LE PARTENAIRE INFORMATIQUE DU PROGRÈS EN FÉDÉRATION WALLONIE-BRUXELLES

Bâtiment 'Le Zénith'
Boulevard du Roi Albert II, 37
1030 Bruxelles

OAuth2
Version 1.0.0

Manuel d'utilisation

Produit :	**OAuth2**
Service :	**token, userinfo**
Version du service :	**1.0**
Type de document :	**Manuel d'utilisation**
Révision du document :	**1.0**

Historique

Révision	Description	Ecrit par	Review	Date
1.0	Version initiale	KSE		03/06/2024
2.0	Ajout permission	KSE		06/06/2024

Objectifs du document

Ce document est destiné aux partenaires informatiques qui souhaitent utiliser les services web de la fédération Wallonie-Bruxelles. Il s'adresse, plus particulièrement, aux consommateurs d'une API sécurisée avec le protocole OAUTH2 afin d'expliquer le fonctionnement pour négocier le token de sécurité nécessaire à l'appel d'une API

Public cible

Ce document s'adresse aux développeurs.

Contacts

Pour toute question ou demande d'assistance technique veuillez contacter le helpdesk de l'Etnic.

Support général
Email : support@etnic.be
Tél : 02 / 800 10 10

LE PARTENAIRE INFORMATIQUE DU PROGRÈS EN FÉDÉRATION WALLONIE-BRUXELLES

Bâtiment 'Le Zénith'
Boulevard du Roi Albert II, 37
1030 Bruxelles

OAuth2
Version 1.0.0

Manuel d'utilisation

Table des matières

LE PARTENAIRE INFORMATIQUE DU PROGRÈS EN FÉDÉRATION WALLONIE-BRUXELLES

Bâtiment 'Le Zénith'
Boulevard du Roi Albert II, 37
1030 Bruxelles

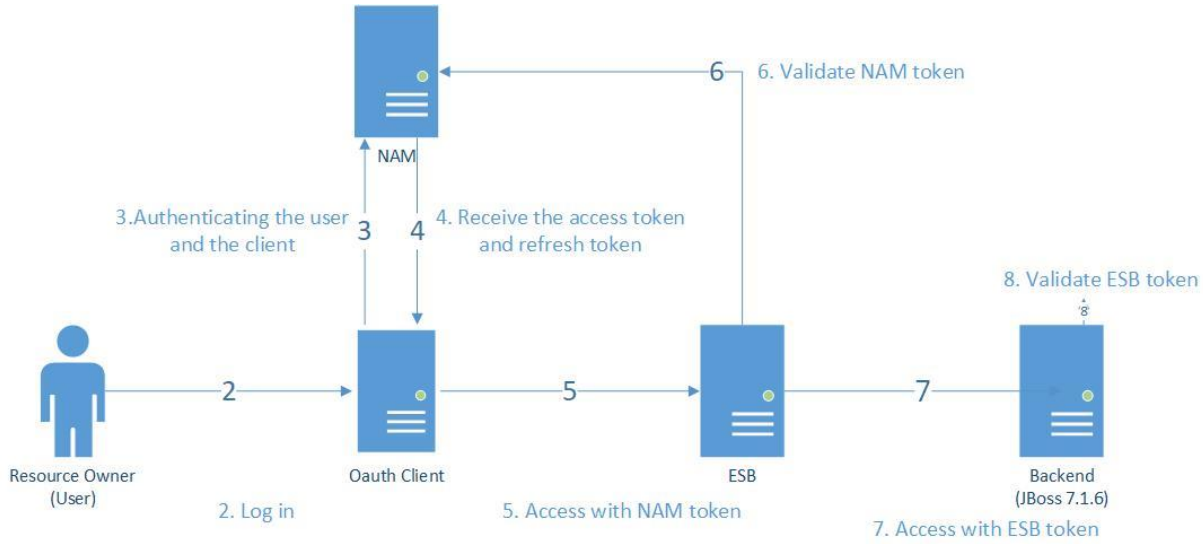
OAuth2
Version 1.0.0

Manuel d'utilisation

1. CADRE

Les API Rest qui sont exposées hors de l'Etnic sont sécurisées avec le protocole OAuth2.

Le client qui souhaite utiliser une API doit donc dans un premier temps négocier un token de sécurité, et ensuite appeler le service au moyen de ce token.



Lors de l'appel à l'API, c'est l'ESB de l'Etnic qui valide le token reçu et permet (ou refuse) l'accès au service demandé.

2. URLS

Les URLs du NAM :

ENV	Service	Url Endpoint
TQ	token	https://secure-acc.etnic.be/nidp/oauth/nam/token
	Userinfo	https://secure-acc.etnic.be/nidp/oauth/nam/userinfo
PROD	token	https://secure.etnic.be/nidp/oauth/nam/token
	Userinfo	https://secure.etnic.be/nidp/oauth/nam/userinfo

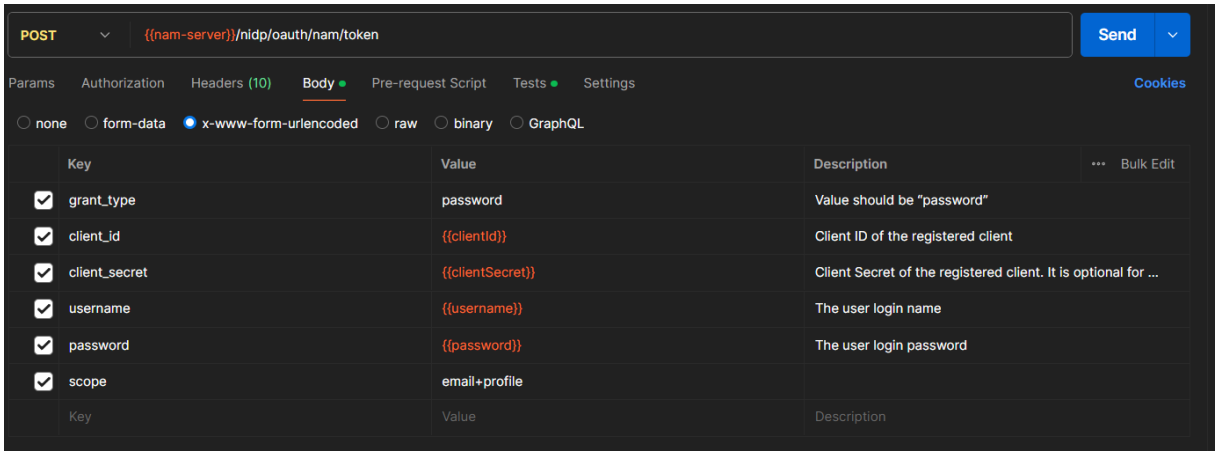
3. OBTENIR UN TOKEN

3.1. APPEL

Type d'appel : **POST**
Url : /nidp/oauth/nam/token

Les paramètres ci-dessous sont à spécifier lors de chaque appel :

Paramètre	Description
grant_type	Valeur fixe : password
client_id	Le ClientID du client qui souhaite se connecter
client_secret	Le client Secret associé au ClientID
username	Le login de l'utilisateur cerbère
password	Le mot de passe de l'utilisateur cerbère
scope	Valeur fixe : email+profile



3.2. RÉPONSE

Voici le format de la réponse :

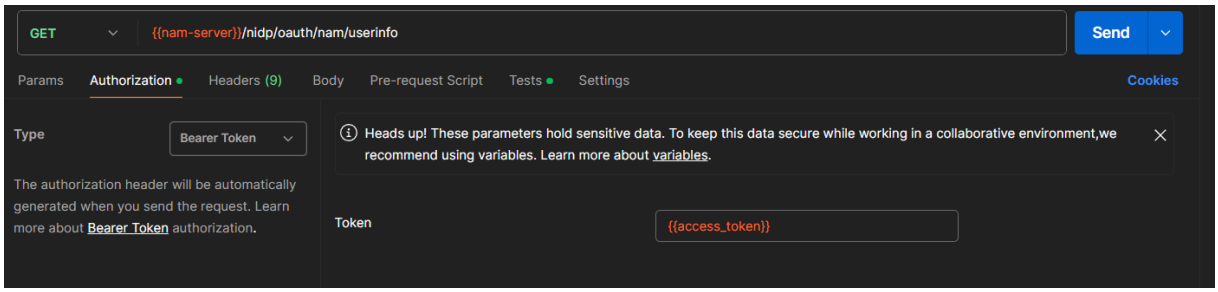
```
{
    "access_token": "…",
    "token_type": "bearer",
    "expires_in": 3599,
    "refresh_token": "…",
    "acr": "IAMV2 - ACC - POW - OAuth",
    "scope": "profile"
}
```

4. VÉRIFIER LE TOKEN

4.1. APPEL

Type d'appel : **GET**
Url : /nidp/oauth/nam/userinfo

Il n'y a pas de paramètres à spécifier lors de l'appel, juste le type d'authentification nécessaire pour l'appel et fournir le token.



4.2. RÉPONSE

Voici le format de la réponse :

```
{
    "sub": "965d7d09588113434d9e965d7d095881",
    "role": [
        "etnic.api.project()"
    ],
    "Groups": "Readers",
    "nickname": "ART000000000011",
    "claims": [],
    "preferred_username": "ART000000000011",
    "given_name": "Compte Artefact",
    "family_name": "PROJECT_NAME",
    "employeeNumber": "ART2R",
    "username": "username"
}
```

L'élément role contient la liste des permissions de l'utilisateur qui a réclamé le token.

5. PROCÉDURE D'ACCÈS

Le token d'accès est négocié sur base de 4 paramètres propres à chaque appel et qui différent d'un environnement à l'autre :

- client_id
- client_secret
- username
- password

Ces 4 paramètres sont en fait 2 paires de paramètres :

- client_id / client_secret : identifie l'applicatif ou le prestataire qui réalise l'appel
- username / password : identifie l'utilisateur qui fait l'appel

En dehors de l'environnement de production, seuls les comptes artefact peuvent obtenir un token d'accès.

Si votre projet a déjà un compte artefact dans l'environnement voulu, alors il faut juste demander l'ajout des permissions applicatives nécessaires à l'appel de GEDI.

Si vous n'avez pas encore de compte artefact, alors il faut demander la création d'un nouveau compte.

La demande pour obtenir ces données se fait via Mantis :

Projet	GEDI-APP-GEDI-WS
Catégorie	[Solution] Exploitation
Résumé	[NomProjet / NomApplicatif / NomPrestataire] demande de clientID pour l'environnement [TQ / Prod]
Description	- Spécifier un mail de contact pour recevoir le clientSecret. - Préciser si un compte artefact doit être créer en TQ - Préciser les FASES qui vont être utilisés pour les appels pour l'ajout des permissions