

CAREERPRO - FEDERAL LEARNING ACCOUNT

Opzetten kanaal REST API

17/09/2024

Een dienst van



Historiek van het document		
Datum	Beschrijving	Betrokken pagina
01/04/2024	Eerste publicatie van het document	
17/09/2024	Toevoegen van de certificaten selfSigned pour la création du compte REST Toevoegen van de hoedanigheid « opleidingsverstrekker »	9.12

Inhoudstabel

1. Inleiding	4
1.1. Doel van het document	4
2. Type gebruik van het API-kanaal	5
2.1. Algemeen gebruik	5
2.2. Specificiteit van de mandatarissen	5
2.2.1. Het aanmaken van een mandaat	5
2.2.2. Gebruik van het kanaal	6
2.3. Specificiteit van de bedrijfsgroepen	8
2.4. Specificiteit van de softwareleveranciers	9
2.5. Specificiteit van de opleidingsverstrekkers	9
3. Configuratie van het API-kanaal	10
4. Stappenplan lokale beheerder werkgever RSZ	11
4.1. Stap 1: Identificeer je als werkgever RSZ op het portaal van de sociale zekerheid	11
4.2. Stap 2: Registreer je als werkgever RSZ op het portaal van de sociale zekerheid	11
4.3. Stap 3: Toegang verkrijgen tot onlinedienst 'ChaMan'	11
4.4. Stap 4: Een REST webservice account activeren	11
4.4.1. Stap 4a: Een REST webservice account aanmaken	11
4.4.2. Stap 4b: Wijzigen bestaande webservice REST account	14
5. Stappenplan ontwikkelaar: een client ontwikkelen	18
5.1. Stap 1: De OAUTH security opzetten	18
5.2. Stap 2: Oproepen van de REST API CareerPro Fla	18
5.3. Testomgeving	19
6. Annex	19
6.1. Je lokale beheerder identificeren	19
6.2. Oauth voorbeeld	20
6.3. Tools	21
6.3.1. restAPI call met PostMan	21
6.3.2. Een certificaat openen	22

1. Inleiding

Voor het FLA-platform werden verschillende kanalen ontwikkeld die het de werkgever zo eenvoudig mogelijk dienen te maken om FLA-opleidingsgegevens door te sturen.

De grotere ondernemingen, die met digitale platformen werken voor het bijhouden van hun opleidingsgegevens, kunnen gebruik maken van de overdracht via BATCH bestanden of via een webservice (onlinekanaal, REST API). De kleine en middelgrote ondernemingen, die de opleidingsgegevens nog niet via een digitaal platform bijhouden/niet gaan bijhouden, kunnen gebruik maken van de WebApp CareerProFLA die ter beschikking gesteld wordt via careerpro.be.

1.1. Doel van het document

Onderstaande documentatie beschrijft de verschillende stappen die doorlopen dienen te worden om de communicatie tussen de informaticasystemen van de werkgever en deze van het FLA-platform (en via het portaal van de Sociale Zekerheid) op te zetten. Dit voor wat betreft de 'CareerProFLA API'- webservice.

Dit document maakt deel uit van de documenten die ter beschikking staan van de werkgever en zijn mandataris:

Document	Beschrijving
Handleiding van het BATCH kanaal	Document dat de noodzakelijke stappen beschrijft om FLA gegevens over te maken via het BATCH kanaal.
Handleiding van het API kanaal	Document dat de noodzakelijke stappen beschrijft om FLA gegevens over te maken via het API kanaal.
Handleiding van de online toepassing	Document dat de noodzakelijke stappen beschrijft om de FLA gegevens in te geven via de online applicatie.
Beschrijving van de anomalieën	Overzicht van alle anomalieën en waarschuwingen (warnings) met betrekking tot de aangifte van FLA gegevens.
Glossarium	Technische documentatie die de gegevensblokken en -zones beschrijft van de batch en de API.
XSD	Technisch schema dat de structuur van de BATCH definieert.
SWAGGER	Technisch schema dat de structuur van de API definieert.
Opzetten van het batch kanaal	Document dat de noodzakelijke stappen beschrijft om het BATCH kanaal te configureren op het portaal van de sociale zekerheid.
Opzetten van het API-kanaal	Document dat de noodzakelijke stappen beschrijft om het webservice kanaal (API) te configureren op het portaal van de sociale zekerheid.
Toegang verkrijgen tot de online toepassing	Document dat de stappen beschrijft die nodig zijn voor een gebruiker om toegang te krijgen tot de online toepassing <i>CareerPro Federal Learning Account</i>

2. Type gebruik van het API-kanaal

2.1. Algemeen gebruik

Gebruikers (werkgevers of hun mandataris) die een groot aantal aangiftes in de Federal Learning Account (FLA) moeten overmaken, kunnen de gegevens overmaken via een REST webservice (API). Deze REST API-calls maken gebruik van het webservicekanaal van de sociale zekerheid.

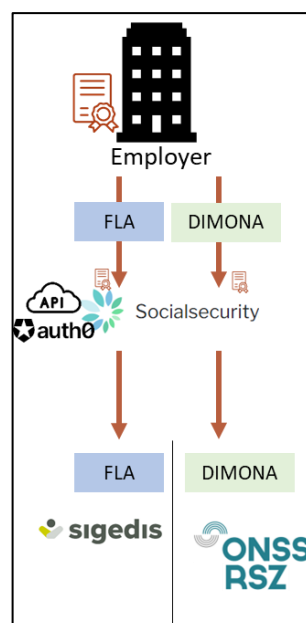
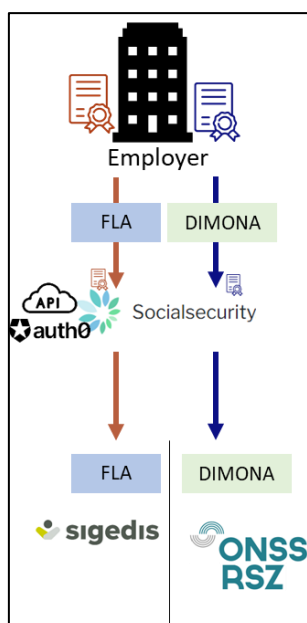
De gebruiker kan

- per flowtype een webservice-account aanmaken. Hij kan bijvoorbeeld een account aanmaken die bestemd is voor DIMONA-gegevens en een andere account die bestemd is voor de gegevens van de Federal Learning Account. Elke account kan een eigen beveiligingscertificaat hebben.
- een webservice-account aanmaken die gemeenschappelijk is voor alle stromen. In dit geval is het beveiligingscertificaat gemeenschappelijk voor alle stromen.

Voorbeeld 1:

Links: Een werkgever gebruikt een webservice-account voor elk van beide services (FLA en DIMONA).

Rechts: Een werkgever gebruikt voor beide diensten een gemeenschappelijke webservice-account.



2.2. Specificiteit van de mandatarissen

Een werkgever kan één (of meerdere) vennootschappen (een dienstverlener of een sociaal secretariaat) machtigen om zijn personeelsdossier te beheren, zijn aangiftes in te vullen en andere administratieve handelingen te verrichten.

Een werkgever kan een bedrijf bijvoorbeeld machtigen om namens hem de DIMONA- en Federal Learning Account-gegevens over te maken. Dit betekent dat de mandataris (= de dienstverlener of het sociaal secretariaat) de gegevens overmaakt met het ondernemingsnummer van de opdrachtgever (= werkgever). Om de overmaking door het systeem te laten accepteren, is het noodzakelijk dat er een actief officieel mandaat bestaat tussen de mandataris en de opdrachtgever voor het gegevenstype.

2.2.1. Het aanmaken van een mandaat

In dit geval is het noodzakelijk om een mandaat aan te maken voor de gewenste dienst, in ons geval "Federal Learning Account". Dit mandaat verbindt de opdrachtgever (de werkgever) en de mandataris (dienstverlener/sociaal secretariaat). Het aanmaken van een mandaat kan gebeuren via de dienst MAHIS van de sociale zekerheid. Deze dienst is beschikbaar op:

www.socialSecurity.be → onderneming → online dienst → MAHIS

Opmerkingen:

- Er moet aan bepaalde voorwaarden worden voldaan voordat een bedrijf mandataris kan worden. Deze voorwaarden zijn tevens te vinden op de servicepagina van MAHIS (document "Guidelines voor sociale dienstverrichters").

- De werkgever kan slechts één agent hebben voor de dienst Federal Learning Account. Anderzijds kan deze mandataris verschillen van die van de andere diensten van de sociale zekerheid.

2.2.2. Gebruik van het kanaal

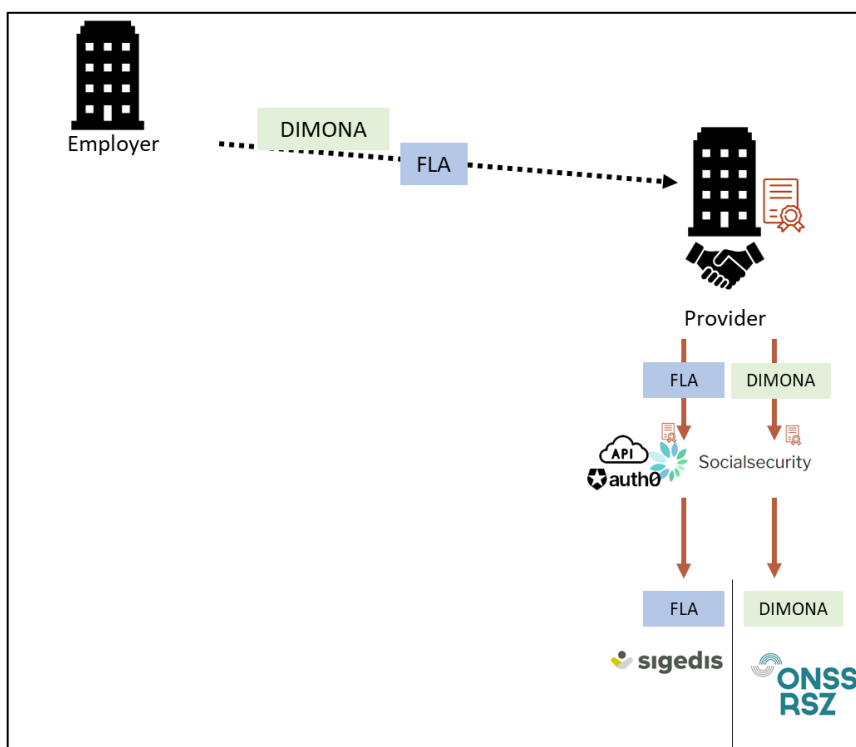
Zodra het mandaat is geactiveerd, kan de mandataris beginnen met het overmaken van gegevens van de Federal Learning Account.

Concreet bezorgt de werkgever zijn mandataris de nodige informatie zodat deze de gegevens van de Federal Learning Account kan aangeven. Deze informatieoverdracht kan verschillende vormen aannemen, afhankelijk van de overeenkomst tussen de mandant en de mandataris. Het kan bijvoorbeeld gaan om een codering van de werkgever in een applicatie van de mandataris.

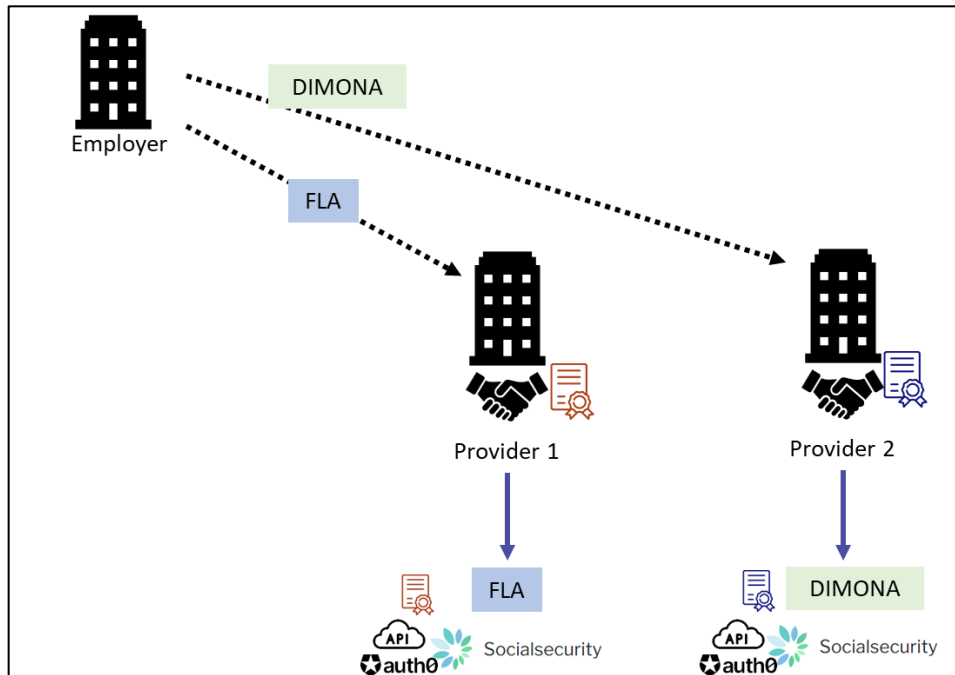
Vervolgens verzendt de mandataris de gegevens van de Federal Learning Account van zijn klanten (werkgevers) met behulp van zijn webservice-account voor dit type gegevens (voorheen geconfigureerd). Dit betekent dat:

- de mandataris de gegevens van al zijn klanten (werkgevers) verzendt met dezelfde webservice-account (die met de dienst Federal Learning Account). Er zal dus gebruik worden gemaakt van hetzelfde beveiligingscertificaat.
- werkgevers geen eigen webservice-account moeten hebben.
- de werkgever een andere mandataris voor de Federal Learning Account kan hebben dan zijn mandataris voor andere diensten (DIMONA, enz.).

Voorbeeld 2: werkgever gebruikt één enkele mandataris (provider genoemd) voor al zijn diensten (FLA en DIMONA). In dit geval heeft de mandataris één webservice-account.

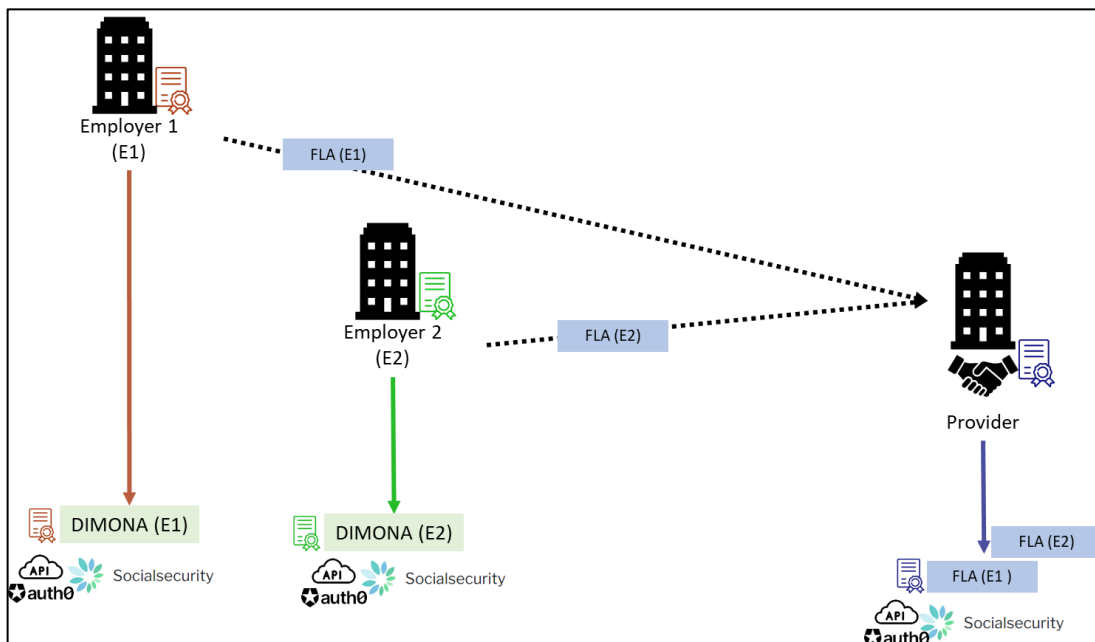


Voorbeeld 3: de werkgever gebruikt een specifieke mandataris (provider genaamd) voor de gegevens van de Federal Learning Account.



Er zijn ook gemengde voorbeelden mogelijk: een deel van de dienstverlening van een werkgever loopt via een mandataris, een ander deel niet.

Voorbeeld 4: twee werkgevers sturen zelf de gegevens van hun DIMONA-diensten door, maar gaan via dezelfde mandataris voor de gegevens van de Federal Learning Account

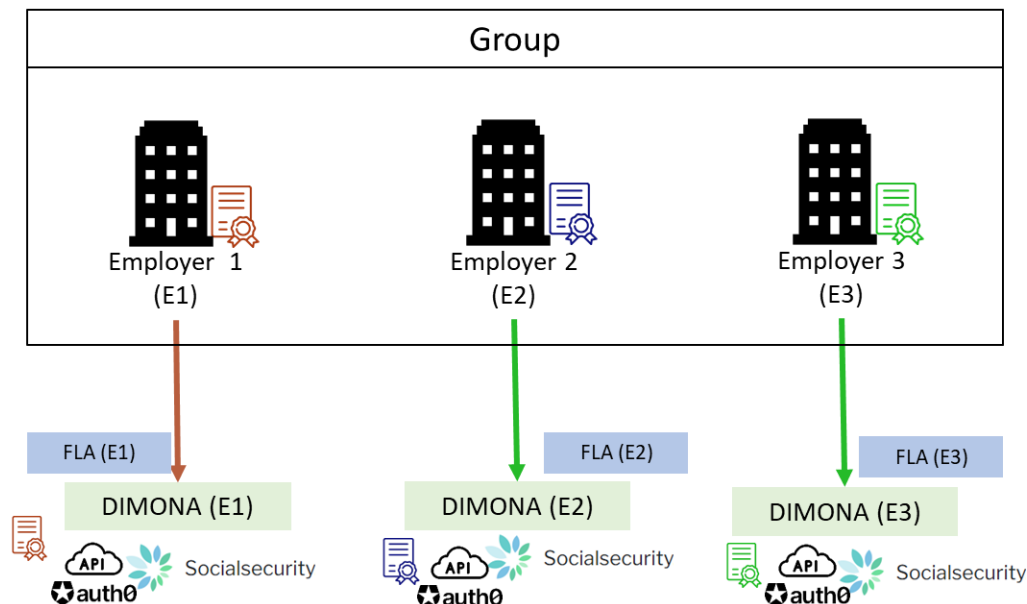


2.3. Specificiteit van de bedrijfsgroepen

Wanneer bedrijven met verschillende ondernemingsnummers (KBO-nummers) aan elkaar gekoppeld zijn (bijvoorbeeld holding/dochteronderneming, groep, enz.), hebben ze twee mogelijkheden om de gegevens van de Federal Learning Account over te maken:

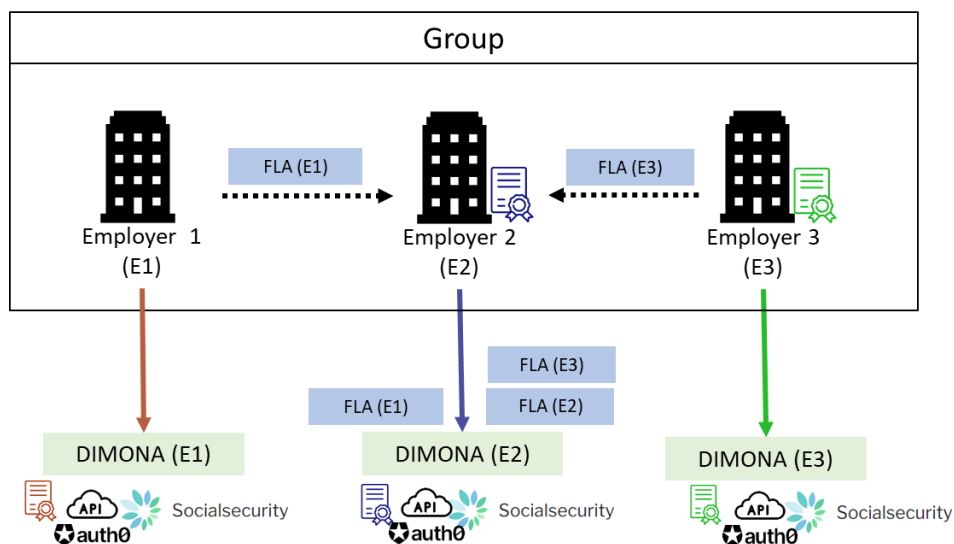
- 1) Elk bedrijf geeft zijn werknemersgegevens aan via zijn eigen kanaal. Bij deze optie moet voor ieder KBO-nummer een webservice-account worden aangemaakt (en is dus één certificaat per KBO-nummer vereist).

Voorbeeld 5: Een groep bestaande uit drie bedrijven. Elk van de drie bedrijven geeft de gegevens van zijn eigen werknemers aan (slechts één webservice-account per bedrijf).



- 2) Een bedrijf wordt, in het kader van de gegevens van de Federal Learning Account, mandataris voor alle andere bedrijven uit de groep. Deze oplossing is identiek aan het geval van de mandatarissen.

Voorbeeld 6: Een groep bestaande uit drie bedrijven. Bedrijf 2 is mandataris van de twee andere bedrijven om de gegevens van de Federal Learning Account voor de hele groep aan te leveren. Dit bedrijf 2 maakt één webservice-account aan voor FLA en Dimona.



Opmerking:

Het versturen van gegevens van de Federal Learning Account van een werknemer gebeurt steeds voor het KBO-nummer van de onderneming die voor diezelfde werknemer de Dimona en DmfA moet uitvoeren. Dit bedrijf kan de entiteit zijn die de groep van de bedrijven vertegenwoordigt.

2.4. Specificiteit van de softwareleveranciers

Wanneer een bedrijf software ter beschikking stelt aan werkgevers om gegevens van de *Federal Learning Account* te versturen, hangt het soort gebruik van het webservicekanaal af van de situatie.

- 1) Als de software gecentraliseerd is op leveranciersniveau of als deze laatste een overeenkomst heeft om FLA-gegevens namens de werkgever te verzenden, moet het mandaatsysteem worden gebruikt (zie 2.2 Specificiteit van mandatarissen). De leverancier zal de databestanden van zijn werkgevers zelf versturen.
- 2) Indien de software "autonoom draait" of de leverancier geen overeenkomst heeft met de werkgever, dan moet er gebruik worden gemaakt van het algemeen gebruik: elke werkgever maakt zijn kanaal/webservice-account aan en stuurt de gegevens naar de restAPI (al dan niet met hulp van de toepassing van de leverancier).

2.5. Specificiteit van de opleidingsverstrekkers

Een onderneming met de hoedanigheid « opleidingsverstrekker » is een onderneming die opleidingsdiensten aanbiedt aan werkgevers. Zij organiseert en geeft opleidingssessies aan deelnemers.

Om het invoeren voor de werkgevers te vergemakkelijken, kan een « opleidingsverstrekker » onderneming de gegevens van de opleidingen die zij georganiseerd heeft, bezorgen aan het FLA platform.

De opleidingsverstrekker maakt de opleidingsgegevens over in eigen naam, t.t.z. met hun eigen KBO-nummer. De gegevens die een opleidingsverstrekker bezorgt, kunnen een werkgever eventueel informeren over een deelnemer. Zelfs als de werkgever van een deelnemer vermeld wordt in de gegevens, dan is het toch niet nodig dat er een mandaat tussen de opleidingsverstrekker en die werkgever bestaat.

3. Configuratie van het API-kanaal

De IT-afdeling van het bedrijf (de werkgever of mandataris afhankelijk van de situatie) of de softwareleverancier integreert deze API in een bestaand (of nieuw) IT-systeem.

Indien het bedrijf nog geen (enige) REST webservice van de Sociale Zekerheid gebruikt en/of het bedrijf niet eerder is geïdentificeerd via het portaal van de sociale zekerheid dan moet dit eerst worden geconfigureerd.

Afhankelijk van de bovenstaande situatie kunnen sommige of de meeste stappen van deze handleiding al als voltooid worden beschouwd.

4. Stappenplan lokale beheerder werkgever RSZ

Alvorens men de REST-service van de FLA kan gebruiken, dient de REST-webservice van de sociale zekerheid geconfigureerd te worden. Volgende stappen dienen door de opdrachtgever (werkgever RSZ) doorlopen te worden om een profiel aan te maken en om de beveiliging te regelen.

4.1. Stap 1: Identificeer je als werkgever RSZ op het portaal van de sociale zekerheid

Indien je reeds als werkgever gekend bent binnen de sociale zekerheid, kan deze stap als voltooid worden beschouwd.

Om de online diensten van de sociale zekerheid te kunnen gebruiken, dient de onderneming gekend te zijn als werkgever RSZ op het portaal van de sociale zekerheid. Gelieve volgende stappen te ondernemen indien dit nog niet het geval is: https://www.socialsecurity.be/site_nl/general/first_visit/access/register-as-employer.htm

4.2. Stap 2: Registreer je als werkgever RSZ op het portaal van de sociale zekerheid

Indien je reeds geregistreerd bent op het portaal, kan deze stap als voltooid worden beschouwd.

Wanneer je binnen de sociale zekerheid gekend bent als werkgever RSZ, dien je te bepalen of je het beheer en gebruik van de beveiligde toegang binnen je onderneming wil houden of uitbesteden.

Via volgende link kan je verder met deze registratie op het portaal:

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

4.3. Stap 3: Toegang verkrijgen tot onlinedienst 'ChaMan'

De configuratie van het technisch kanaal (BATCH of API) kan enkel opgezet worden door een gebruiker die toegang heeft tot de ChaMan-onlinedienst van de sociale zekerheid.

De personen die toegang hebben tot dit kanaal zijn:

- De « **lokale beheerder** » onder het statuut 'RSZ werkgever' (of dienstverlener, sociaal secretariaat of opleidingsverstrekker). Dit laatste wordt gedefinieerd wanneer het bedrijf zich registreert op het portaal.
- Elke gebruiker die toegang heeft gekregen via zijn lokale beheerder. De lokale beheerder van het type RSZ-werkgever (dienstverlener, sociaal secretariaat of opleidingsverstrekker) kan toegang verlenen tot de onlinedienst 'Chaman' via de onlinedienst 'Toegangsbeheer' van de sociale zekerheid (socialsecurity.be).

Als u geen toegang heeft tot Chaman, moet u uw lokale beheerder vragen om u 'Beheer van de technische kanalen' toe te kennen in de online service 'Toegangsbeheer'.

4.4. Stap 4: Een REST webservice account activeren

Als uw onderneming als een REST webservice account heeft aangemaakt voor uw hoedanigheid (werkgever, sociaal secretariaat, dienstverlener of opleidingsverstrekker) in het kader van een andere toepassing van de sociale zekerheid (DmfA, Dimona, ...) dan kan je die gebruiken in het kader van FLA. In dat geval ga je verder met stap 4b « wijziging bestaande REST webservice account ».

In het andere geval ga je verder met stap 4a « Een REST webservice account aanmaken ».

Voor bepaalde ondernemingen is het mogelijk dat het FLA platform onder verschillende hoedanigheden gebruikt wordt:

- De hoedanigheid werkgever die het de onderneming mogelijk maakt om FLA gegevens over te maken van hun eigen medewerkers;
- de hoedanigheid mandataris (dienstverlener of sociaal secretariaat) die een onderneming de mogelijkheid biedt FLA gegevens van de medewerkers van hun klanten over te maken;
- de hoedanigheid opleidingsverstrekker die een onderneming de mogelijkheid biedt om gegevens van opleidingen, die ze georganiseerd heeft voor werkgevers, over te maken.

In dit geval is het nodig meerdere REST webservice accounts aan te maken: minstens één per hoedanigheid.

4.4.1. Stap 4a: Een REST webservice account aanmaken

Te volgen stap indien je onderneming nog geen REST webservice account heeft in de gewenste hoedanigheid of als u een specifieke account voor CareerPro Federal Learning Account wenst op te zetten. In het andere geval kan er direct doorgegaan worden naar stap 4b.

Vereisten:

Om een nieuwe REST webservice account aan te maken, dien je te beschikken over een gekwalificeerd certificaat, geëxporteerd¹ onder de vorm « .cer ». U hebt verschillende opties:

- U bestelt het certificaat bij een erkende certificatie-autoriteit. Dit is de certificatie-autoriteit die wij momenteel ondersteunen:

Certificatie-autoriteit	Type certificaat	Link
GlobalSign	PersonalSign 3 Pro	https://shop.globalsign.com/en/belgian-government-services

- U gebruikt een zelfondertekend (self-signed) certificaat op naam van uw onderneming. De procedure om dit type certificaat te genereren, beschrijven we hier voorlopig niet. Normaal gezien maakt de IT-dienst van uw onderneming dit type certificaat aan met een tool zoals OpenSSL. Houd rekening met de volgende beperkingen bij het aanmaken van uw zelfondertekend certificaat:

Geldigheidscriteria	Toegestane waarden
Algoritme om het sleutelpaar te maken	RSA of EC
Sleutelgrootte (bits)	voor RSA: 2048, 3072 of 4096
voor EC: P-384 of P-521	
Digest-algoritme van de handtekening van het certificaat	SHA-256, SHA-384 of SHA-512
Key Usage van het certificaat	Digital Signature

Dit certificaat zal gebruikt worden:

- om de webservice account aan te maken
- om je informaticasysteem te authenticeren op het portaal, via het securityprotocol OAuth, meer bepaald om het securitytoken te bekomen dat nodig is voor het oproepen van de REST API.

Stappen

1. De gebruiker (die toegang heeft tot ChaMan) verbindt zich met de onlinedienst 'ChaMan'
www.socialSecurity.be → onderneming → Naar alle onlinediensten → ChaMan → Beheer uw technische kanalen
2. Kies het doelpubliek 'Onderneming'

¹ Cf « Een certificaat »

3. Log in met CSAM en volg de instructies voor de geselecteerde methode (eID, itsme, ...)

4. Als uw bedrijf meerdere hoedanigheden heeft, moet u de gewenste hoedanigheid kiezen:
- o “RSZ werkgever” in geval van gebruik van het API-kanaal door een werkgever zonder tussenkomst van een mandataris.
 - o “Sociaal Secretariaat” of “dienstverlener” bij gebruik van het API-kanaal door een mandataris.
 - o “Opleidingsverstrekker” bij gebruik van het API-kanaal om opleidinggegevens te versturen die de onderneming georganiseerd heeft voor werkgevers.

Voorbeeld van werkgevershoedanigheid

Opmerking :

Als de gewenste hoedanigheid niet beschikbaar is, moet uw hoofdtoegangsbeheerder deze aanmaken in de tool “toegangsbeheer”. Andere hoedanigheden laten niet toe dat je een API-kanaal aanmaakt voor de Federal Learning Account.

5. U komt terecht op de startpagina van de onlinedienst ChaMan.

Opmerking: indien u het bericht ‘geen toegang’ te zien krijgt, dient de lokale beheerder nog toegang te verlenen tot ChaMan.

6. Klik op 'Een webservice account toevoegen'. In de zone 'Type' dient 'REST' geselecteerd te worden.

Een Webservice account toevoegen

Type*
Selecteren

REST

7. Vervolledig het formulier :

Een Webservice account toevoegen

Type*
REST

Accountnaam*

Beveiligde machtigingen

☐ CareerPro - Federal Learning Account - Aangifte ☐ Check in And Out @ Work - Consultatie

☐ Consultatie van de Dimona-aangifte ☐ Dimona-aangiftes verrichten

☐ WITA Amateur - Werkgever

Certificaatbeheer

Certificaat* Certificaatnaam*

Bevestigen Annuleren

- Accountnaam: vrij te kiezen (interne keuze)
- Bij de machtigingen: vink 'CareerPro – Federal Learning Account' aan.
- Certificaat: laad de publieke sleutel (.cer-bestand) van je certificaat op (zie vereisten).
- Certificaatnaam: Geef je certificaat een naam

8. Klik op 'Bevestigen'.

Het 'Client ID' wordt weergegeven voor de webservice account REST die zonet aangemaakt werd. Deze 'Client ID' zal later gebruikt worden voor de OAuth (= clientId oauth). Het is aldus raadzaam deze bij te houden.

Webservices account			
Een Webservice account toevoegen			
Naam	Type	Client ID	Actie
My Soap Account	SOAP	-	
My REST Account	REST	self_service_expeditor_10	

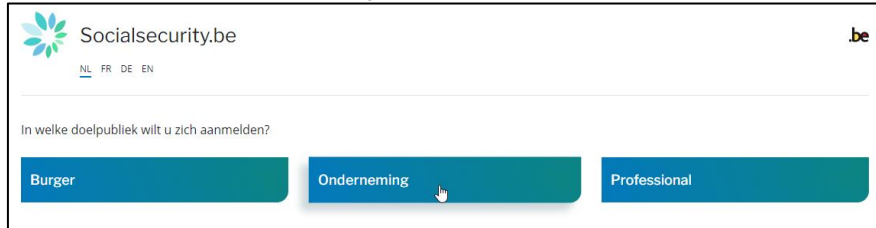
4.4.2. Stap 4b: Wijzigen bestaande webservice REST account

Stap te volgen indien de onderneming reeds een webservice REST account heeft in de gewenste hoedanigheid die ze wenst te hergebruiken voor de 'CareerPro Federal Learning Account'. In het andere geval, gelieve stap 4a te volgen.

Indien er reeds een webservice account REST actief is in de gewenste hoedanigheid, die men wil hergebruiken, dan is het niet nodig om een nieuw certificaat aan te leveren. Er zal gebruik worden gemaakt van het reeds bestaande certificaat.

Stappen :

1. De gebruiker (die toegang heeft tot ChaMan) verbindt zich met de onlinedienst 'ChaMan'
www.socialSecurity.be → onderneming → Naar alle onlinediensten → ChaMan → Beheer uw technische kanalen
2. Kies het doelpubliek 'Onderneming'



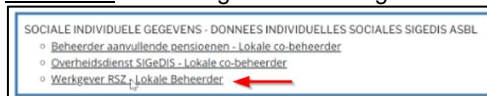
3. Log in met CSAM en volg de instructies voor de geselecteerde methode (eID, itsme, ...)



Als uw bedrijf meerdere hoedanigheden heeft, moet u volgende hoedanigheid kiezen:

- o "RSZ-werkgever" in geval van gebruik van het API-kanaal door een werkgever zonder tussenkomst van een mandataris.
- o "Sociaal Secretariaat" of "dienstverlener" bij gebruik van het API-kanaal door een mandataris.
- o "Opleidingsverstrekker" bij gebruik van het API-kanaal om opleidinggegevens te versturen die de onderneming georganiseerd heeft voor werkgevers.

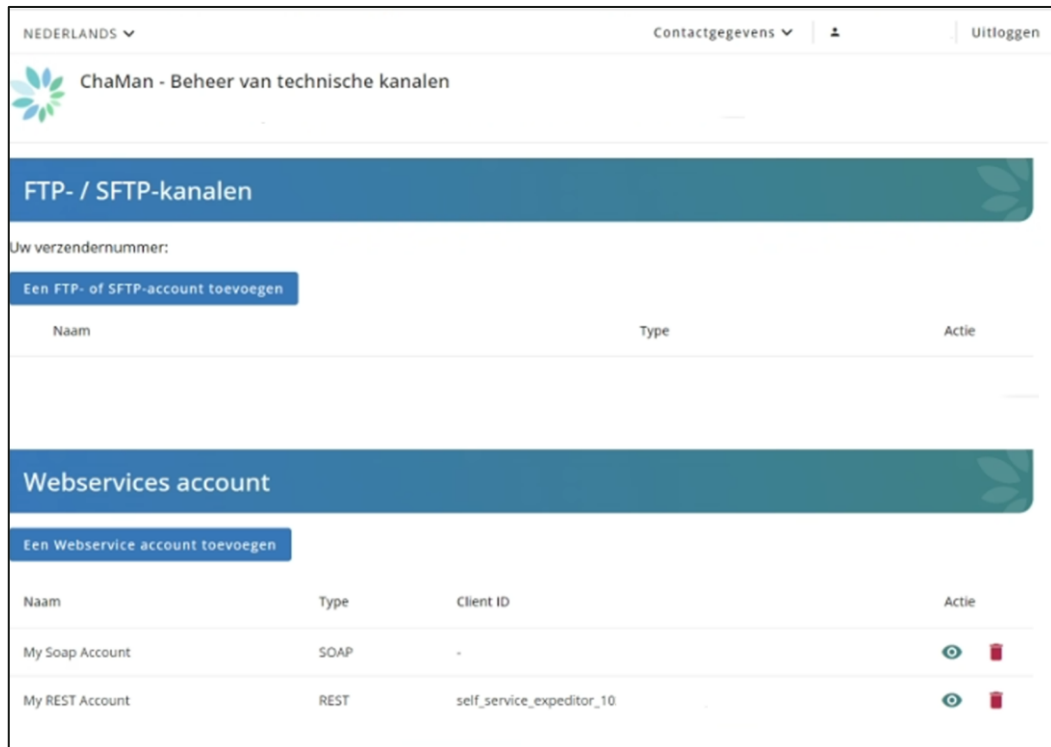
Voorbeeld van werkgevershoedanigheid:



Opmerking:

Als de gewenste hoedanigheid niet beschikbaar is, moet uw hoofdtoegangsbeheerder deze aanmaken in de tool "toegangsbeheer". Andere hoedanigheden laten niet toe dat je een API-kanaal aanmaakt voor de Federal Learning Account.

4. U komt terecht op de startpagina van de onlinedienst ChaMan.



NEDERLANDS Contactgegevens Uitleggen

ChaMan - Beheer van technische kanalen

FTP- / SFTP-kanalen

Uw verzendernummer:


[Een FTP- of SFTP-account toevoegen](#)

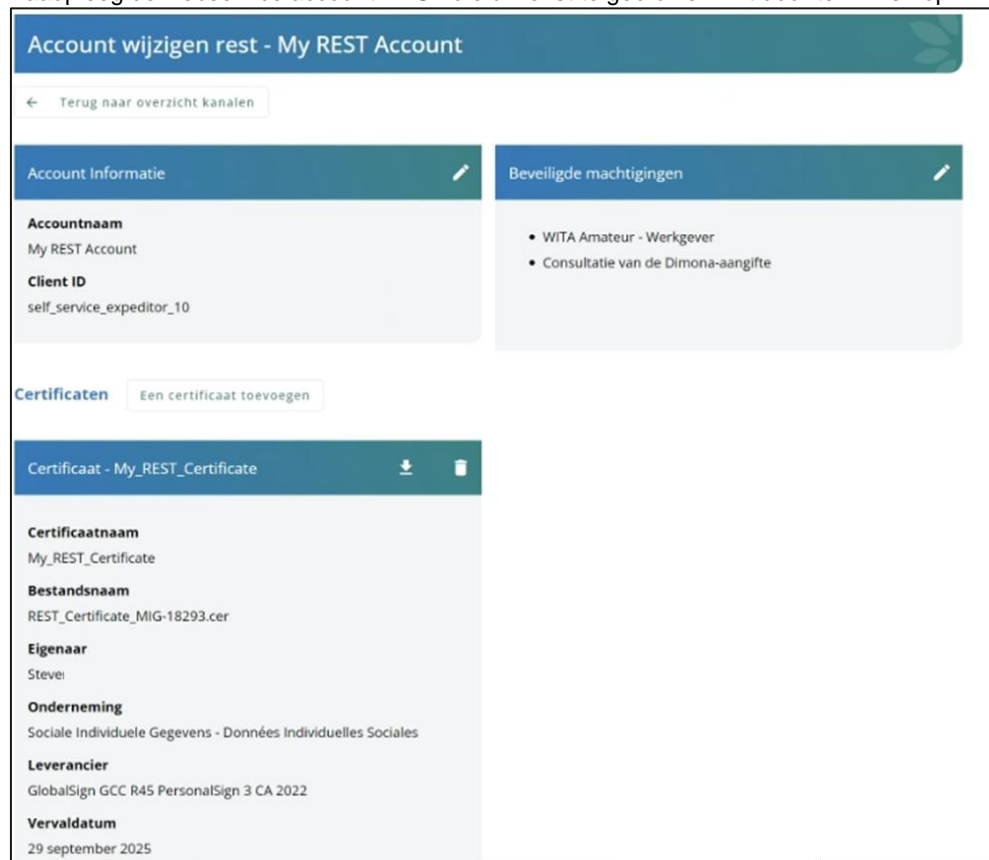
Naam	Type	Actie

Webservices account

[Een Webservice account toevoegen](#)

Naam	Type	Client ID	Actie
My Soap Account	SOAP	-	
My REST Account	REST	self_service_expeditior_10	

5. Raadpleeg de webservice account REST die u wenst te gebruiken. Dit door te klikken op .



Account wijzigen rest - My REST Account

[← Terug naar overzicht kanalen](#)

Account Informatie

Accountnaam
My REST Account

Client ID
self_service_expeditior_10

Beveiligde machtigingen

- WITA Amateur - Werkgever
- Consultatie van de Dimona-aangifte

Certificaten [Een certificaat toevoegen](#)

Certificaat - My_REST_Certificate

Certificaatnaam
My_REST_Certificate


Bestandsnaam
REST_Certificate_MIG-18293.cer

Eigenaar
Stevei

Onderneming
Sociale Individuele Gegevens - Données Individuelles Sociales

Leverancier
GlobalSign GCC R45 PersonalSign 3 CA 2022

Vervaldatum
29 september 2025

6. Klik bij 'beveiligde machtigingen' op  om deze aan te passen.
7. Vink de toepassing 'CareerPro - Federal Learning Account' aan.

Beveiligde machtigingen

<input type="checkbox"/> CareerPro - Federal Learning Account - Aangifte	<input type="checkbox"/> Check In And Out @ Work - Consultatie
<input type="checkbox"/> Consultatie van de Dimona-aangifte	<input type="checkbox"/> Dimona-aangiftes verrichten
<input type="checkbox"/> WITA Amateur - Werkgever	

8. Klik op 'bevestigen'.

Account wijzigen rest - My REST Account

← Terug naar overzicht kanalen

Account Informatie 

Accountnaam
 My REST Account

Client ID
 self_service_expeditor_10

De 'Client ID' wordt weergegeven voor de webservice account REST die zonet gewijzigd werd. Deze 'Client ID' zal later gebruikt worden voor de OAuth (=clientId oauth).

5. Stappenplan ontwikkelaar: een client ontwikkelen

5.1. Stap 1: De OAUTH security opzetten

De webservice REST API van de Federal Learning Account is beveiligd volgens het OAUTH protocol. Alvorens die te kunnen gebruiken dien je dit OAuth security protocol te implementeren. Deze implementatie moet aan je webservice client toelaten een security « token » te bekomen bij de OAUTH server. Dit token zal gebruikt worden bij het oproepen van de REST API van de Federal Learning Account.

Anders gezegd, uw toepassing moet een call uitvoeren naar de Oauth server van de sociale zekerheid met de parameters die aantonen « wie je bent » (clientId, certificaat, scope, ...). Als antwoord krijg je een security token dat bevestigt dat OAUTH je geïdentificeerd heeft en dat je wel degelijk toegang hebt tot de FLA API. Zonder dat token zal de sociale zekerheid je call weigeren.

We verwijzen hiervoor naar de volgende documentatie :

Oauth2 Integration Client Credential:

https://www.socialsecurity.be/site_nl/general/helpcentre/rest/documents/pdf/doc_portal_oauth2_client_credential_NL.pdf

Voorbeeld van code om de OAUTH security te implementeren:

Zie annex 6.2

De parameters voor een aanvraag van een OAUTH token zijn:

Grant type	client_credentials
Scope	De waarde van scope hangt af van de hoedanigheid waarmee je je webservice REST account hebt aangemaakt in CHAMAN. Hoedanigheid werkgever => Scope = "scope:sigedis:gestion:careerpro-federal-learning-account:employer" Hoedanigheid mandataris (sociaal secretariaat of dienstverlener) => Scope = "scope:sigedis:gestion:careerpro-federal-learning-account:provider" Hoedanigheid opleidingsverstrekker => Scope =
ClientId	De clientID OAUTH verkregen bij de activering van het kanaal (cf vorige paragraaf)
Certificaat	Het certificaat gebruikt bij de activering van het kanaal (cf vorige paragraaf)
Token endpoint	https://services.socialsecurity.be/REST/oauth/v5/token
Audience url	https://services.socialsecurity.be/REST/oauth/v5/token

en je krijgt een access token terug.

Voorbeeld van de inhoud van de JWT

De documentatie « Oauth2 Integration Client Credential » verwijst naar een *client_assertion* die een JWT moet bevatten. Hier is een concreet voorbeeld van een JWT om te gebruiken als onderdeel van de FLA API:

```
{
  "sub": "self_service_chaman_123456_78912",    #uw client id
  "aud": "https://services.socialsecurity.be/REST/oauth/v5/token", #de URL om het token te bekomen
  "iss": "self_service_chaman_123456_78912",    #uw client id
  "exp": 1719411261,    #een timestamp, de vervalttermijn mag niet groter zijn dan 10 minuten
  "jti": "dNw0cvXR3NKX9rN3WX4hAp0AEXKVNWZxKpMxQHCImh8" #een GUID naar keuze
}
```

5.2. Stap 2: Oproepen van de REST API CareerPro Fla

Voor het oproepen van de REST API FLA moet je webserviceclient het toegangstoken gebruiken dat in de vorige stap bekomen is.

URL PROD RestAPI FLA

<https://services.socialsecurity.be/REST/federalLearningAccount/v1>

Voor werkgever, mandataris (sociaal secretariaat of dienstverlener)	
URL PROD RestAPI FLA voor opleidingsverstrekker	to be defined

5.3. Testomgeving

Het is mogelijk de FLA API te testen in een testomgeving. Deze omgeving staat volledig los van de productieomgeving. Je moet dus ook een kanaal aanmaken in deze omgeving.

Hieronder vind je de lijst van de URL's die nodig zijn voor de testomgeving.

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 Voor werkgever, mandataris (sociaal secretariaat of dienstverlener)	https://services-acpt.socialsecurity.be/REST/federalLearningAccount/v1
URL RestAPI FLA voor opleidingsverstrekker	to be defined

Opgepast: Deze testomgeving is niet standaard toegankelijk voor ondernemingen. Wij moeten uw onderneming in deze omgeving integreren. Hiervoor moet je een aanvraag voor toegang indienen bij ContactCenter@support.eraanova.fgov.be.

6. Annex

6.1. Je lokale beheerder identificeren

Voor de werkgevers RSZ die al op het portaal van de sociale zekerheid geregistreerd zijn is het niet altijd evident om te weten wie als « **lokale beheerder** » werd aangeduid. Als je al een online dienst van het portaal gebruikt is het mogelijk om die informatie terug te vinden door in te loggen op de toepassing « **toegangsbeheer** ».

www.socialSecurity.be → onderneming → Alle online diensten → Toegangsbeheer → Toegangsbeheer.

De naam van de « **lokale beheerder** » vind je op de pagina « **Uw verantwoordelijken** » onder de hoedanigheid van «RSZ-werkgever» (of, voor mandatarissen, dienstverleners of sociaal secretariaat).



6.2. Oauth voorbeeld

```

/*
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() +
            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());
}

```

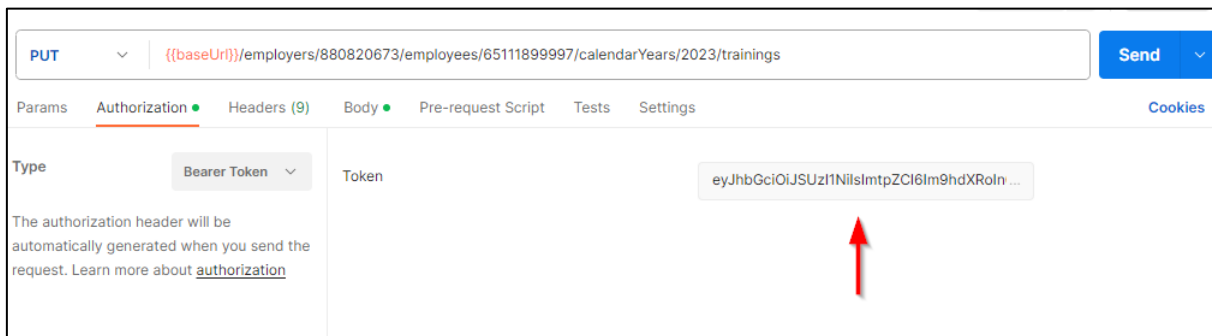
6.3. Tools

6.3.1. restAPI call met PostMan

Er zijn toepassingen waarmee je manueel een REST API kan aanroepen zonder dat er ontwikkeling komt bij kijken (PostMan, Insomnia, ...). Deze toepassingen zijn compatibel met de oauth tokens en kunnen gebruikt worden om de API beter te leren kennen alvorens met de ontwikkeling te starten.

In de "PostMan"-toepassing bijvoorbeeld kunnen de calls naar de REST API FLA gerealiseerd worden door het token dat in de vorige stap bekomen werd, toe te voegen.

Om het token toe te voegen, moet je naar de tab "Authorization" gaan, het type "Bearer Token" kiezen en de waarde van het token toevoegen in het voorziene veld.



6.3.2. Een certificaat openen

Gekwalificeerde certificaten zijn doorgaans van het type « .PFX ». Er bestaan toepassingen waarmee je dit soort bestanden kan openen en er bepaalde informatie kan uithalen zoals de alias, de publieke sleutel, de priv sleutel of het ".cer" certificaat.

Een voorbeeld met de tool « Key store explorer »

In dit voorbeeld is de alias van het certificaat « 1 ». Door rechts te klikken, kan je het certificaat exporteren in het gevraagde formaat tijdens de configuratie van het kanaal: « .cer » bestand.

