



Gestion des authentifications et des accès avec LemonLDAP::NG 2.0

Clément OUDOT @clementoudot
Worteks @worteks_com

28 Janvier 2019

Worteks (\vɔʁ.teks\)

Services

Infrastructures complexes et hétérogènes,
cloud, messagerie, authentification, sécurité

- Étude, audit et conseil
- Expertise technique
- Support technique
- Formations
- R&D



Édition



Portail applicatif
et collaboratif



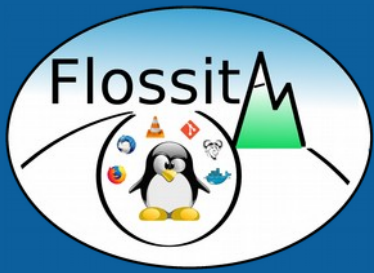
Plateforme collaborative
mutualisée de
développement



Gestion des identités et
des accès

Partenaires

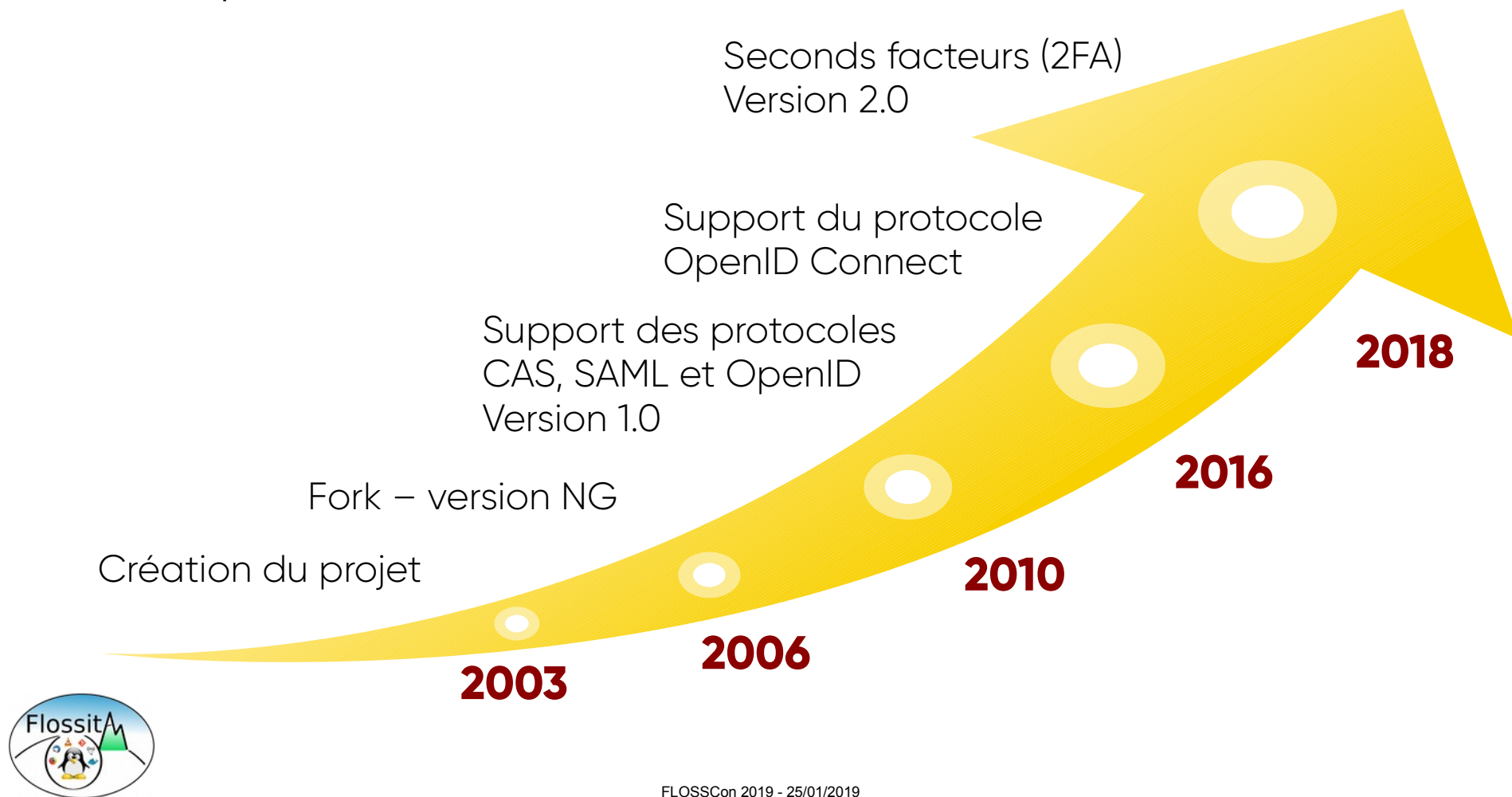




Le logiciel LemonLDAP::NG



Historique



Principales fonctionnalités

- Authentification unique (WebSSO)
- Contrôle d'accès
- Portail d'applications
- Chaînage et choix des modules d'authentification
- Gestion du mot de passe, création de compte
- Authentification multi-facteurs
- Protection des applications Web et des API/WebServices
- Personnalisation graphique
- Paquets Debian/Ubuntu/RHEL/CentOS



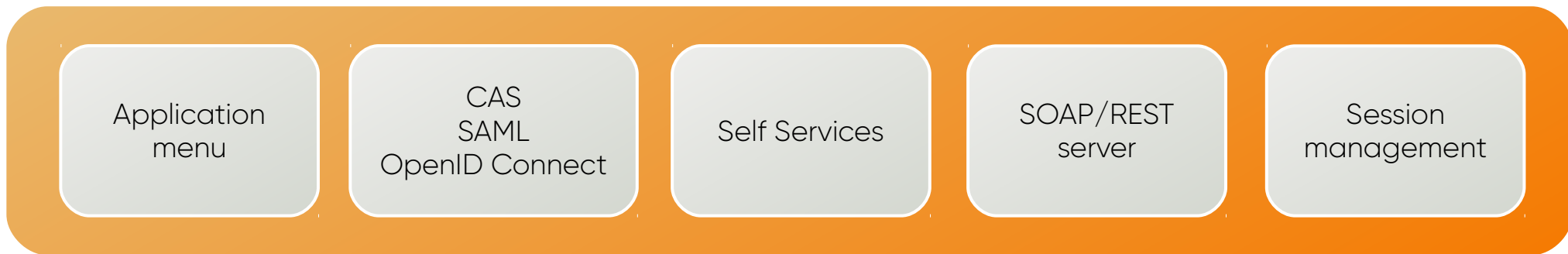
Logiciel Libre

- Licence GPL
- Projet OW2
- Forge : <https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng>
- Site : <https://lemonldap-ng.org>
- OW2 Community Award en 2014
- Composant SSO du projet FusionIAM : <https://fusioniam.org/>

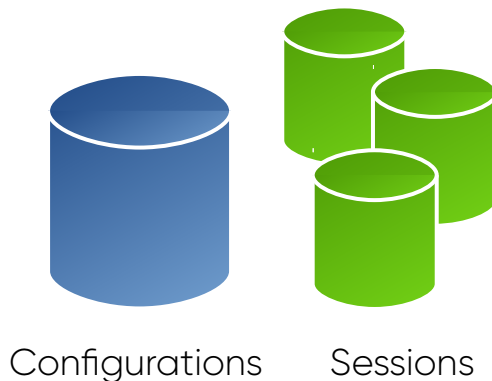
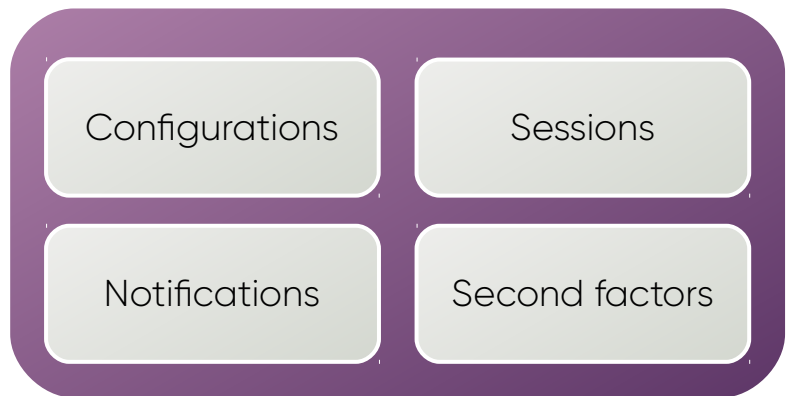


Rôle des composants

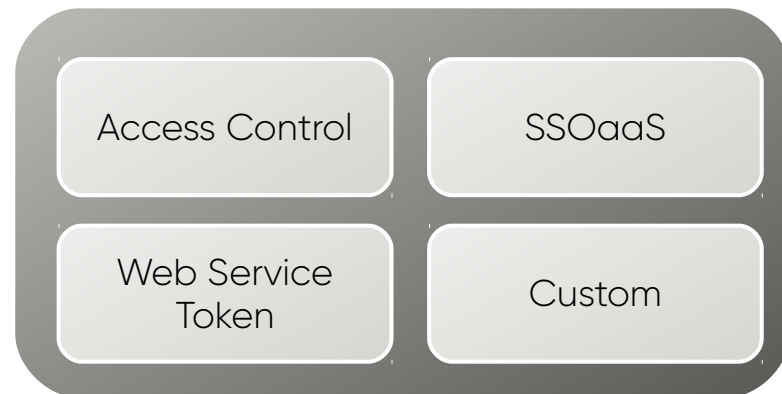
Portal

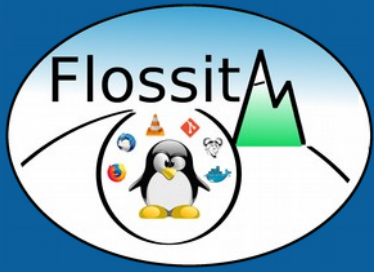


Manager



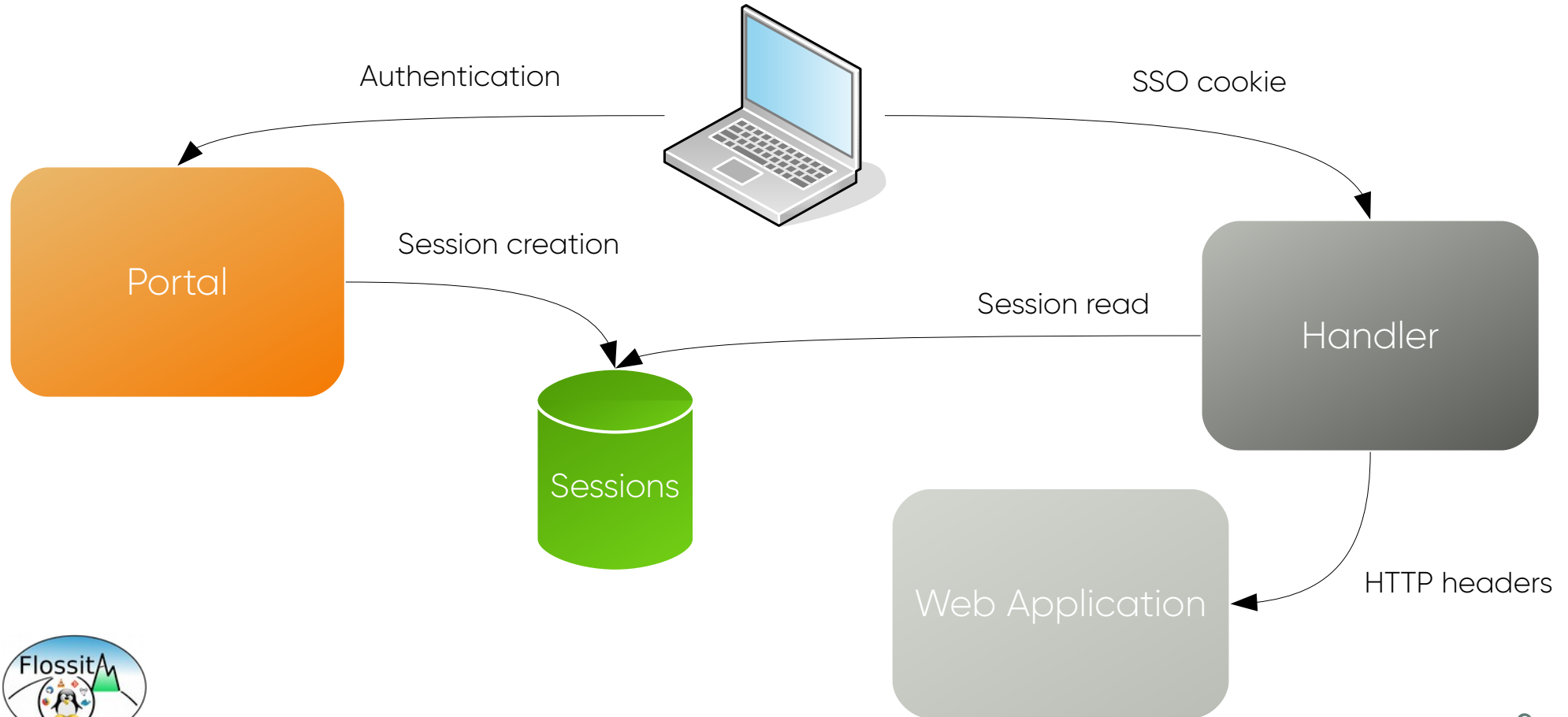
Handler



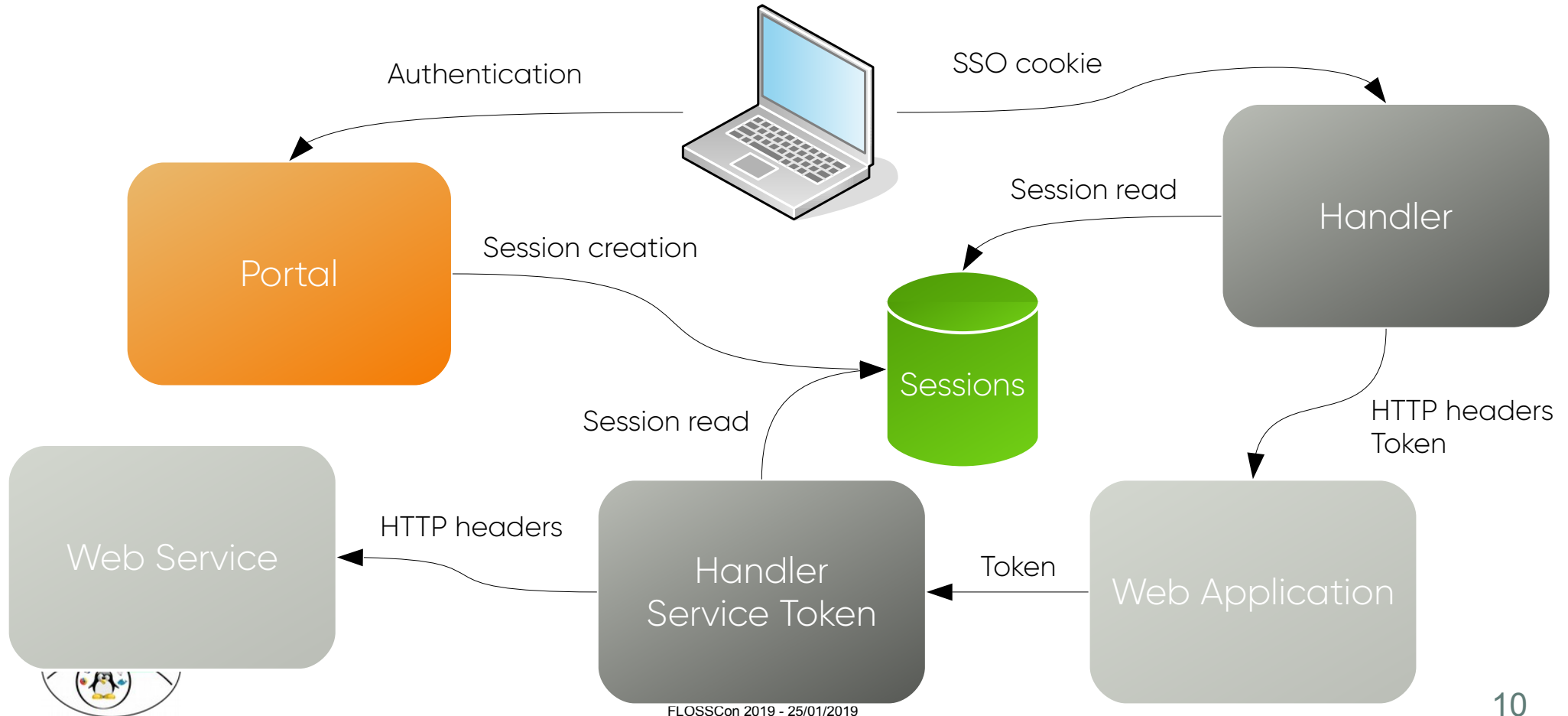


Fonctionnement par agent (Handler)

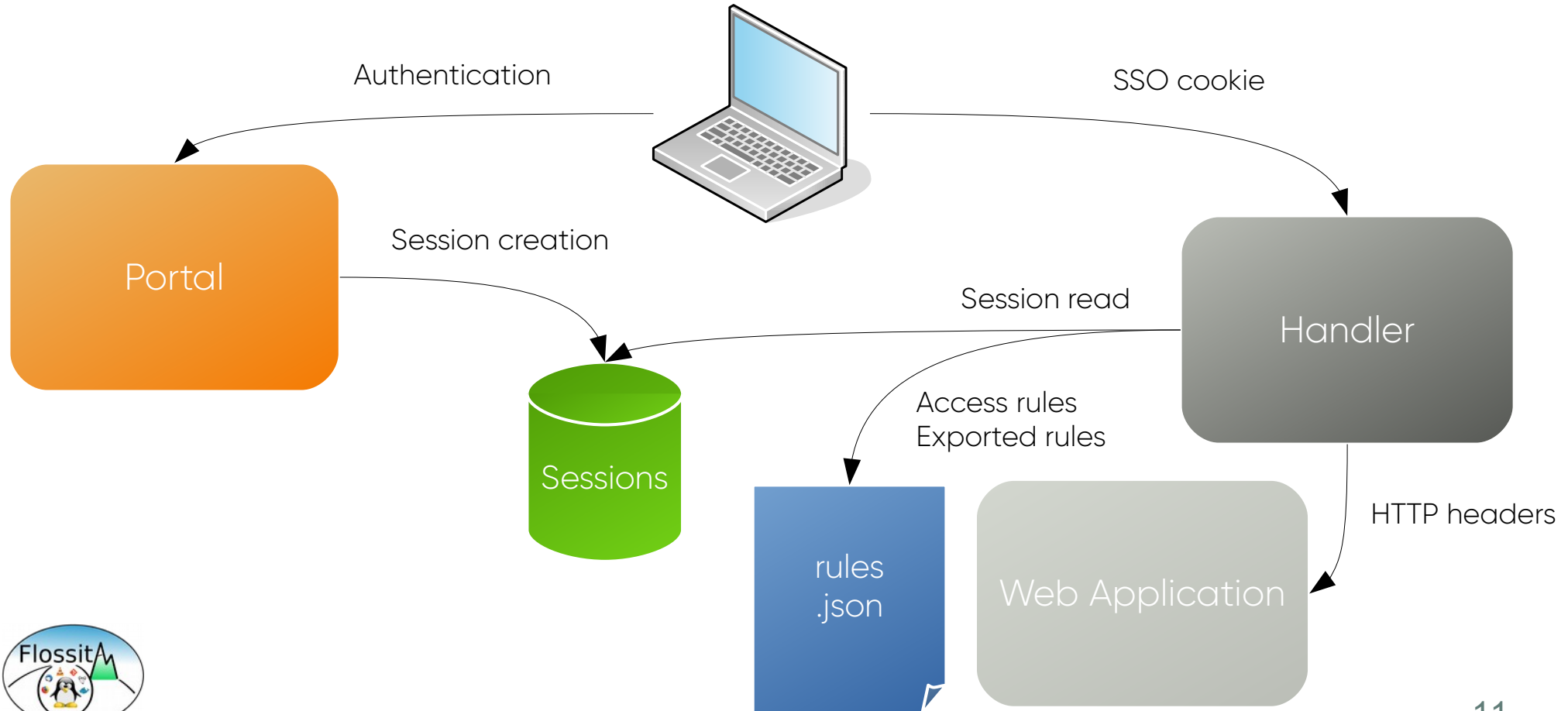
Application Web

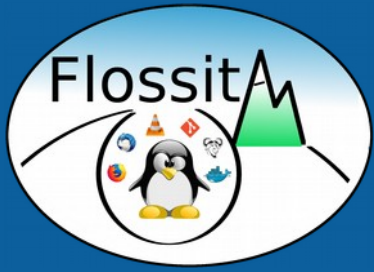


API – Service Token



Mode DevOps (SSO as a Service)





Les protocoles CAS, SAML et OpenID Connect

Principales fonctionnalités

- Modes "client" et "serveur"
- Échange d'attributs
- Gestion des niveaux et des contextes d'authentification
- Génération automatique des clés publiques et privées
- Contrôle d'accès par services
- Publication des données de configuration (metadata)
- Passerelle mutli-protocoles
- Transfert de la déconnexion

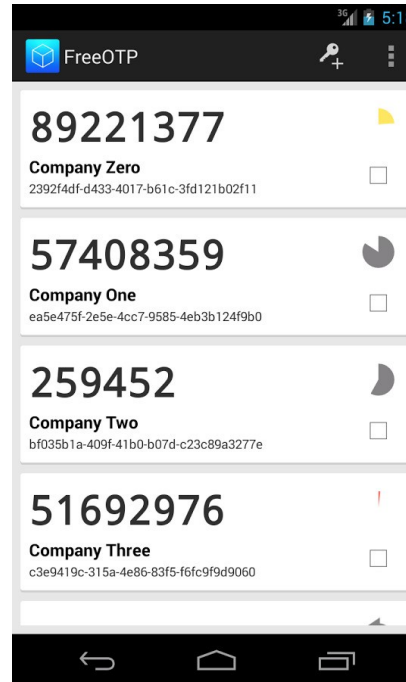




Nouveautés de la version 2.0

Seconds facteurs d'authentification (2FA)

- LemonLDAP::NG peut demander un second facteur d'authentification après que la première authentification ait été validée :
 - TOTP
 - U2F
 - TOTP ou U2F
 - Externe
 - REST
 - Yubikey



fido
ALLIANCE



Backends de configuration

- Backends déjà existants :
 - Fichier JSON
 - Base de données
 - LDAP
 - NoSQL (MongoDB)
 - SOAP
- Nouveaux backends :
 - Fichier YAML
 - REST
 - Local (utilisation du fichier lemonldap-ng.ini uniquement)



Handler NodeJS

- Intégration native dans une application Express
- Règles et en-têtes à écrire en Javascript
- <https://github.com/LemonLDAPNG/node-lemonldap-ng-handler>

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



SSO as a Service

- L'authentification est toujours réalisée par le portail
- Les contrôles d'accès et la liste des en-têtes est gérée par l'application, dans un fichier JSON à la racine
- Cela permet un déploiement rapide d'application en mode "DevOps" : aucune déclaration n'est nécessaire dans la configuration globale



Protection des API / Webservice

- Nouveau Handler "Service Token" en rupture de flux entre l'application et le Web Service
- Génération d'un jeton par le Handler principal en incluant le temps (time), l'identifiant de session (session_id) et la liste des hôtes virtuels (vhostList)
- Transmission du jeton par l'application au Web Service
- Validation du jeton par le Handler "Service Token" et à l'aide de l'identifiant de session, contrôle d'accès et envoi des en-têtes



Modules d'authentications

- Nouveaux modules :
 - PAM
 - REST
 - Kerberos (GSSAPI)
 - CAS (lecture des attributs)
- Remplacement de Multi par Combination
- Utilisation possible d'un module Custom



Interface d'administration

- Ajout d'un comparateur de configurations : les différences entre deux configurations sont affichées sous forme d'arbre
- Module d'administration des seconds facteurs (recherche, révocation)
- Tri des sessions par date de création et date de modification



RENATER

- Support de la fédération RENATER via SAML2 :
 - Fournisseur de Service
 - Fournisseur d'identité
- Appel de la page de choix du fournisseur (WAYF) via SAML Discovery Protocol
- Script d'import en masse des metadata publiées par Renater



Moteur de plugins

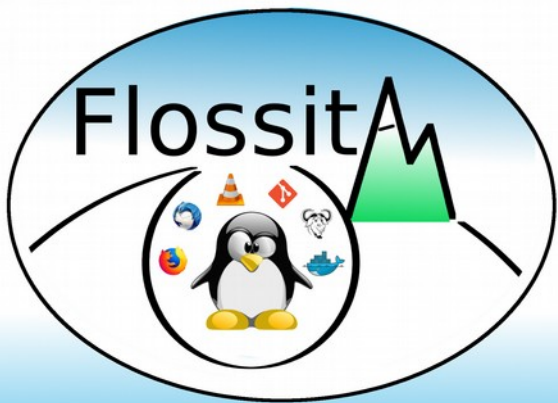
- Le code du portail a été réécrit pour permettre le développement simple de nouveaux plugins
- Exemple de plugins fournis par défaut :
 - Auto Signin : authentification directe pour certaines IP
 - Brute Force : protection des attaques par force brute
 - Stay Connected : possibilité de garder sa session même après fermeture du navigateur
 - Public Pages : création de pages statiques reprenant le thème du portail
- Écrire son propre plugin :
<https://lemonldap-ng.org/documentation/latest/plugincustom>



Autres nouveautés

- Un utilisateur peut recharger ses droits sans se déconnecter/reconnecter
- Services REST natifs (configurations et sessions)
- Sélection de la langue avant la connexion
- Nouveau thème graphique basé sur Bootstrap 4
- Personnalisation du logo (repris dans le thème graphique et les mails envoyés)
- Choix du système de logs (syslog, Apache, Log4Perl, Sentry...)





FLOSSCON 2019

**FREE / LIBRE / OPEN SOURCE
SOFTWARE CONFERENCE**

27 AU 29 JANVIER
WWW.FLOSSCON.ORG

Contact
clement.oudot@worteks.com

Pour plus d'informations :



info@worteks.com



[@worteks_com](https://twitter.com/worteks_com)



linkedin.com/company/worteks

du
24.01
au
31.01
2019

Festival numérique
100% alpin

T R
A N
S F



le
numérique
et nous

Grenoble
Valence-Romans
Chambéry
Annecy
Genevois

#FestivalTransfo

www.festival-transfo.fr

[f](#) [i](#) [i](#) [n](#) @FestivalTransfo



Propulsé par :



LA CASEMIATE



Logiciels et données libres pour une transformation numérique maîtrisée

Dimanche 27 janvier 2019, journée "Libre et **grand public**" au Secours Catholique Isère à Grenoble

Lundi 28 janvier 2019, journée "Libre et **technologie**" à CGI à Grenoble

Mardi 29 janvier 2019, journée dédiée "Libre et **secteur public**" à La Source à Fontaine



Grenoble



Trois jours d'ateliers,
conférences, démos,
tables rondes par les
libristes alpins

Co-propulsé avec ♥ par

LA CASEMATE

Partenaires



Soutiens

