Vorteks

make IT work, make IT free

Introduction au **2FA**/**MFA** et mise en application pratique avec le logiciel libre **LemonLDAP::NG**

Séminaire sur la double authentification
Lyon, le 25 juin 2024

$ ldapwhoami

Clément OUDOT
Identity Solutions Manager
Worteks

@clementoudot

LemonLDAP::NG
LDAP Tool Box
LDAP Synchronization Connector
FusionIAM

KPTN
DonJon Legacy
Improcité
Les Amis Causent

Worteks

Société d’expertise et d’édition de logiciels libres et Open Source.

Contributeurs actifs de différents logiciels libres comme LSC, LemonLDAP::NG ou LDAP Tool Box.

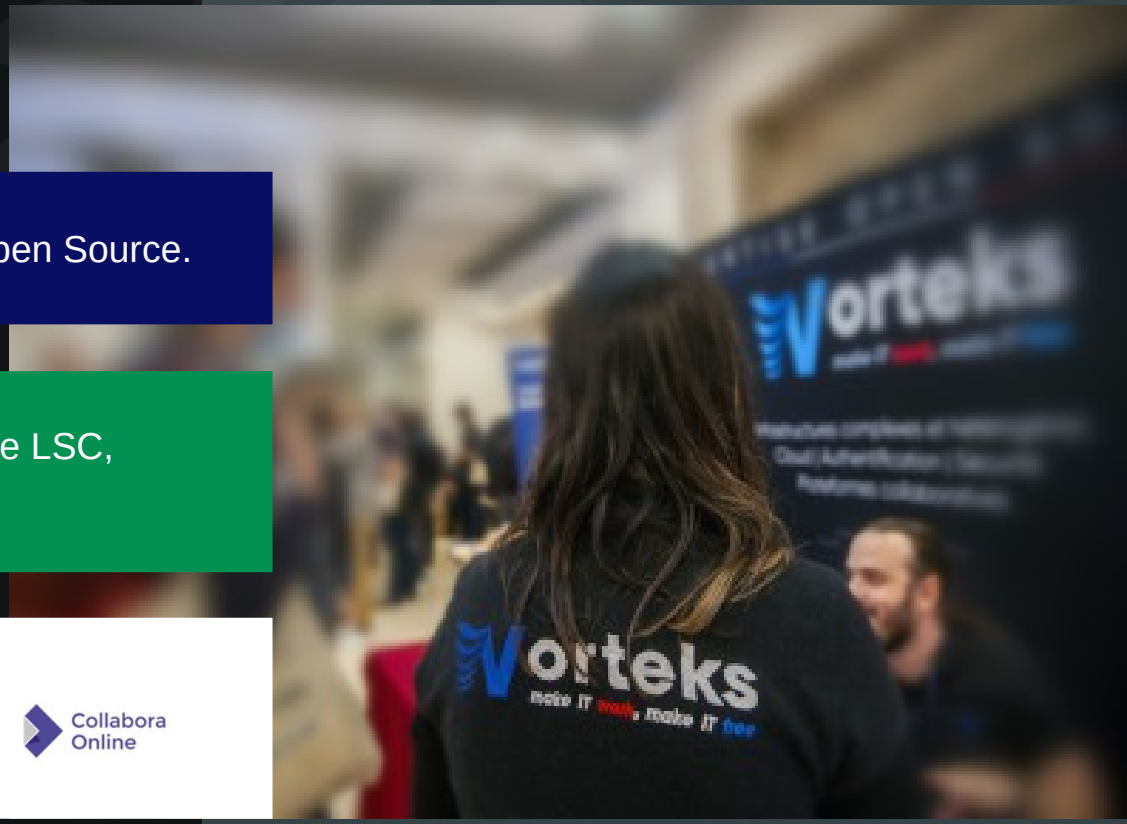
Partenaires

Red Hat Advanced Business Partner Reseller

BlueMind

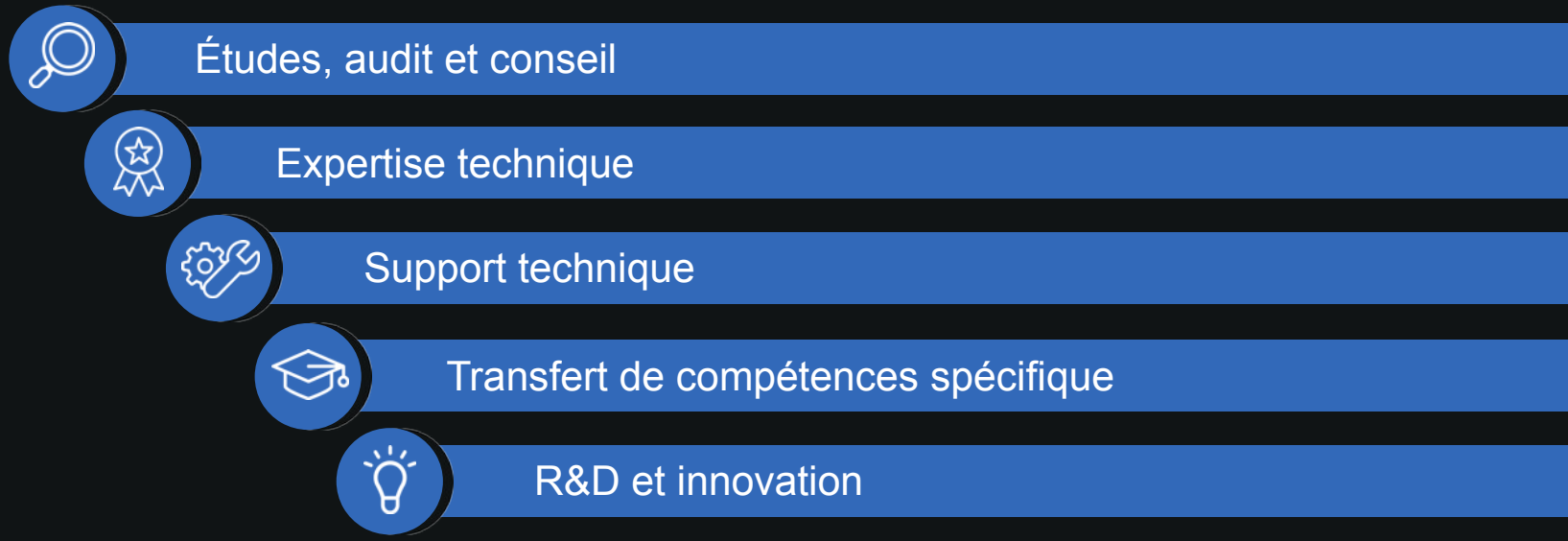
ONLYOFFICE

Collabora Online



Une offre globale

Infrastructures hétérogènes et complexes, troubleshooting, cloud, mail, identité, authentification, securité…
Worteks intervient sur une multitude de problématiques associées à votre système d'information.



Des solutions adaptées

Worteks utilise son savoir-faire pour mettre à la disposition de ses clients des solutions packagées, intégralement composées des briques majeures de l'écosystème Open Source

Ces solutions sont disponibles, au choix, **On Premise** ou en **SaaS** et en **PaaS** sur nos environnements

V'Sweet

Portail de travail collaboratif

V'IDaaS

Solution de gestion d'identités et d'accès

V'Opla

Solution de déploiement d'infrastructures complexes

Authentification multifacteur

Définitions

- **Authentification** : processus permettant à un système (application, serveur) de vérifier l'identité de l'acteur (utilisateur, machine) souhaitant y accéder.
- **Authentification forte** : l'authentification forte correspond à un mécanisme basé sur de la cryptographie et faisant intervenir un défi (challenge) étant différent à chaque authentification.
- **Authentification multifacteur** : consiste à exiger plusieurs facteurs de nature distincte pour authentifier un acteur. La nature de ces facteurs peut être :
  - Connaissance : ce que l'acteur sait (un mot de passe, une information personnelle)
  - Possession : ce que l'acteur possède (téléphone, clé, carte à puce)
  - Biométrie : ce que l'acteur est (appelé aussi facteur inhérent par l'ANSSI)

Mais on peut aussi dire...

MFA : Multi Factor Authentication

2FA : Second Factor Authentication

Envoi d'un code

- L'utilisateur s'authentifie sur un service
- Le service génère un code à usage unique (OTP = One Time Password)
- Ce code est transmis à l'utilisateur par un *moyen de confiance* :
  - Mail
  - SMS
  - Discussion instantanée
  - …
- L'utilisateur saisit le code reçu sur le service

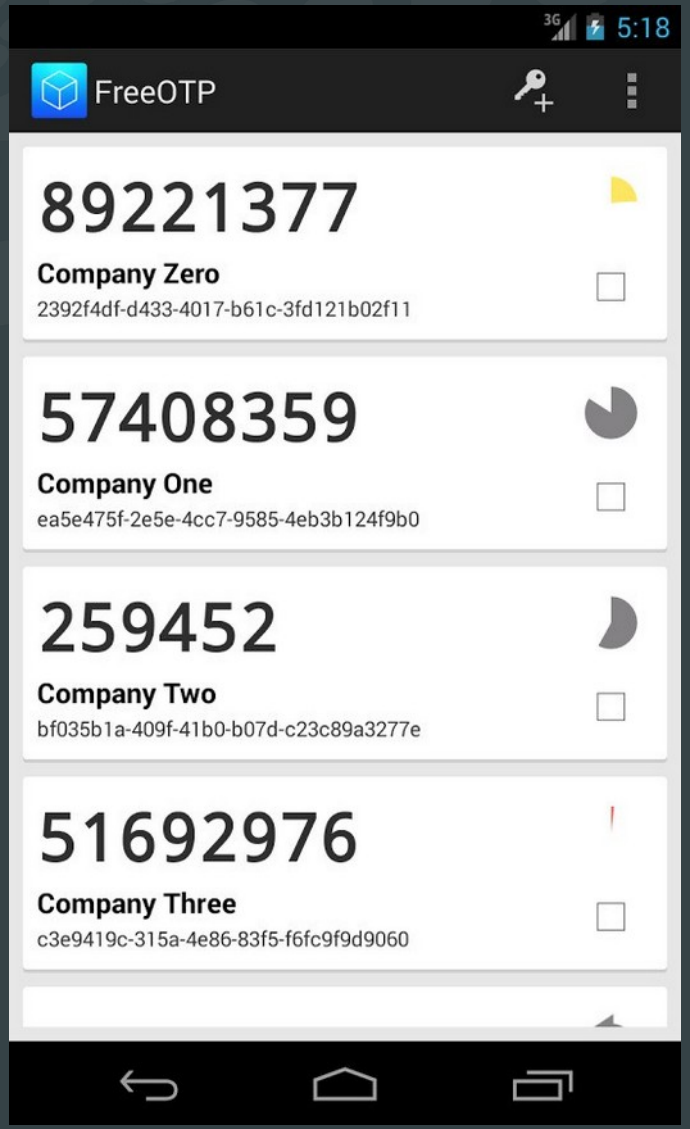
HOTP et TOTP

HOTP (RFC 4226)

HMAC-Based One-Time Password

TOTP (RFC 6238)

Time-Based One-Time Password



TOTP : un peu de maths...

- K : secret partagé
- T0 : Horodatage de départ
- TI : Intervalle de temps
- TC : Compteur de temps

  `floor((unixtime(now) – unixtime(T0)) / TI)`

- d : Nombre de chiffres souhaités
- Calcul du code :

  `( Truncate( SHA1(K ⊕ 0x5c5c… ‖ SHA1(K ⊕ 0x3636… ‖ TC)) ) & 0x7FFFFFFF ) mod 10d`

FIDO

Fast IDentity Online

https://fidoalliance.org

Définit les standards :

- U2F (Universal Second Factor)
- UAF (Universal Authentication Framework)
- CTAP (Client to Authenticator Protocols)

WebAuthn

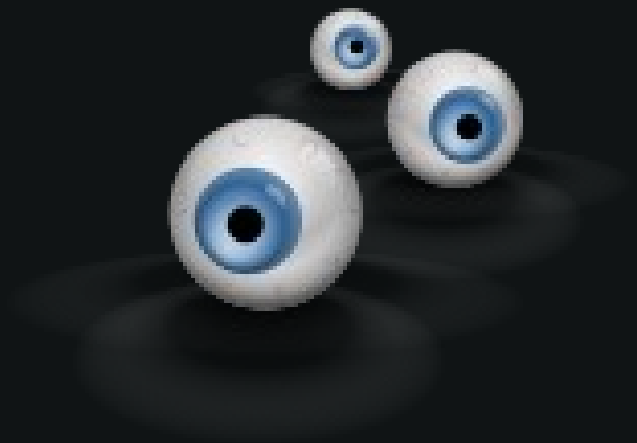
Norme du W3C

Définit l’extension javascript permettant aux navigateurs d’utiliser FIDO2

https://www.w3.org/TR/webauthn-2/

Autres systèmes

- Mode “push” : une application est installée sur le téléphone, il suffit de valider une notification
- Appel téléphonique
- Carte à code
- Biométrie...



Risque

Authentification basée sur le risque

Risk based authentication / **RBA**

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

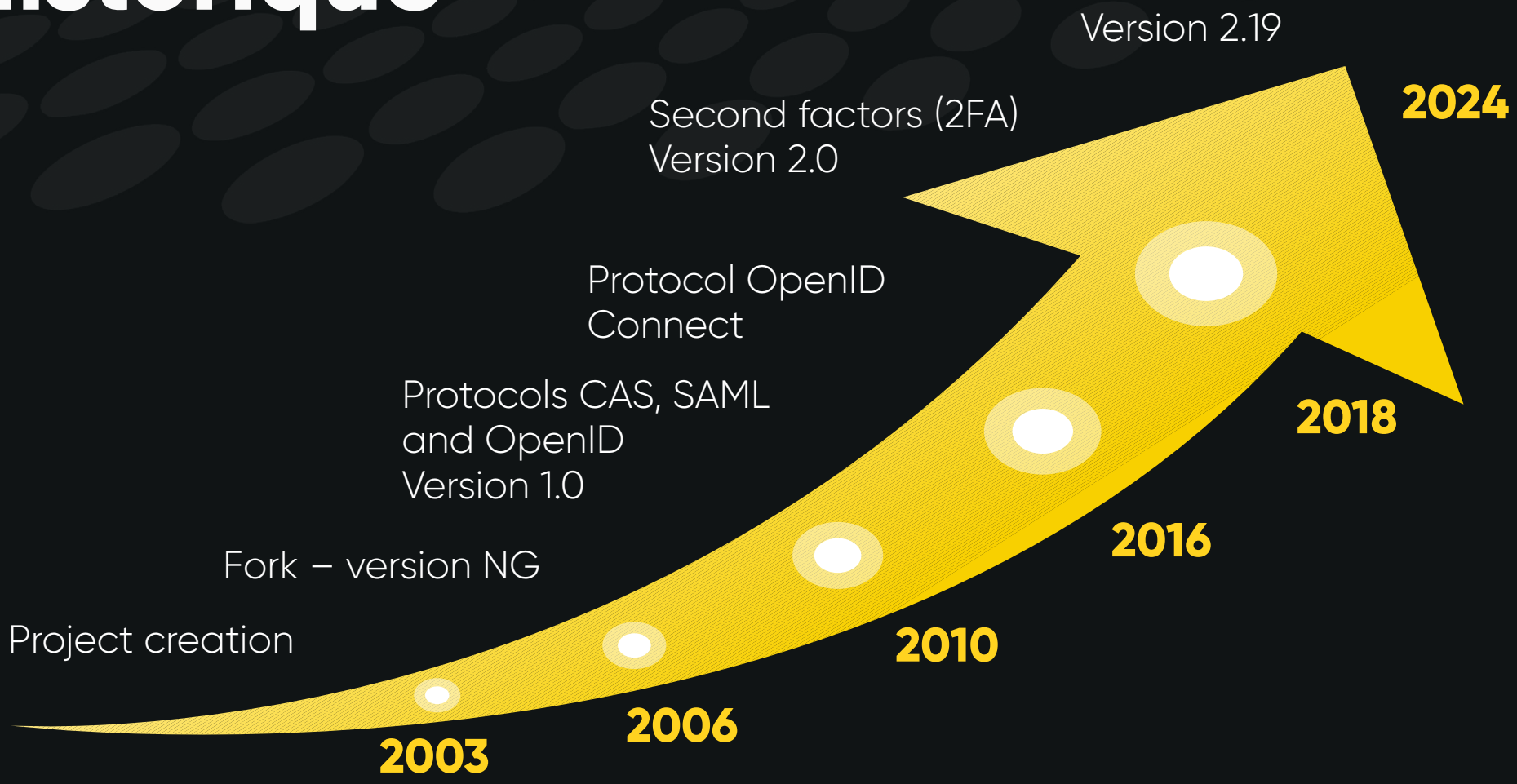
- Géographie (localisation par IP)
- Nouveau périphérique
- Horaires

Mise en pratique avec LemonLDAP::NG

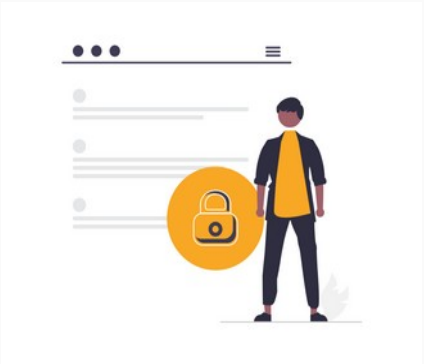
Logiciel libre

- 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

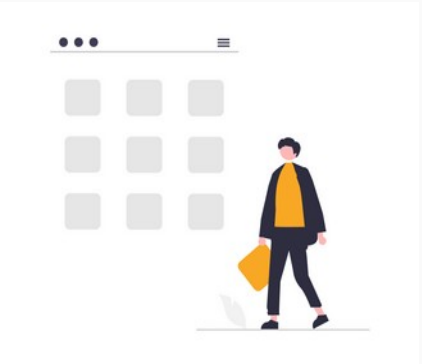
Historique


Version 2.19
2024
Second factors (2FA)
Version 2.0
Protocol OpenID
Connect
2018
Protocols CAS, SAML
and OpenID
Version 1.0
2016
Fork – version NG
2010
Project creation
2006
2003

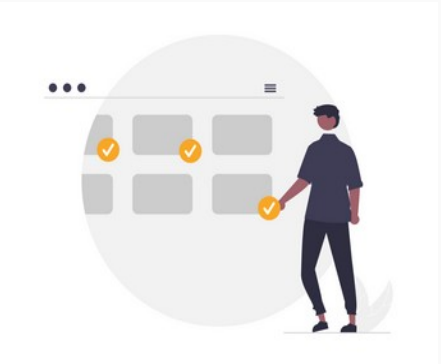
Fonctionnalités



SSO & Contrôle d'accès



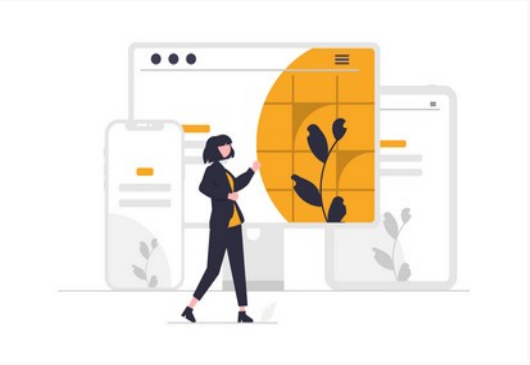
Menu des applications



CAS / SAML / OIDC

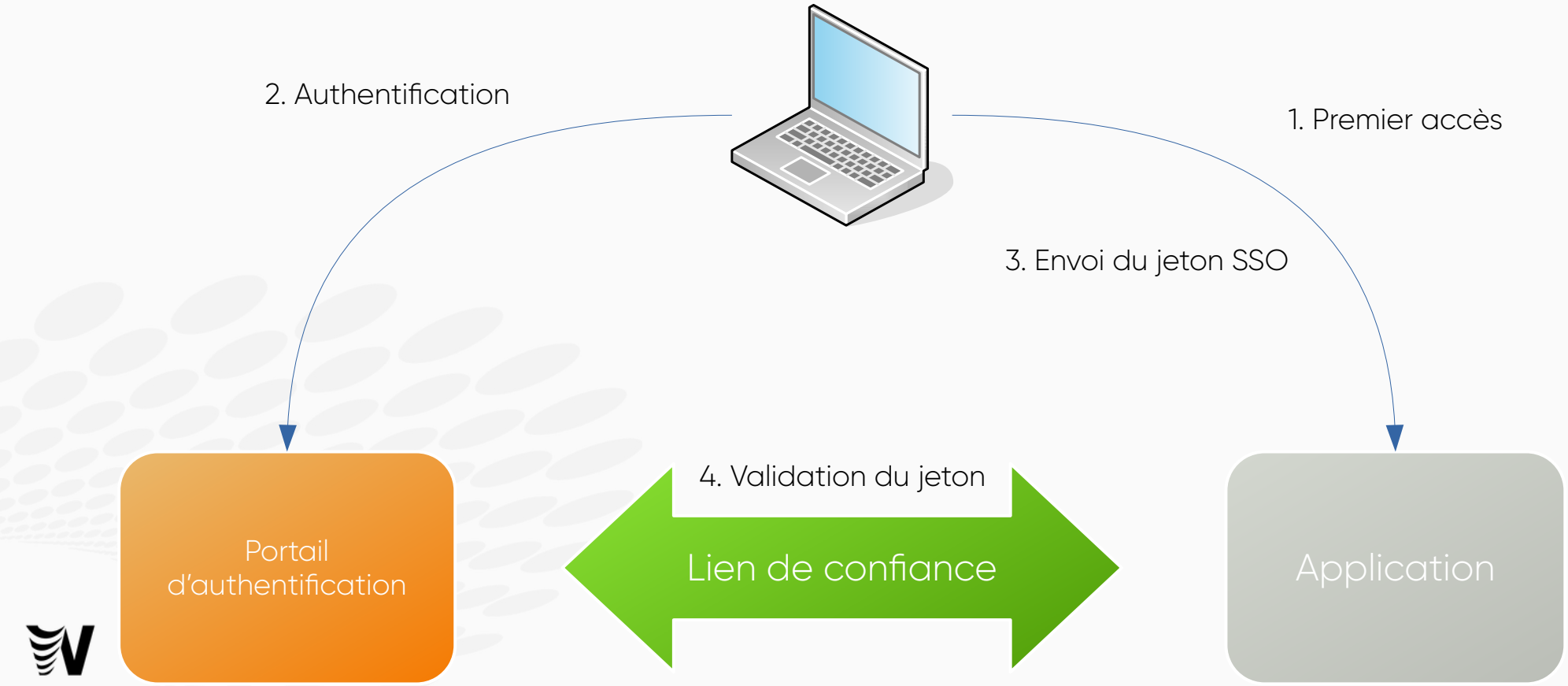
Second facteurs (2FA)

Gestion du mot de passe



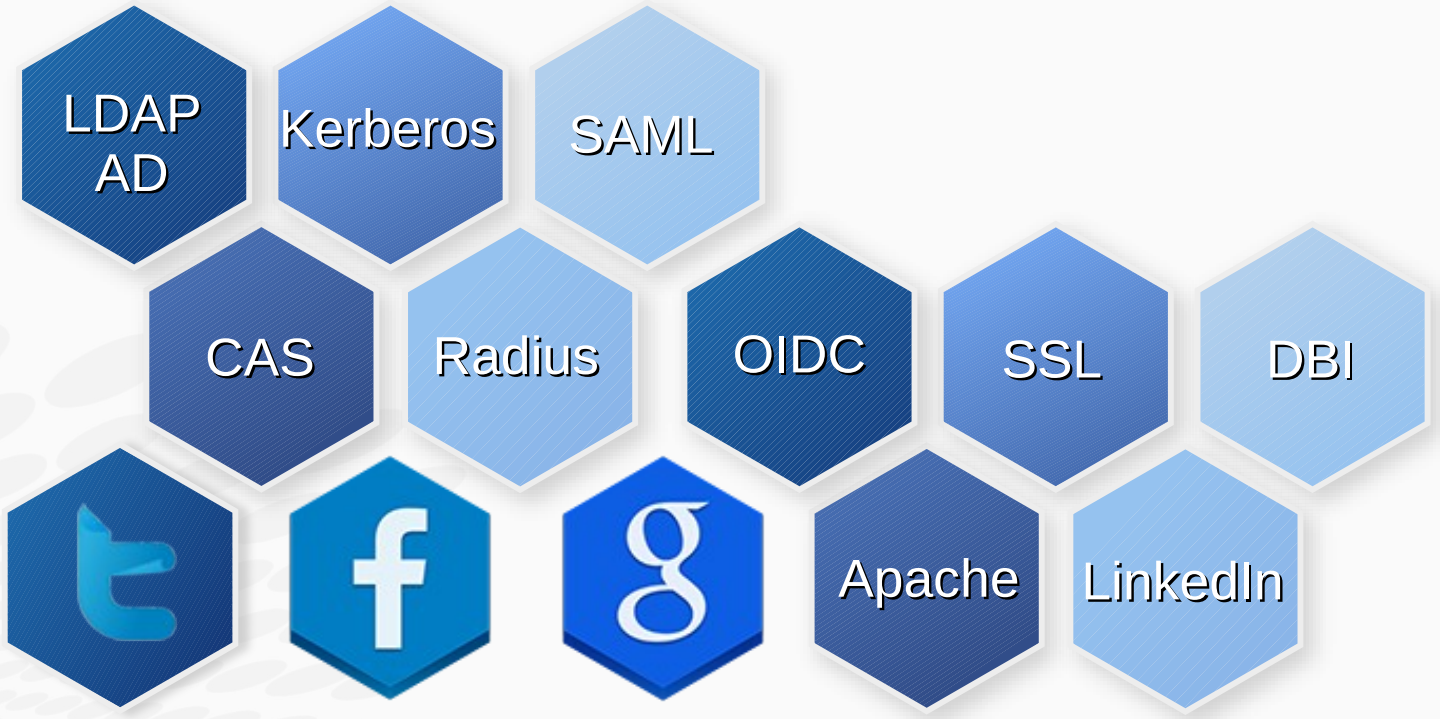
Personnalisation graphique

Principe du Single Sign On



You Only Log Once

Modules d'authentification



2FA

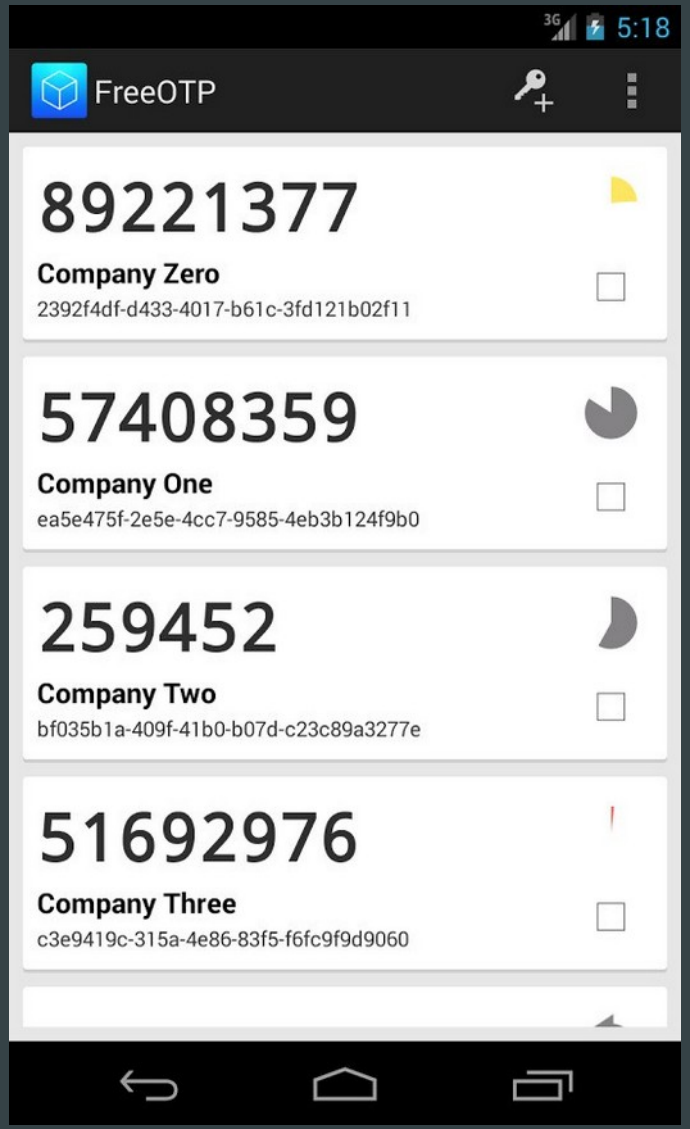
- TOTP
- WebAuthn/FIDO2
- Mail
- Externe (SMS, API, …)
- Radius
- Password/Passphrase

Fonctions avancées

- Plusieurs modules en simultané
- Activation par profils
- Auto enregistrement
- Activation à l’authentification ou lors d’accès à une application

Démo 1 – TOTP

- Activation du module 2FA TOTP
- Enregistrement d'un TOTP sur application mobile
- Connexion avec TOTP



Démo 2 – FIDO2

- Activation du module 2FA WebAuthn
- Enregistrement d’une clé WebAuthn
- Connexion avec FIDO2
- Inspection de la clé FIDO2

www.worteks.com

info@worteks.com
+33 1 84 20 86 47
worteks_com
worteks