



IDENTITY DAYS

7^{ème} édition

@IdentityDays
#identitydays2025

21 octobre 2025 - PARIS

IAM Open Source pour Active Directory



David COUTADEUR
Clément OUDOT

David COUTADEUR
Clément OUDOT

Experts Identité Worteks

Contributeurs LemonLDAP::NG,
LDAP Tool Box, LSC et
FusionIAM

AGENDA DE LA CONFÉRENCE

- Qui a les droits ?
- Protocole LDAP et Active Directory
- Des outils Open Source compatibles :
 - LemonLDAP::NG
 - LDAP Synchronization Connector
 - LTB Self Service Password
 - LTB White Pages
 - LTB Service Desk



Qui a les droits ?

Qui a les droits

On m'avait dit : "Te pose pas trop d'questions"
Active Directory comme annuaire il est bon
Il gère les groupes, les comptes et les mots de
passe

On l'interroge pour savoir ce qu'il se passe

Qui a les droits, qui a les droits,
Qui a les droits d' faire ça
Dans le système d'information
On veut son mail et puis son nom

Patrick BrueLDAP

On m'avait dit les annuaires sont tous pareils
Le protocole LDAP tout le monde le respecte
Mais pour AD, il faut s'adapter
Changer son code pour pouvoir renseigner

Qui a les droits, qui a les droits,
Qui a les droits d' faire ça
Dans le système d'information
On veut son mail et puis son nom

On passe sa vie à la merci,
d'Active Directory
Mais avec l'aide des logiciels libres
À l'administrer on y arrive

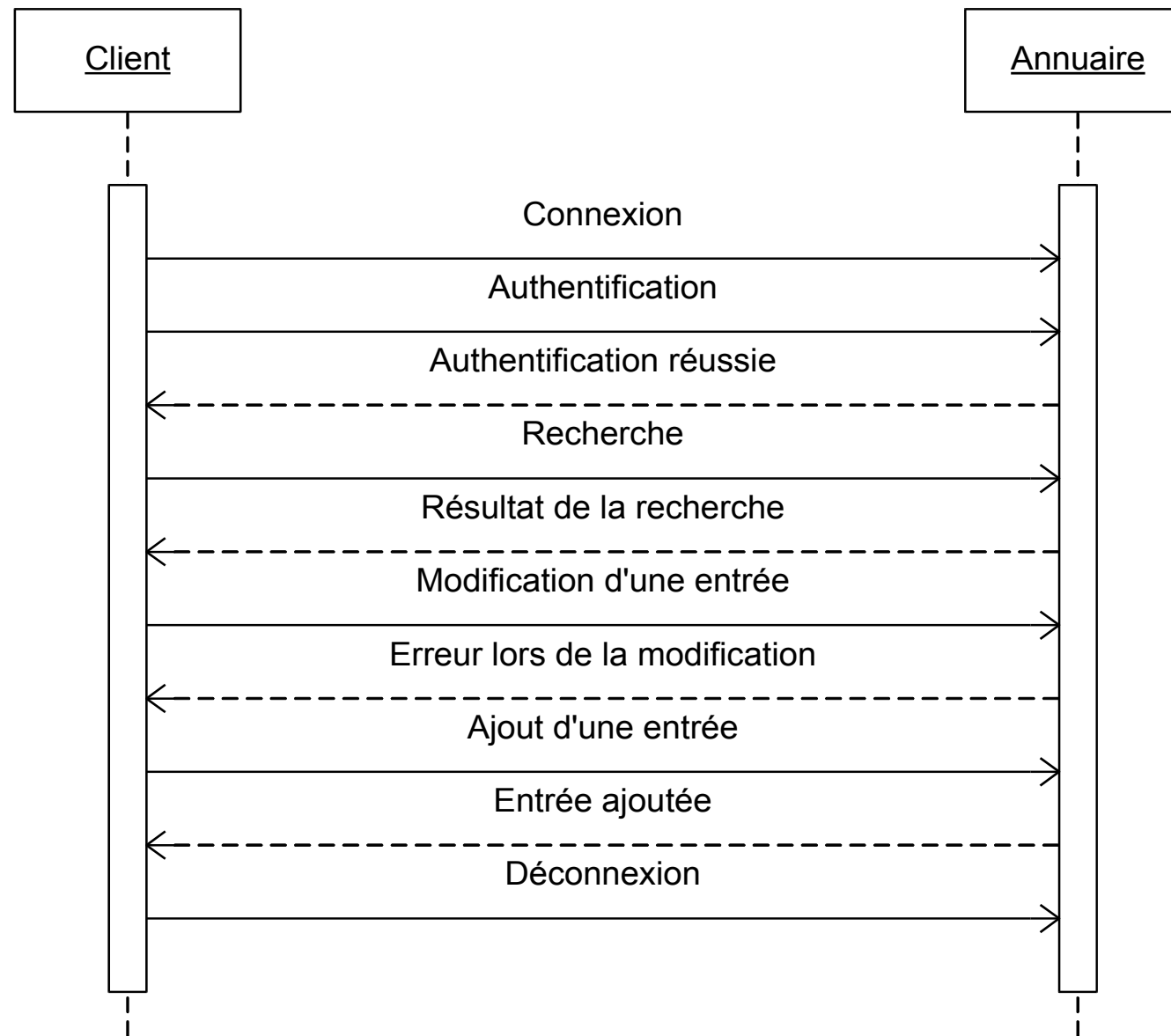


Protocole LDAP et Active Directory

Le protocole LDAP

- Lightweight Directory Access Protocol
- Issu de X.500, apparu à la fin des années 1980
- LDAP v3 publié en 1998
- Définitions du modèle de données et des opérations : authentification, recherches, comparaisons, écritures...







Les particularités AD

- Active Directory est, entre autres, un serveur LDAP
- Mais il prend quelques libertés avec le standard :
 - Stockage du mot de passe dans *unicodePwd* (en écriture seule)
 - Pagination par défaut à 1000 entrées
 - Pagination des valeurs d'attribut (range)
 - Classes d'objet "user" et "group"
 - Attributs spéciaux *userAccountControl*, *objectGuid*, *ObjectSid*
 - Date = nb d'intervalles de 100ns depuis le 1er janvier 1601

 **Il faut adapter son code à AD**



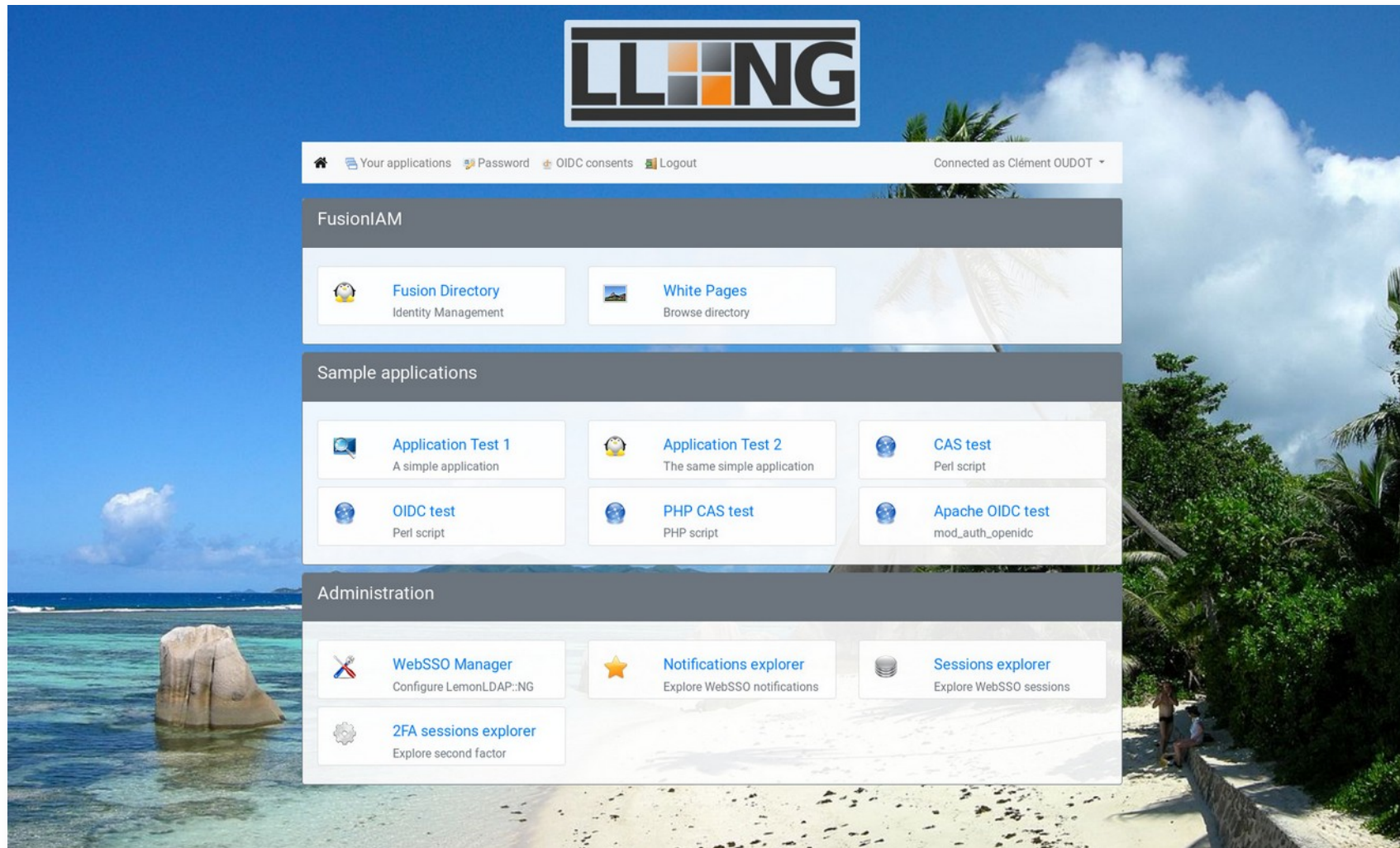
Des outils Open Source compatibles

On peut faire de l'Open Source avec AD ?

- **Active Directory n'est pas Open Source** et ne peut s'exécuter que sur un serveur Windows
- Il existe des alternatives Open Source à AD, mais ce n'est pas l'objet de cette présentation
- Les outils Open Source mentionnés ici peuvent remplacer d'autres logiciels propriétaires, comme ADFS, SailPoint, Okta...
- En plus d'être libres, ils sont disponibles **gratuitement**
- Du **support** est disponible via des sociétés d'expertise comme **Worteks**

LemonLDAP::NG

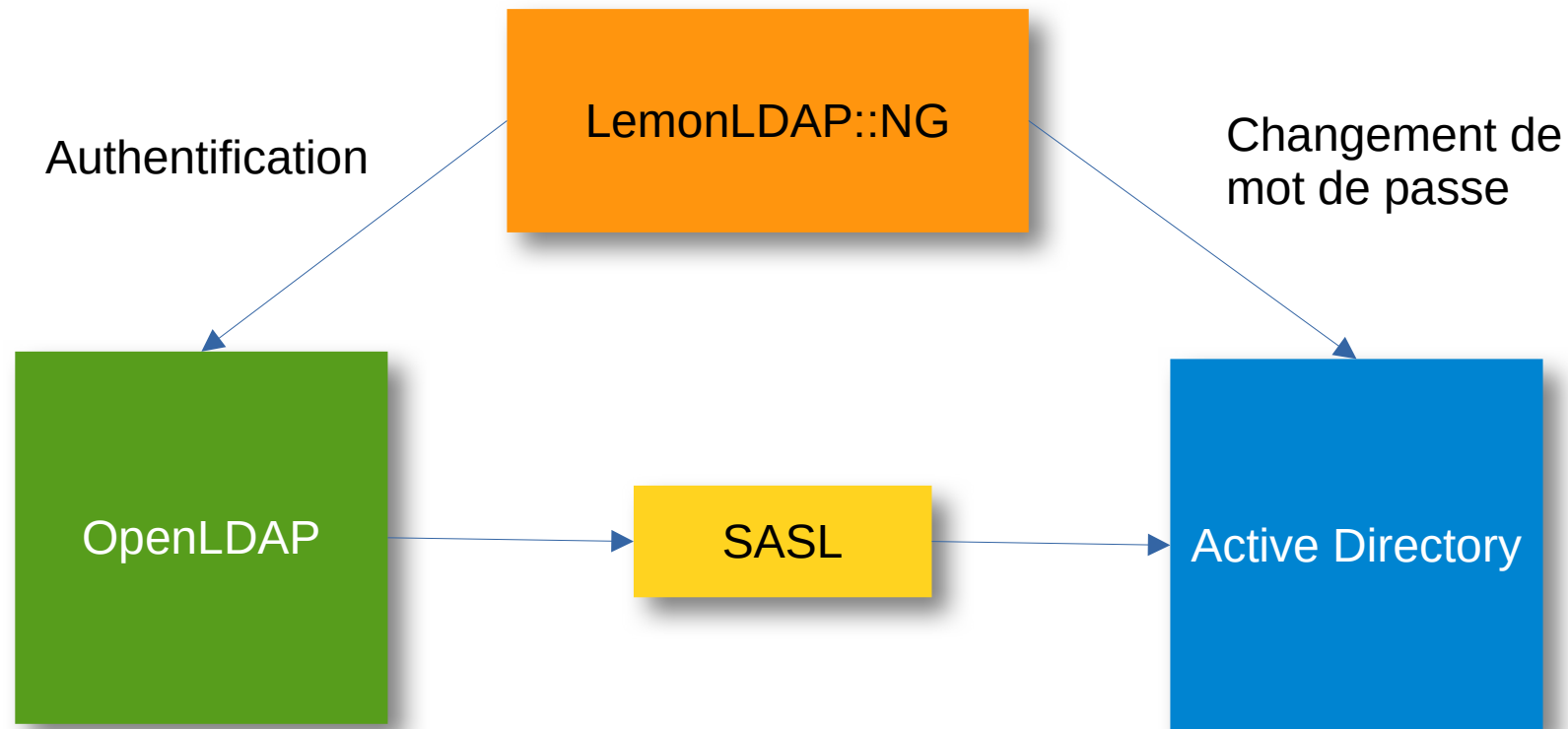




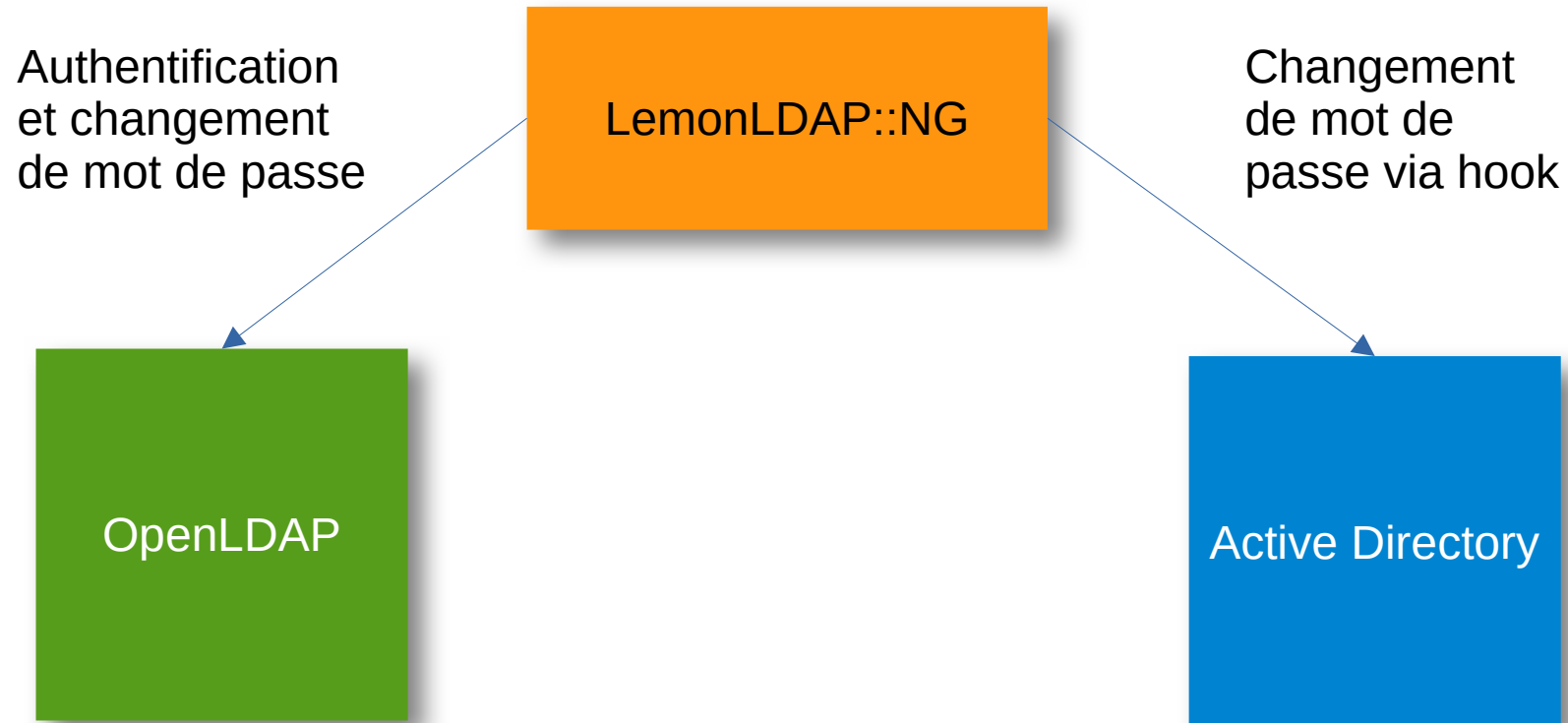
Authentification

- Modules dédiés à AD pour l'authentification (Auth), la récupération d'attributs (UserDB) et le changement de mot de passe (PasswordDB)
- Module d'authentification **Kerberos** pour l'authentification transparente
- Gestion des **groupes récursifs**
- Réinitialisation du mot de passe à la prochaine connexion
- Alerte d'expiration du mot de passe

AD connecté via SASL

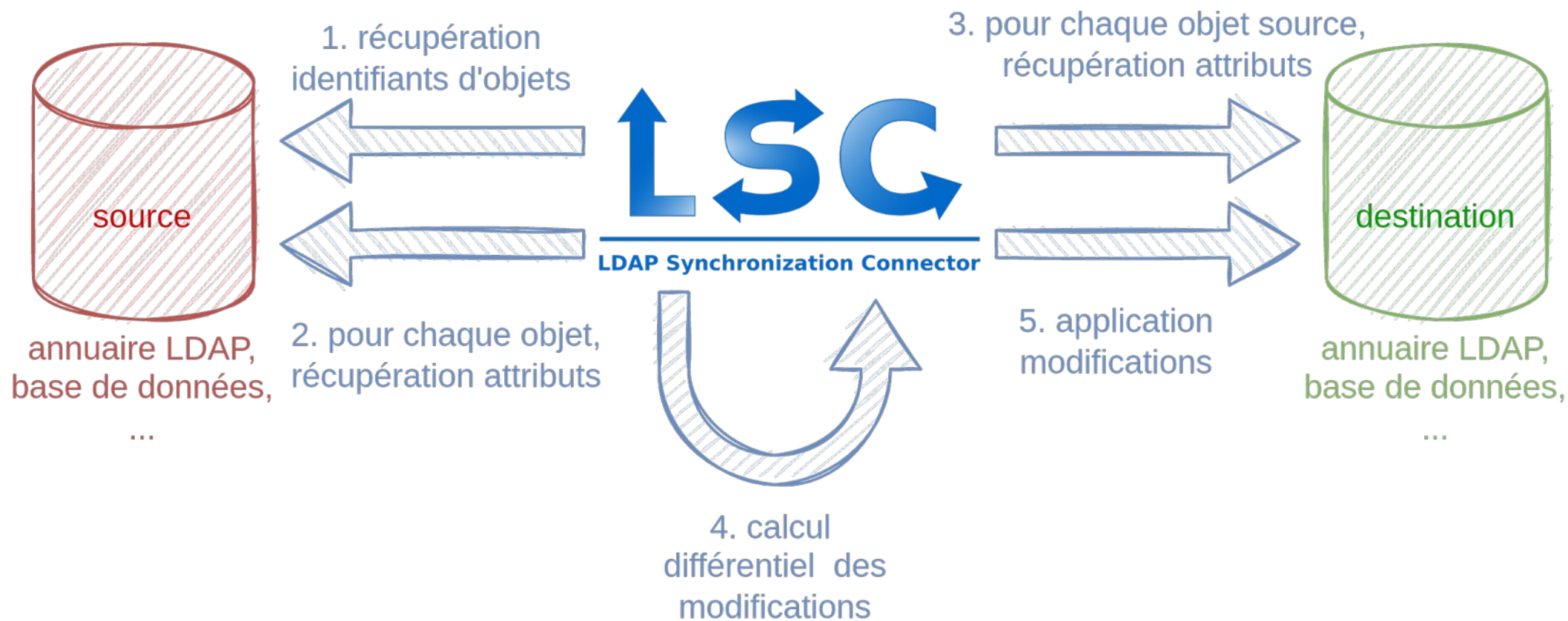


AD autonome



LDAP Synchronization Connector





Fonctions adaptées à AD

- Paramètre **pageSize** dans la connexion LDAP
- Possibilité de déclarer les attributs binaires (*objectGuid*, *objectSid*)
- Gestion du “range” par javascript dans le dataset des attributs
- Fonction pour l’encodage du mot de passe : *getUnicodePwd*
- Fonctions de manipulation de l’attribut *userAccountControl* :
userAccountControlSet, *userAccountControlCheck*,
userAccountControlToggle
- Fonctions de conversion de dates : *unixTimestampToADTime*,
aDTimeToUnixTimestamp

Exemple : conversion de objectGUID

```
function readUUID(bytes) {  
    var hex = new  
java.lang.String(org.apache.commons.codec.binary.Hex.encodeHe  
x(bytes));  
    return hex.replace(/^(..)(..)(..)(..)(..)(..)(..)(..)(..)  
(..)(..)(..)(..)(..)(..)(..)$/, "$4$3$2$1-$6$5-$8$7-$9$10-$  
$11$12$13$14$15$16").toUpperCase();  
}
```

Quelques exemples d'usages

- Convertir les groupes dynamiques OpenLDAP dans des groupes statiques AD
- Synchroniser le statut de blocage des comptes entre OpenLDAP et AD
- Provisionner les comptes utilisateurs avec un mot de passe à changer à la prochaine connexion

LTB Self Service Password



 Self service password
 Question
 Email
 SMS
 SSH Key



☒ Change your password

1 Enter your old password and choose a new one.

Your password must conform to the following constraints:

- ✓ Minimum length: 2
- ✓ Maximum length: 15
- ✓ Minimum number of lowercase characters: 1
- ✓ Minimum number of uppercase characters: 1
- ✓ Forbidden characters: @%
- ✓ Your new password may not be the same as your old password
- ✓ Password strength

100%

Login

Old password

New password

Confirm



☒ Send

LDAP Tool Box Self Service Password - version 1.6.0

Le mode Active Directory

- Le paramètre “ad_mode” permet d’utiliser le format d’encodage pour *unicodePwd*, et donc l’écriture du mot de passe dans Active Directory
- Plusieurs options supplémentaires sont disponibles :
 - *force_unlock* : déverrouille le compte lors du changement de mot de passe
 - *force_pwd_change* : force le changement à la prochaine connexion
 - *change_expired_password* : autorise le changement d’un mot de passe expiré

LTB White Pages



Star Pages
Advanced search
Directory
Gallery
Map

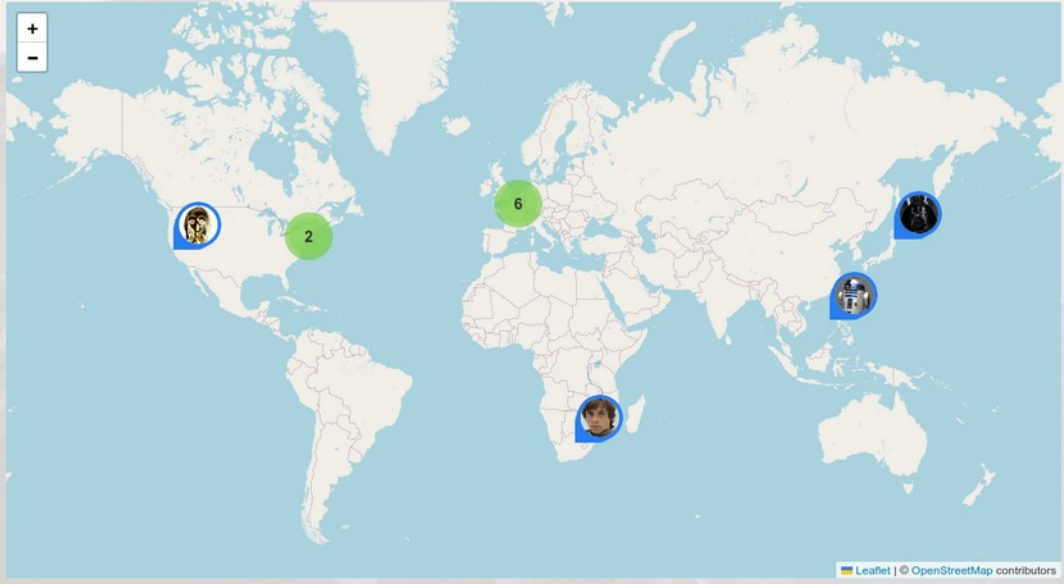
Leia Organa



First name	Leia
Last name	Organa
Employee type	Rebel
Mail	leia@alderaan.com
Street	Princess Road
Locality	Newton
Member of groups	Episode III Episode IV Episode V Episode VI

LDAP Tool Box White Pages - version 0.4

Star Pages
Advanced search
Directory
Gallery
Map



Map showing locations of Star Wars planets and characters. Pins are located in North America (2), Europe (6), Asia, and Africa.

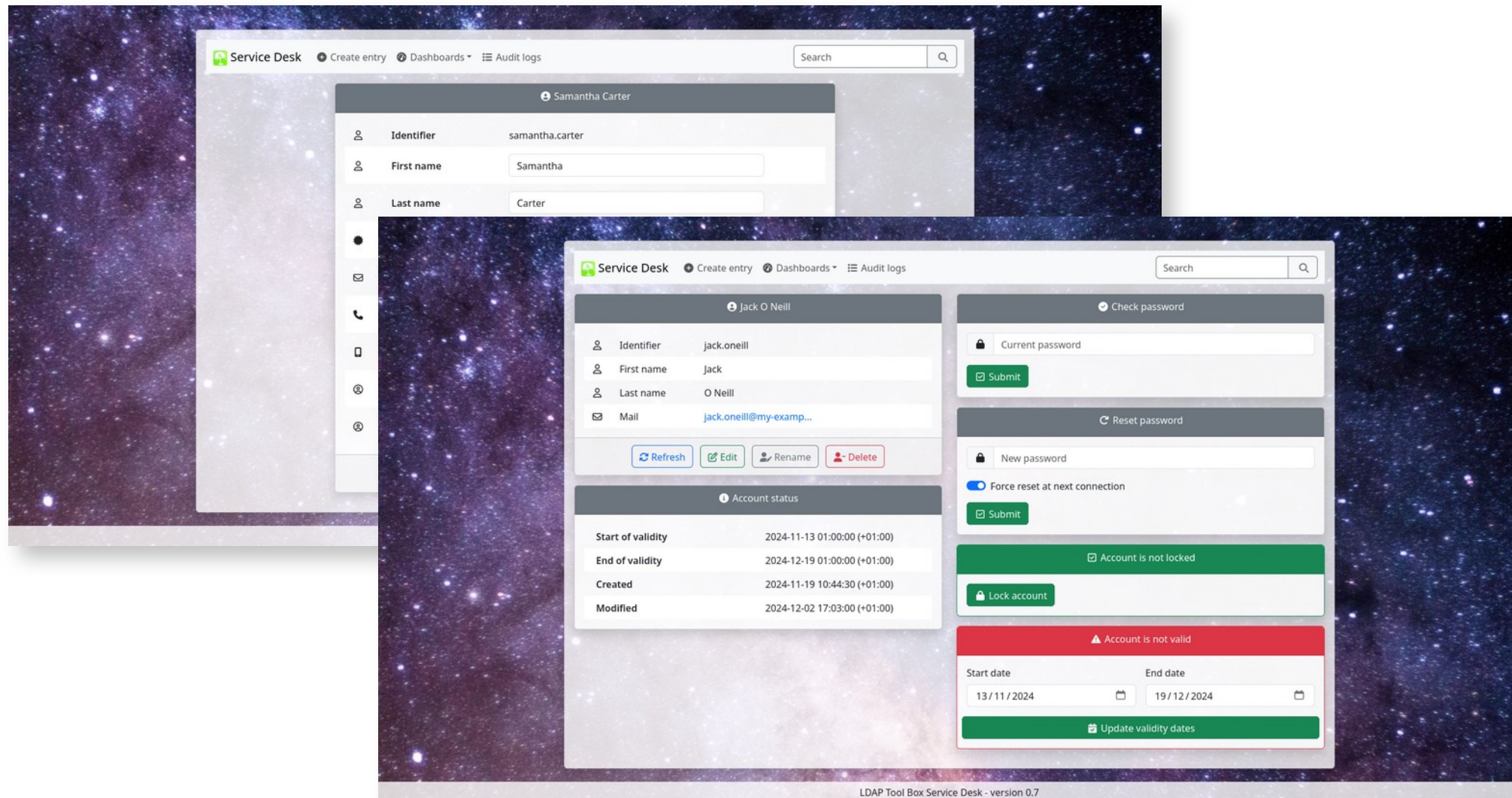
LDAP Tool Box White Pages - version 0.4

Configuration pour AD

- Les paramètres de connexion LDAP peuvent être adaptés pour Active Directory :
 - Pagination des résultats
 - Filtre de recherche des utilisateurs
 - Filtre de recherche des groupes
 - Liste des attributs à afficher
 - Attribut contenant la photo

LTB Service Desk





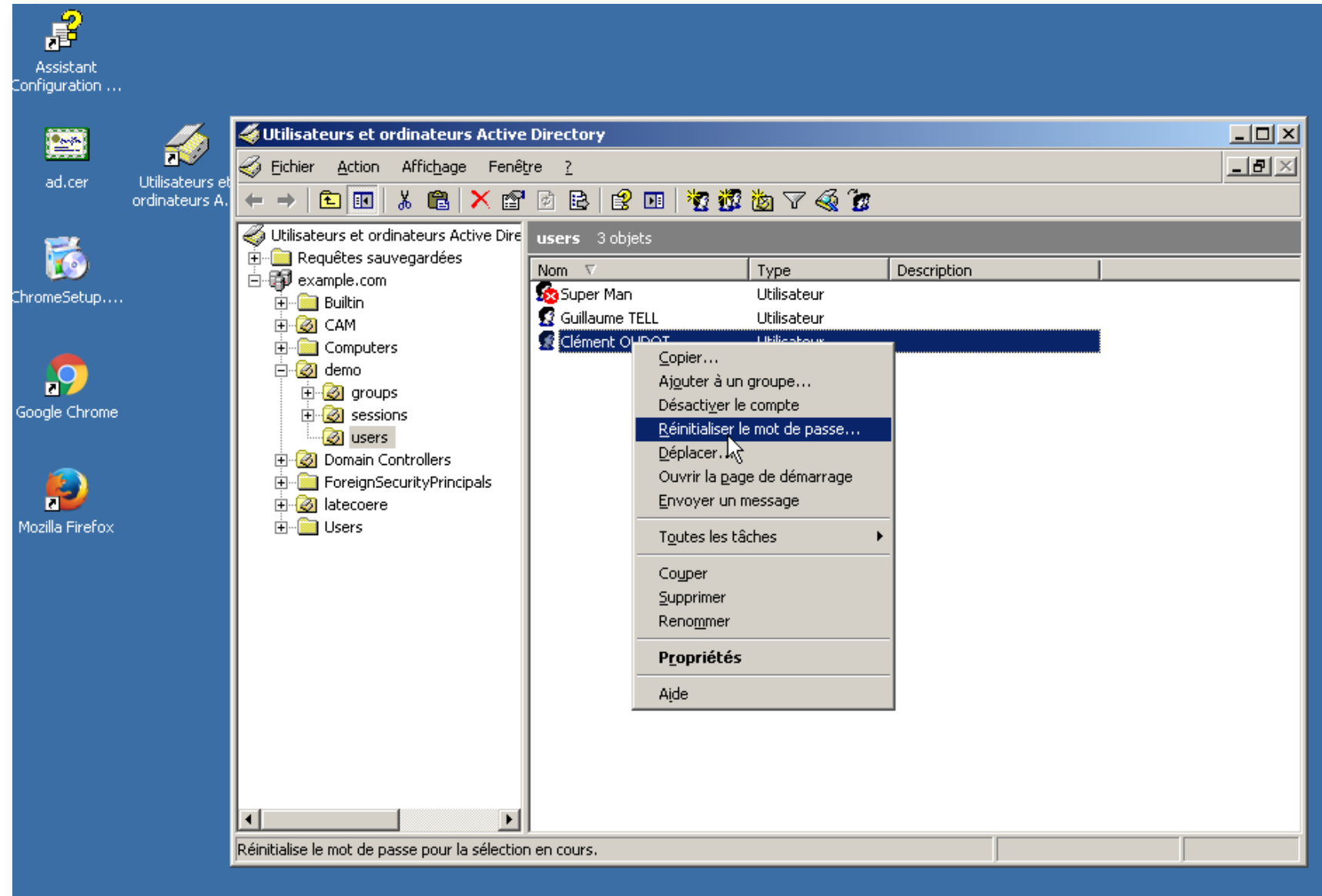
Un support AD avancé

- Module PHP dans la bibliothèque ltb-common :
Ltb/Directory/ActiveDirectory.php

=> Aucun code spécifique OpenLDAP ou AD dans Service Desk !

- Variable de configuration “ldap_type” pour indiquer si on utilise OpenLDAP ou Active Directory
- Type “ad_date” pour gérer les dates AD
- Gestion du statut activé/désactivé (indépendant du statut bloqué/débloqué)

Avant



Après

Guichet de service

Tableaux de bord

oudot

Clément OUDOT

Identifiant	coudot
Prénom	Clément
Nom	OUDOT
Courriel	cleoud@worteks.com
Téléphone	1234
Portable	06 99 66 51 31

Statut du compte

Dernier changement de mot de passe	27/12/2024 - 11:15:40 (CET)
Derniers échecs d'authentification	30/12/2024 - 12:14:35 (CET)
Dernière authentification	14/05/2018 - 15:23:47 (CEST)
Fin de validité	30/03/2025 - 00:00:00 (CET)
Créé	19/05/2014 - 17:40:41 (CEST)
Modifié	07/02/2025 - 11:53:35 (CET)
Date de verrouillage	30/12/2024 - 12:14:35 (CET)
Date d'expiration	08/02/2025 - 10:03:11 (CET)

Vérification du mot de passe

Mot de passe actuel

Envoyer

Réinitialisation du mot de passe

Nouveau mot de passe

Forcer la réinitialisation à la prochaine connexion

Envoyer

Le compte n'est pas verrouillé

Le compte est activé

Désactiver le compte

Le compte est valide

Date de fin

30 / 03 / 2025

Modifier les dates de validité

21 octobre 2025 - PARIS

The logo consists of three stylized human figures of increasing height, colored green, white, and white from left to right.

iID IDENTITY DAYS



@IdentityDays
#identitydays2025