traitement à :

**ANFS/DSA/D2S, 4 rue Claude Bernard – 92130 Issy-les-Moulineaux.**

#### Information complémentaire

Pour toute information complémentaire sur vos droits informatique et libertés, vous pouvez contacter le délégué à la protection des données du ministère de l'Intérieur (avec copie de votre pièce d'identité en cas d'exercice de vos droits) :

- via l'adresse mail suivante : [delegue-protection-donnees@interieur.gouv.fr](mailto:delegue-protection-donnees@interieur.gouv.fr)
- ou par courrier à l'adresse suivante :

**Ministère de l'Intérieur**  
A l'attention du délégué à la protection des données (DPO)  
Place Beauvau 75800 Paris CEDEX 08

#### Réclamation

Vous disposez également du droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés sise :  
**3 place de Fontenay, TSA 80715 75334 PARIS Cedex 07.**

Fermer

# PLATEFORMES SSO DES FSI

INSTANCES CURASSO & CALYPSSO – CARACTÉRISTIQUES & SPÉCIFICITÉS

Plateformes	Prod.	PréProd.
LDAP en DMZ	2	1
Portail + RVPRX	2	1
RVPRX	4	2
BDD SSO	PostGreSQL	PostGreSQL
Extension	ContextSwitching	
	CheckUser & CheckHIBP	

**Comptes alimentés par LSC depuis LDAP Proxyma & Cheops**

⇒ LDAP administrés avec ServiceDesk (profils ≠ → multi-tenant!!!)

# PLATEFORMES DES FSI

INSTANCES CURASSO & CALYPSO – SERVICEDESK ADMIN

Interface Sesame | Tableaux de bord | 173668

**Christophe MAUDOUX**

Identifiant	173668
Nom	MAUDOUX
Prénom	Christophe
Catégorie	ACT
Identifiants applicatifs	AGOO92341653 CAND00254981 FORM8724CQ02
Courriel	christophe.maudoux@gondamania.intel ieur.gov.fr

**Vérification du mot de passe**

Mot de passe actuel

Envoyer

**Réinitialisation du mot de passe**

Nouveau mot de passe

Forcer la réinitialisation à la prochaine connexion:

Envoyer

Le compte n'est pas bloqué

Réinitialiser le compte

**Statut du compte**

Dernier changement de mot de passe	19-07-2024 17:06:37
Réinitialisation du mot de passe à la prochaine connexion	Oui
Créé	19-04-2024 11:54:42
Modifié	22-07-2024 17:29:49
Date d'expiration	19-07-2025 17:06:37

▶ LL::NG ◀

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxyma

Instances Curasso &  
Calypso

Instances Cheops  
& TOTP

LLNG

# PLATEFORMES DES FSI

INSTANCES CURASSO & CALYPSO – SERVICEDESK CNAU



Interface Sésame | Tableaux de bord | 173668

Christophe MAUDOUX

Identifiant	173668
Nom	MAUDOUX
Prénom	Christophe
Catégorie	ACT
Courriel	christophe.maudoux@gendarmerie.interieur.gouv.fr

Réinitialisation du mot de passe

Niveau mot de passe

Envoyer

Le compte n'est pas bloqué

Statut du compte

Dernier changement de mot de passe	19-07-2024 17:06:37
Réinitialisation du mot de passe à la prochaine connexion	Oui
Créé	19-04-2024 11:54:42
Modifié	22-07-2024 17:28:49
Date d'expiration	19-07-2025 17:06:37



▶ LL::NG ◀

Plateformes SSO  
ANFSI

Worteks Paris XVI<sup>ème</sup>  
21 octobre 2024

christophe.maudoux  
ANFSI

WebSSO & LL : :NG

Plateformes SSO FSI

Instances Cheops

Instances Proxyma

Instances Curasso &  
Calypso

Instances Cheops  
& TOTP

LLNG

MERCI DE VOTRE ATTENTION !

☺ GARDONS LE CONTACT... ☺



*christophe.maudoux@gendarmerie.interieur.gouv.fr*  
*admin-ss0@gendarmerie.interieur.gouv.fr*



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

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

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