

# Modalités techniques d'accès aux API pour l'EDI Douane

Modalités techniques  
Documentation d'accès aux API Douane  
pour les opérateurs

Version v1.9 du 10/01/2023

## LEXIQUE

Terme	Définition
Certifie	Le Correspondant Entreprise certifie ou dé-certifie (confirme ou rejette officiellement) le rattachement des comptes douane.gouv des collaborateurs de l'entreprise. Le Correspondant Entreprise peut par la suite nommer d'autres correspondants depuis le portail douane.gouv.fr avec son compte. Ne pas confondre avec la certification logicielle attestée par la Douane.
API	Interface de programmation (Application Programming Interface)
Token	Jeton
REST	REpresentational State Transfer
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secured
OAuth	Protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur. ( <i>wikipédia</i> )
OAuth2.0	Successeur du protocole OAuth 1.0, est un framework d'autorisation permettant à une application tierce d'accéder à un service web. ( <a href="https://zestedesavoir.com">https://zestedesavoir.com</a> )
Correspondant Entreprise	Dans le document, cette notion peut désigner : - Le nom de l'application qui remplace « Admin Prodouane » - Personne physique (ou employé) désignée par l'entreprise pour gérer son compte API
Compte API	Compte technique permettant de s'interfacer avec les API's de la douane avec une authentification basée sur Oauth2.0

## SOMMAIRE

1 INTRODUCTION.....	4
2 ARCHITECTURE TECHNIQUE.....	4
3 DEMANDE D'ACCÈS AUX API.....	5
3.1 PRINCIPES GÉNÉRAUX.....	5
3.2 CRÉATION ET HABILITATION DE COMPTE API.....	6
3.2.1 Création d'un compte API.....	6
3.2.2 Demande d'habilitation d'un compte API.....	7
3.2.3 Finalisation d'un compte API.....	7
3.2.4 Modification du compte api.....	9
4 PARAMÈTRES TECHNIQUES DES APPELS ET EXEMPLES D'UTILISATION.....	10
4.1 REQUÊTE D'AUTHENTIFICATION.....	10
4.2 EXEMPLE DE REQUÊTE HTTPS.....	11
4.3 EXEMPLE DE RÉPONSE DU SERVEUR D'AUTORISATION.....	11
4.4 APPELS À L'API.....	13

## 1 INTRODUCTION

Ce document a pour objectif de fournir aux opérateurs les informations leur permettant de s'interfacer en mode EDI avec des API avec le système informatique douanier. Ce nouvel EDI remplacera progressivement la solution EDI « Mareva » qui restera le mode d'interconnexion pour DeltaG, DeltaXI, DeltaXE, DeltaT, ICS, ECS, Gamma, Isope et Pablo. Le nouvel EDI est mis en place avec les applications DeltaH7, Gamma2, DeltaE et PNTS.

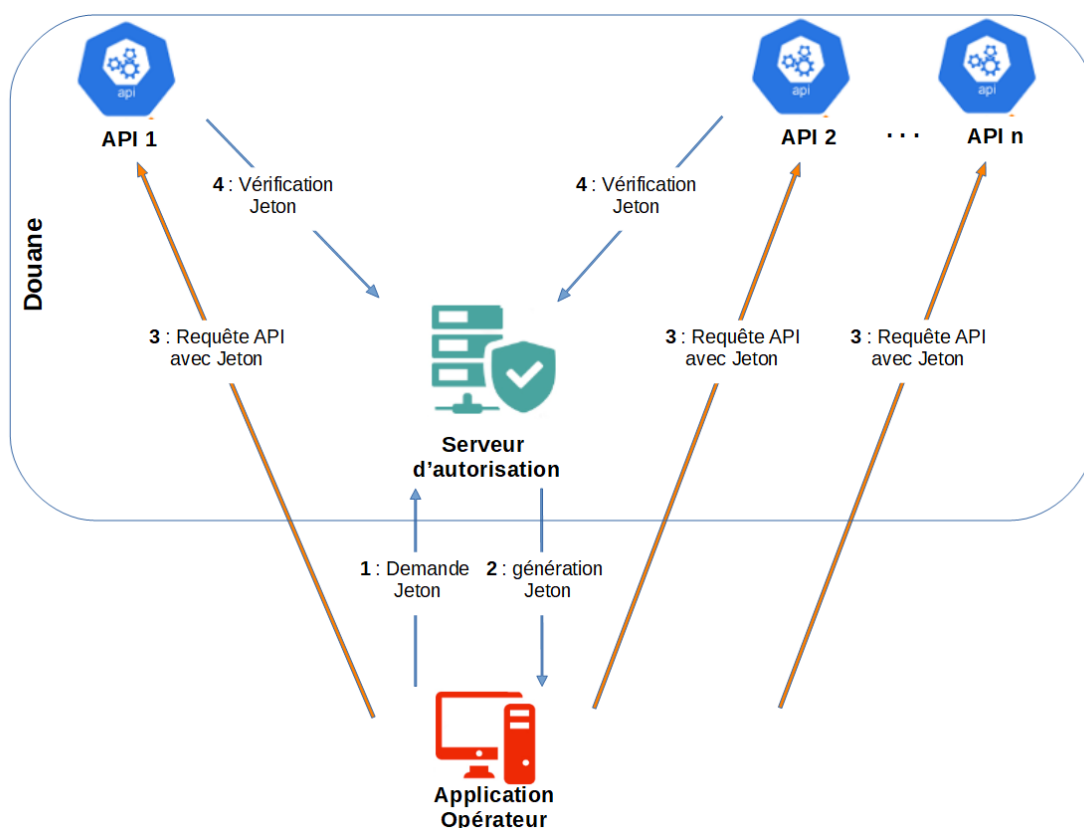
Ces modalités font suite à un contrat d'utilisation de l'EDI Douane via API conclu entre l'opérateur et la Douane (effectuer la demande au service gestionnaire de certification : certification-edi@douane.finances.gouv.fr en précisant le numéro SIRET de votre entreprise, le logiciel utilisé par votre société et le compte douane.gouv du correspondant entreprise qui sera le gestionnaire du compte API). Si vous ne disposez pas encore de compte douane.gouv, merci de vous rapprocher de votre PAE (pôle action économique).

Ce document décrit le process à suivre et l'architecture technique à mettre en œuvre. Les paramètres techniques (chapitre 4 du présent document) seront communiqués lors de la remise du contrat d'utilisation. Une version restreinte de ce document est publiée sur le portail de la Douane (douane.gouv.fr).

Le service gestionnaire de certification va également être votre interlocuteur pour créer et habiller votre compte API tel que décrit dans le présent document. Il vous transmettra les coordonnées des services douaniers qui seront ensuite vos interlocuteurs pour la réalisation des tests libres et la certification des solutions logicielles.

## 2 ARCHITECTURE TECHNIQUE

L'architecture fonctionnelle mise en œuvre lors d'un appel aux API fournies par la Douane est présentée ci-dessous. Elle se base sur l'utilisation des standards OAuth2 :



L'appel à une API Douane s'effectue en **REST** via HTTPS et nécessite l'obtention d'un **jeton d'accès** (Access Token) auprès du serveur d'autorisation de la Douane.

Le jeton d'accès est valable pour toutes les connexions entre l'application de l'opérateur et toutes les API de la Douane selon les habilitations accordées au compte API utilisé par l'application de l'opérateur.

La récupération du jeton d'accès est soumise à une authentification préalable. Pour ce faire, l'application appelante utilise un **compte API** enregistré auprès de la Douane et s'authentifie auprès du serveur d'autorisation de la Douane.

Une fois cette authentification réussie, l'application récupère le jeton d'accès, constitué d'une chaîne de caractères opaque. Ce jeton d'accès devra être ajouté à l'en-tête HTTPS de chaque requête REST envoyée à l'API (Une information complémentaire sera fournie dans la version technique de ce document).

La validité de ce jeton d'accès est limitée dans le temps. Lorsque le jeton expire, l'application doit se ré-authentifier auprès du serveur d'autorisation afin de récupérer un nouveau jeton. Cette durée est fixée à 5 min.

Le chapitre 3 présente les étapes de l'établissement d'une connexion avec la Douane. Ceci nécessite en particulier la création du compte API permettant la récupération du jeton d'accès et son habilitation pour l'API Douane souhaitée.

Les paramètres techniques nécessaires à la création des requêtes d'obtention du jeton d'accès et d'appel aux API sont présentés en chapitre 4 (Existe uniquement dans la documentation technique).

### 3 DEMANDE D'ACCÈS AUX API

#### 3.1 PRINCIPES GÉNÉRAUX

Lorsqu'un organisme externe à la Douane souhaite utiliser une ou plusieurs API de la Douane, il est nécessaire d'échanger un ensemble d'informations entre cet organisme et la Douane. Cet échange d'information est matérialisé par une demande d'accès aux API.

Pour ces échanges, un **correspondant entreprise** devra être désigné et habilité pour la création et la gestion des **comptes API**. Ces étapes sont explicitées dans la section 3.2 .

Pour être nommé en tant que Correspondant Entreprise, un formulaire existe sur le lien suivant : Formulaire Administrateur Douane (Correspondant Entreprise / Gestionnaire Service en Ligne)

**Etape 1** : Le Correspondant Entreprise devra :

- Créer le compte API nécessaire (cf 3.2.1)
- Puis demander l'habilitation du compte API pour initier une demande d'accès aux API souhaitées. (cf 3.2.2)

**Etape 2** : La Douane examinera cette demande d'habilitation et d'accès, et si elle est approuvée :

- Fournira une documentation technique développeur comprenant
  - les URL d'accès à utiliser pour
    - le serveur d'autorisation
    - les serveurs d'API

- des exemples d'utilisation pour les demandes de jeton
- la documentation d'utilisation des API souhaitées (Disponible en téléchargement sur le portail douane.gouv.fr)
- La douane adressera en retour les accréditations nécessaires à l'obtention de jetons d'accès
- Donnera les habilitations nécessaires au(x) compte(s) API

### 3.2 CRÉATION ET HABILITATION DE COMPTE API

#### 3.2.1 CRÉATION D'UN COMPTE API

Après avoir obtenu le droit de gérer les comptes API, le correspondant entreprise aura accès à un nouvel espace, dédié à l'administration des comptes API, dans l'application « Correspondant Entreprise » (anciennement Admin Prodouane).



Voici la liste des comptes API. Sélectionnez un compte que vous souhaitez modifier en tant que Gestionnaire Comptes API.

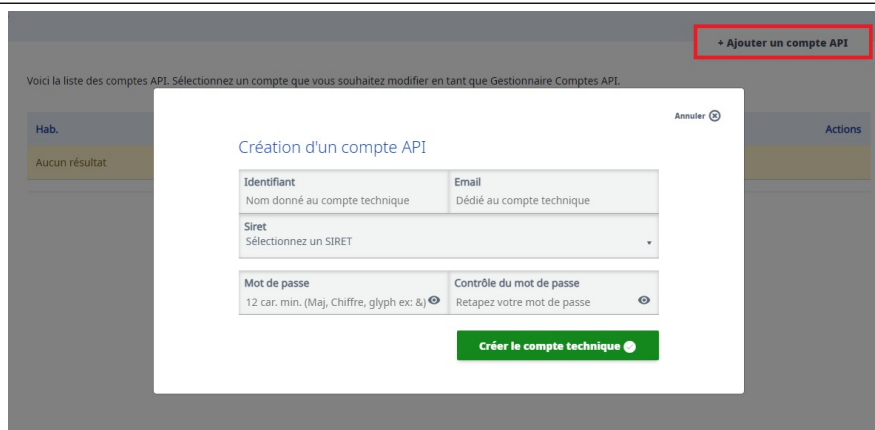
Sur cette page, le correspondant entreprise visualisera l'ensemble des comptes API dans son périmètre. Il aura également la possibilité d'en créer via le bouton « +Ajouter un compte API ».

Après avoir cliqué sur ce bouton, plusieurs informations seront demandées pour pouvoir procéder à la création du compte :




1. **Identifiant** – Correspond au nom donné au compte API
2. **Email** – Adresse mail dédiée au compte API
3. **SIRET**<sup>1</sup> – Si le correspondant entreprise est habilité sur plusieurs SIRET, il devra choisir celui sur lequel le compte API sera rattaché (il ne peut y avoir qu'un compte API rattaché à un SIRET)
4. **Mot de passe** – Choix d'un mot de passe robuste pour le compte

NB : Le mot de passe du nouveau compte technique doit respecter les conditions de sécurité suivantes : 12 caractères constitués de majuscules, minuscule, chiffres, caractères spéciaux.

1. Si le SIRET souhaité n'apparaît pas, le correspondant entreprise n'est pas habilité pour cet établissement (voir paragraphe 3.1).



Une fois le compte créé, il apparaît sur l'écran principal.

Hab.	SIRET	Identifiant	Email	Actions
	 12345678910123 NOM OPERATEUR	api-1234	xxxxxx@yyyyy.zz	

L'interface utilisateur apporte des informations via l'utilisation de code couleur et de pictogrammes dans les colonnes Hab. et Actions (Pictogramme « ! » dans un cercle rouge » sur l'image ci-dessus). Voici la signification de ces codes :

- **Rouge + Picto « ! » dans un cercle rouge** : Le compte API n'a aucune habilitation
- **Jaune + Picto « ! » dans un triangle jaune** : Le compte API est habilité mais certaines données requises sont manquantes sur une ou plusieurs API
- **Vert + Aucun Picto** : Le compte API est habilité et les données concernant les API sont complètes.

### 3.2.2 DEMANDE D'HABILITATION D'UN COMPTE API

Après avoir créé un compte API, il est nécessaire de l'habilitier sur une API pour pouvoir l'utiliser. Pour cela, le correspondant entreprise doit faire une demande pour que le compte API ait le droit en accès sur l'API ciblée.



Cette demande doit être adressée à la Douane en indiquant :

- L'identifiant de l'opérateur de l'établissement opérateur (SIRET)
- L'identifiant du compte API créé
- Les API sur lesquelles le compte API sera habilité




### 3.2.3 FINALISATION D'UN COMPTE API

Après traitement de la demande par la Douane,

**a) Si l'API ne nécessite pas de données complémentaires**, le code couleur passera au vert et le compte API sera prêt à être utilisé.


Hab.	SIRET	Identifiant	Email	Actions
	 12345678910123 NOM OPERATEUR	api-1234	xxxxxxxxx@yyyyy.zz	


b) Si l'API nécessite la saisie de données complémentaires, une fois le droit attribué, le code couleur évoluera pour passer du rouge au jaune. Cela signifie que le compte possède désormais au moins une habilitation et qu'il est nécessaire de compléter les valeurs attendues.

Hab.	SIRET	Identifiant	Email	Actions
	 12345678910123 NOM OPERATEUR	api-1234	xxxxxxxxx@yyyyy.zz	

Le correspondant entreprise devra alors les renseigner avant d'utiliser ce compte.



Pour cela dans la liste des comptes, il faut tout d'abord identifier le compte API et cliquer sur la ligne du tableau afin d'afficher les détails et habilitations de ce compte.



 12345678910123  
NOM OPERATEUR

api-1234


xxxxxxxxx@yyyyy.zz





Modifier le compte

Modifiez les infos de ce compte



Siret	Identifiant	Email	Mot de passe
12345678910123	api-1234	xxxxxxxxx@yyyyy.zz	.....

Changer l'email 

Changer le mot de passe 

---


API habilitées

API_xx 	url
Modifier 	token

La section **API habilitées** liste l'ensemble des API ainsi que les valeurs associées aux différents champs à renseigner.

Pour saisir ou modifier les valeurs, cliquer sur le bouton «Modifier» sous le nom de l'API.

API habilitées


API\_xx 

url

https://URLxxxxxx.fr

token

AjklhjkDEghjgZiygyu134

Annuler 

Enregistrer

Deux données sont modifiables pour chaque API :

- url : il s'agit de l'adresse commune des endpoints qui doivent être exposés pour recevoir les appels retours de la Douane
  - le nom de domaine devra au préalable avoir été ouvert sur le réseau de la Douane, pour cela adresser une demande à l'adresse de contact Douane de l'API concernée ;
  - le changement d'une URL n'est pas pris en compte immédiatement mais au plus tard au bout de 4h, toute modification devra donc être préparée avec le contact Douane de l'API concernée pour éviter toute rupture de service.
- token : c'est le jeton d'authentification vers le SI opérateur



- le changement d'une URL n'est pas pris en compte immédiatement mais au plus tard au bout de 15 minutes, toute modification devra donc être préparée avec le contact Douane de l'API concernée pour éviter toute rupture de service.

Si une API nécessite plus de données complémentaires, il convient de se référer à la documentation spécifique à l'utilisation de cette API.

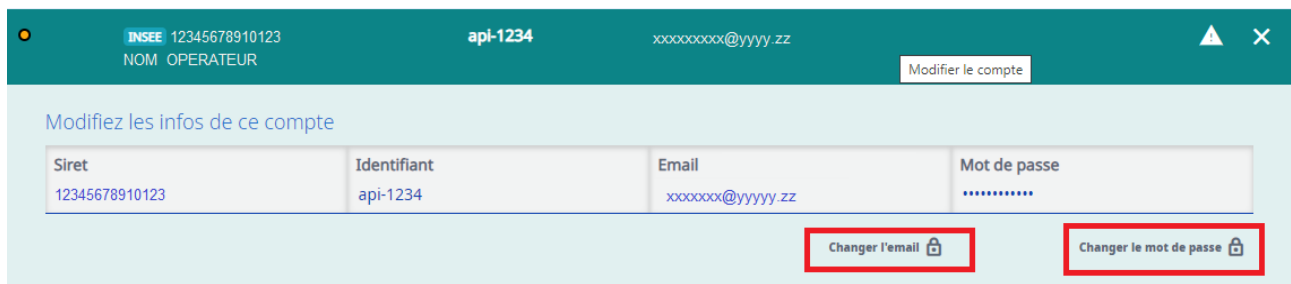
Après avoir enregistré, le compte API passe en vert au niveau du tableau. Cela signifie que ce compte technique est prêt à être utilisé.

Hab.	SIRET	Identifiant	Email	Actions
●	<b>INSEE</b> 12345678910123 NOM OPERATEUR	api-1234	xxxxxxxx@yyyyy.zz	

### 3.2.4 MODIFICATION DU COMPTE API

Depuis l'interface ci-dessous, il est possible au correspondant entreprise de modifier les informations suivantes concernant le compte :

- Email : Cette adresse servira pour notifier les administrateurs du compte API de changements ou d'incidents.
- Mot de passe



La modification du mot de passe par le correspondant entreprise est une opération pouvant impacter l'utilisation du compte API par des tiers s'ils ne sont pas synchronisés sur ce changement. Avant cette opération, le correspondant entreprise doit s'assurer que le changement, à effet immédiat, est pris en compte de manière synchronisée avec tous les systèmes informatiques qui utilisent ce compte API.

Le compte API est un compte douane.gouv (anciennement appelé compte Prodouane). Le changement de mot de passe, la fréquence de renouvellement, l'information aux clients et la bonne synchronisation du changement du mot de passe relèvent de la responsabilité de l'opérateur. Les opérateurs doivent se conformer aux bonnes pratiques concernant la gestion des mots de passe.

## 4 PARAMÈTRES TECHNIQUES DES APPELS ET EXEMPLES D'UTILISATION

Deux environnements sont ouverts aux opérateurs: **Production** et **Formation** (ce dernier environnement servant aux tests et à la certification, en sus d'éventuelles formations sur les applications effectuées en interne Douane ou opérateurs).

Les URL d'accès au serveur d'autorisation (serveur de jetons) et aux API sont déclinées dans ces 2 environnements :

- **URL d'authentification (récupération du jeton):**
  - PRODUCTION : <https://connexion-api.douane.gouv.fr/oauth2/token>
  - FORMATION : <https://connexion-api-form.douane.gouv.fr/oauth2/token>
- **URL d'API (appels des APIs avec le jeton) :**
  - PRODUCTION : <https://api.douane.gouv.fr/example/api>
  - FORMATION : <https://api-form.douane.gouv.fr/example/api>

Les données à utiliser pour l'obtention des jetons et l'accès aux API sont détaillées dans le tableau suivant. Elles peuvent varier pour chaque environnement (en particulier les données propres à l'entreprise seront différentes sur chaque environnement).

Donnée	Description	Commentaires
Client ID	Identifiant de l'application qui doit accéder à l'API - chaîne de caractères - Donnée statique : <b>gun-api</b>	Toujours utiliser la valeur 'gun-api'
Scope	Propriétés de l'appelant (application ou utilisateur) - chaîne(s) de caractères - Donnée statique : <b>openid</b>	Toujours utiliser la valeur 'openid'
Identifiant de compte API	Identifiant de l'utilisateur de l'application - chaîne de caractères - exemple_username	Renseigné par l'opérateur lors de la création du compte
Mot de passe du compte API (sensible)	Secret d'authentification de l'utilisateur - chaîne de caractères - exemple_password	Renseigné par l'opérateur lors de la création du compte. Information sensible à protéger

### 4.1 REQUÊTE D'AUTHENTIFICATION

Munie des paramètres présentés dans la section précédente, l'application souhaitant faire appel à l'API doit vérifier si elle dispose déjà d'un jeton d'accès valide :

- Si oui, elle doit l'utiliser pour appeler l'API (voir paragraphe suivant)
- Si non, elle doit demander un nouveau jeton au serveur d'authentification

La requête permettant d'obtenir un jeton d'accès « *Access Token* » correspond au flux « *Resource Owner Password Credentials Grant* » de la spécification OAuth 2.0.

Les applications doivent tenir compte du fait que

- Le jeton d'accès est valide pour une durée limitée (5 minutes) dans le temps, et il peut être utilisé pendant toute sa durée de validité pour plusieurs requêtes différentes
- Le jeton d'accès ne doit donc être renouvelé ou re-demandé que lorsqu'il a expiré ou que le serveur d'autorisation le rejette
- Un token non expiré ne doit pas être re-demandé sauf besoin impératif
- Il faut synchroniser les serveurs clients via le protocole NTP pour pouvoir assurer la cohérence des temps entre la Douane et l'application cliente. Un décalage de l'ordre de quelques millisecondes peut nativement prendre place entre les différentes machines

synchronisées via le protocole NTP, mais ce dernier rentre dans les limites tolérées par NTP.

•

Selon l'utilisation que les applications opérateurs souhaitent faire des API's, en particulier lors de pics de charge, il est recommandé à l'opérateur de mettre en place un service de mutualisation du jeton pour plusieurs requêtes. Cela correspond au développement d'une procédure automatique de récupération d'un nouveau Token lorsque le Token précédent a expiré.

#### 4.2 EXEMPLE DE REQUÊTE HTTPS

La requête HTTPS à envoyer au serveur d'authentification doit être de type POST, et passer les paramètres suivants via l'encodage application/x-www-form-urlencoded:

- grant\_type doit contenir la chaîne : password
- client\_id doit contenir le paramètre "Client ID"
- scope doit contenir le paramètre "Scope"
- username doit contenir le paramètre "Identifiant du compte API"
- password doit contenir le paramètre "Mot de passe" du compte API

Voici un exemple de capture de la requête HTTPS d'authentification, avec les paramètres d'exemple:

```
POST /oauth2/token HTTP/1.1
Host: connexion.moa.douane.gouv.fr
Accept: application/json
Content-Length: 118
Content-Type: application/x-www-form-urlencoded

grant_type = password & client_id = gun-api & scope = openid & username =
Compte_API_username&password = Compte_API_password
```

Voici un exemple d'utilisation de la commande curl permettant de tester une requête d'authentification :

```
curl -s \
-d grant_type=password \
-d client_id=gun-api \
-d scope="openid" \
-d username=example_username \
-d password="example_password" \
https://connexion-api-moa.douane.gouv.fr/oauth2/token
```

#### 4.3 EXEMPLE DE RÉPONSE DU SERVEUR D'AUTORISATION

Le serveur d'autorisation répond à la requête en fournissant le code HTTPS 200 et un document au format JSON. Ce document, une fois dé-sérialisé, doit être de type "Objet".

Si le code de réponse du serveur d'autorisation est 200, alors le document doit contenir les clés suivantes :

- `access_token`: de type "Chaîne", contient l'Access Token à utiliser
- `expires_in`: de type "Entier", contient le nombre de secondes à compter de la réponse du serveur pendant lequel ce jeton sera valide
- `token_type` : de type "Chaîne", le type de token ex : "Bearer"
- `refresh_token` : de type « Chaîne », permet de récupérer un nouveau `access_token` lorsque celui-ci devient invalide
- `id_token` : Un ID Token est un jeton qui contient l'identité d'un utilisateur. Il est véhiculé au format JWT .

Si le code de réponse du serveur d'autorisation est 400, alors le document peut contenir les clés suivantes:

- `error` (obligatoire): indique le code technique de l'erreur survenue pendant la tentative d'authentification
- `error_description` (optionnel): fournis une chaîne descriptive de l'erreur

Tout autre code HTTP doit être également traité comme une erreur. Les codes techniques d'erreur disponibles sont détaillés dans la section 5.2 de la norme OAuth2.0.

## Réponse d'autorisation avec succès

Voici un exemple de réponse indiquant un succès d'authentification :

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Fri, 03 Apr 2020 09:13:42 GMT

{
  "refresh_token": "5fc5974da9bbf6c821d63b9a3eca7f0aac999b0f984c3e619396b734d2574b2f",
  "expires_in": 300,
  "id_token":
    "eyJhbGciOiJSUzUxMiIsInR5cCI6IkpXVCJ9.eyJhY3IiOiJsbnE2EtMiIsImV4cCI6MTY3MTUyNjJE
    xOSwiaXNzIjoiaHR0cHM6Ly90ZXN0Y29ubmV4aW9uLmRvdWFuZS5nb3V2LmZyLyIsImF1d
    GhfdGlZSI6MTY3MTUxODkxOSwic3ViIjoiaSDdfQVBjIiwiaWF0IjoxNjcNTE4OTE5LCJhen
    AiOiJndW4tYXBpIiwiaXYXRfaGFzaCI6ImlVDSjk3ZzdMWUpzd0JzWWZDckV3dTTF2elQya1JYcE9
    aajQ0OFdBZW51VEkiLCJhdWQiOiolsiZ3VuLWFwaSJdfQ.Qtn6hTWarS4tPbFNLU8Xbmq674q
    AwLh0IaRCD3PyrAOJKMJ2i_GT3nDkcBUWiFGYmAnUmeBVACDPW5QO2Wd0rQE-
    pGMWtVIPGnxqycWwPdXxjQdqGYp1XcHs52OcdVpYhZe3PIRnpUrd-
    5gqubQ5EK_MMCPDWJ4a5x0HsNnwG43ux5XVXhct1QuOffccjct4ushtcjVvS-PFVG6q-
    tY9JCnqnZCLRJJRtR1A6TX8yZfhsDHZZa_IDv2d3hH5TVegCM_zhSPHE394R4zf2AceABc4j
    YlG6AsEY44B449-1tpHUABO8rr-0WZu0eEnIE_XM_7EAEEh6YR1eN5DFmkg",
  "access_token": "13af94aee8ee878666b3d89091ff3b544448ceb98bdd489bf48e1dc36e7ad7ae",
  "token_type": "Bearer"
}
```

## Réponse d'autorisation en erreur

Voici un exemple d'échec d'authentification :

```
HTTP/1.1 400 Bad request
Content-Type: application/json
Date: Fri, 03 Apr 2020 09:21:00 GMT
```

```
{  
  "error": "invalid_grant"  
}
```

#### 4.4 APPELS À L'API

Une fois qu'un jeton a été obtenu, ce dernier doit être utilisé pendant toute sa durée de vie afin de ne pas surcharger le serveur d'autorisation. Il est toutefois permis de prendre une marge de sécurité de quelques minutes au moment du renouvellement.

L'appel à l'API se fait via la sémantique REST détaillée dans la documentation de l'API.

Chaque requête REST envoyée à l'API devra présenter un jeton valide via un en-tête HTTP, comme indiqué dans la section 2.1 de la RFC6750 (Bearer Token usage).

L'en tête HTTP à utiliser est `Authorization` et son contenu doit être le mot clé `Bearer` suivi d'un espace suivi de la chaîne représentant un jeton valide, fourni par le serveur d'authentification.

#### Exemple d'appel à l'API

Pour cet exemple, nous utiliserons une API fictive répondant à une requête GET sur l'URL `https://api.douane.gouv.fr/example/api`.

```
GET example/api  
Host: api-moa.douane.gouv.fr  
Authorization: Bearer c3MiXX0slnNjb3Blljoib3Blbm  
La commande curl permettant de simuler cette requête est la suivante:  
curl \  
  -H "Authorization: Bearer c3MiXX0slnNjb3Blljoib3Blbm" \  
  https://api-moa.douane.gouv.fr/example/api
```

#### Exemple de réponse du serveur

Si le jeton fourni via l'en-tête `Authorization` est valide, le serveur répondra avec un code HTTP 200.

En revanche, si le jeton n'est pas valide, le serveur répondra avec un code d'erreur compris entre 400 (inclus) et 500 (exclus), et la réponse contiendra un en-tête `WWW-Authenticate` détaillant l'erreur rencontrée, suivant la section 3 de la RFC6750. Le code d'erreur `invalid_token` sera utilisé pour indiquer un jeton invalide ou expiré.

Voici un exemple de réponse du serveur en cas de jeton invalide :

```
HTTP/1.1 401 Unauthorized  
WWW-Authenticate: Bearer error="invalid_token"
```

## Références

- Resource Owner Password Credentials Grant : <https://tools.ietf.org/html/rfc6749#section-4.3>
- OAuth 2.0 Error response: <https://tools.ietf.org/html/rfc6749#section-4.3>
- Bearer Token usage: <https://tools.ietf.org/html/rfc6750#section-2.1>
- Bearer Token errors: <https://tools.ietf.org/html/rfc6750#section-3>