CAREERPRO - FEDERAL LEARNING ACCOUNT

Établir le canal REST API

31/01/2025

Un service de

asbl Sigedis vzw Place Victor Horta / Victor Hortaplein 11(P3) Bruxelles 1060 Brussel T +32 (0)2 791 50 00 M info@sigedis.fgov.be www.sigedis.be

Historique du document		
Date	**Description**	**Page concernée**
01/04/2024	Première publication du document	
17/09/2024	Ajout des certificats selfSigned pour la création du compte REST. Ajout de la qualité « prestataire de formation »	9,12
31/01/2025	Ajout du lien vers la documentation généraliste du portail de la sécurité sociale https://www.rest-documentation.socialsecurity.be/index.html	4

Table des matières

1. Introduction ... 4

1.1. Objectif du document ... 4

2. Type d'utilisation du canal API ... 5

2.1. Utilisation générale ... 5

2.2. Spécificité des mandataires ... 5

2.2.1. Création d'un mandat ... 5

2.2.2. Utilisation du canal ... 6

2.3. Spécificité des groupes d'entreprises ... 8

2.4. Spécificité des fournisseurs de logiciel ... 9

2.5. Spécificité des prestataires de formation ... 9

3. Configuration du canal API ... 10

4. Plan étape par étape du gestionnaire de l'entreprise ... 11

4.1. Étape 1 : Identifiez-vous comme employeur sur le portail de la Sécurité Sociale ... 11

4.2. Étape 2 : S'inscrire comme employeur sur le portail de la Sécurité Sociale ... 11

4.3. Étape 3 : obtenir un accès au service en ligne 'CHAMAN' ... 11

4.4. Etape 4 : activer un compte Webservice REST ... 11

4.4.1. **Étape 4a : créer un compte Webservice REST** ... 11

4.4.2. **Étape 4b : modifier un compte Webservice REST existant** ... 15

5. Activer une nouvelle qualité (ex prestataire de formation) ... 18

6. Plan étape par étape du développeur de l'application ... 19

6.1. Étape 1 : mettre en place la sécurité OAUTH ... 19

6.2. Étape 2 : appel vers la restAPI CareerPro Fla ... 20

6.3. Environnement de test ... 20

7. Annexe ... 22

7.1. Identifier son gestionnaire local d'accès ou son responsable d'accès entité ... 22

7.2. Oauth exemple ... 22

7.3. Outils ... 23

7.3.1. Appel restAPI avec PostMan ... 23

7.3.2. Ouvrir un certificat ... 24

1. Introduction

Différents canaux ont été développés pour la plateforme FLA afin de permettre à l'employeur de transmettre aussi facilement que possible des données de formation FLA.

Les grandes entreprises qui travaillent avec des plateformes numériques pour sauvegarder leurs données de formation peuvent utiliser le transfert via des fichiers BATCH ou via un service web (canal en ligne, REST API). Les petites et moyennes entreprises qui ne sauvegardent pas encore ou ne sauvegarderont pas de données de formation via une plateforme numérique peuvent utiliser la WebApp CareerProFLA mise à disposition via careerpro.be.

1.1. Objectif du document

La documentation ci-dessous décrit les différentes étapes à suivre pour mettre en place la communication entre les systèmes informatiques de l'employeur et ceux de la plateforme FLA (via le portail de la Sécurité Sociale) en ce qui concerne le service web « CareerProFLA API ».

La majeure partie des informations sont extraites de la documentation du portail de la sécurité sociale :

https://www.rest-documentation.socialsecurity.be/index.html

Ce document fait partie des documents mis à disposition de l'employeur et de son mandataire :

Document	Description
Manuel du canal BATCH	Document qui décrit les étapes nécessaires pour transmettre les données FLA via le canal BATCH.
Manuel du canal API	Document qui décrit les étapes nécessaires pour transmettre les données FLA via le canal API.
Manuel de l'application en ligne	Document qui décrit les étapes nécessaires pour encoder les données FLA via l'application en ligne.
Description des anomalies	Aperçu de toutes les anomalies et avertissements (warnings) relatifs à la déclaration des données FLA.
Glossaire	Documentation technique qui décrit les blocs et zones de données du batch et de l'API.
XSD	Schéma technique qui définit la structure du BATCH.
SWAGGER	Schéma technique qui définit la structure de l'API.
Etablir le canal BATCH	Document qui décrit les étapes nécessaires pour configurer le canal BATCH sur le portail de la sécurité sociale.
Etablir le canal API	Document qui décrit les étapes nécessaires pour configurer le canal webservice (API) sur le portail de la sécurité sociale.
Obtenir un accès à l'application en ligne	Document qui décrit les étapes nécessaires pour qu'un utilisateur obtienne un accès à l'application en ligne *CareerPro Federal Learning Account*.

2. Type d'utilisation du canal API

2.1. Utilisation générale

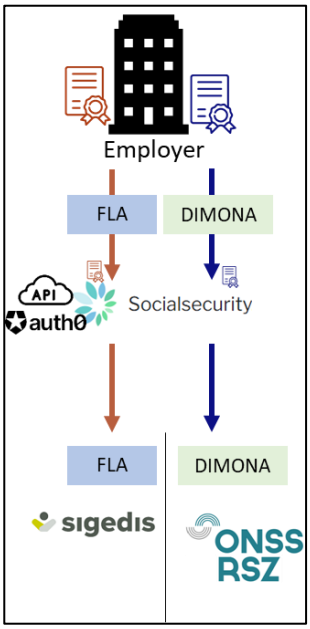
Les utilisateurs (les employeurs ou leur mandataire) devant faire un grand nombre d'enregistrements dans le *Federal Learning Account (FLA)* ou les prestataires de formation peuvent envoyer les données par le biais d'appel webservice REST API. Ces appels REST API utilisent le canal webservice de la sécurité sociale.

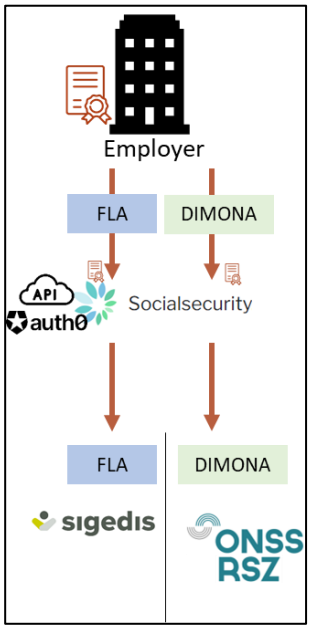
Pour une qualité donnée (employeur, prestataire de service, secrétariat social, prestataire de formation), l'utilisateur peut

- soit créer un compte webservice par type de flux. Par exemple, il peut créer un compte dédié aux données Dimona et un autre compte dédié aux données *Federal Learning Account*. Chaque compte peut avoir son propre certificat de sécurité;
- soit créer un compte webservice commun à tous les flux. Dans ce cas, le certificat de sécurité est commun à tous les flux.

Exemple 1 :
À gauche : Un employeur utilise des comptes webservices dédiés pour deux services (FLA et Dimona).

À droite : un employeur utilise un compte webservice commun pour les deux services.





2.2. Spécificité des mandataires

Un employeur peut mandater une (ou plusieurs) entreprises (un prestataire de service ou un secrétariat social) pour gérer son fichier du personnel, remplir ses déclarations et accomplir d'autres actes administratifs.

Par exemple, un employeur peut mandater une entreprise pour envoyer ses données Dimona et *Federal Learning Account* en son nom. Cela signifie que le mandataire (= le prestataire ou le secrétariat social) envoie les données avec le numéro d'entreprise du mandant (= employeur). Pour que l'envoi soit accepté par le système, il est nécessaire qu'un mandat officiel actif existe entre le mandataire et le mandant pour le type de données.

2.2.1. Création d'un mandat

Dans ce cas de figure, il est nécessaire de créer un mandat pour le service souhaité, dans notre cas « *Federal Learning Account ».* Ce mandat liera le mandant (l'employeur) et le mandataire (prestataire/secrétariat social). La création d'un mandat peut être réalisée à l'aide du service MAHIS de la sécurité sociale. Ce service est disponible sur :

www.socialSecurity.be → entreprise → service en ligne → MAHIS

Remarques :

- Certaines conditions doivent être respectées pour qu'une entreprise puisse devenir mandataire. Ces conditions se trouvent également sur la page du service MAHIS (document « *Lignes de conduite pour prestataires de services* »).
- L'employeur ne peut avoir qu'un seul mandataire pour le service *Federal Learning Account*. Par contre ce mandataire peut être différent de celui (ceux) des autres services de la sécurité sociale.

2.2.2. Utilisation du canal

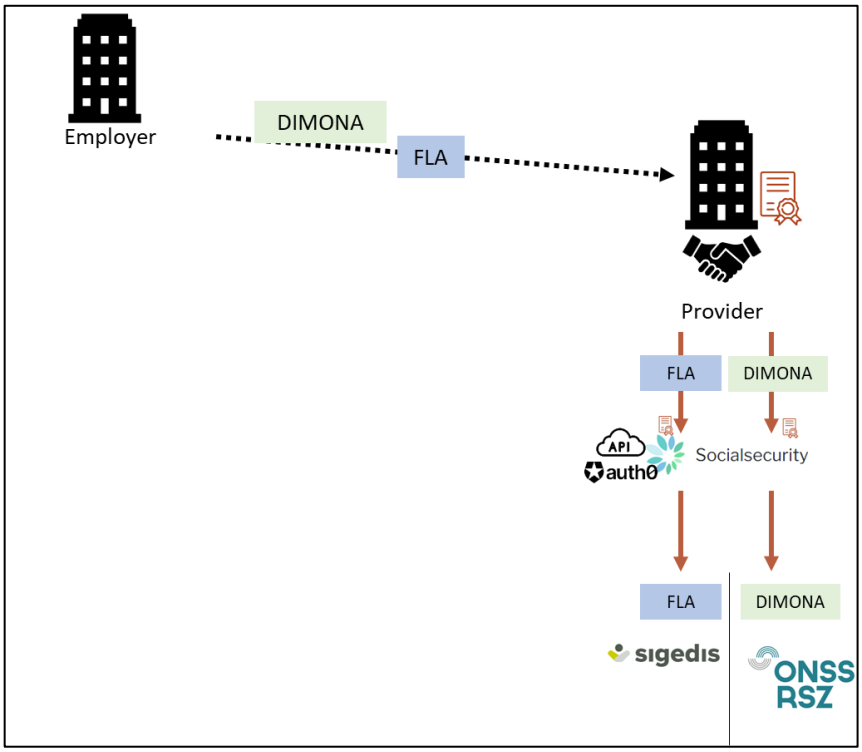
Une fois que le mandat est activé, l'envoi des données du *Federal Learning Account* par le mandataire peut commencer.

Concrètement, l'employeur fournit à son mandataire les informations nécessaires pour que ce dernier puisse déclarer les données du *Federal Learning Account*. Ce transfert d'information peut prendre différentes formes selon la convention établie entre le mandant et le mandataire. Par exemple, il peut s'agir d'un encodage de l'employeur dans une application du mandataire.

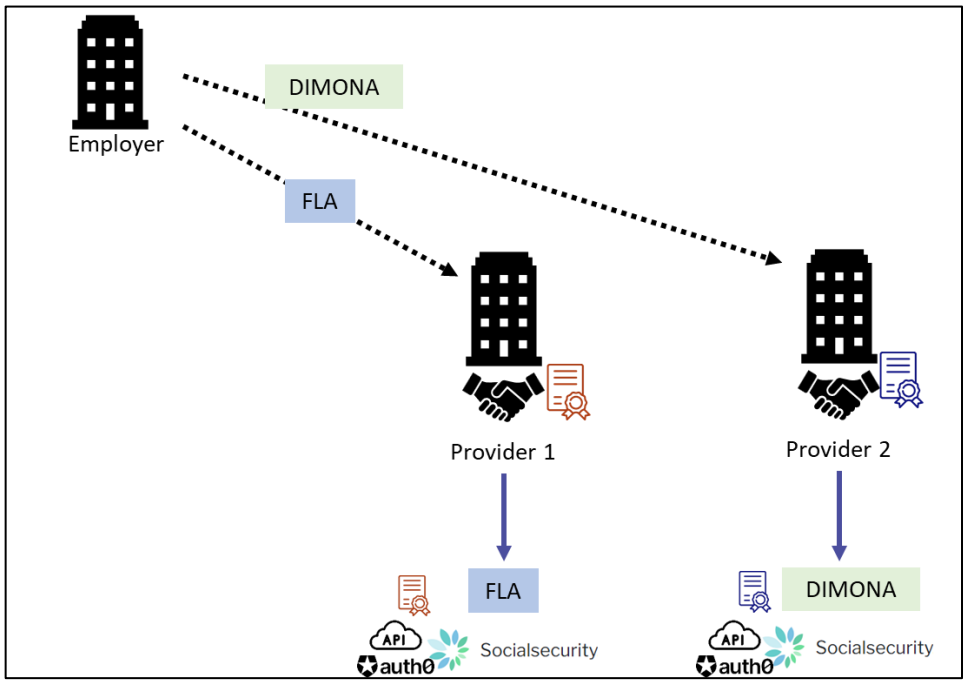
Ensuite, le mandataire envoie les données *Federal Learning Account* de ses clients (employeurs) à l'aide de son compte webservice mandataire pour ce type de données (configuré au préalable). Cela signifie que :

- le mandataire enverra les données de tous ses clients (employeurs) avec le même compte webservice (celui avec le service *Federal Learning Account*). Le même certificat de sécurité sera donc utilisé;
- les employeurs n'ont pas besoin d'avoir leur propre compte webservice;
- l'employeur peut avoir un mandataire *Federal Learning Account* différent de son mandataire des autres services (Dimona, ...).

Exemple 2 : employeur passe par un seul mandataire (appelé provider) pour tous ses services (FLA et Dimona). Dans ce cas-ci, le mandataire à un seul compte webservice.

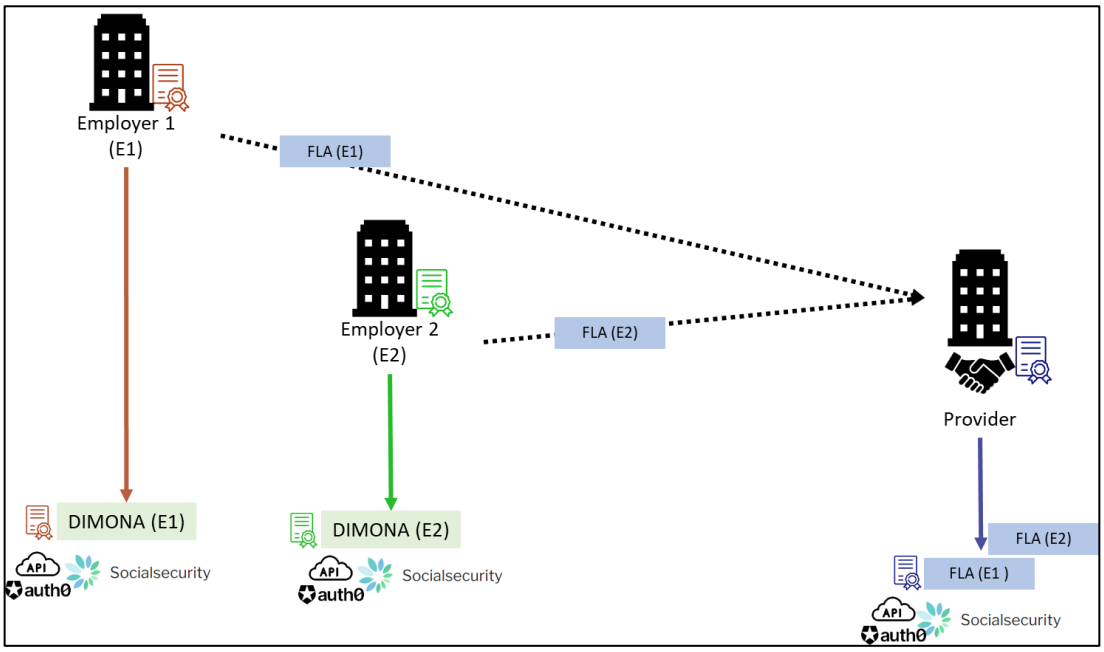


Exemple 3 : employeur passe par un mandataire (appelé provider) spécifique pour les données du *Federal Learning Account*.



Il est possible également d'avoir des exemples mixtes : une partie des services d'un employeur passe via un mandataire, tandis que l'autre partie non.

Exemple 4 : deux employeurs envoient eux-mêmes leurs données des services Dimona mais passent par un même mandataire pour les données du *Federal Learning Account*.

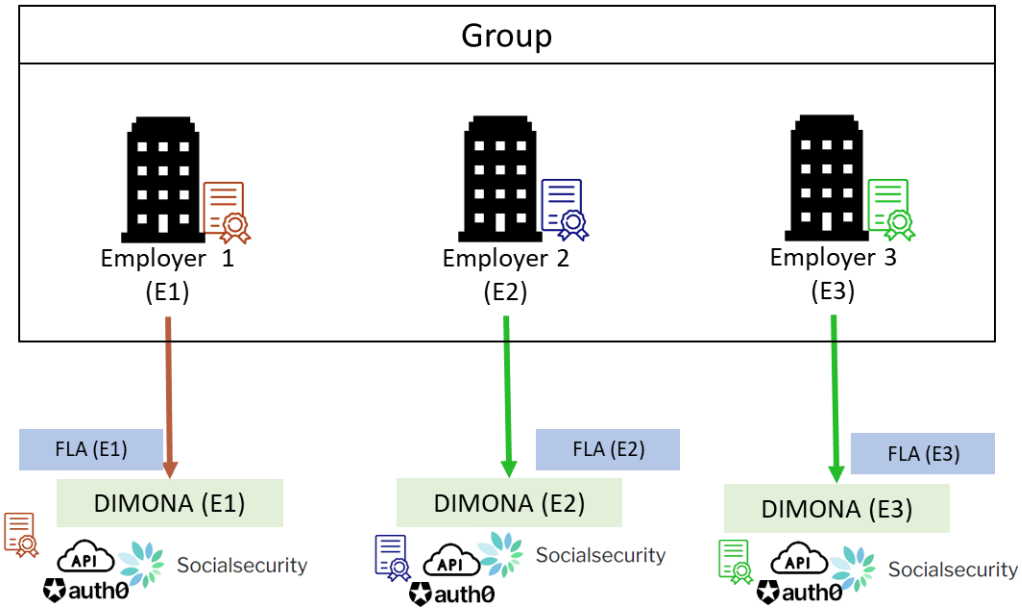


2.3. Spécificité des groupes d'entreprises

Lorsque des sociétés avec des numéros d'entreprise (n° BCE) distincts sont liées entre-elles (ex : holding/filiale, groupement, …), elles ont deux possibilités pour transmettre les données du *Federal Learning Account :*

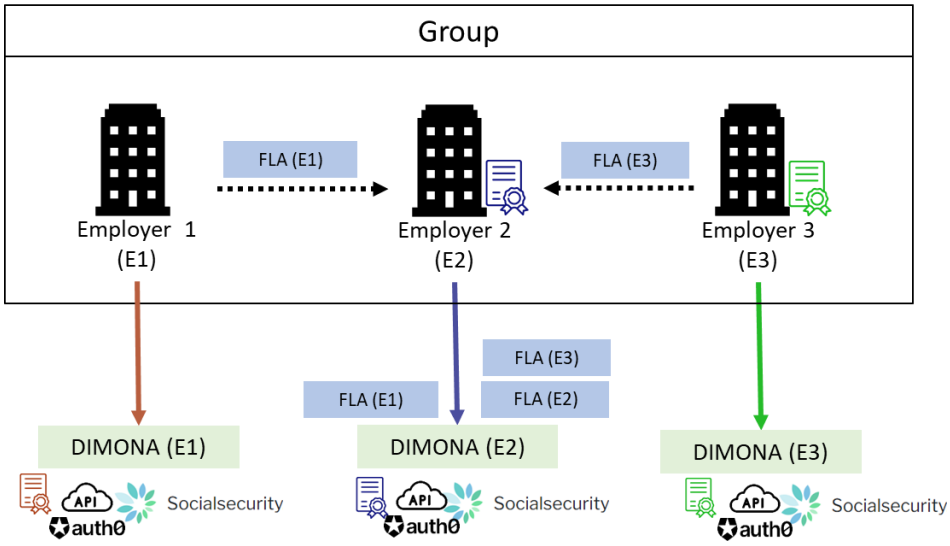
1) Chaque entreprise déclare les données de ses travailleurs en utilisant son propre canal. Dans cette option, un compte webservice doit être créé pour chaque n° BCE (et donc besoin d'un certificat par n° BCE).

   Exemple 5 : Soit un groupe composé de trois entreprises. Chacune des trois entreprises déclarent les données de ses propres travailleurs (un seul compte webservice par entreprise).



2) Une entreprise devient, dans le cadre des données *Federal Learning Account*, mandataire pour toutes les autres entreprises du groupe. Cette solution est identique au cas des mandataires.

   Exemple 6 : Soit un groupe composé de trois entreprises. L'entreprise 2 est mandatée par les deux autres entreprises pour fournir les données du *Federal Learning Account* pour l'entièreté du groupe. Cette entreprise 2 crée un seul compte webservice pour les FLA et Dimona.



Remarque :

L'envoi des données du *Federal Learning Account* d'un travailleur se fait toujours pour le n° BCE de l'entreprise qui doit effectuer les Dimona et DmfA de ce même travailleur. Cette entreprise peut être l'entité représentant le groupement d'entreprises.

2.4. Spécificité des fournisseurs de logiciel

Lorsqu'une entreprise fournit à des employeurs un logiciel permettant d'envoyer des données du *Federal Learning Account*, le type d'utilisation du canal webservice dépend de la situation.

1) Si le logiciel est centralisé au niveau du fournisseur ou que ce dernier a une convention pour envoyer les données FLA au nom de l'employeur, alors le système de mandat doit être utilisé (cf. 2.2 Spécificité des mandataires). Le fournisseur enverra lui-même les fichiers de données de ses employeurs.
2) Si le logiciel « tourne en autonomie» ou que le fournisseur n'a pas de convention avec l'employeur, alors l'utilisation générale doit être utilisé : chaque employeur créé son canal/compte webservice et envoi les données vers la restAPI (avec ou sans aide de l'application du fournisseur).

2.5. Spécificité des prestataires de formation

Une entreprise de qualité « prestataire de formation » est une entreprise qui offre des services de formations à des employeurs. C'est elle qui organise et donne les sessions de formation à des participants.

En vue de faciliter la tâche d'encodage des employeurs, une entreprise « prestataire de formation » peut fournir à la plateforme FLA les données sur les formations qu'elle a organisées. Dans ce cadre, l'entreprise utilise le canal technique BATCH/API avec la qualité « prestataire de formation ».

Le prestataire de formation envoie les données de formation en leur propre nom, c'est-à-dire avec leur propre numéro BCE. Les données fournies par un prestataire de formation peuvent, éventuellement, renseigner l'employeur d'un participant. Même si l'employeur d'un participant est précisé dans les données, aucun mandat entre le prestataire de formation et cet employeur n'est nécessaire.

Pour créer un canal technique dans cette qualité-là, il est d'abord nécessaire de créer la qualité. Cf « 5. Activer une nouvelle qualité (p.e. prestataire de formation) »

3. Configuration du canal API

Le service informatique de l'entreprise (l'employeur ou du mandataire selon la situation) ou le fournisseur de logiciel intègre cette API dans un système informatique existant (ou nouveau).

Si l'entreprise n'utilise pas encore (aucun) service web REST de la Sécurité Sociale et/ou si l'entreprise n'a pas été préalablement identifiée via le portail de la Sécurité Sociale, celui-ci doit d'abord être configuré.

En fonction de la situation ci-dessus, certaines ou la plupart des étapes de ce manuel peuvent déjà être considérées comme terminées.

4. Plan étape par étape du gestionnaire de l'entreprise

Avant de pouvoir utiliser le service REST FLA, le service web REST de la Sécurité Sociale doit être configuré. Le client (employeur) doit suivre les étapes suivantes pour créer un profil et organiser la sécurité.

4.1. Étape 1 : Identifiez-vous comme employeur sur le portail de la Sécurité Sociale

Si vous êtes déjà connu comme employeur au sein de la Sécurité Sociale, cette étape peut être considérée comme terminée.

Pour utiliser les services en ligne de la Sécurité sociale, l'entreprise doit être connue comme employeur sur le portail de la sécurité sociale. Veuillez suivre les étapes suivantes si ce n'est pas déjà le cas : https://www.socialsecurity.be/site_fr/general/first_visit/access/register-as-employer.htm

4.2. Étape 2 : S'inscrire comme employeur sur le portail de la Sécurité Sociale

Si vous êtes déjà inscrit sur le portail, cette étape peut être considérée comme terminée.

Si vous êtes connu au sein de la Sécurité Sociale comme employeur ONSS, vous devez déterminer si vous souhaitez conserver la gestion et l'utilisation des accès sécurisés au sein de votre entreprise ou l'externaliser.

Vous pouvez poursuivre cette inscription sur le portail via le lien suivant :

https://www.socialsecurity.be/site_fr/employer/infos/employer_onss/registration_gen/register/register.htm

4.3. Étape 3 : obtenir un accès au service en ligne 'CHAMAN'

La configuration d'un canal technique (BATCH ou API) peut être réalisée uniquement par un utilisateur qui a accès à l'application Chaman de la sécurité sociale dans la qualité voulue.

Les personnes qui ont accès à Chaman sont :

- le « **Gestionnaire local** » de la qualité voulue (Employeur ONSS, prestataire de service, secrétariat social ou prestataire de formation). Ce dernier est défini lors de l'inscription de l'entreprise sur le portail ou lors de l'activation d'une nouvelle qualité. Cf « 5. Activer une nouvelle qualité (p.e. prestataire de formation) »;
- tout utilisateur qui a reçu un accès via son gestionnaire local. Le gestionnaire local de la qualité voulue (employeur ONSS, prestataire de service, secrétariat social ou prestataire de formation) peut donner un accès au service en ligne 'Chaman' à l'aide du service en ligne 'Gestion des accès' de la sécurité sociale (socialsecurity.be).

  Si vous n'avez pas accès à Chaman, vous devez demander à votre gestionnaire local de vous attribuer la 'Gestion des canaux techniques' dans le service en ligne 'Gestion des accès'.

4.4. Etape 4 : activer un compte Webservice REST

Si votre entreprise a déjà créé un compte webservice REST pour la qualité qui vous concerne (qualité employeur, secrétariat social, prestataire de service ou prestataire de formation) dans le cadre d'une autre application de la sécurité sociale (Dmfa, Dimona, …), alors il est possible de l'utiliser pour le cadre FLA. Dans ce cas de figure, veuillez suivre « l'étape Étape 4b : modifier un compte Webservice REST existant»

Dans le cas contraire, veuillez suivre « Étape 4a : créer un compte Webservice REST».

Remarque

Pour certaines entreprises, il est possible que la plateforme FLA soit utilisée sous plusieurs qualités différentes :

- la qualité employeur pour permettre à l'entreprise d'envoyer les données FLA de ses propres travailleurs
- la qualité mandataire (prestataire de service ou secrétariat social) pour permettre à l'entreprise d'envoyer les données FLA des travailleurs de ses clients
- la qualité prestataire de formation pour permettre à l'entreprise d'envoyer les données de formation qu'elle a organisé pour des employeurs

Dans ce cas de figure, il sera nécessaire de créer plusieurs compte webservice REST : au minimum, un par qualité.

4.4.1. Étape 4a : créer un compte Webservice REST

Étape à suivre si votre entreprise n'a pas encore de compte webservice REST dans la qualité voulue ou que vous souhaitez créer un compte spécifique pour l'application CareerPro Federal Learning Account. Dans le cas contraire, allez à l'étape 4b.

Prérequis :

Pour créer un nouveau compte Webservice REST, vous devez disposer d'un certificat qualifié exporté[1] sous la forme « .cer ». Plusieurs options s'offrent à vous :

- Vous pouvez commander ce certificat auprès d'une autorité de certification reconnue. Voici la liste des autorités de certification actuellement supportées :

Autorité de certification	Type de certificat	Lien
GlobalSign	PersonalSign 3 Pro	https://shop.globalsign.com/en/belgian-government-services

- Vous pouvez utiliser un certificat self-signed au nom de votre entreprise. La procédure pour générer ce type de certificat n'est pour l'instant pas décrite ici. La génération de ce type de certificat est généralement prise en charge par le service informatique de votre entreprise via l'utilisation d'un outil tel que OpenSSL. Veuillez respecter les contraintes suivantes lors de la création de votre certificat self-signed :

Critère à respecter	Valeurs admises
Algorithme de génération de la paire de clés	RSA ou EC
Taille des clés (bits)	Pour RSA : 2048, 3072 ou 4096
Pour EC : P-384 ou P-521	
Algorithme de digest associé à la signature du certificat	SHA-256, SHA-384 ou SHA-512
Key Usage du certificat	Digital Signature

Ce certificat sera utilisé

- pour créer le compte webservice;
- pour authentifier votre système informatique sur le portail via le protocole de sécurité oAuth, c'est à dire pour obtenir le token de sécurité nécessaire lors d'un appel vers la REST API FLA.

Étapes :

1. L'utilisateur (qui a accès à Chaman) se connecte à l'application « Chaman »

   www.socialSecurity.be → entreprise → Vers tous les services en ligne → Chaman → gérer vos canaux techniques

2. Choisissez le public cible « Entreprise »

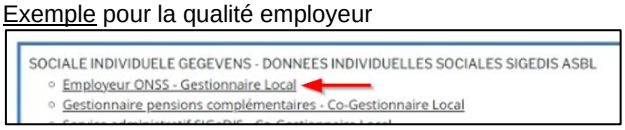
3. Connectez-vous avec CSAM et suivez les instructions pour utiliser la méthode voulue (eID, itsme, ...)

4. Si votre entreprise possède plusieurs qualités, vous devez choisir la qualité voulue:

[1] Cf « 7.3.2 Ouvrir un certificat »

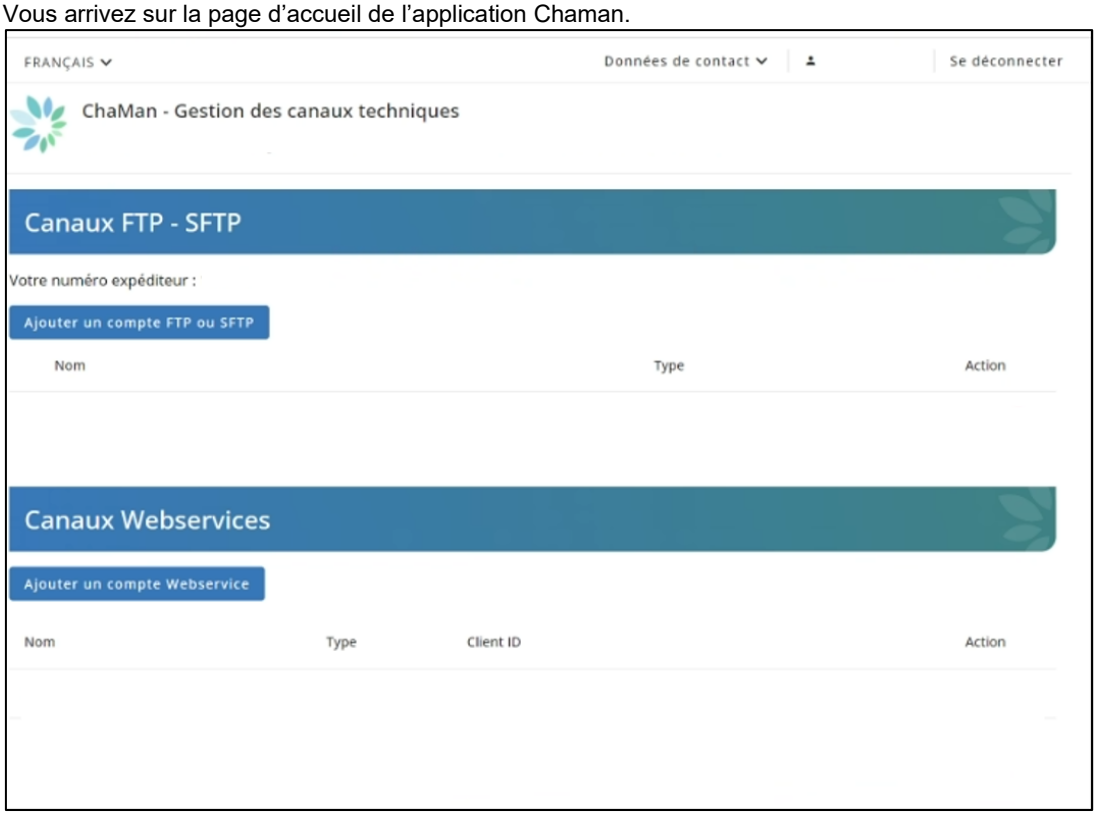
- « Employeur ONSS » dans le cas de l'utilisation du canal API par un employeur sans passer par un mandataire;
- « Secrétariat social » ou « prestataire de service » dans le cas de l'utilisation du canal API par un mandataire.
- « Prestataire de formation » dans le cas de l'utilisation du canal API pour l'envoi de données de formation que l'entreprise a organisé pour des employeurs

Exemple pour la qualité employeur



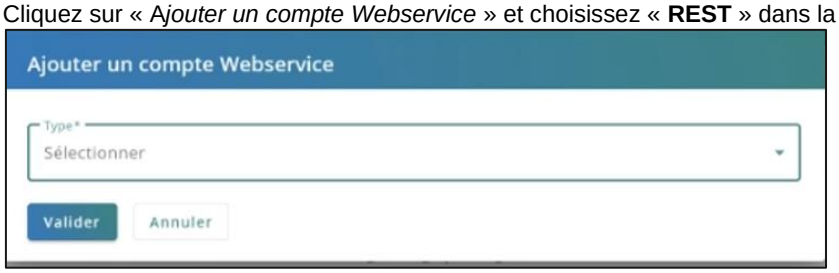
Remarque :
Si la qualité voulue n'est pas disponible, alors votre gestionnaire d'accès principal doit la créer dans l'outil « gestion des accès ». Les autres qualités ne permettent pas de créer un canal API pour le Federal Learning Account.

5. Vous arrivez sur la page d'accueil de l'application Chaman.

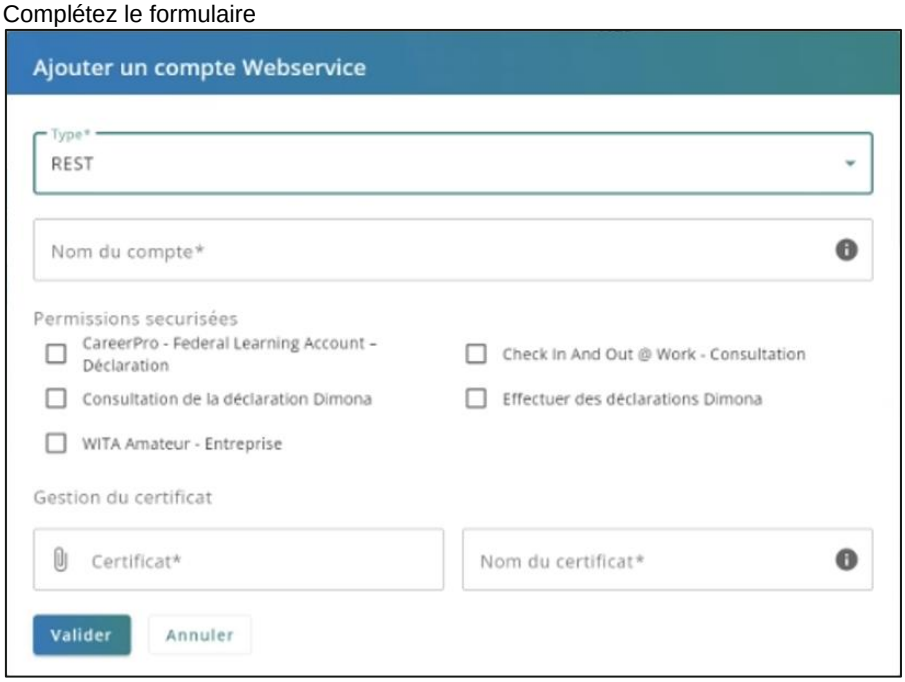


Remarque : si vous obtenez un message d'erreur « accès interdit », contactez votre gestionnaire local pour qu'il vous attribue un accès à Chaman.

6. Cliquez sur « *Ajouter un compte Webservice* » et choisissez « **REST** » dans la zone « *Type** »



7. Complétez le formulaire



- Nom du compte : donnez un nom libre purement indicatif.
- Dans les permissions, cochez « CareerPro – Federal Learning Account - Déclaration ».
- Certificat : chargez dans ce champ la clé publique (.cer) de votre certificat (cf. prérequis).
- Nom du certificat : donnez un nom à votre certificat.

8. « Valider »

Le Client ID sera affiché dans la ligne du compte webservice REST que vous venez de créer. Il est conseillé de conserver cette information car elle sera utilisée ultérieurement(= clientId oauth).

4.4.2. *Étape 4b : modifier un compte Webservice REST existant*

Étape à suivre si votre entreprise a déjà un compte webservice REST dans la qualité voulue et que vous souhaitez le réutiliser pour l'application CareerPro Federal Learning Account. Dans le cas contraire, passez à l'étape 4a.

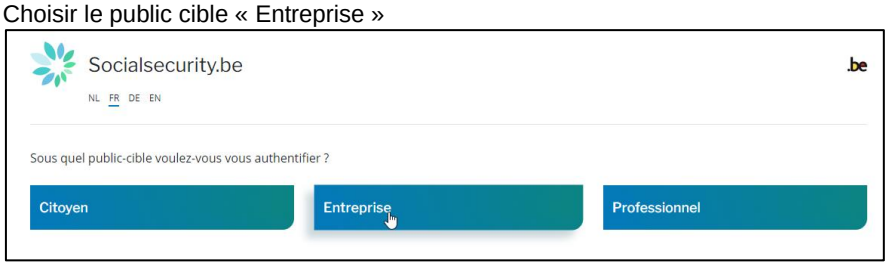
Si vous avez déjà un canal webservice REST actif dans la qualité voulue et que vous souhaitez le réutiliser, il ne sera pas nécessaire de prévoir un nouveau certificat. Le certificat existant sera utilisé.

Étapes :

1. L'utilisateur (qui a accès à Chaman) se connecte à l'application « Chaman ».

   www.socialSecurity.be → entreprise → service en ligne → Chaman → gérer vos canaux techniques

2. Choisir le public cible « Entreprise »

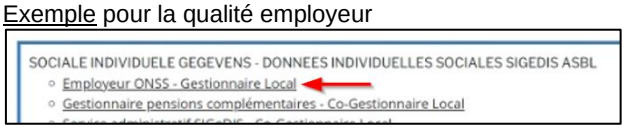


3. Se connecter avec CSAM et suivre les instructions pour utiliser le eID ou itsme

Si votre entreprise possède plusieurs qualités, vous devez choisir la qualité :

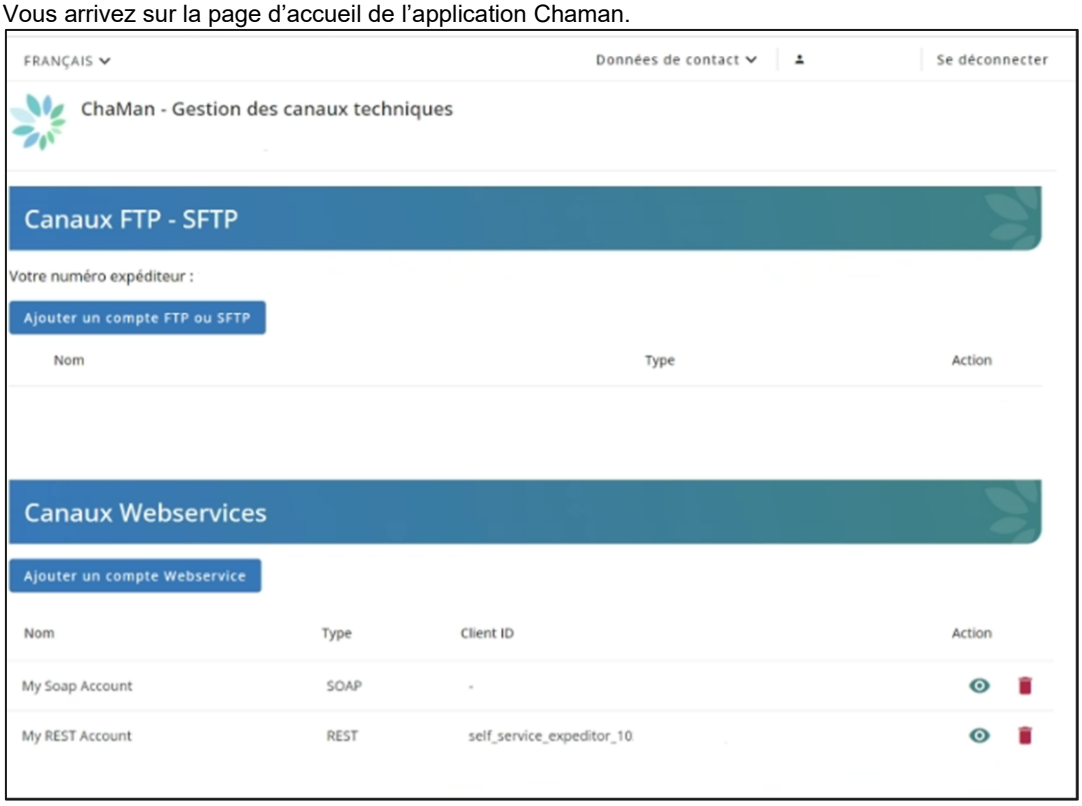
- « Employeur ONSS » dans le cas de l'utilisation du canal API par un employeur sans passer par un mandataire.
- « Secrétariat social » ou « prestataire de service » dans le cas de l'utilisation du canal API par un mandataire.
- « Prestataire de formation » dans le cas de l'utilisation du canal API pour l'envoi de données de formation que l'entreprise a organisé pour des employeurs

Exemple pour la qualité employeur

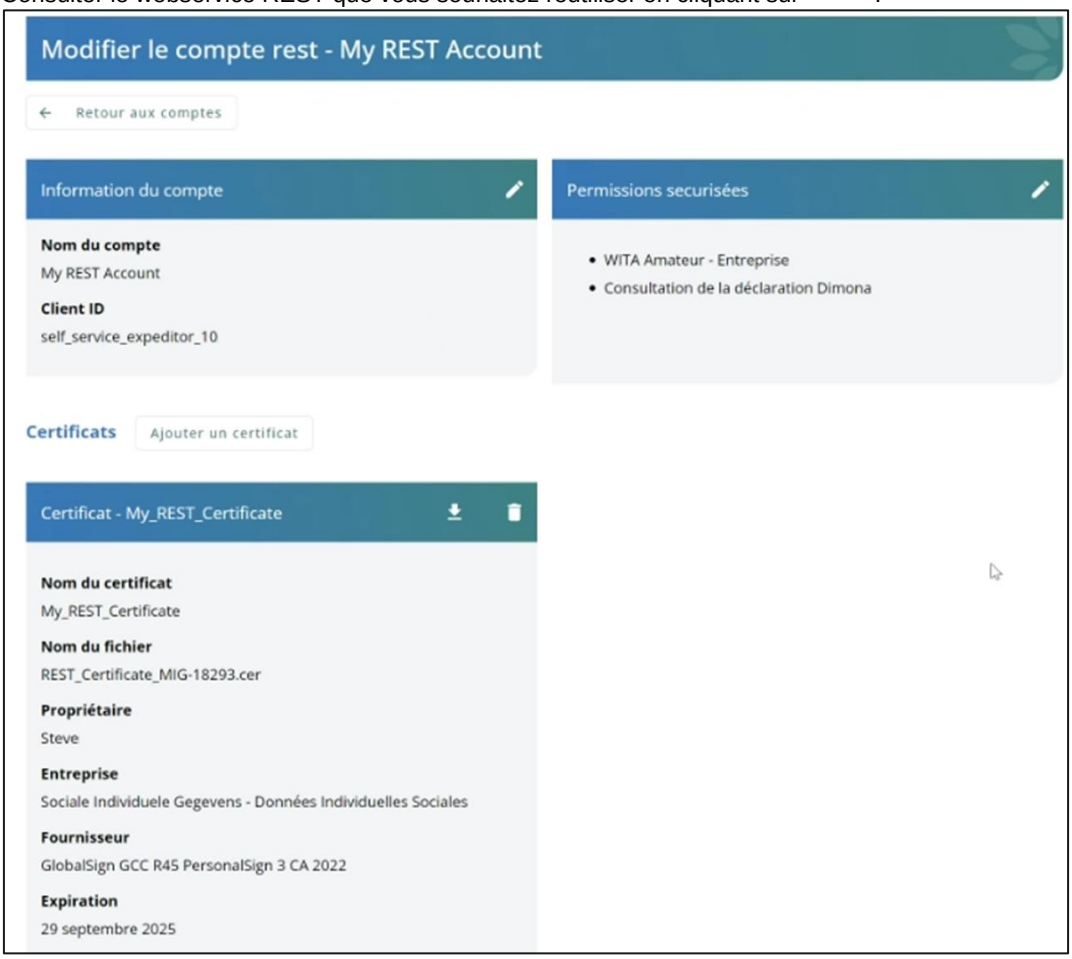


Remarque :
Si la qualité voulue n'est pas disponible, alors votre gestionnaire d'accès principal doit la créer dans l'outil « gestion des accès ». Les autres qualités ne permettent pas de créer un canal API pour le Federal Learning Account.

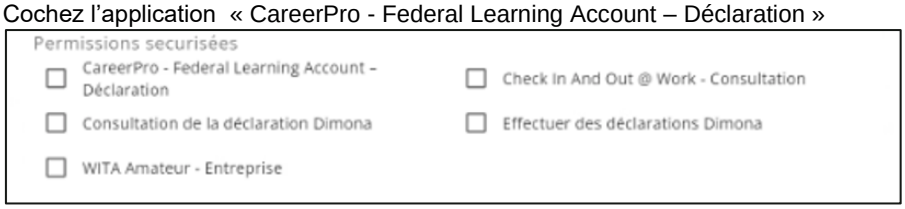
4. Vous arrivez sur la page d'accueil de l'application Chaman.



5. Consulter le webservice REST que vous souhaitez réutiliser en cliquant sur .



6. Cliquez sur le de **Permissions sécurisées**
7. Cochez l'application « CareerPro - Federal Learning Account – Déclaration »



8. « Valider »

Le Client ID sera affiché à l'écran. Il est conseillé de conserver cette information car elle sera utilisée ultérieurement (= clientId oauth).

5. Activer une nouvelle qualité (p.e. prestataire de formation)

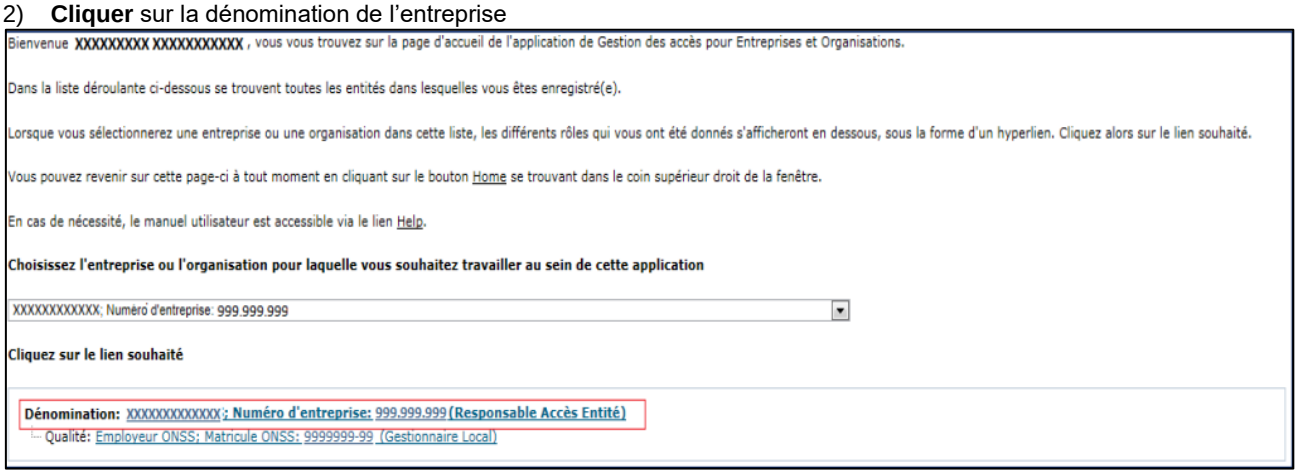
Lorsqu'une entreprise souhaite activer une nouvelle qualité, le responsable d'accès de l'entité doit activer cette qualité et désigner un gestionnaire local dans cette qualité. Ces étapes se déroulent dans l'application **gestion des accès** (UMAN) de la sécurité sociale.

Cette section prend l'exemple d'un employeur qui souhaite activer sa qualité « prestataire de formation » afin de créer un canal technique dans cette qualité là.

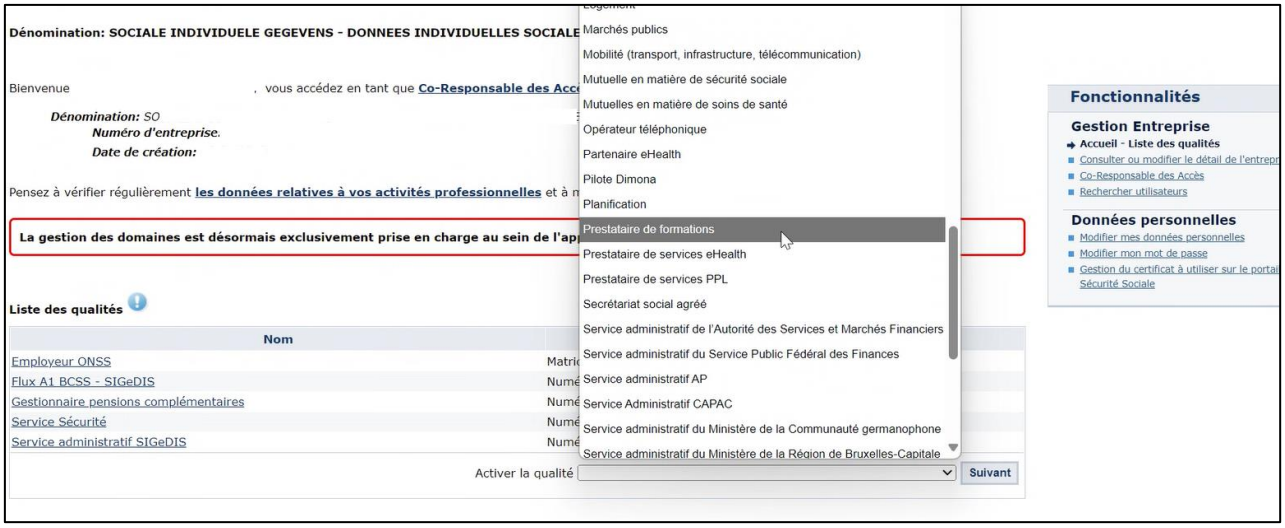
1) Le **responsable d'accès de l'entité** doit se connecter sur l'application « gestion des accès » avec la qualité employeur.

   www.socialSecurity.be → Entreprise → SERVICES EN LIGNE → Gestion des accès → Gestion des accès.

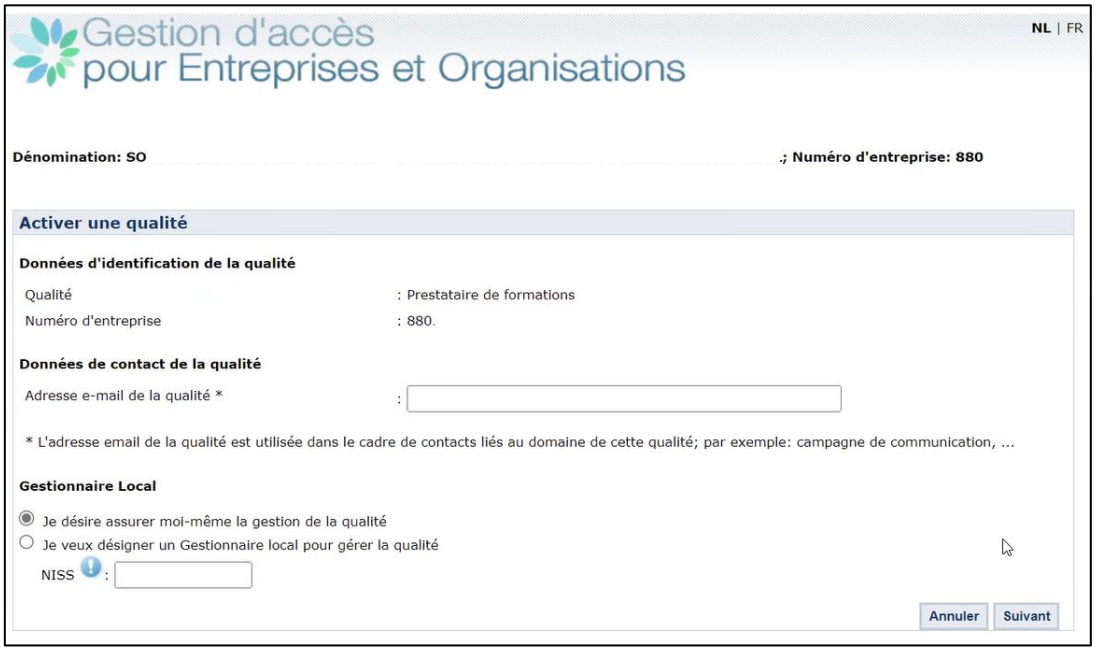
2) **Cliquer** sur la dénomination de l'entreprise



3) Dans la liste déroulante « Activer la qualité », choisir « Prestataire de formation » et faire « **suivant** »



4) Compléter l'écran d'activation, cliquer sur « **suivant** » et ensuite « **confirmer** » Les gestionnaires local définit dans cette écran aura automatiquement un accès CHAMAN pour créer un canal technique dans cette nouvelle qualité.



Après avoir confirmé, le message « La qualité a bien été activée » sera affiché.

⇨ A présent, la personne renseignée comme gestionnaire local à l'étape 4 peut se connecter sur CHAMAN avec la qualité « prestataire de formation » et créer un canal technique (BATCH/API).

6. Plan étape par étape du développeur de l'application

6.1. Étape 1 : mettre en place la sécurité OAUTH

Le webservice REST API du Federal Learning Account est sécurisé en suivant le protocole OAUTH. Avant de pouvoir l'utiliser, vous devez implémenter ce protocole de sécurité Oauth. Cette implémentation doit permettre à votre client du service web d'obtenir un "jeton" de sécurité auprès du serveur OAUTH. Ce jeton devra être utilisé lors des appels à la REST API du Federal Learning Account.

En d'autres mots, votre application doit tout d'abord effectuer un appel au server Oauth de la sécurité sociale avec les paramètres permettant d'indiquer « qui vous êtes » (clientId, certificat, scope, ..). En retour, vous obtiendrez un jeton de sécurité qui atteste que OAUTH vous a bien identifié et que vous avez bien accès à l'API FLA. Ce jeton expire et doit être renouvelé régulièrement. Ce jeton est à intégrer dans tous vos appels à l'API FLA. Sans ce jeton, la sécurité sociale refusera votre appel.

Référez-vous pour cela à la documentation suivante :

Oauth2 Integration Client Credential : https://www.socialsecurity.be/site_fr/general/helpcentre/rest/documents/pdf/doc_portal_oauth2_client_credential_FR.pdf
Exemple de code implémentant la sécurité OAUTH : Voir annex 7.2

Les paramètres à fournir lors de la demande de token OAUTH sont :

Grant type	client_credentials
Scope	La valeur du scope dépent de la qualité sous laquelle vous avez créé le compte webservice REST sur CHAMAN. Qualité employeur, → Scope = “scope:sigedis:gestion:careerpro-federal-learning-account:employer” Qualité mandataire (secretariat social ou prestataire de service) → Scope = “scope:sigedis:gestion:careerpro-federal-learning-account:provider” Qualité prestataire de formation →Scope =
ClientId	Le clientID OAUTH obtenu lors de l’activation du canal (cf. section précédente)
Certificat	le certificat utilisé lors de l’activation du canal (cf. section précédent)
Token endpoint	https://services.socialsecurity.be/REST/oauth/v5/token
Audience url	https://services.socialsecurity.be/REST/oauth/v5/token

En retour, vous obtiendrez un access token.

Exemple de contenu du JWT

La documentation « Oauth2 Integration Client Credential » fait référence à un *client_assertion* devant contenir un JWT. Voici un exemple concret de JWT à utiliser dans le cadre de l’API FLA :

```
{
  "sub": "self_service_chaman_123456_78912",    #votre client id
  "aud": "https://services.socialsecurity.be/REST/oauth/v5/token",  #l’url pour obtenir le token
  "iss": "self_service_chaman_123456_78912",    #votre client id
  "exp": 1719411261,  #un timestamp, l’expiration ne peut dépasser 10minutes
  "jti": "dNw0cvXR3NKX9rN3WX4hAp0AEXKVNWZxKpMxQHCImh8"  #un GUID au choix
}
```

6.2. Étape 2 : appel vers la restAPI CareerPro Fla

Pour appeler la restAPI FLA, votre client du webservice doit utiliser l’access token obtenu à l’étape précédente.

URL PROD RestAPI FLA For employer, social secretariat and provider.	https://services.socialsecurity.be/REST/federalLearningAccount/v1
URL PROD RestAPI FLA for Training Provider only	https://services.socialsecurity.be/REST/federalLearningAccount/trainingProvider/v1

6.3. Environnement de test

Il est possible de tester l’API FLA dans un environnement de TEST. Cet environnement est complètement séparé de l’environnement des production. Il sera nécessaire de créer un canal dans cet environnement.

Ci-dessous se trouve la liste des URL à utiliser pour l’environnement de test.

Application from socialSecurity.be	
Access management	https://uman.acc.socialsecurity.be/uman/
Chaman URL	https://chaman.acc.socialsecurity.be/
API – URL	
Token endpoint	https://services-acpt.socialsecurity.be/REST/oauth/v5/token
Audience url	https://services-acpt.socialsecurity.be/REST/oauth/v5/token
URL RestAPI FLA For employer, social secretariat and provider.	https://services-acpt.socialsecurity.be/REST/federalLearningAccount/v1
URL RestAPI FLA For training provider	https://services-acpt.socialsecurity.be/REST/federalLearningAccount/trainingProvider/v1

ATTENTION, cet environnement de TEST n'est pas accessible par défaut pour les entreprises. Nous devons intégrer votre entreprise dans cet environnement. Pour ce faire, vous devez envoyer une demande d'accès à ContactCenter@support.eranova.fgov.be

7. Annexe

7.1. Identifier son gestionnaire local d'accès ou son responsable d'accès entité

Pour les entreprises qui sont déjà enregistrées sur le portail de la sécurité sociale, il n'est pas toujours évident de savoir qui a été désigné comme étant le « **gestionnaire local** » ou le « responsable d'accès entité ». Si vous utilisez déjà une application du portail, il est possible de trouver cette information en vous connectant à l'application « Gestion des Accès » du portail.

www.socialSecurity.be → entreprise → service en ligne → gestion des accès → gestion des accès.

Le nom du « **gestionnaire local** » se trouvera dans la page « **Vos responsables** » sous Niveau Qualité - Employeur ONSS (ou, pour les mandataires, prestataires de service ou secrétariat social).

Le nom du « Responsable des accès » se trouvera dans la même page mais sous Niveau Entité.

Exemple

Dans cet exemple,

- Danny et Mery sont (co-)gestionnaire local de la qualité employeur. Ils peuvent donner un accès à un user sur CHAMAN pour la qualité Employeur
- Steven et Barbara sont (co-)responsable d'accès : Ils peuvent activer une nouvelle qualité et désigner des gestionnaires locaux.

7.2. Oauth exemple

```
/*
  This exemple is based on nimbus library (groupId:com.nimbusds, artifactId : oauth2-oidc-sdk)

  */

  public String getToken(E_Env env, String endPointUrl, String clientId, String audUrl, List<String> scopes)
throws Exception {
            AuthorizationGrant clientGrant = new ClientCredentialsGrant();

        URI tokenEndpoint = new URI(endPointUrl);
        // The credentials to authenticate the client at the token endpoint
        ClientID clientID = new ClientID(clientId);

        ClientAuthentication clientAuth = new PrivateKeyJWT(clientID,
              new URI(audUrl), JWSAlgorithm.RS256, (RSAPrivateKey) getKey(env), null,
              null);
        // The request scope for the token
        Scope scope = new Scope();
        for (String s : scopes) {
           scope.add(s);
```

```
        }

        TokenRequest request = new TokenRequest(tokenEndpoint, clientAuth, clientGrant, scope);
        HTTPRequest httpRequest = request.toHTTPRequest();


        //}
        Calendar now = Calendar.getInstance();
        TokenResponse response = TokenResponse.parse(httpRequest.send());

        if (!response.indicatesSuccess()) {
            String error = "TokenRequest was unsuccessful: " +
                    TokenErrorResponse.parse(response.toHTTPResponse()).toHTTPResponse().getStatusCode()  +
"\n" +
                    response.toHTTPResponse().getStatusMessage()                    +                    "\n"                    +
response.toHTTPResponse().getContent();
            System.out.println(error);
            throw new Exception(error);
        }
        AccessTokenResponse                                    successResponse                                    =
AccessTokenResponse.parse(response.toHTTPResponse());


                            String token = successResponse.getTokens().getBearerAccessToken().getValue();

                            return token;
                }


private Key getKey(E_Env env) throws Exception {
        KeyStore keyStore = KeyStore.getInstance("PKCS12");
        String alias = null;
        String password = null;
        switch (env) {
            case ACC:
                keyStore.load(this.getClass().getClassLoader().getResourceAsStream(certificate.pfx"),
"Password".toCharArray());
                alias = "alias";
                password = "Password";
                break;
            case INT:
                keyStore.load(this.getClass().getClassLoader().getResourceAsStream("certificate.pfx"),
"Password".toCharArray());
                alias = "alias";
                password = "Password";
                break;
        }

        return keyStore.getKey(alias, password.toCharArray());

    }
```

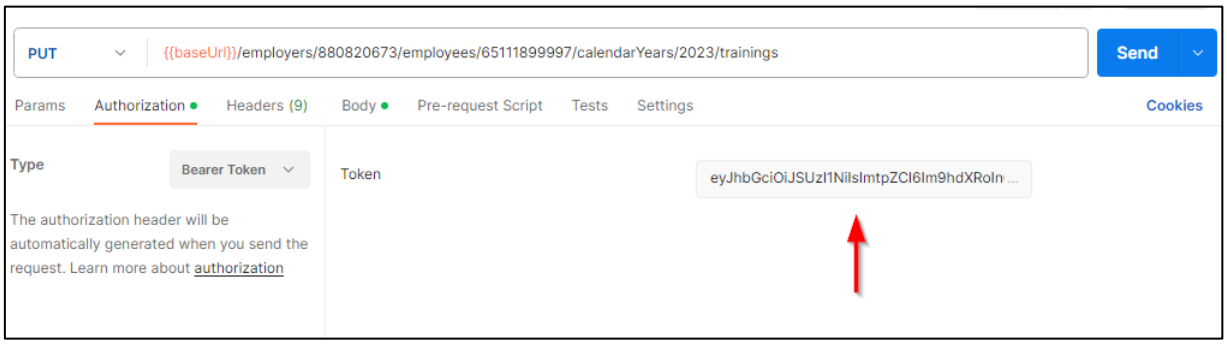
7.3. Outils

7.3.1. Appel restAPI avec PostMan

Il existe des applications qui permettent d'appeler une REST API manuellement sans développement (PostMan, Insomnia, …). Ces applications sont compatibles avec les tokens oauth et peuvent être utilisées pour mieux comprendre l'API avant de démarrer vos développements.

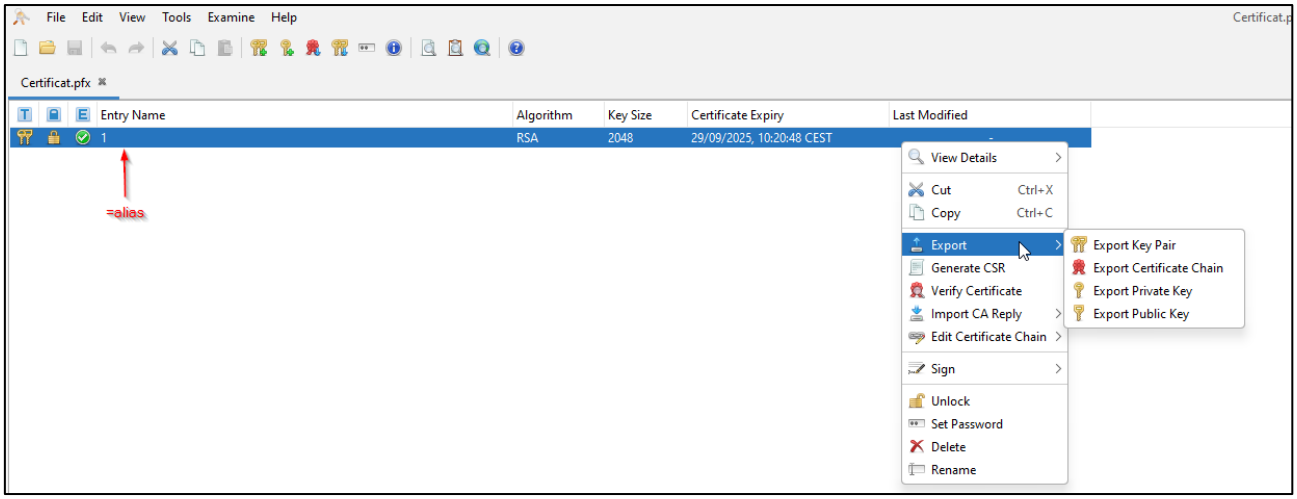
Par exemple, dans l'application "PostMan", les appels vers la REST API FLA peuvent être réalisés en ajoutant le token obtenu à l'étape précédente.

Pour ajouter le token, vous devez aller dans l'onglet "Authorization", choisir le type "Bearer Token" et ajouter la valeur du token dans le champ prévu.



7.3.2. *Ouvrir un certificat*

Les certificats qualifiés sont généralement des fichiers de type « .PFX ». Il existe des applications qui permettent d'ouvrir ce genre fichier et d'en extraire certaines informations comme l'alias, la clé publique, la clé privée ou encore le certificat .cer.

Exemple avec l'outil « Key store explorer » :

Dans cet exemple, l'alias du certificat est « 1 ». En faisant clique droit, il est possible d'exporter le certificat sous la forme demandée lors de la configuration du canal : fichier « .cer ».