Vorteks

make IT work, make IT free

SSO et fédération d'identités avec le logiciel libre LemonLDAP::NG, retour d'expérience d'un client

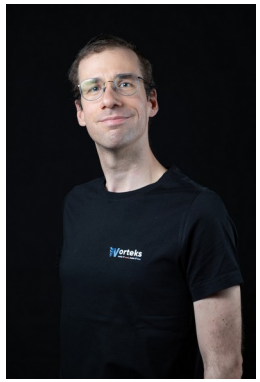
OPEN SOURCE EXPERIENCE

Ordre du jour

1. Présentation
2. LemonLDAP::NG
3. Fédération d'identité
3. Mise en place chez [client]

Présentation

Présentation



David COUTADEUR

architecte en gestion d'identité

~10 ans d'expérience dans le domaine

passionné d'open-source

david.coutadeur@worteks.com

@dcoutadeur@toot.aquilenet.fr

www.linkedin.com/in/david-coutadeur-06571a1a4

Worteks (\vɔʁ.tɛks\)

Service

Infrastructures hétérogènes et complexes,
cloud, mail, authentification, securité

- Etudes, audit et consulting
- Expertise technique
- Support technique
- Formation
- R&D et innovation

Édition

V'Sweet — Portail d'applications collaboratif

V'Opla — Plateforme mutualisée de développement

V'IDaaS — Gestion des identités et des accès

Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

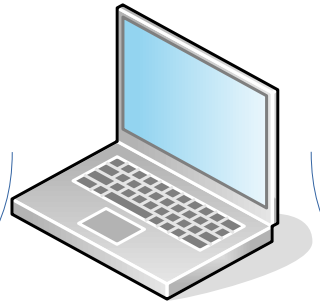
Collabora Online

Worteks (\vɔʁ.tɛks\)

https://www.worteks.com/rejoindre/

LemonLDAP::NG

Cinématique SSO



2. Authentification

1. Premier accès

3. Envoi du jeton SSO

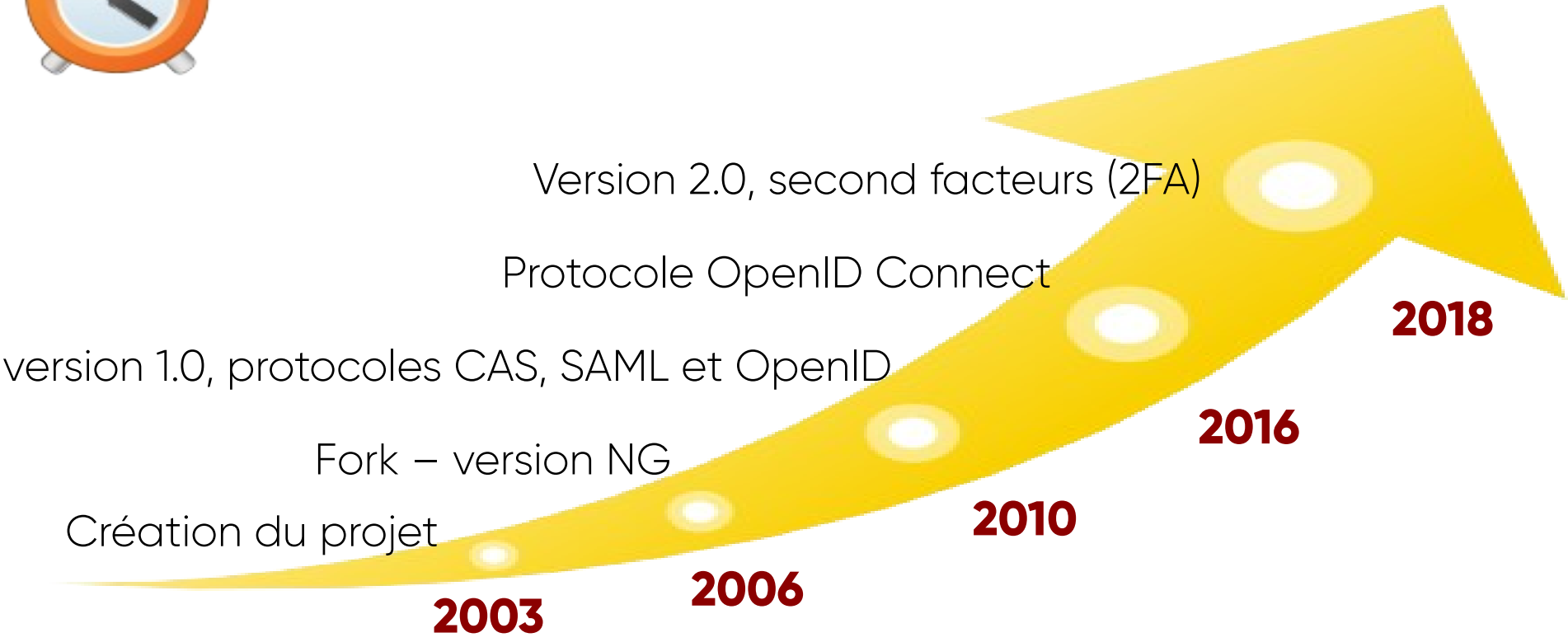
4. Validation du jeton SSO

Portail d'authentification

Lien de confiance

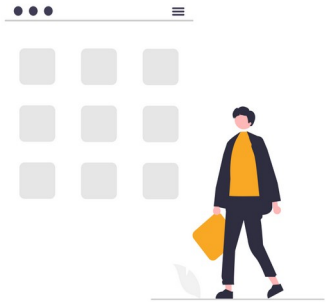
Application

Historique

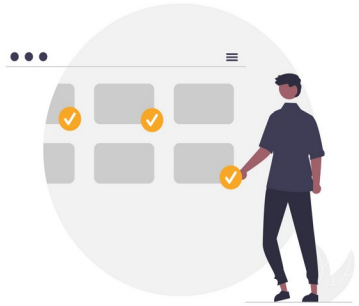

Version 2.0, second facteurs (2FA)
Protocole OpenID Connect
2018
version 1.0, protocoles CAS, SAML et OpenID
2016
Fork – version NG
2010
Création du projet
2006
2003

Principales fonctionnalités

SSO & Contrôle d'accès

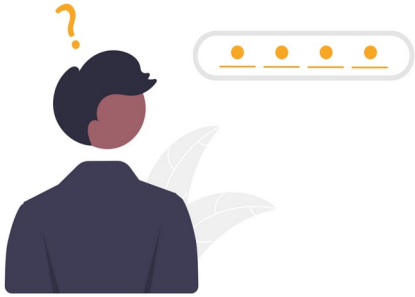


Menu des applications

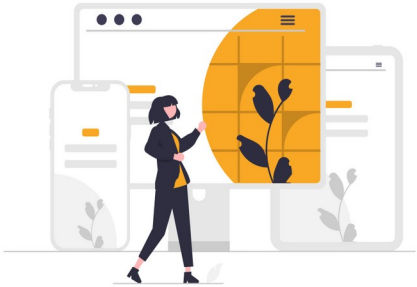


CAS / SAML / OIDC

Second facteurs (2FA)



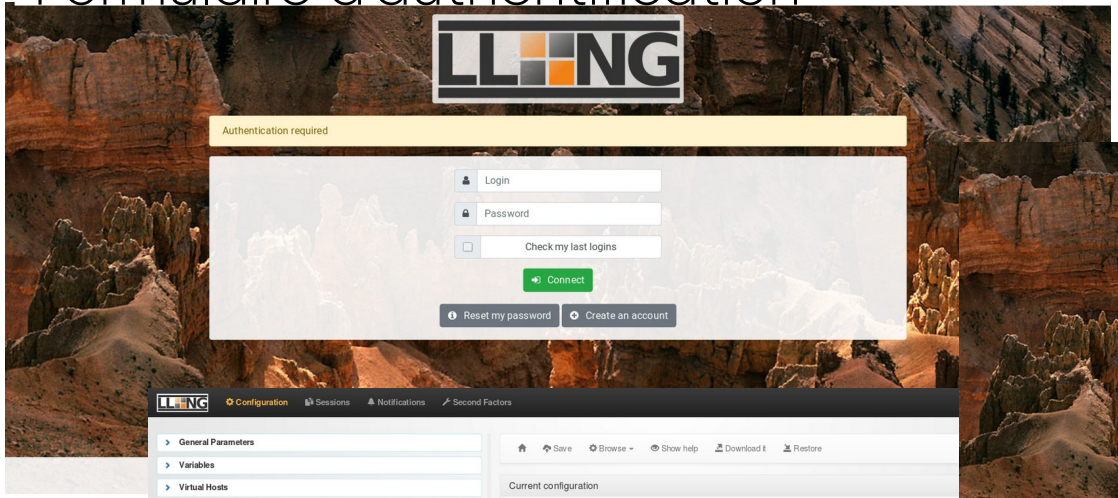
Gestion du mot de passe



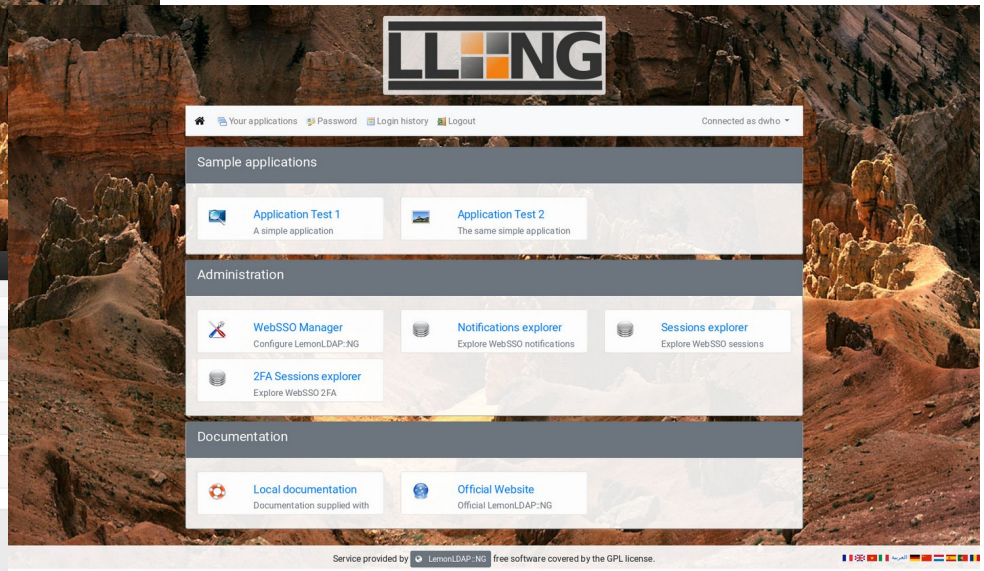
Personnalisation graphique

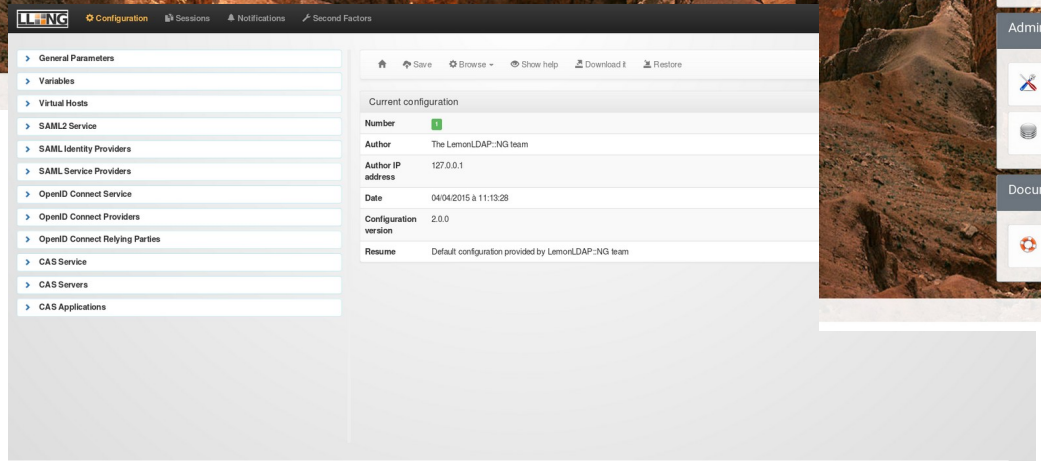
Interfaces

Formulaire d'authentification



Menu des applications





Interface d'administration

Interface CLI

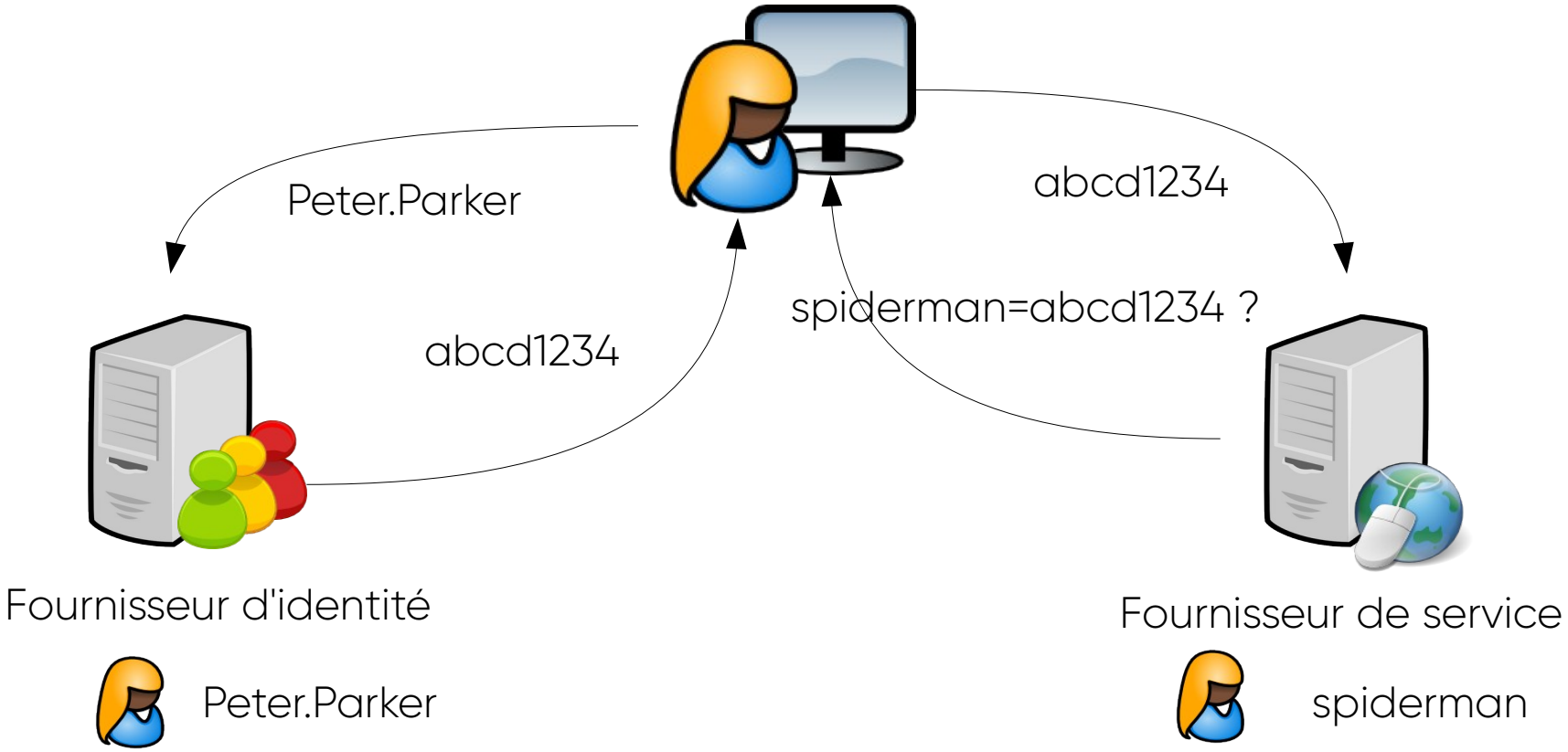
```
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli info

Num      : 88
Author   : clement
Author IP: localhost
Date     : Tue Dec 18 09:57:58 2018
Log      : Edited by lmConfigEditor
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli help
Usage: /usr/share/lemonldap-ng/bin/lemonldap-ng-cli <options> action <parameters>

Available actions:
 - help                          : print this
 - info                          : get currentconfiguration info
 - update-cache                  : force configuration cache to be updated
 - get    <keys>                 : get values of parameters
 - set    <key> <value>          : set parameter(s) value(s)
 - addKey <key> <subkey> <value> : add or set a subkey in a parameter
 - delKey <key> <subkey>         : delete subkey of a parameter

See Lemonldap::NG::Common::Cli(3) or Lemonldap::NG::Manager::CLi(3) for more
root@ader-worteks:~# /usr/share/lemonldap-ng/bin/lemonldap-ng-cli set ldapServer 'ldap://ldap.example.com'
```

Logiciel libre

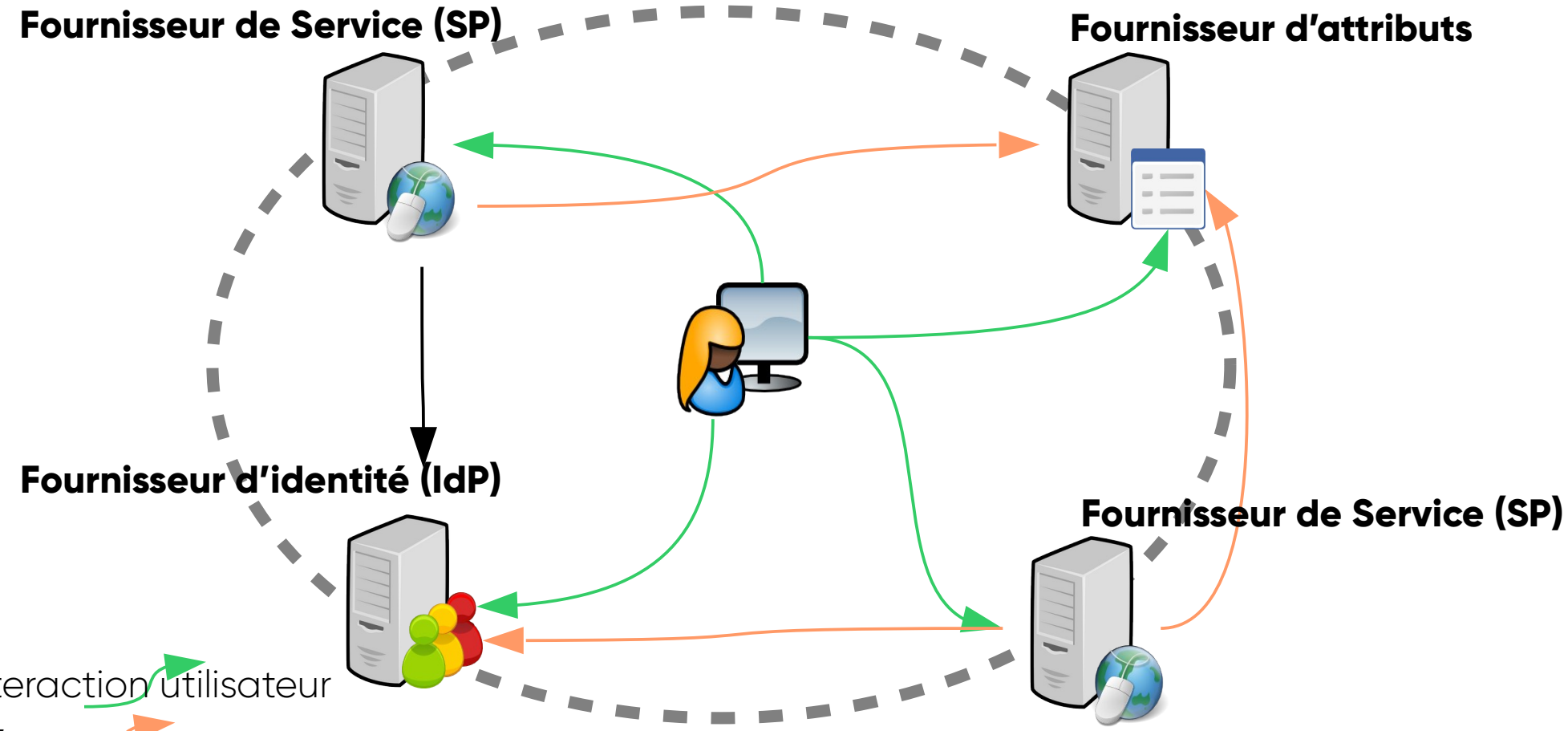
- Licence GPL
- Projet OW2
- Forge : https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng
- Site: https://lemonldap-ng.org
- « OW2 Community Award en 2014 »
- Composant SSO du projet FusionIAM : https://fusioniam.org/

Fédération d’identité

Fédération d'un compte



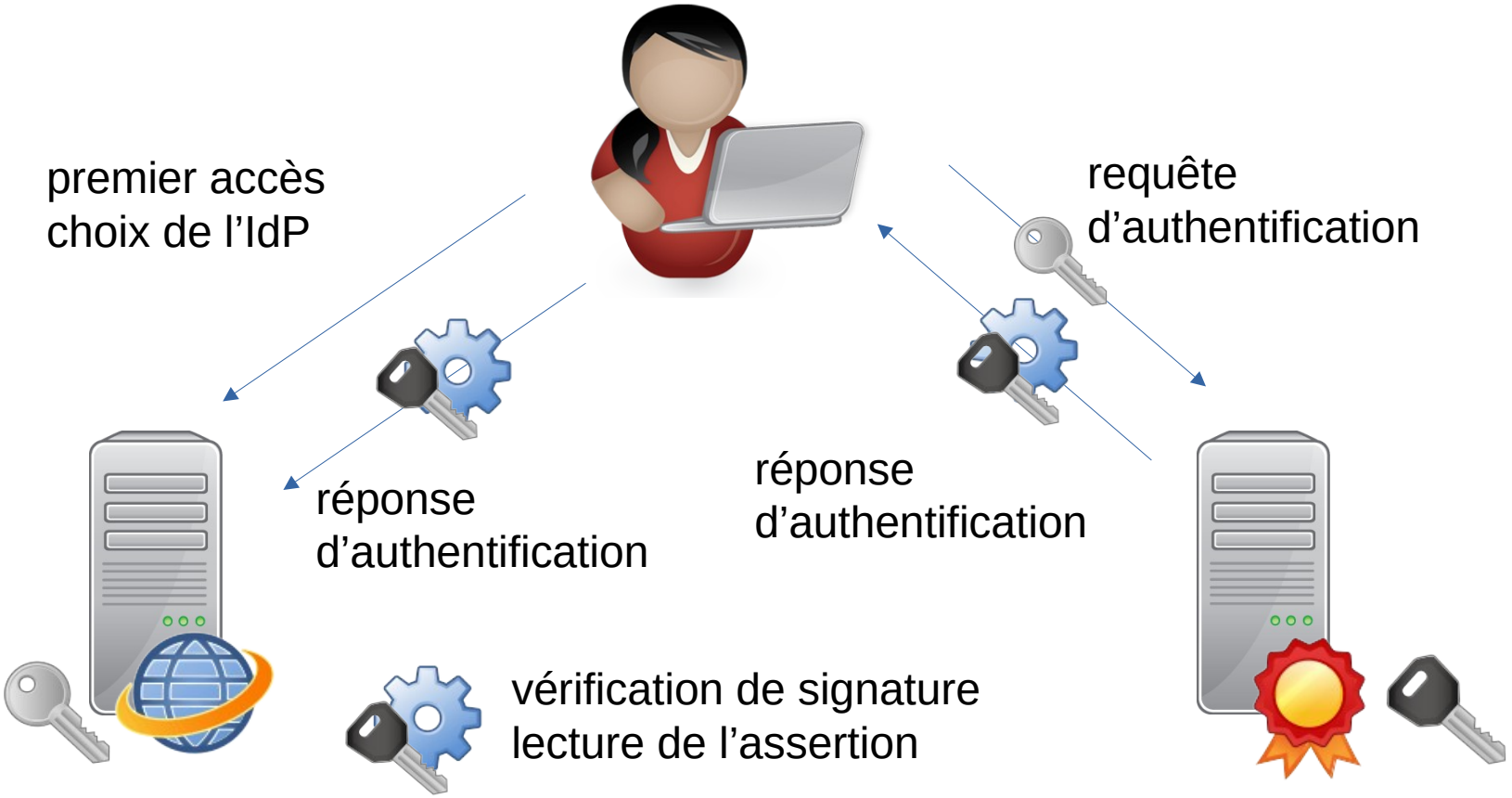
Cercle de confiance



Fédération et protocoles

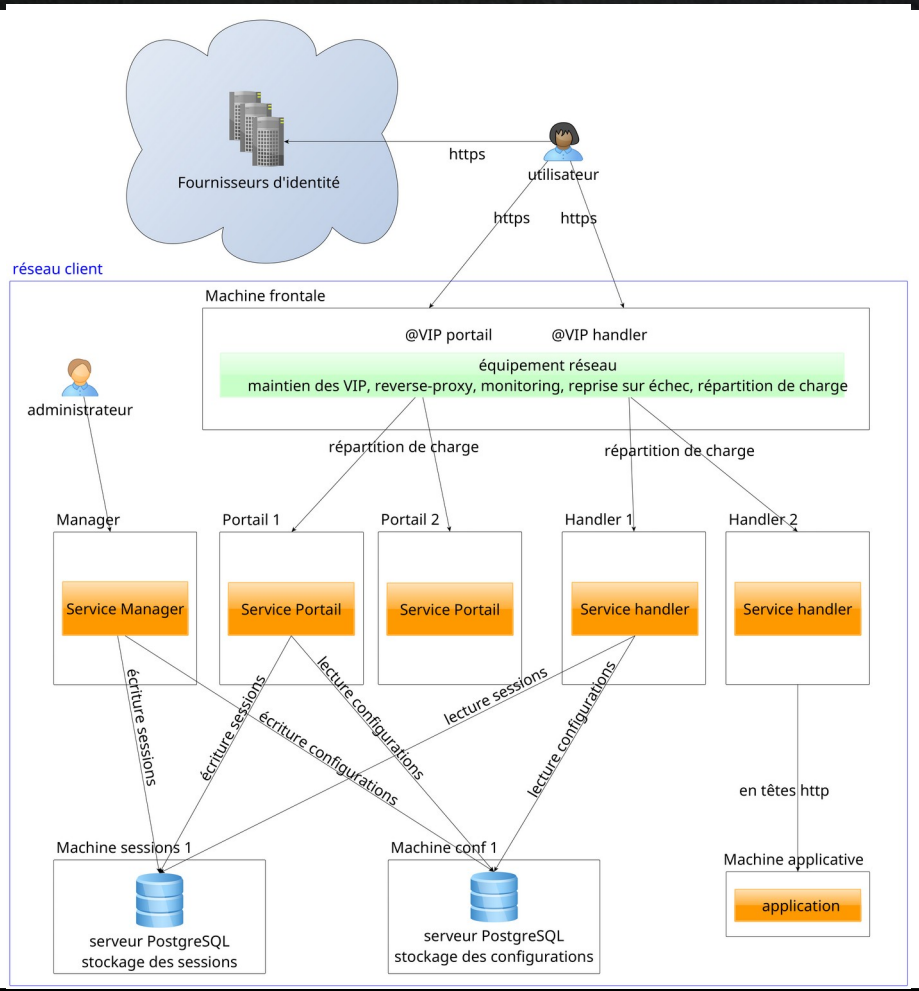
- fédération d'identité crée des **cercles de confiance** entre SP et IdP
- les comptes des SP peuvent être fédérés avec le compte de l'IdP (= compte principal)
- chaque SP dialogue avec l'IdP pour s'assurer que l'utilisateur est bien reconnu sur le cercle de confiance
- notion de fédération apparue avec SAML
- Aujourd'hui, par abus de langage, les protocoles de fédération d'identité sont ceux qui permettent l'**interconnexion d'une application** avec un SSO :
  - CAS
  - SAML
  - OpenID Connect

cinématique de connexion SAML



Mise en place chez [client]

Architecture



Démarche

- Étude comparative Keycloak vs LemonLDAP::NG
  - sélection de LemonLDAP::NG. Critères déterminants :
    - gestion intégrée des applications protégées par en-têtes HTTP
    - pas de stockage des données utilisateurs dans un contexte de pure fédération (respect de la RGPD)
    - support du produit
    - logiciel souverain
- Mise en place de l'environnement de qualification
- Mise en place de l'environnement de préproduction
- Mise en place de l'environnement de production

État des lieux

- Cas d'usage : utilisateurs issus des différents « Fournisseurs d'identité » accèdent à 2-3 applications fournies par le client
- Le portail LemonLDAP::NG joue le rôle de passerelle protocolaire :
  - interconnexion aux fournisseurs d'identité en SAML
  - interconnexion aux applications par Reverse-proxy (en-têtes HTTP)
- Données personnelles issues des fournisseurs transférées aux applications au cas par cas, suivant ce dont elles ont besoin
- État des lieux :
  - Interconnexion avec le fournisseur d'identité « principal » terminée
  - Interconnexion avec un second fournisseur prévu dans l'année

Difficultés rencontrées

- Mobilisation des acteurs : fournisseurs d'identité, responsables applicatifs, infrastructure, service de certificats
- Fourniture de documents « Contrat de service » aux applicatifs pour normaliser l'interconnexion au SSO
- Organisation d'ateliers pour aider les applications à la « SSOisation »

Bilan

Projet très positif :

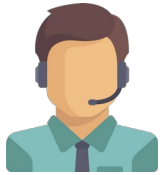
pour l'utilisateur :

- ouverture de nouveaux services applicatifs
- amélioration du parcours (pas de ré-authentification)

pour les développeurs applicatifs :

- externalisation complète de la fonction d'authentification (plus de problématique de changement de mot de passe,...)

pour le client :



- ouverture de nouveaux services sécurisés (via l'interconnexion SAML) sans stockage de données personnelles
- logiciel LemonLDAP::NG libre, facile à maintenir et faire évoluer

Worteks

make IT work, make IT free

Merci


info@worteks.com


@worteks_com


linkedin.com/company/worteks