IDENTITY DAYS

27 octobre 2022 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

Systancia

IDENTITY DAYS

Authentification multi-facteurs et gestion du risque avec du logiciel 100% libre

Clément OUDOT

Vorteks
make IT work, make IT free

IDENTITY DAYS

Clément OUDOT

Identity Solutions Manager

PRO :

- Worteks
- LemonLDAP::NG
- LDAP Tool Box
- LDAP Synchronization Connector
- FusionIAM
- W'Sweet
- W'IDaaS

PERSO :

- KPTN
- DonJon Legacy
- Improcité
- Les Amis Causent

AGENDA DE LA CONFÉRENCE

Introduction en chanson

- Single Sign On
- MFA et gestion du risque
- Mise en pratique avec LemonLDAP::NG

Vorteks

make IT work, make IT free

Service

Infrastructures hétérogènes et complexes, cloud, 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 des accès

Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

ONLYOFFICE

Collabora Online

Worteks

make IT work, make IT free

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

IDENTITY DAYS

La chanson du MFA

Je veux vous parler
du SSO de demain
Où le vol des mots de passe
Ne servira presque à rien
Je veux vous parler
De la mise en place
Du MFA

En fonction du profil
De ton navigateur
On pourra te demander
Un second facteur

Une clé physique,
un code unique
L'empreinte de ton doigt

Des applications mobiles pour ton **TELEPHONE**
Des protocoles standards basés sur du JSON

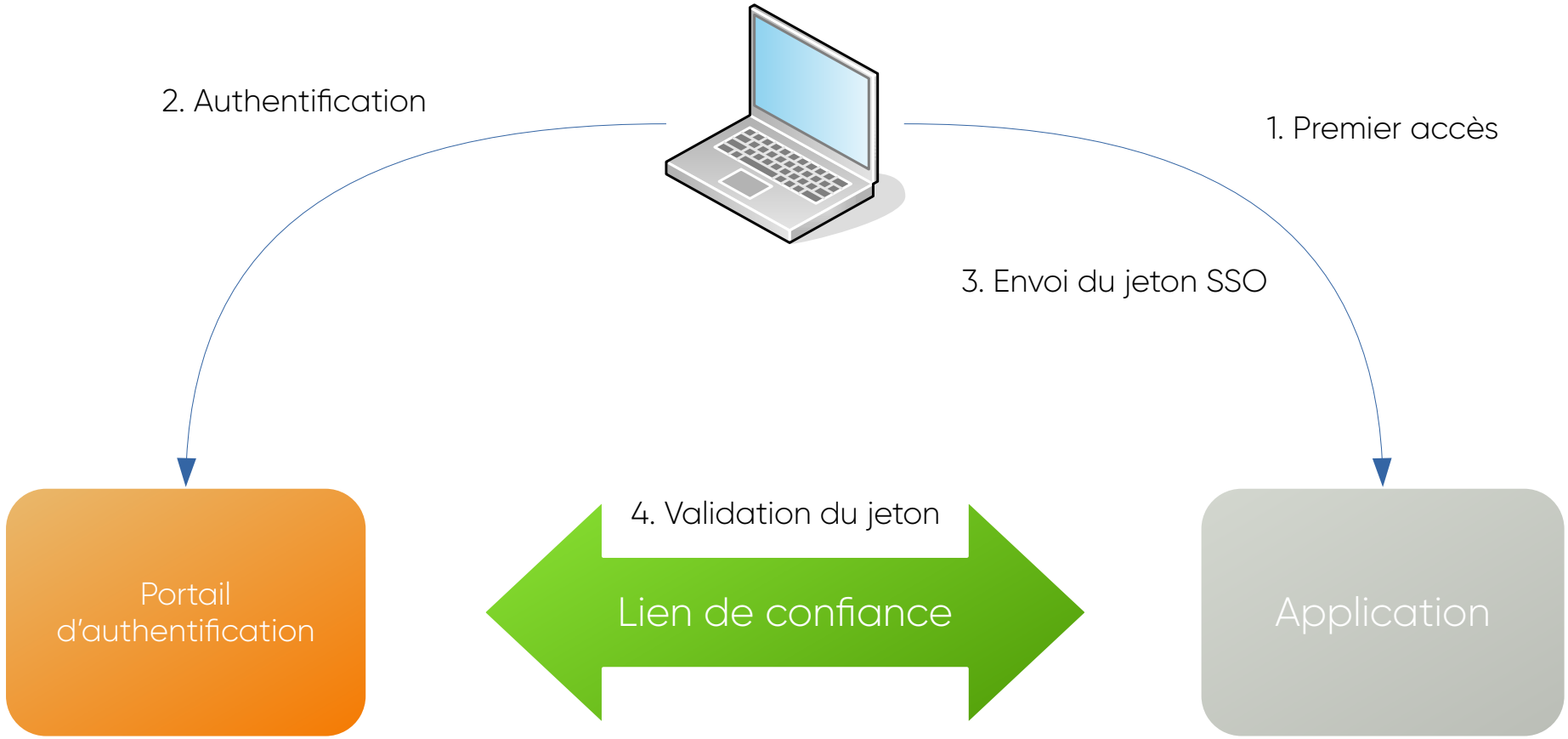
Pour t'authentifier
Tu pourras dès demain
En plus de ton mot de passe
Utiliser d'autres moyens

La clé WebAuthn
Tu la tiens dans ta main
Mais si tu laisses quelqu'un
Prendre ce que tu détiens
C'est la fin…

IDENTITY DAYS

Single Sign On

Fonctionnement du SSO

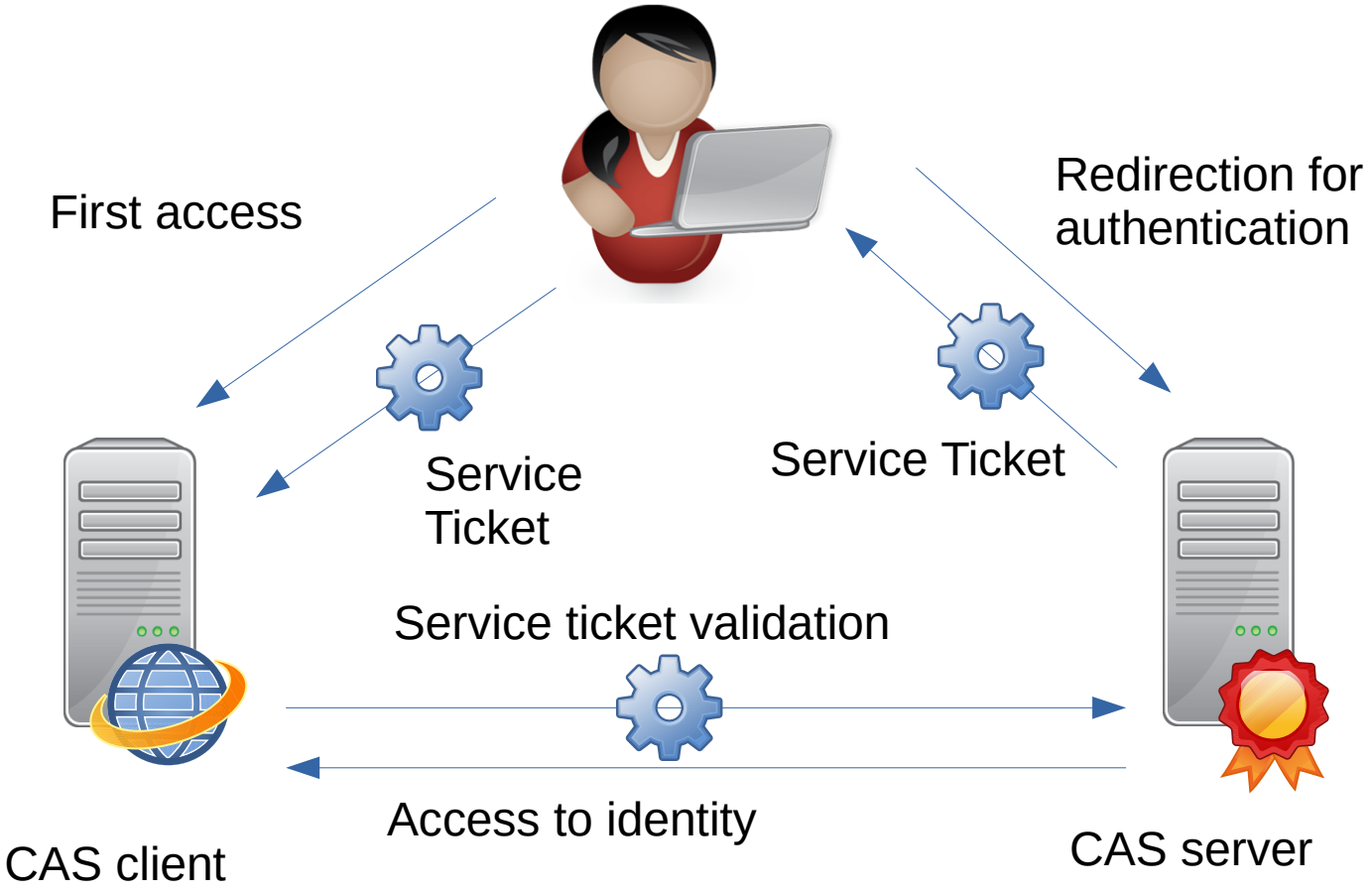


You Only Log Once

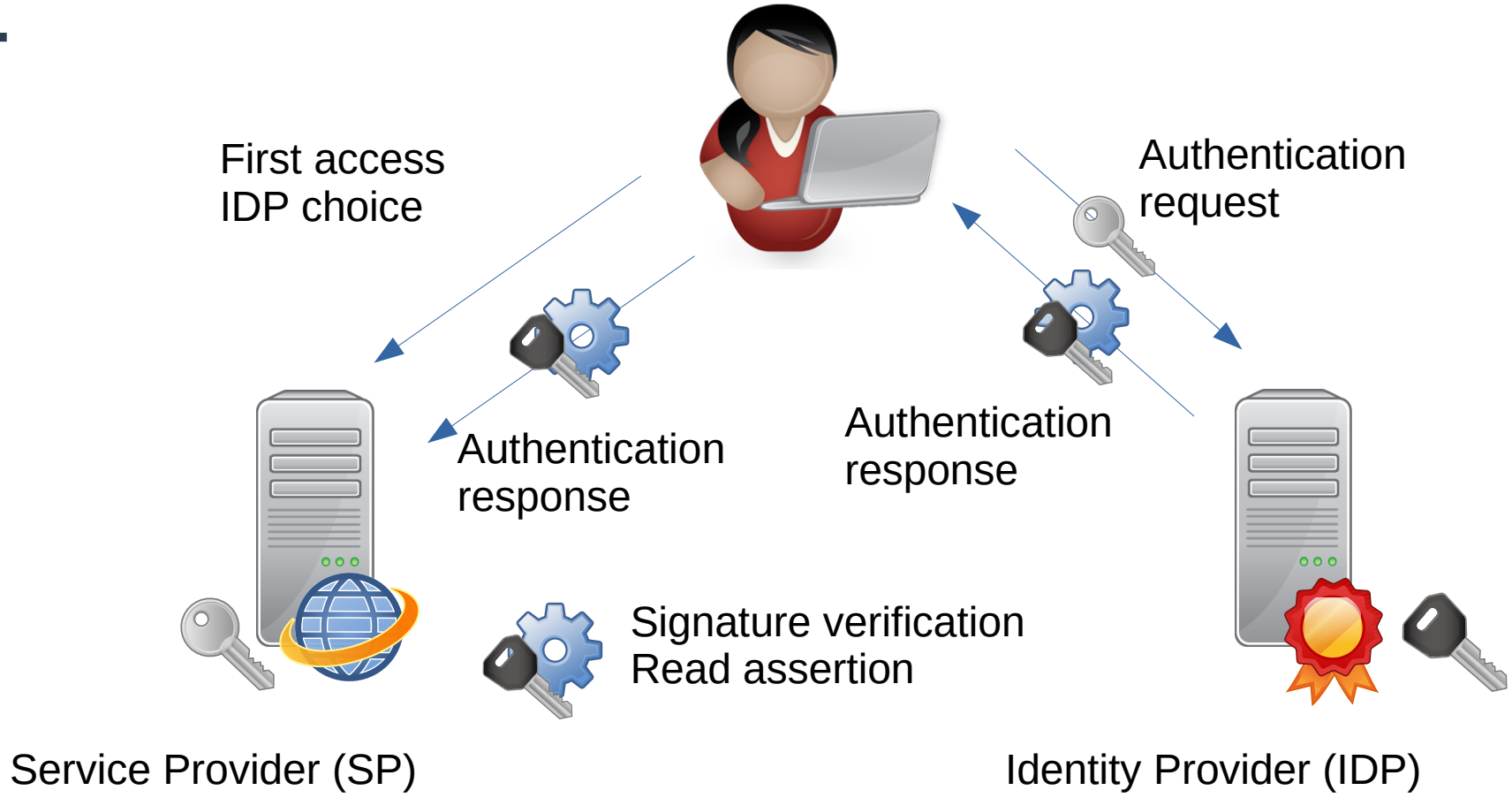
Des protocoles standards

- CAS (Central Authentication Service)
- SAML (Security Assertion Markup Language)
- OpenID Connect

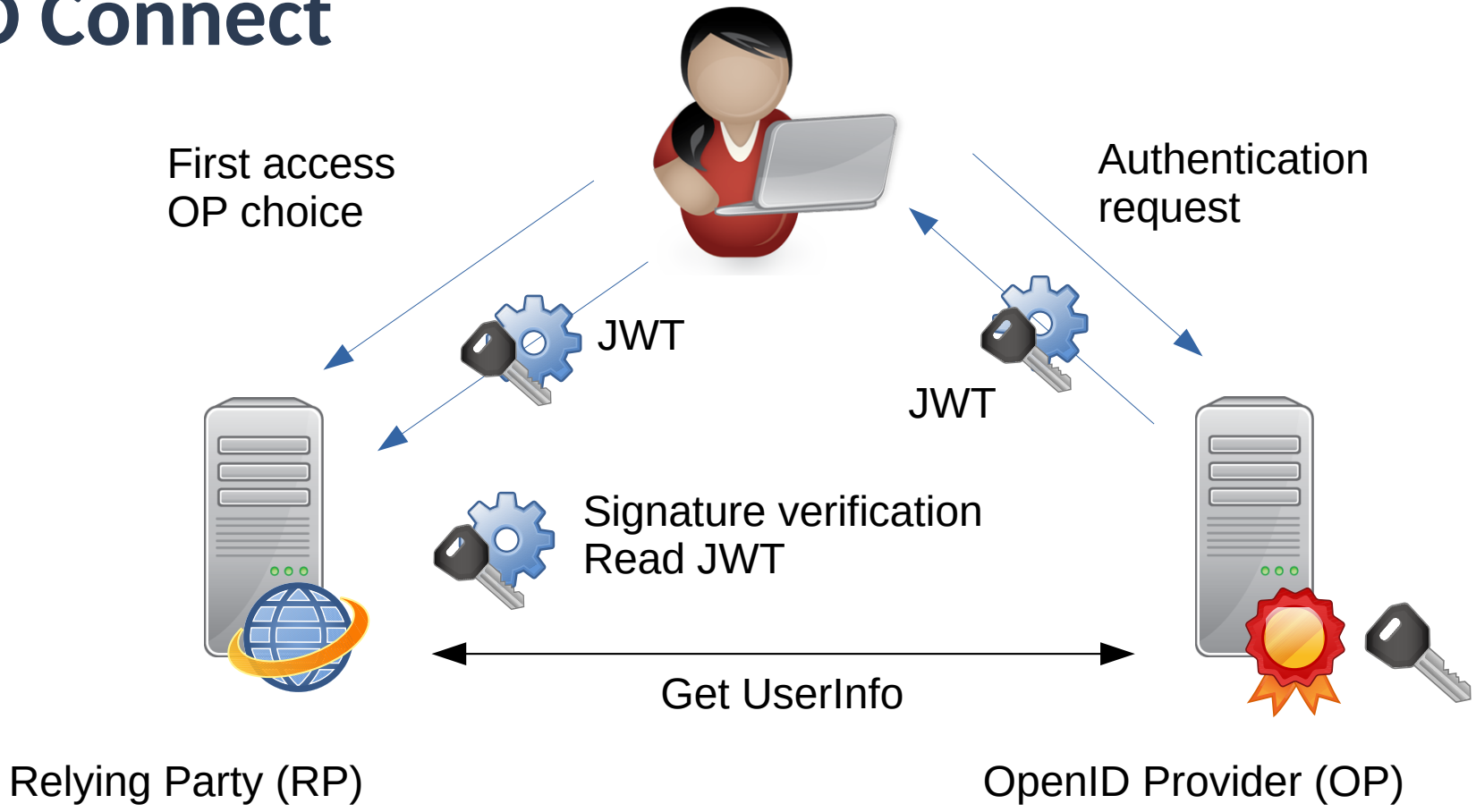
CAS


First access
Redirection for authentication
Service Ticket
Service Ticket
Service ticket validation
Access to identity
CAS client
CAS server

SAML


First access
IDP choice
Authentication
request
Authentication
response
Authentication
response
Signature verification
Read assertion
Service Provider (SP)
Identity Provider (IDP)

OpenID Connect



IDENTITY DAYS

MFA et gestion du risque

MFA : Multi Factor Authentication

2FA : Second Factor Authentication

Types de facteurs d'authentification

- Facteur mémoriel (ce que l'on sait) : mot de passe, nom de son premier instituteur, …
- Facteur matériel (ce que l'on possède) : clé USB, téléphone, carte d'identité électronique, …
- Facteur corporel (ce que l'on est) : empreinte digitale, voix, vitesse de frappe au clavier, …

Authentification forte ?

En 2021, l'ANSSI distingue l'authentification forte de l'authentification multifacteur : l'authentification forte, dans cette définition, repose sur des mécanismes cryptographiques jugés forts mais pas nécessairement sur plusieurs facteurs d'authentification.

https://fr.wikipedia.org/wiki/Authentification_forte

Principaux seconds facteurs utilisés

- Code à usage unique, transmis par mail, SMS, chat…
- Code à usage unique HOTP / TOTP (application mobile ou poste de travail)
- Applications mobiles spécifiques (mode PUSH)
- Clés FIDO2 / WebAuthn

Facteurs de risques

- Connexion en dehors du réseau local, en dehors du pays, du continent, via VPN, via Proxy, etc.
- Connexion depuis un nouveau périphérique
- Connexion en dehors des horaires de travail

Authentification basée sur le risque
Risk based authentication / RBA

On exige un second facteur en fonction du niveau de risque de la connexion

IDENTITY DAYS

Mise en pratique avec LemonLDAP::NG

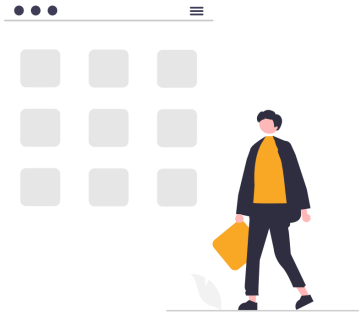
LemonLDAP::NG

- Logiciel libre sous licence GPL, créé en 2005
- Projet OW2
- Certifié France Connect

https://lemonldap-ng.org/

Fonctionnalités principales

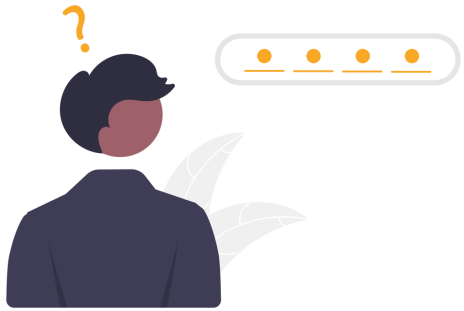
SSO & Access Control



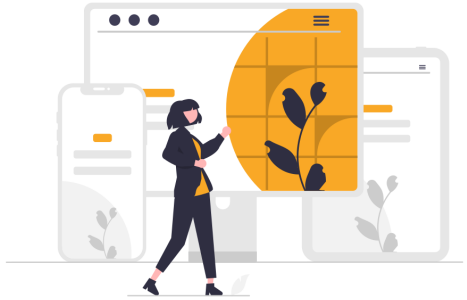
Application menu

CAS / SAML / OIDC

Second Factor (2FA)

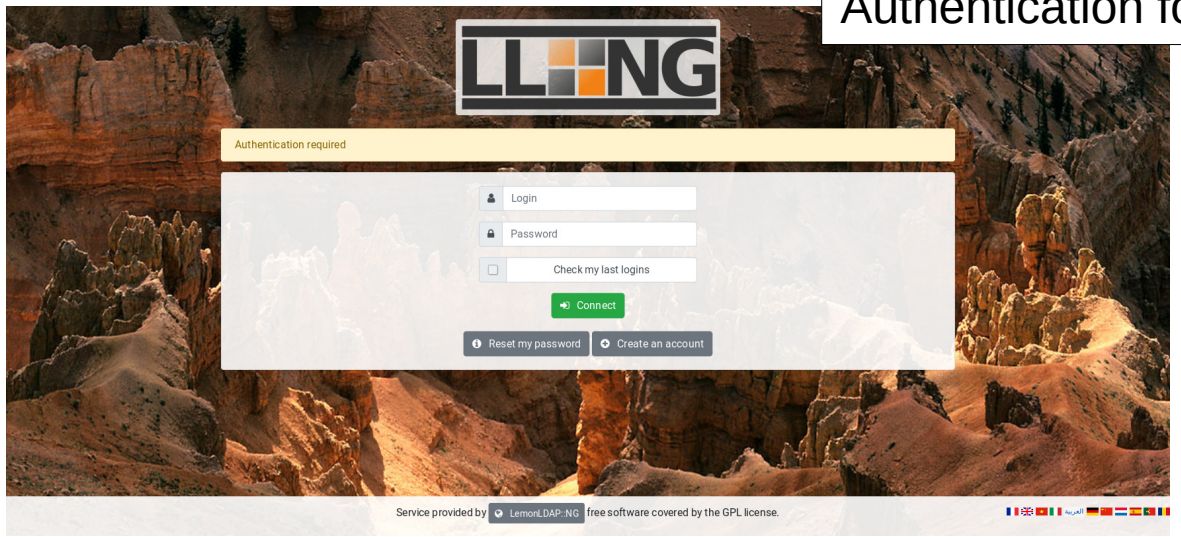


Password management

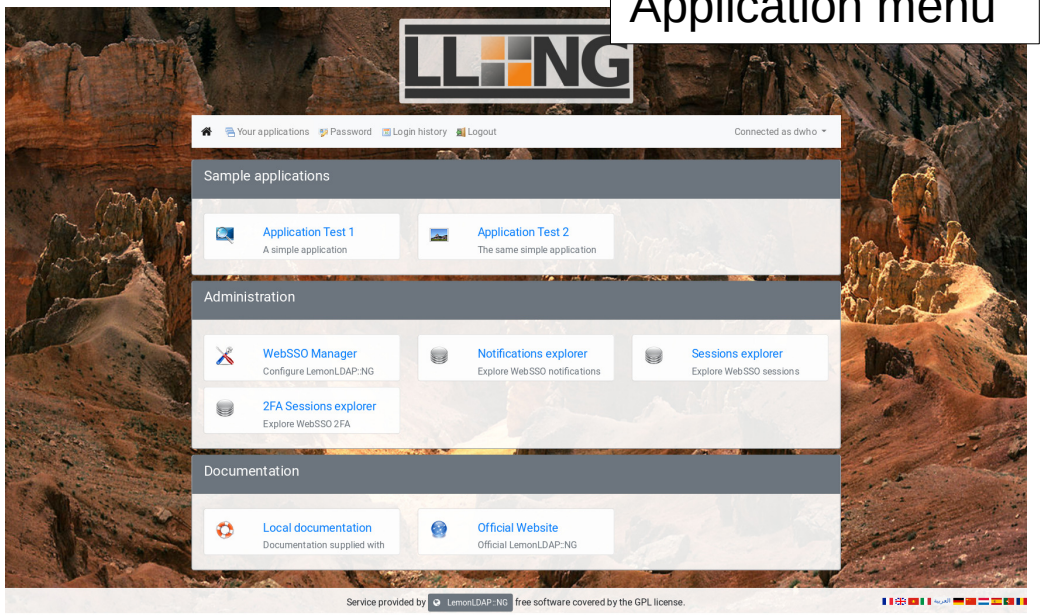


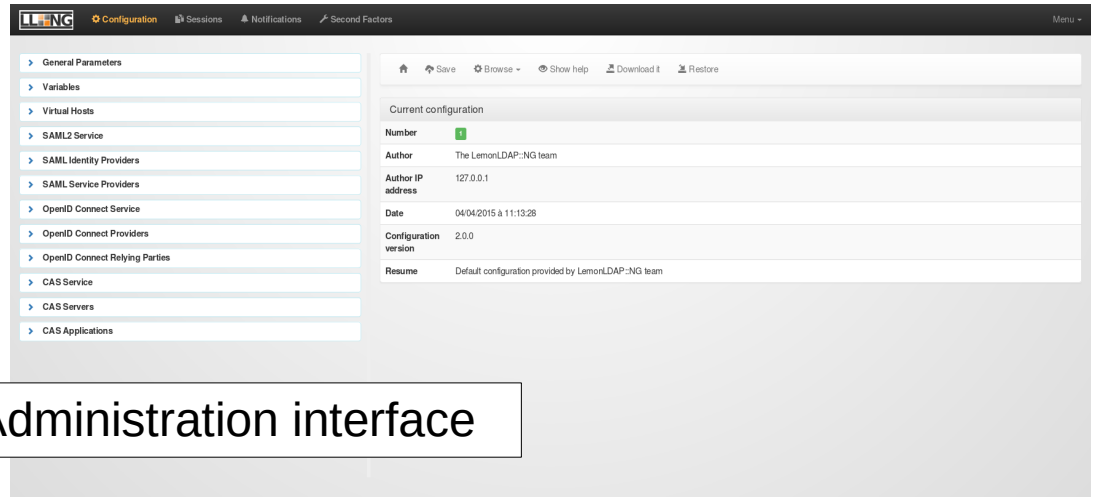
Graphical customization

Authentication form



Application menu

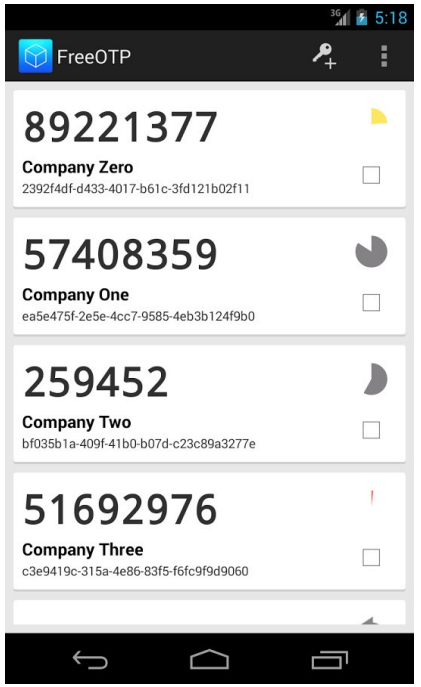




Administration interface

Modules de seconds facteurs natifs

- Envoi d'un code par mail
- Envoi d'un code par commande externe (API SMS)
- TOTP
- WebAuthn
- REST
- Radius



Modules en cours d'intégration

- Phrase de passe
- Envoi d'un mail (adresse mail saisie par l'utilisateur)
- Envoi d'un SMS (numéro de téléphone saisi par l'utilisateur)

Gestion du risque

- Utilisation de modules de détection de risque, qui vont renseigner les variables *_riskLevel* and *_riskDetails*

- Déclenchement des modules de seconds facteurs par des règles :

has2f('OTP') and $_riskLevel > 0

- Refus d'ouverture de session par des règles :

$_riskLevel < 2

Extension du logiciel

- Implémentation de son propre module de gestion de risque
- Utilisation de solutions externes de second facteur (via Radius ou commande spécifique)
- Implémentation de son propre module de second facteur, en se basant sur les bibliothèques fournies :
  - Lemonldap::NG::Portal::Lib::2fDevices
  - Lemonldap::NG::Portal::Lib::Code2F

Démonstration

- Utilisation d’un code TOTP
- Activation de l’envoi d’un code par mail en fonction du navigateur utilisé

IDENTITY DAYS

27 octobre 2022 - PARIS

@IdentityDays #identitydays2022

Merci à tous nos partenaires !

Microsoft

Vorteks
make IT work, make IT free

BeyondTrust

ermetic

Exakis Nelite
MagellanPartners

FUSION DIRECTORY

jumpcloud

KERBEROS CONSULTING

Kleverware

METSYS

okta

ONE IDENTITY by Quest

ManageEngine

SailPoint

semperis

SILVERFORT

Systancia