




IDENTITY DAYS

6^{ème} édition



@IdentityDays
#identitydays2024

**22 octobre 2024 -
PARIS**



Mise en place des recommandations de l'ANSSI pour la sécurisation du protocole OpenID Connect

Clément OUDOT



Clément OUDOT

Identity Solutions Manager

PRO :

- [Worteks](#)
- [LemonLDAP::NG](#)
- [LDAP Tool Box](#)
- [LDAP Synchronization Connector](#)
- [FusionIAM](#)
- [W'IDaaS](#)

PERSO :

- [KPTN](#)
- [DonJon Legacy](#)
- [Improcité](#)
- [Les Amis Causent](#)

AGENDA DE LA CONFÉRENCE

- Introduction en musique
- Le protocole OpenID Connect
- Recommandations de l'ANSSI
- Mise en œuvre avec LemonLDAP::NG



Expertise, édition et hébergement
Open Source



Intégration, Support et Expertise



Portail d'applications collaboratif

Plateforme mutualisée de développement



Gestion des identités des accès



Étude, audit et conseil



Expertise technique



Support technique



Transfert de compétences spécifique

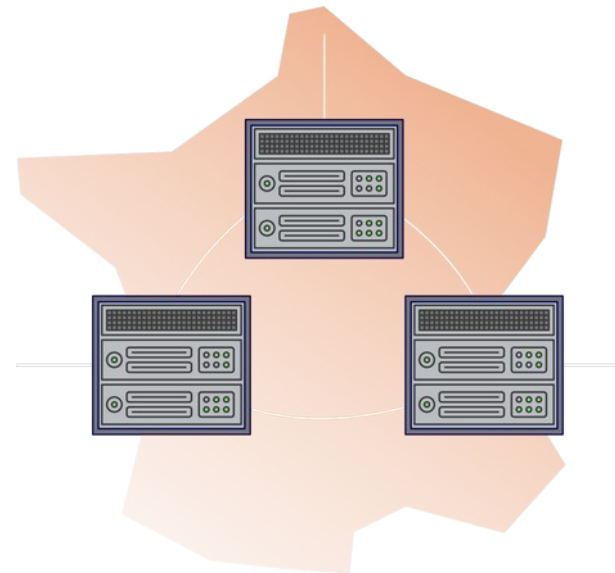


R&D et innovation

W'aaS

W'aaS est une offre d'hébergement souverain, infogéré et sur-mesure.

- ◆ **Souveraineté géographique**
Stockage des données en France
- ◆ **Souveraineté technique**
Briques logicielles Open Source
- ➔ **Souveraineté numérique**



Hébergement **privé**
Datacenters dans **3 zones**
géographiques distantes
Réseau privé interconnecté au
moyen de fibres optiques dédiées



<https://www.vorteks.com/rejoindre/>

Introduction en musique



Firewall

OASYS (One Auth SYStem)

Aujourd'hui je veux vous parler d'un protocole de sécurité
Qui peut être utilisé par les applications HTTP
Il se nomme OpenID Connect et n'est pas trop compliqué
Vous verrez...

Des GET, des POST, et des JWT
Un peu de JSON et des messages signés ou chiffrés
Il se nomme OpenID Connect et n'est pas trop compliqué
Vous verrez...

Les routes, les ports, les adresses et les tickets
Les claims, les scopes, les paramètres à renseigner
Vous saurez tout si vous restez bien jusqu'au bout
Venez découvrir...

OpenID
Et les recommandations de l'ANSSI
Configurez vos algos
Et votre firewall !





Le protocole OpenID Connect



Le protocole OpenID Connect

 <https://openid.net/developers/specs/>

Basé sur OAuth2, REST, JSON, JWT, JOSE

Adapté aux navigateurs Web et aux applications mobiles natives

Publication des informations de configuration au format JSON

Consentement de l'utilisateur requis sur le partage d'attributs



Les rôles OAuth 2



Resource owner
(end-user)



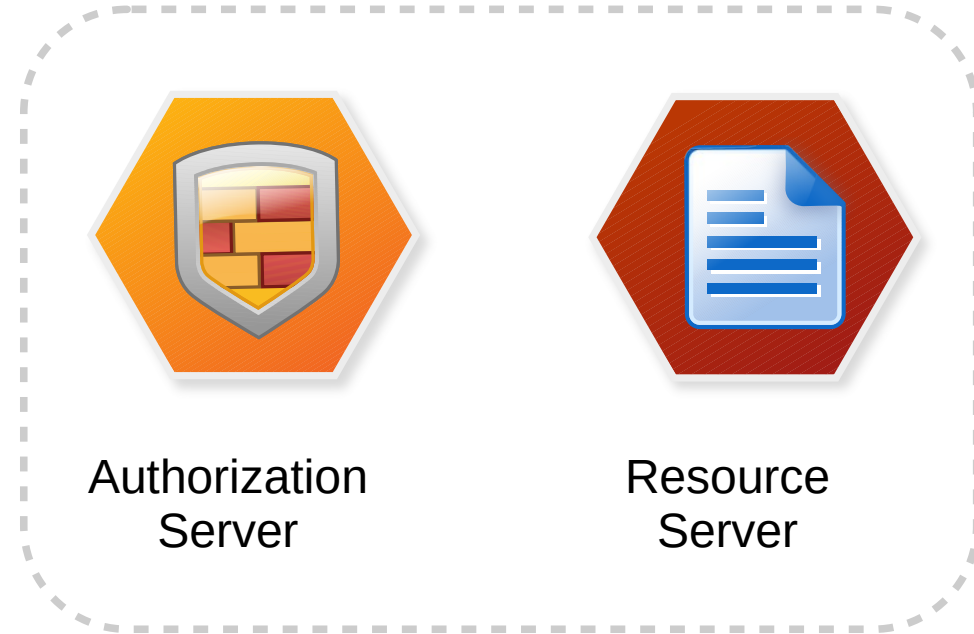
Client
(third-party)



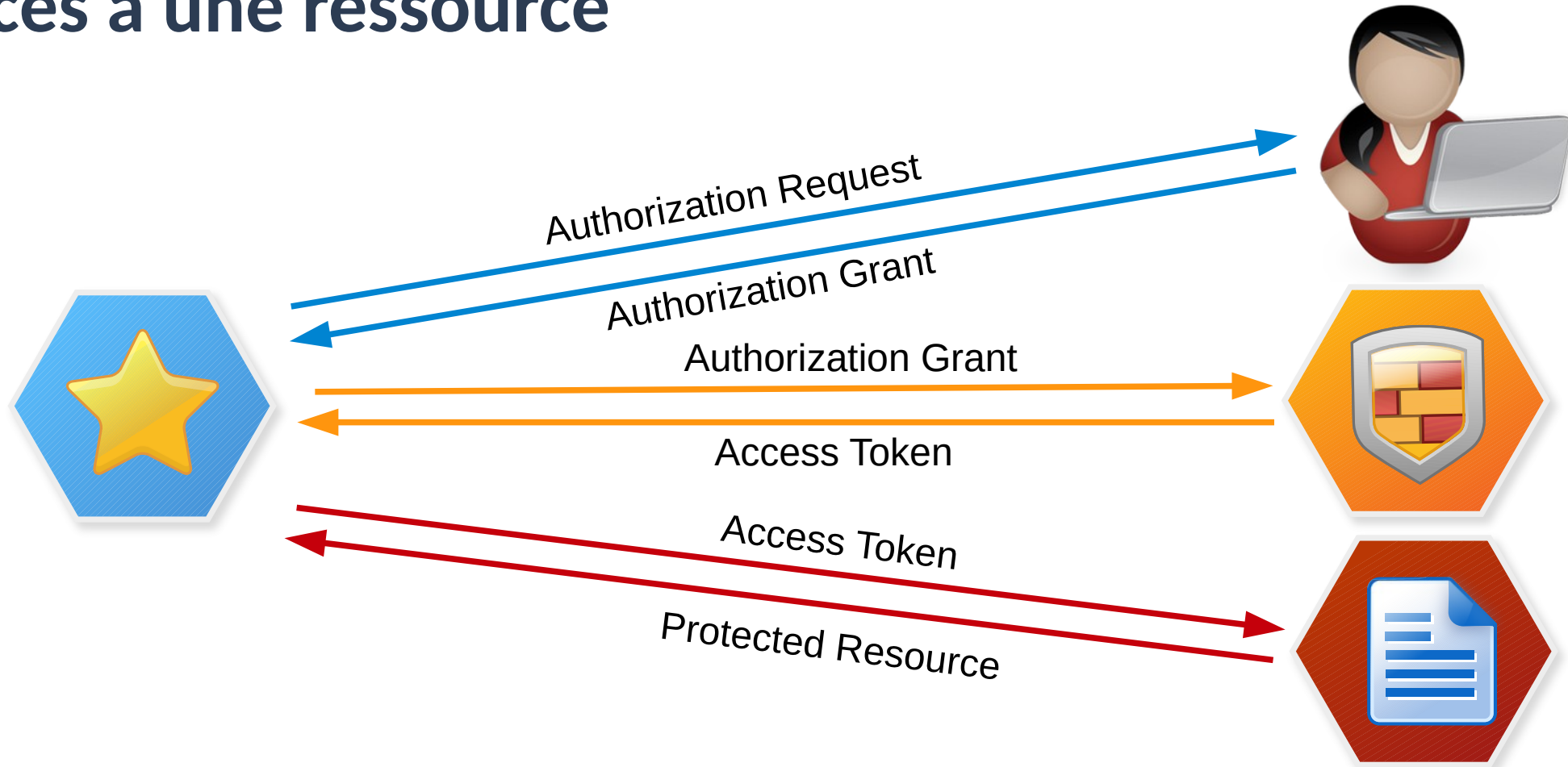
Authorization
Server

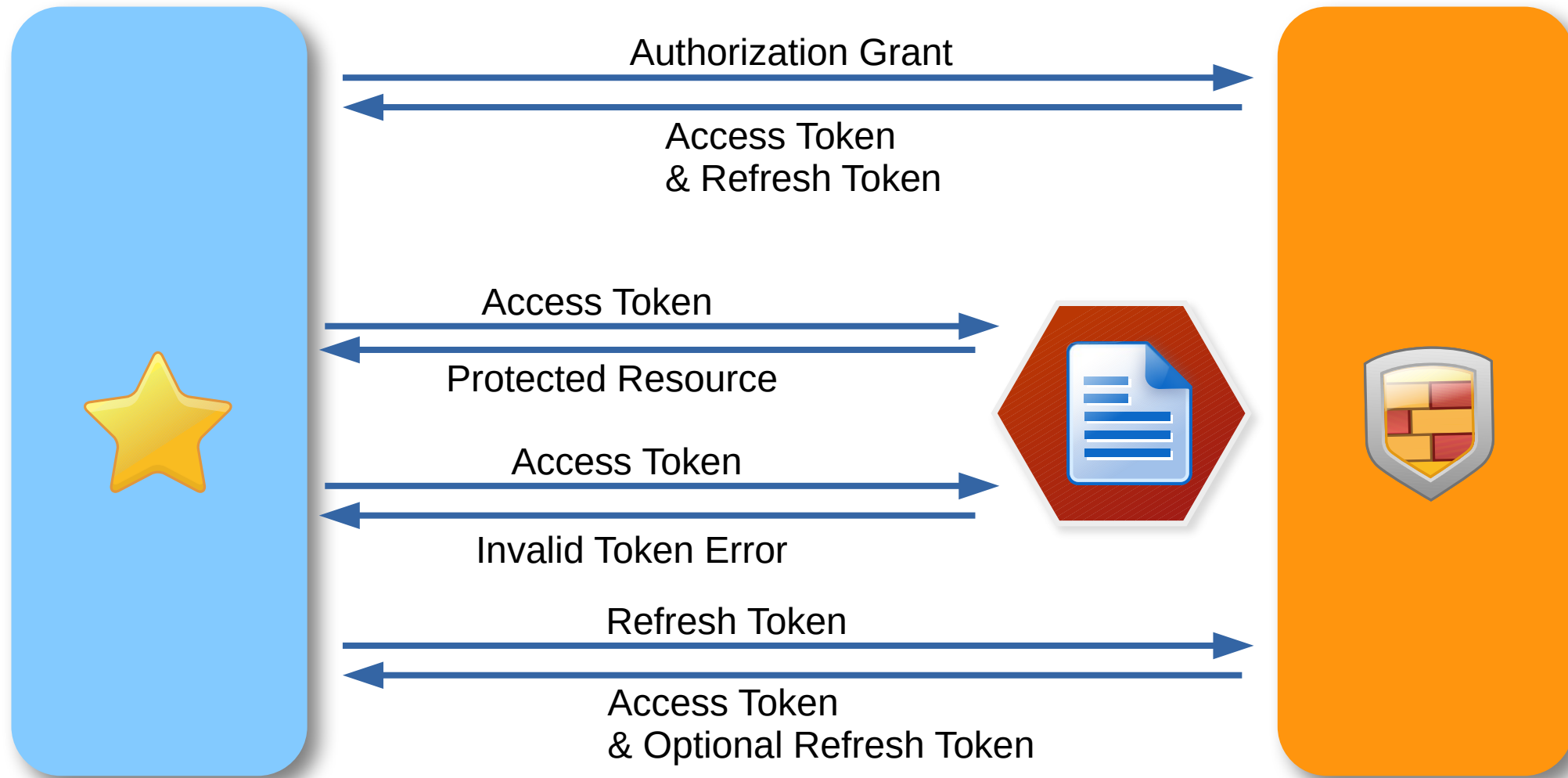


Resource
Server



Accès à une ressource





Évolutions du protocole OpenID



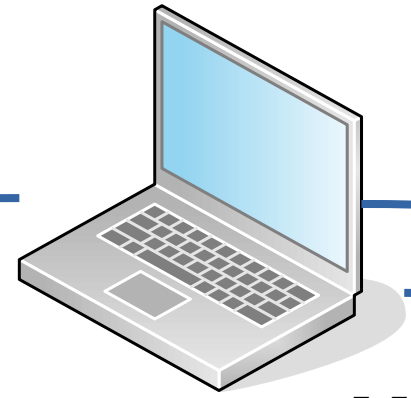
OpenID 1.0



OpenID 2.0



OpenID Connect



1. Premier accès,
Redirection vers l'URL *Authorize* du OP

2. Authentification
Génération d'un *code*

3. Envoi du *code* à
l'application via URL callback

Flux « Authorization Code »

URL *authorize*

OpenID Provider
(Serveur SSO)

URL *token*

4a. Échange du *code* contre
ID Token et *Access Token*

URL *userinfo*

4b. Échange de l'*Access Token*
contre les *claims* (attributs)

Relying Party
(Application)

JSON / JOSE / JWT / JWS / JWE

JOSE → Javascript Object
Signing and Encryption

JWT → JSON Web Token

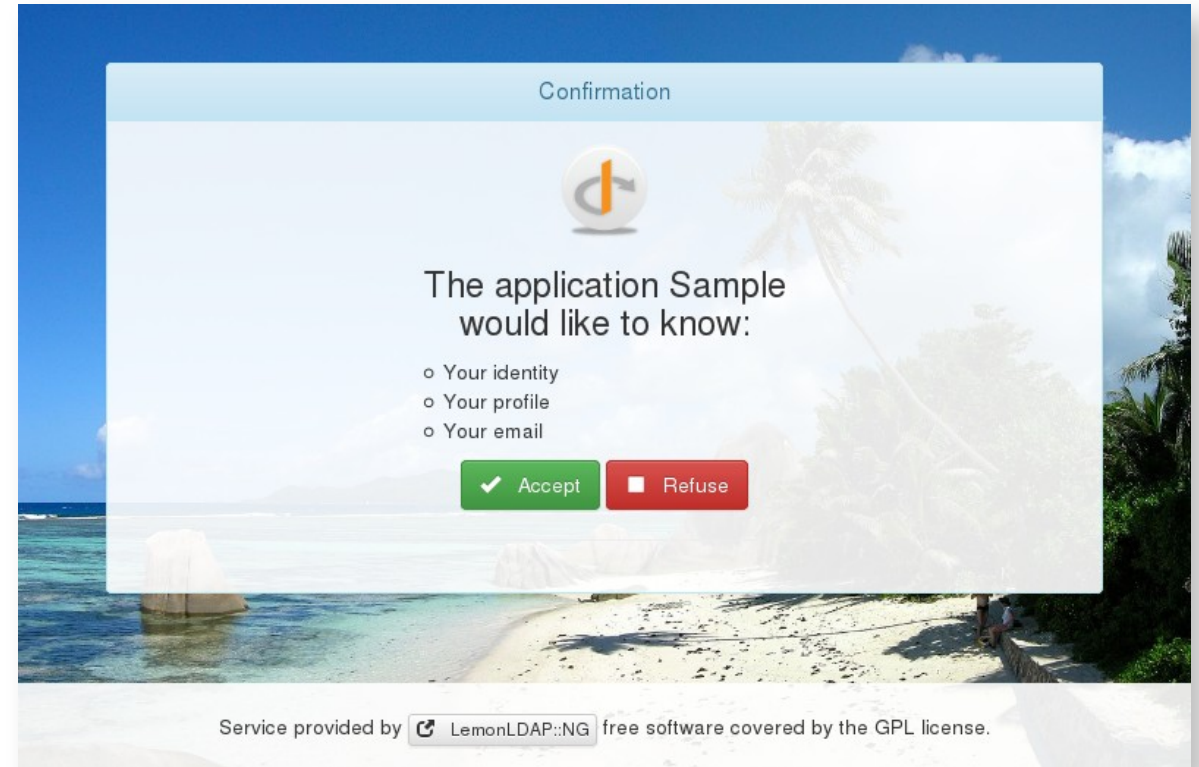
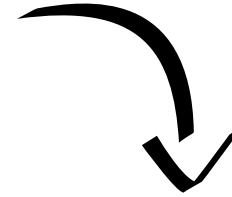
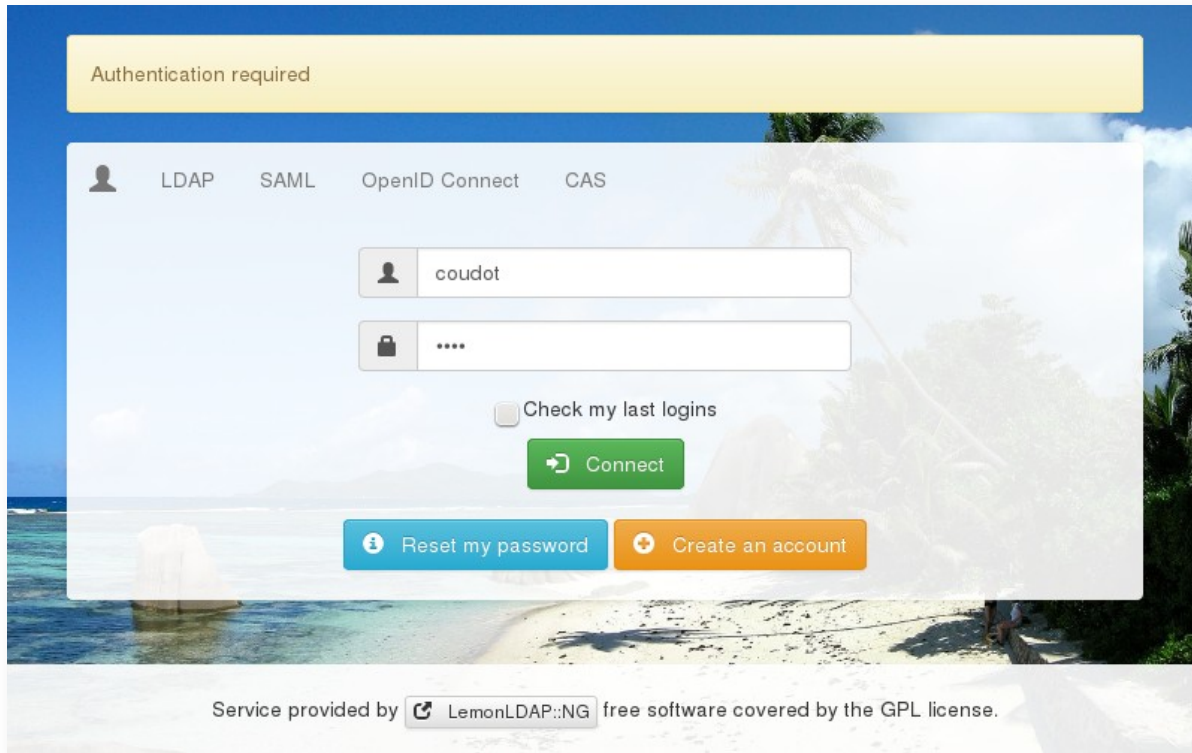




```

http://auth.example.com/oauth2/authorize?
response_type=code
&client_id=lemonldap
&scope=openid%20profile%20email
&redirect_uri=http%3A%2F%2Fauth.example.com
%2Foauth2.pl%3Fopenidconnectcallback%3D1
&state=ABCDEFGHIJKLMNQRSTUUVWXXZ
    
```







```
http://auth.example.com/oauth2.pl?  
openidconnectcallback=1;  
code=f6267efe92d0fc39bf2761c29de44286;  
state=ABCDEFGHIJKLMNOPQRSTUVWXYZ
```



```

POST /oauth2/token HTTP/1.1
Host: auth.example.com
Authorization: Basic xxxx
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
&code=f6267efe92d0fc39bf2761c29de44286
&redirect_uri=http%3A%2F%2Fauth.example.com
%2Foauth2.pl%3Fopenidconnectcallback%3D1
    
```





```
{
  "token_type" : "Bearer",
  "id_token" :
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhY3IiOiJsb2EtMiIsImF1dG8iOiJtZSI6MTQzMjExMzU5MywiaWF0IjoxNDMyMTEzOTY2LCJhdF9oYXNoIjoiOWF4enNOaTlwTkRrNXpXZWZlc002QSIsImZlcnV4IjoiImh0dHA6Ly9hdXRoLmV4YWwgfno0mg",
  "expires_in" : "3600",
  "access_token" : "512cdb7b97e073d0656ac9684cc715fe"
}
```

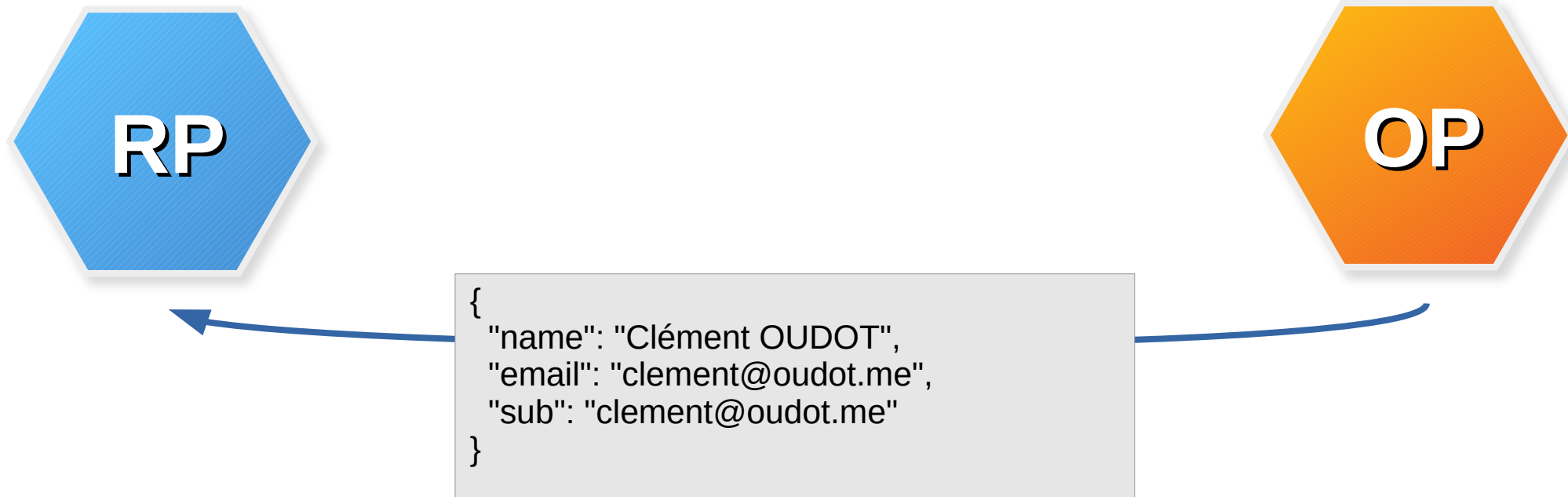


ID Token payload

```
{
  "acr": "loa-2",
  "auth_time": 1432113593,
  "iat": 1432113966,
  "at_hash": "9axzsNi9pNDk5zWefKsM6A",
  "iss": "http://auth.example.com/",
  "exp": "3600",
  "azp": "lemonldap",
  "nonce": "1234567890",
  "sub": "clement@oudot.me",
  "aud": [
    "lemonldap"
  ]
}
```

```
POST /oauth2/userinfo HTTP/1.1  
Host: auth.example.com  
Authorization: Bearer 512cdb7b97e073d0656ac9684cc715fe  
Content-Type: application/x-www-form-urlencoded
```





Recommandations de l'ANSSI



Recommandations de l'ANSSI

Version 1.0 sortie le 08/09/2020

- 52 recommandations réparties entre :
 - Fournisseur de service
 - Fournisseur d'identité
 - Les deux !

<https://cyber.gouv.fr/publications/recommandations-pour-la-securisation-de-la-mise-en-oeuvre-du-protocole-openid-connect>



Quelle entité doit implémenter quelles recommandations ?

Le but de cette annexe est d'indiquer les recommandations devant être mises en œuvre soit par les fournisseurs de service, soit par les fournisseurs d'identité, soit par les deux.

| Fournisseur de service | Fournisseur d'identité |
|--|--|
| R3 R4 R6 R7 R8 R8+ R10 R11 R13 R14 R15 R22 R26 R27 R28 R31 R32 R34 R40 R42 R44 R45 R46 R47 | R1 R2 R3 R4 R5 R9 R12 R16 R17 R18 R19 R20 R21 R23 R24 R25 R29 R30 R32 R33 R35 R36 R37 R38 R39 R41 R42 R43 R44 R45 R46 R47 R48 R49 R50 R51 |

Quelques exemples

R1

Utiliser en priorité la cinématique *authorization code* pour les applications Web

Il est recommandé d'utiliser la cinématique *authorization code* pour les applications Web. Elle permet :

- de protéger en confidentialité l'*access token* de l'environnement de l'utilisateur ;
- de mettre en œuvre un mécanisme d'authentification entre le client OIDC et le *Token Endpoint*.

R3

Mettre en œuvre HTTPS

Toutes les communications HTTP dans le cadre de la norme OIDC ainsi que celles entre l'utilisateur et le site du fournisseur de service doivent mettre en œuvre le protocole TLS.

Quelques exemples

R5

Imposer aux clients OIDC des suites cryptographiques recommandées pour les communications serveur à serveur

Il est recommandé au fournisseur d'identité d'imposer aux fournisseurs de service d'utiliser des suites cryptographiques robustes fournies dans le guide TLS[5] publié par l'ANSSI.

R8

Utiliser un JWS protégé par un HMAC

Pour éviter la manipulation de paramètres sensibles dans une demande d'authentification, il est recommandé qu'un client OIDC envoie les paramètres dans un JWS protégé par un HMAC.

Standard OIDC ?

R9

Imposer un mode de transmission des paramètres dans une demande d'authentification

Il est recommandé au fournisseur d'identité de n'autoriser qu'un seul mode de demande d'authentification par client OIDC. Par exemple, un client OIDC ayant opté pour un JWS signé ne doit pas pouvoir transmettre autrement les paramètres dans l'URL. Le mode de transmission et le mécanisme de protection (signature ou HMAC) doivent être fixés lors de l'enrôlement du client par le fournisseur de service.



Attention

Une implémentation certifiée par la fondation OpenID respecte strictement la norme OIDC, celle-ci n'indique pas de restreindre au client OIDC un unique mode de transmission des paramètres (JWS, chaînes de paramètre etc). Une stricte conformité ne permettra donc pas la mise en œuvre de la recommandation R9 et diminue fortement l'intérêt de mettre en œuvre les recommandations R8 et R8+.

Standard OIDC !

R17

Se protéger contre les redirections ouvertes

Pour se protéger contre les redirections ouvertes, le fournisseur d'identité doit vérifier l'appartenance de l'URL reçue dans le paramètre *redirect_uri* à une liste blanche d'URL associée à l'identifiant du client OIDC. Cette liste aura été fournie lors de l'enrôlement. De plus, cette vérification peut avoir lieu dès la réception de la demande d'authentification.

➔ https://openid.net/specs/openid-connect-core-1_0.html#AuthRequest

redirect_uri

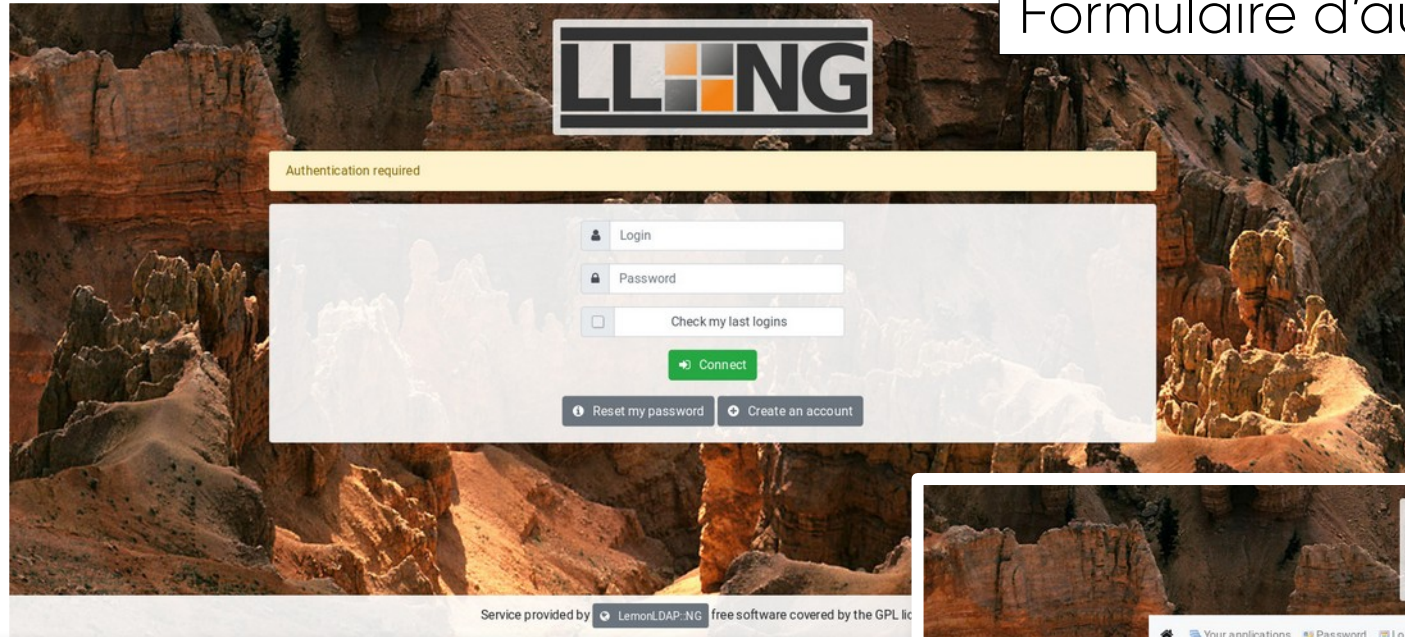
REQUIRED. Redirection URI to which the response will be sent. This URI MUST exactly match one of the Redirection URI values for the Client pre-registered at the OpenID Provider, with the matching performed as described in Section 6.2.1 of [RFC3986] (Simple String Comparison).



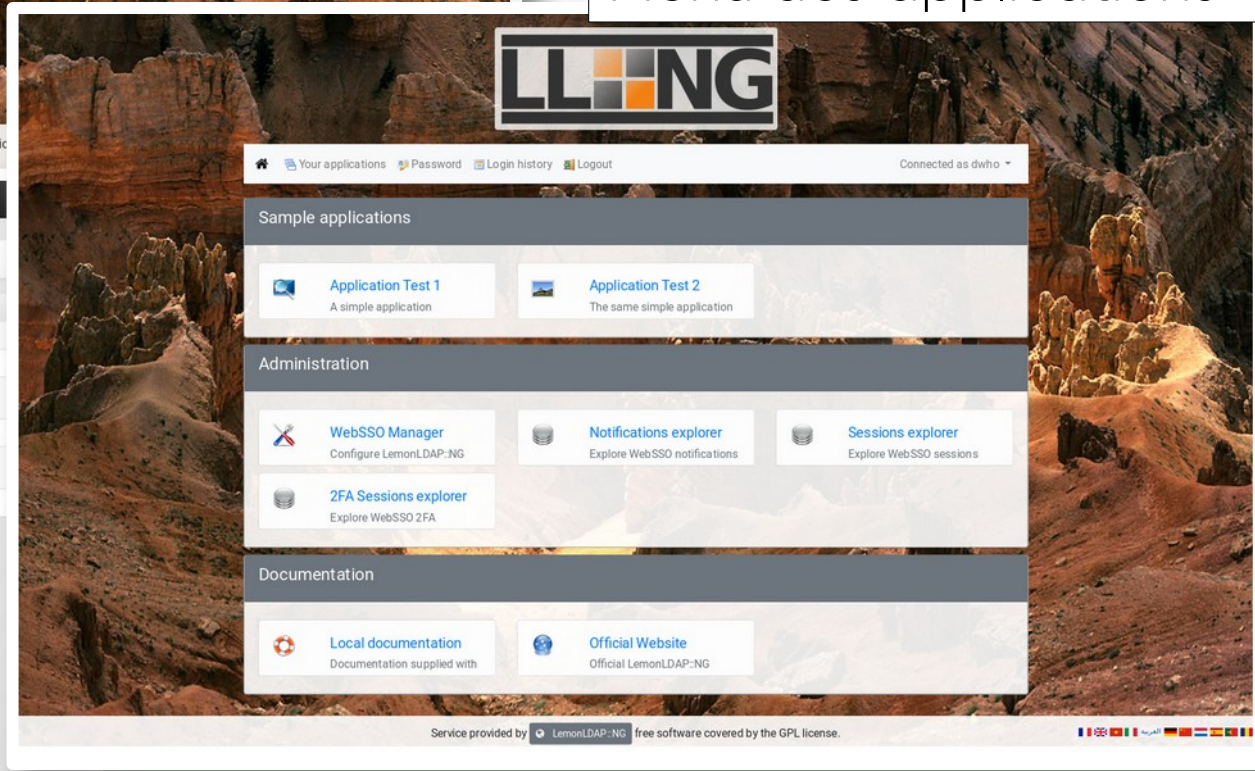
Mise en œuvre avec LemonLDAP::NG



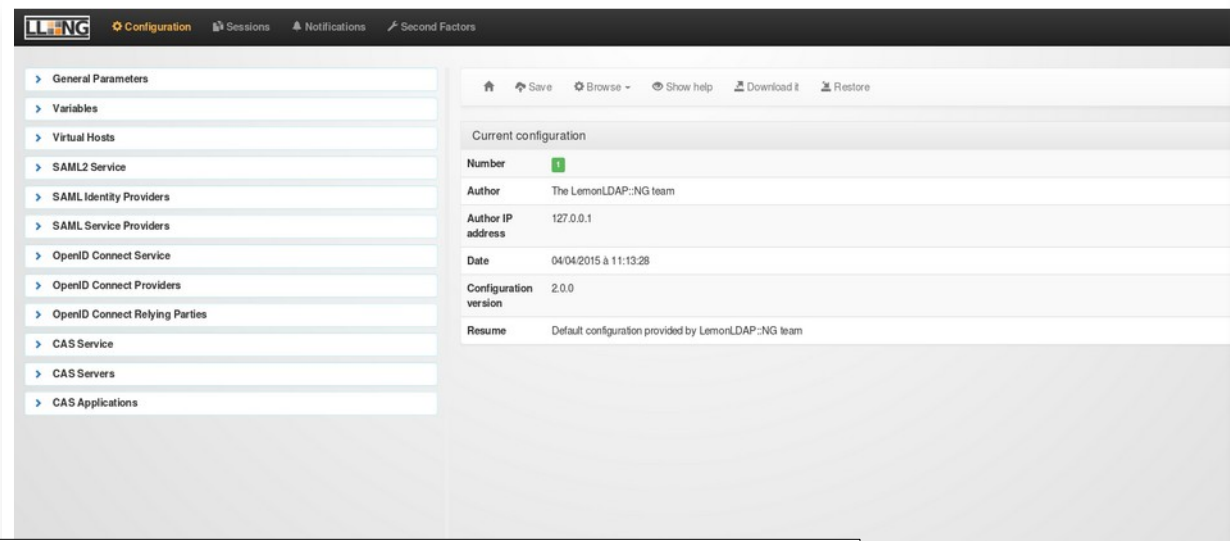
Formulaire d'authentification



Menu des applications



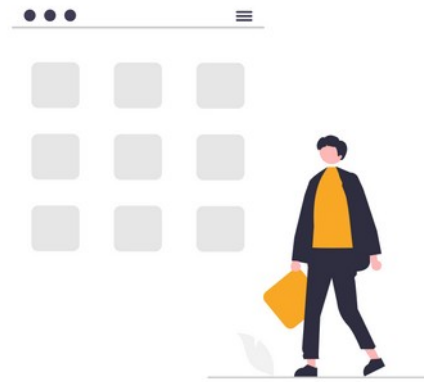
Interface d'administration



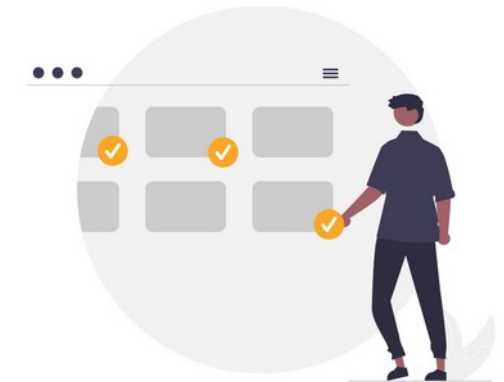
Principales fonctionnalités



SSO & Contrôle d'accès



Menu des applications



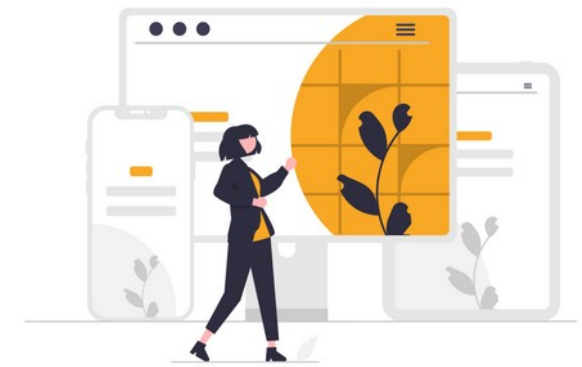
CAS / SAML / OIDC



Second facteurs (2FA)



Gestion du mot de passe



Personnalisation graphique

Recommandations ANSSI implémentées par défaut

R1 Utiliser en priorité la cinématique authorization code pour les applications Web

R6 Vérifier le nom de domaine

R10 Systématiser l'envoi du paramètre state

R11 Générer aléatoirement le paramètre state

R13 Utiliser les cookies de session

R15 Générer aléatoirement le paramètre nonce

R17 Se protéger contre les redirections ouvertes

R18 Générer aléatoirement les authorization code

R19 Limiter la durée de vie d'un authorization code

R20 Associer le code authorization code au client OIDC

Recommandations ANSSI implémentées par défaut

R24 Générer aléatoirement les access token

R26 Vérifier l'intégrité de l'ID Token

R28 Vérifier les informations d'un ID Token

R29 Vérifier le niveau d'authentification de l'utilisateur

R30 Rendre inutilisables les authorization code

R31 Transmettre les access token par l'entête Authorization

R33 Restreindre la durée de validité d'un access token

R34 Croiser les informations du UserInfo et de l'ID Token

R46 Mettre en oeuvre un système de journalisation

R47 Journaliser les événements importants

Recommandations ANSSI configurables

Serveur Web :

R3 Mettre en œuvre HTTPS : lié au serveur Web

R4 Appliquer les recommandations de sécurité relatives à TLS

R5 Imposer aux clients OIDC des suites cryptographiques recommandées pour les communications serveur à serveur

Recommandations ANSSI configurables

LemonLDAP::NG en tant que RP :

- R8 Utiliser un JWS protégé par un HMAC
- R8+ Utiliser un JWS protégé par une signature
- R14 Systématiser l'envoi du paramètre nonce
- R23 Utiliser une authentification du client OIDC adaptée
- R32 Ne pas écrire dans les journaux les access token
- R38 Restreindre l'accès au secret d'authentification
- R40 Restreindre l'accès à la clé privée de signature
- R42 Utiliser des fonctions de hachage recommandées
- R43 Utiliser des mécanismes de signature recommandés
- R44 Fixer l'algorithme utilisé pour le JWS

Recommandations ANSSI configurables

LemonLDAP::NG en tant que IDP :

R9 Imposer un mode de transmission des paramètres dans une demande d'authentification

R12 Détecter les demandes d'authentification sans le paramètre state

R16 Détecter les demandes d'authentification sans le paramètre nonce

R23 Utiliser une authentification du client OIDC adaptée

R32 Ne pas écrire dans les journaux les access token

R35 Générer aléatoirement les secrets d'authentification partagés

R36 Renouveler les secrets d'authentification partagés

R37 Utiliser un secret différent par client OIDC

Recommandations ANSSI configurables

LemonLDAP::NG en tant que IDP :

- R38 Restreindre l'accès au secret d'authentification
- R39 Utiliser des certificats pour authentifier les JWS
- R40 Restreindre l'accès à la clé privée de signature
- R42 Utiliser des fonctions de hachage recommandées
- R43 Utiliser des mécanismes de signature recommandés
- R44 Fixer l'algorithme utilisé pour le JWS
- R48 Désactiver la découverte automatisée
- R49 Ne pas utiliser l'enrôlement automatisé

Recommandations ANSSI configurables

LemonLDAP::NG et le paramètre « hashedSessionStore » activé :

R21 Stocker les authorization code sous forme d'empreinte

R25 Stocker les access token sous formes d'empreintes

Documentation officielle LemonLDAP::NG

ANSSI security guidelines



Presentation

The [Agence Nationale de la Sécurité des Systèmes d'Information \(ANSSI\)](#) is a French Agency for the Security of Information Systems. They published a [document to secure OpenID-Connect](#). This document explain what to do to follow it.

<https://lemonldap-ng.org/documentation/latest/anssi-oidc.html>



Merci de votre attention !

 IDENTITY DAYS



@IdentityDays
#identitydays2024