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

Worteks Paris *XVI*^{eme}
21 octobre 2024

Christophe Maudoux

Worteks Paris XVI^{eme}
21 octobre 2024

WebSSO & LemonLDAP::NG

Principes de base

Christophe Maudoux

LemonLDAP::NG [1]

Authentification unique AAA

Solution complète AAA :

Authentication Vérification d'identité ($\neq$ identification)

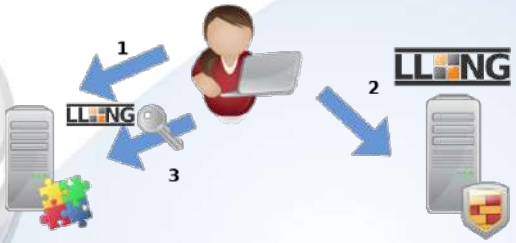
Authorization Contrôle d'accès (règles)

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 [2]

Équipe de développement

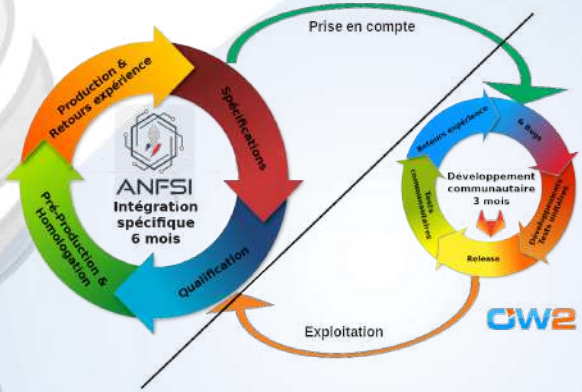
- Xavier Guimard (Yadd)
- Christophe Maudoux

- 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[3] (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.

Worteks Paris XVI^{eme}
21 octobre 2024

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

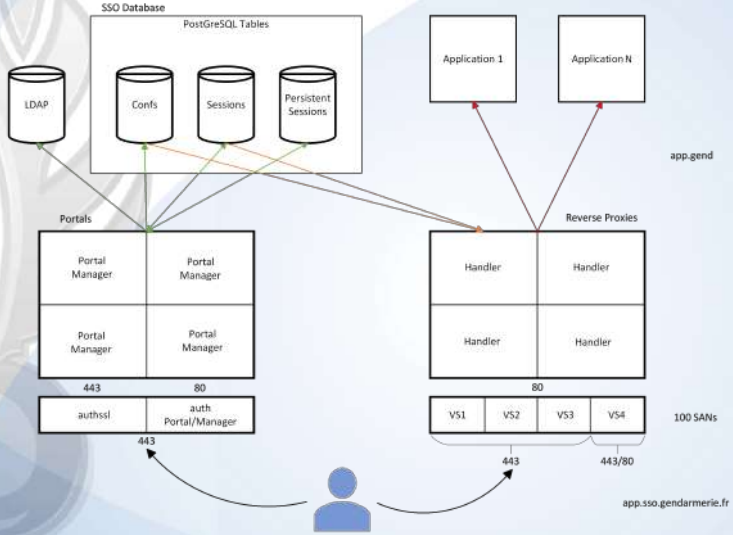
Internet

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



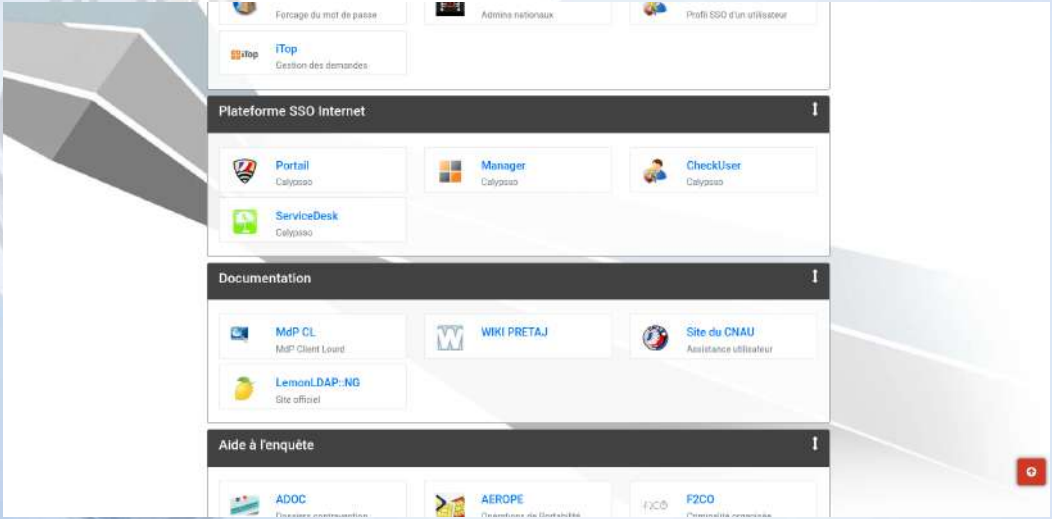
- LDAP *multi-maîtres* ou différents *esclaves* par instance SSO

Plateformes des FSI

Instances Cheops – Portail

Plateformes des FSI

Instances Cheops – Menu



Plateformes des FSI

Instances Cheops – Second facteur d'authentification (TOTP)

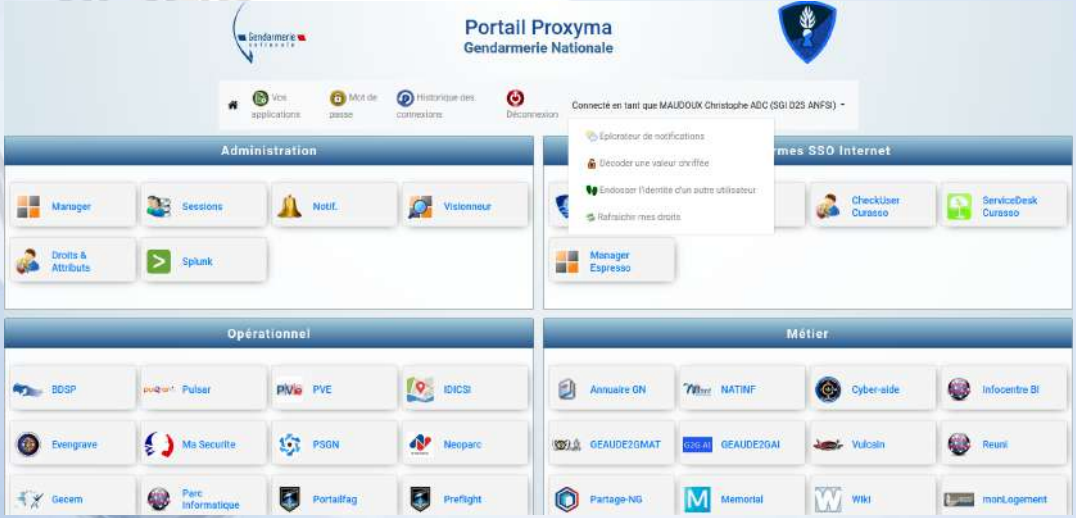
Plateformes	Prod.	Form.	PréProd.
LDAP maîtres	2	2	2
Portail	4	2	2
RVPRX	4	2	2
BDD SSO	PostGreSQL	PostGreSQL	PostGreSQL
Extension	ContextSwitching	\	\
	TOTP, CheckUser & Notifications		
Gestion des comptes – droits décentralisée gérants habilitations			

Time-based One Time Password

Perte carte professionnelle

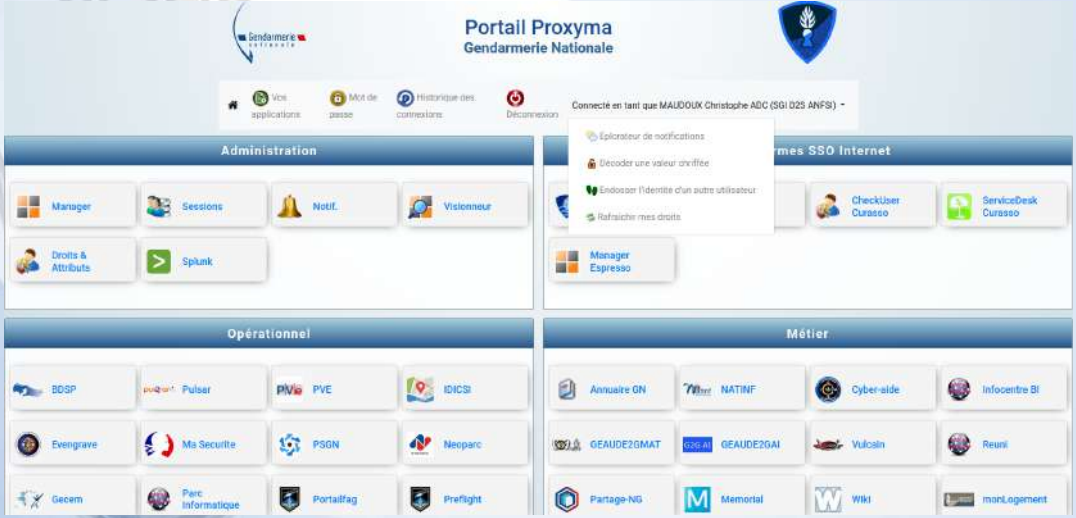
Plateformes des FSI

Instances Proxyma – Portail



Plateformes des FSI

Instances Proxyma – Menu



Plateformes SSO des FSI

Instances Proxyma – Caractéristiques & Spécificités

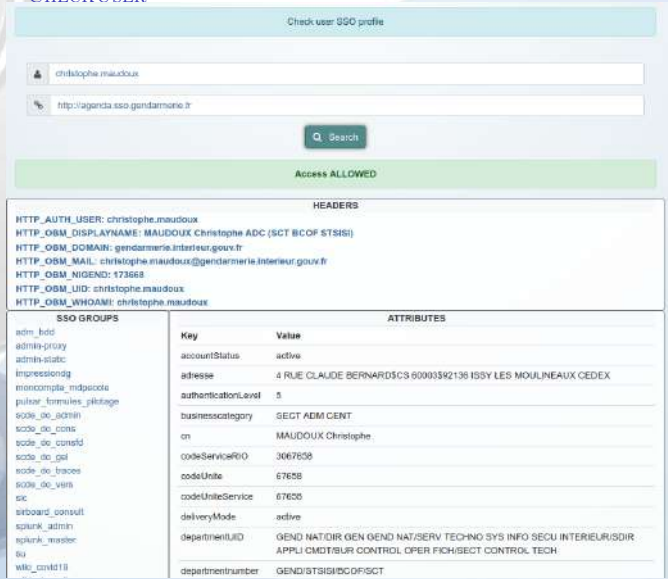
Plateformes	Prod.	Form.	PréProd.	Dév.
LDAP esclaves	6	2	2	1
Portail	4	2	2	1
RVPRX	4	2	2	1
BDD SSO	PostGreSQL	PostGreSQL	PostGreSQL	PG & Redis
Extension	ContextSwitching	FindUser	Impersonation	GenericPwd
	CheckUser & Notifications			
Gestion des comptes et droits centralisée & automatisée				

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

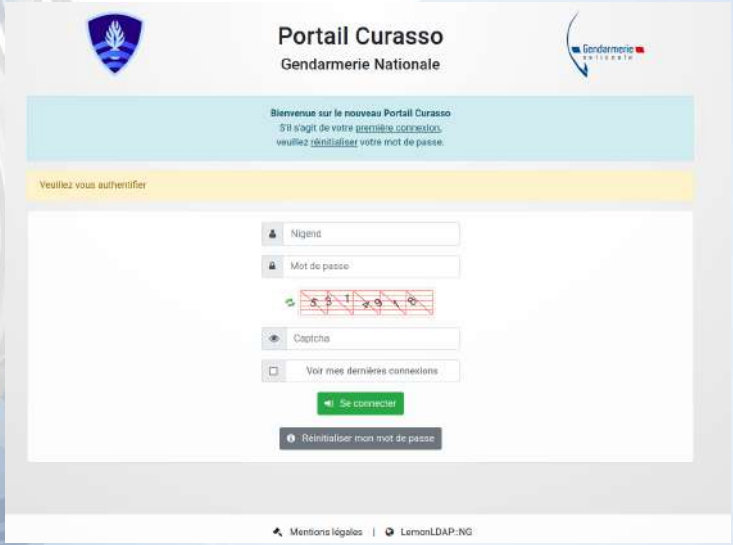
Plateformes des FSI

Instances Proxyma – CheckUser



Plateformes des FSI

Instances Curasso & Calypsso – Portail



Plateformes des FSI

Instances Curasso & Calypsso – 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 oeuvre 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 :
ANFSI/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**
- 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 Fontenoy, TSA 80715 75334 PARIS Cedex 07.

Fermer

Plateformes SSO des FSI

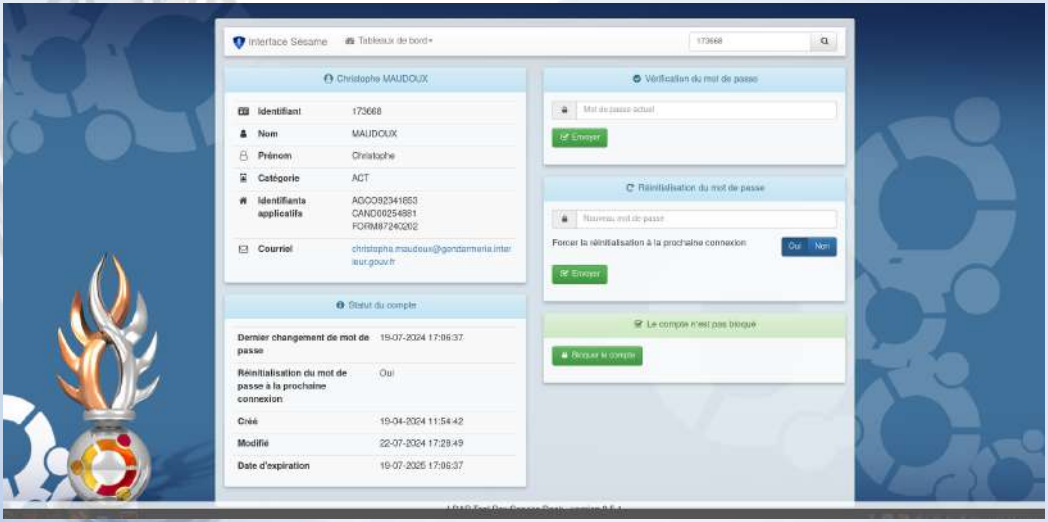
Instances Curasso & Calypsso – Caractéristiques & Spécificités

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 $\neq \rightarrow$ multi-tenant ! ! !)

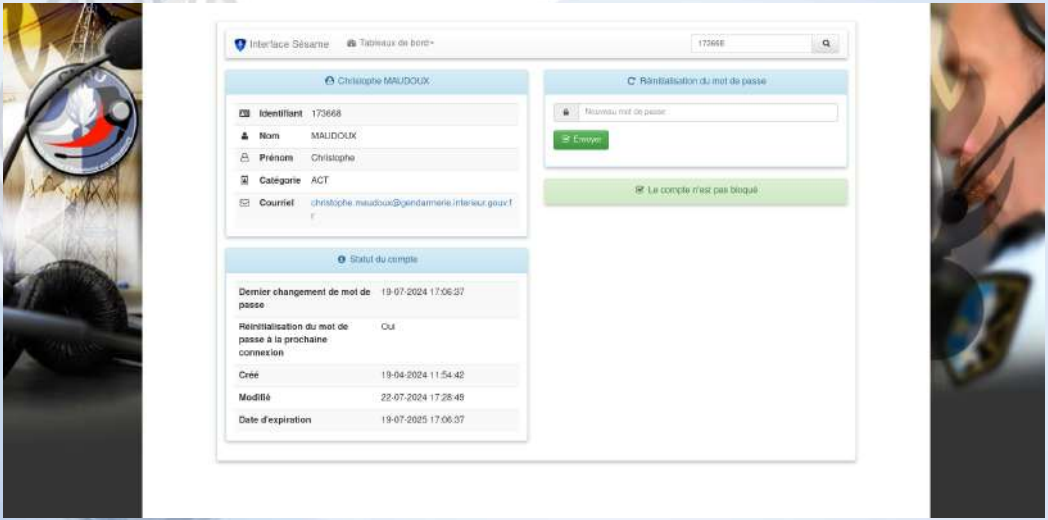
Plateformes des FSI

Instances Curasso & Calypsso – ServiceDesk Admin



Plateformes des FSI

Instances Curasso & Calypsso – ServiceDesk CNAU



Merci de votre attention !

☺ Gardons le contact... ☺

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

Site officiel ► `https://lemonldap-ng.org`
Versions ► `https://releases.ow2.org/lemonldap`
Forge ► `https://gitlab.ow2.org/lemonldap-ng`