CAREERPRO - FEDERAL LEARNING ACCOUNT

Setting up the REST API channel

27/03/2024

A service provided by

sɪgedɪs

Table of Contents

1. Introduction

For the FLA platform various channels have been developed which are to make it as easy as possible for employers to transmit FLA training data.

Major companies, using digital platforms to keep their training data up-to-date, can transfer the data by using BATCH files or by using a web service (online channel, REST API). Small and medium-sized companies, which do not yet use or will not use a digital platform to keep the training data up-to-date, can use the CareerPro FLA WebApp that is made available through careerpro.be.

1.1. Purpose of the document

The documentation below describes the various steps that need to be followed to set up communications between the employer's information systems and those of the FLA platform (and through the Social Security portal), with respect to the 'CareerProFLA API' web service.

This document is part of the set of documents that are at the disposal of the employer and its authorized representative:

Document	Description
BATCH Channel Manual	Document describing the necessary steps to transmit FLA data by using the BATCH channel.
API Channel Manual	Document describing the necessary steps to transmit FLA data by using the API channel.
Online Application Manual	Document describing the necessary steps to enter the FLA data by using the online application.
Description of the anomalies	List of all anomalies and warnings related to the declaration of FLA data.
Glossary	Technical documentation describing the data blocks and zones of the batch and API.
XSD	Technical scheme defining the BATCH structure.
SWAGGER	Technical scheme defining the API structure.
Setting up the batch channel	Document describing the necessary steps to configure the BATCH channel on the social security portal.
Setting up the API channel	Document describing the necessary steps to configure the web service channel (API) on the social security portal.
Getting access to the online application	Document describing the steps that are necessary for a user to get access to the *CareerPro Federal Learning Account* online application

2. Type of use of the API channel

2.1. General usage

Users (employers or their representatives) who need to transfer a large number of declarations to the Federal Learning Account (FLA) can transfer the data via a REST web service (API). These REST API calls use the social security web service channel.

The user can

- create a web service account per flow type. For example, he can create an account dedicated to DIMONA data and another account dedicated to Federal Learning Account data. Each account can have its own security certificate.

- create a web service account that is common to all flows. In this case, the security certificate is common to all flows.

Example 1:

Left: An employer uses a web service account for each of the two services (FLA and DIMONA).

Right: An employer uses a common web service account for both services.
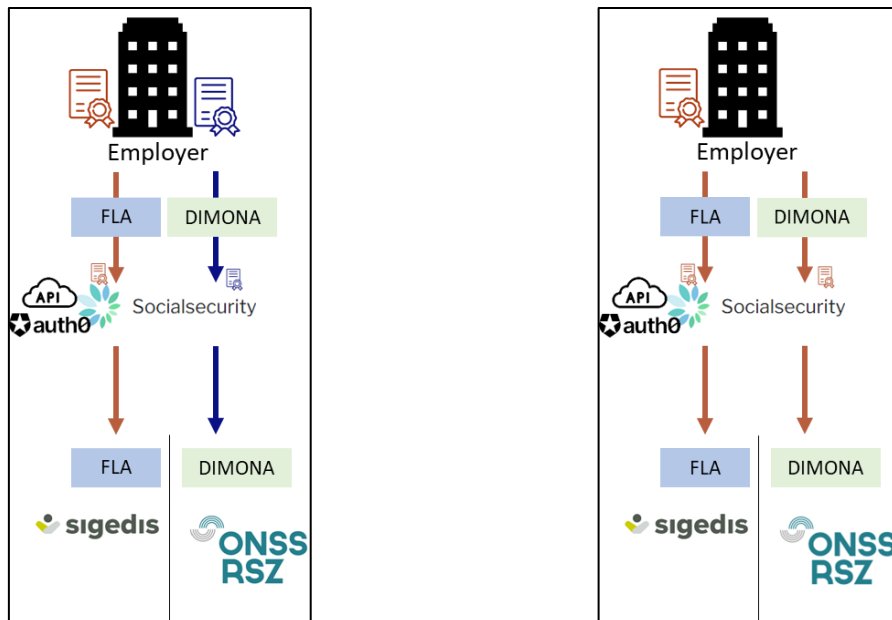
2.2. Specificity of the authorized representatives

An employer can authorize one (or more) companies (a service provider or a social secretariat) to manage his personnel file, complete his tax returns and perform other administrative actions.

For example, an employer can authorize a company to transfer DIMONA and Federal Learning Account information on his behalf. This means that the representative (= the service provider or the social secretariat) transfers the data with the company number of the client (= employer). In order for the transfer to be accepted by the system, it is necessary that there is an active official mandate between the mandate holder and the originator for the data type.

2.2.1. Creating a mandate

In this case it is necessary to create a mandate for the desired service, in our case "Federal Learning Account". This mandate connects the client (the employer) and the mandate holder (service provider/social secretariat). A mandate can be created via the MAHIS service of the social security system. This service is available on:

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

Notes:

- Certain conditions must be met before a company can become a representative. These conditions can also be found on the MAHIS service page (document "guidelines for service providers").

- The employer can have only one agent for the Federal Learning Account service. On the other hand, this representative may differ from that of the other social security services.

2.2.2. Use of the channel

Once the mandate is activated, the authorized representative can begin transferring Federal Learning Account data.

In concrete terms, the employer provides his authorized representative with the necessary information so that he can declare the data of the Federal Learning Account. This information transfer can take different forms, depending on the agreement between the agent and the authorized representative. For example, it may involve coding by the employer in an application of the authorized representative.
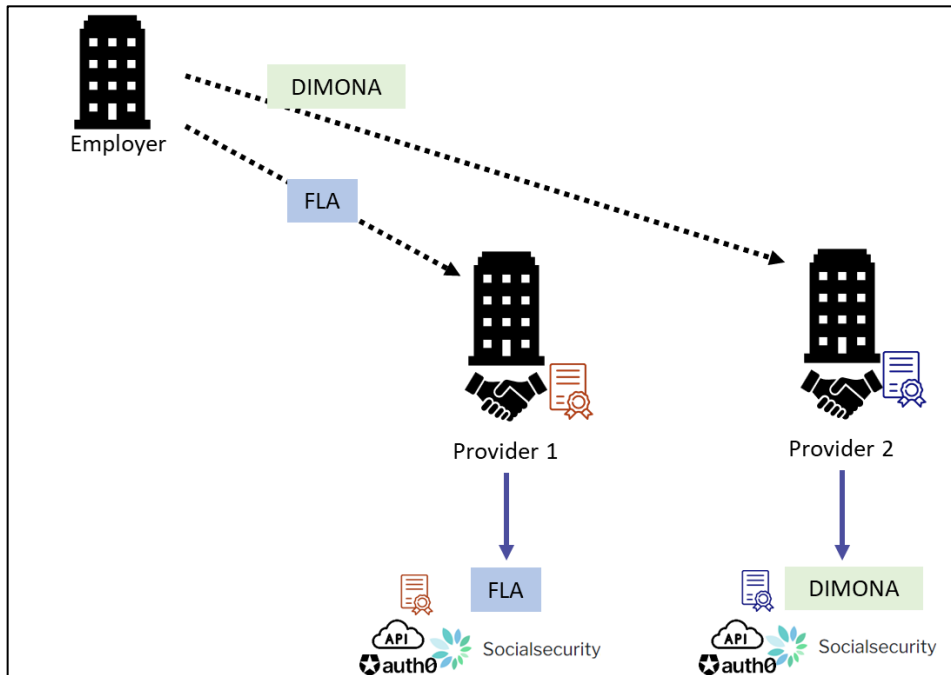
Then the authorized representative sends the Federal Learning Account data of its customers (employers) using its web service account for this type of data (previously configured). This means that:

- the authorized representative sends the data of all his customers (employers) with the same web service account (the one with the Federal Learning Account service). The same security certificate will therefore be used.

- employers do not need to have their own web service account.

- the employer may have a different authorized representative for the Federal Learning Account than his authorized representative for other services (DIMONA, etc.).

Example 2: employer uses a single authorized representative (called a provider) for all its services (FLA and DIMONA). In this case, the authorized representative has one web service account.
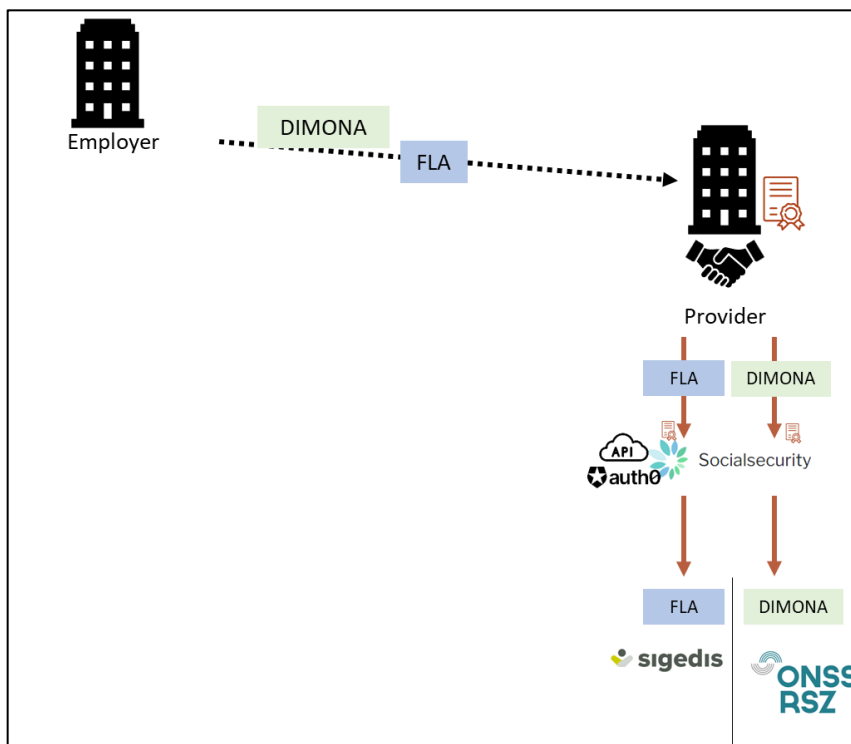

Example 3: the employer uses a specific authorized representative (called a provider) for the Federal Learning Account data.

Mixed examples are also possible: some of an employer's services are provided through an authorized representative, while others are not.

Example 4: two employers forward the data for their DIMONA services themselves, but go through the same authorized representative for the Federal Learning Account data.
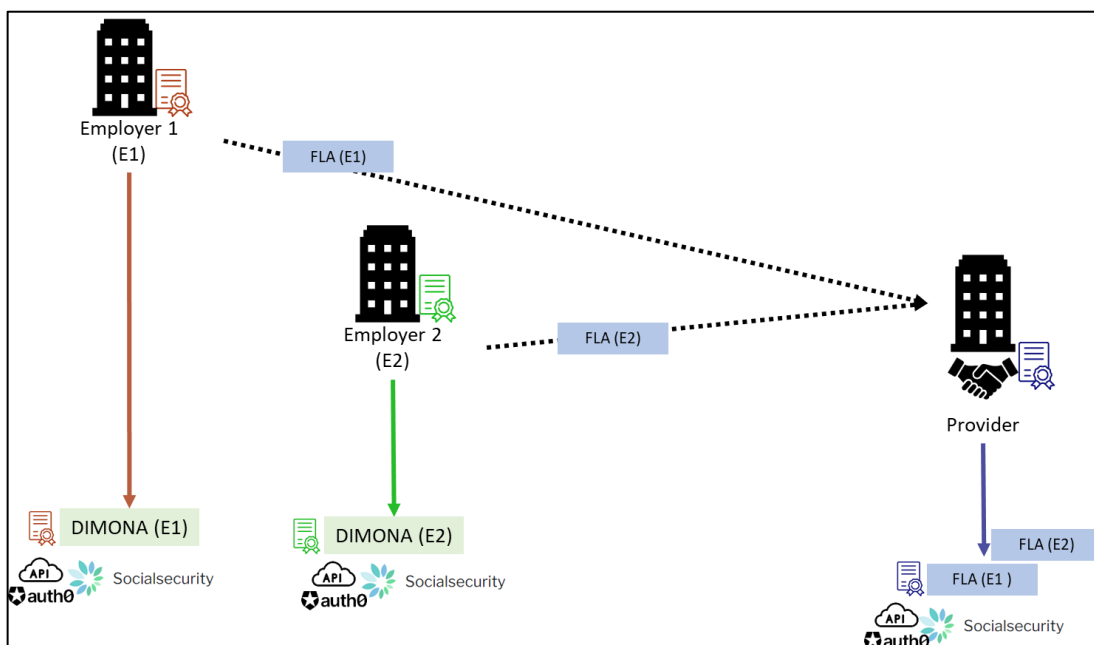

2.3. Specificity of the business groups

When companies with different company numbers (CBE numbers) are linked to each other (e.g. holding/subsidiary, group, etc.), they have two options to transfer the Federal Learning Account data:

1) Each company provides its employee data through its own channel. With this option, a web service account must be created for each CBE number (and therefore one certificate per CBE number is required).

Example 5: A group consisting of three companies. Each of the three companies declares the data of its own employees (only one web service account per company).
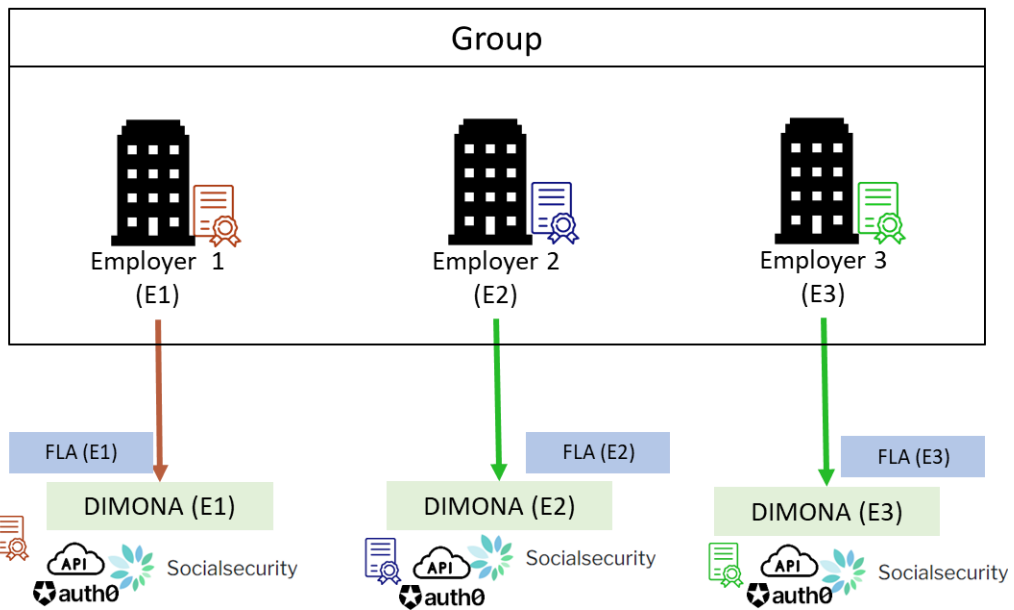
2) In the context of the data from the Federal Learning Account, a company becomes the authorized representative for all other companies in the group. This solution is identical to the case of the authorized representatives.

Example 6: A group consisting of three companies. Company 2 is the authorized representative of the two other companies to provide the Federal Learning Account data for the entire group. This company 2 creates one web service account for FLA and Dimona.
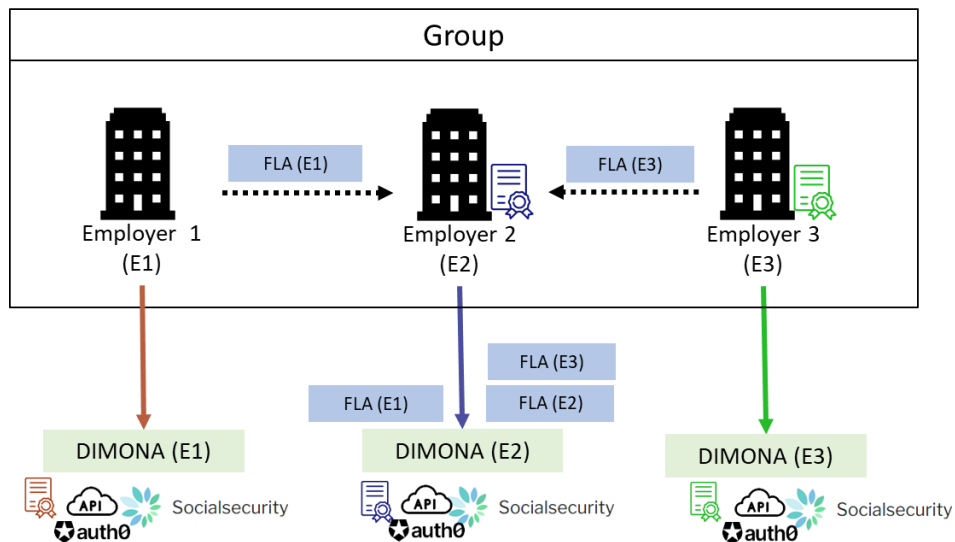
Note:

Sending data from an employee's Federal Learning Account always takes place for the CBE number of the company that must carry out the Dimona and DMFA for that same employee. This company may be the entity representing the group of companies.

2.4. Specificity of the software suppliers

When a company provides software to employers to send *Federal Learning Account* data, the type of use of the web service channel depends on the situation.

1) If the software is centralized at supplier level or if the latter has an agreement to send FLA data on behalf of the employer, the mandate system must be used (see 2.2 Specificity of authorized representatives). The supplier will send the data files of its employers itself.

2) If the software "runs autonomously" or the supplier does not have an agreement with the employer, then general use must be used: each employer creates his channel/web service account and sends the data to the restAPI (with or without help from the supplier's application).

3. Configuration of the API channel

The company's IT department (the employer or the authorized representative depending on the situation) or a software supplier shall integrate the API in an existing (or new) information system.

If your company does not yet use a social security REST web service and/or if your company has not yet been identified before through the social security portal, it is to be set up first.

Depending on the above situation some or most of the steps described in this manual could be considered already completed.

> Important note: on the portal of the Social Security the steps to follow are available only in Dutch and French!

4. Step-by-step plan for the NOSS employer's local manager

Before being able to use the FLA REST service, the social security REST web service is to be configured. The steps below are to be followed by the client (NOSS employer) in order to create a profile and handle security.

4.1. Step 1: Identify yourself as an NOSS employer on the social security portal

If you are already known as an employer within social security, this step can be considered completed.

In order to be able to use the social security online services, the company is to be known as an NOSS employer on the social security portal. Please take the following steps if that is not yet the case: https://www.socialsecurity.be/site_nl/general/first_visit/access/register-as-employer.htm (NL) or https://www.socialsecurity.be/site_fr/general/first_visit/access/register-as-employer.htm (FR)

4.2. Step 2: Register yourself as an NOSS employer on the social security portal

If you have already been registered on the portal, this step can be considered completed.

When you are known as a NOSS employer within social security, you are to decide whether you want to keep the management and use of the secured access within your company or want to outsource it.

Using the following link you can continue your registration on the portal:

https://www.socialsecurity.be/site_nl/employer/infos/employer_onss/registration_gen/register/register.htm (NL) or
https://www.socialsecurity.be/site_fr/employer/infos/employer_onss/registration_gen/register/register.htm (FR)

4.3. Step 3: Obtain access to the online service 'CHAMAN'

The configuration of a technical channel (BATCH or API) can only be done by a user who has access to the Social Security 'Chaman' application.

The persons who have access to Chaman are:

- The **"Local Manager"** under the quality 'NOSS employer' (or in case of authorized representatives: provider or social secretariat). This one was defined during the registration of the enterprise on the portal.
- Any user who received access through the 'Local Manager'. The local manager under the quality NOSS employer (or for authorized representatives: provider or social secretariat) can provide access to the online service 'Chaman' using the online service 'Access management' (socialsecurity.be) .
-
  If you don't have access to Chaman, you must ask your local manager to grant you 'Technical channel management' in the 'Access management' online service
  - o www.socialSecurity.be → onderneming → Alle online diensten → Toegangsbeheer → Toegangsbeheer. (NL)
  - o www.socialSecurity.be → entreprise → service en ligne → gestion des accès → gestion des accès. (FR)

4.4. Step 4a: Create webservice account REST

Follow this step if your enterprise does not yet have a REST webservice account, or if you wish to create a specific account for the CareerPro Federal Learning Account application. Otherwise, go to step 4b .

Requirements:

To create a new account REST Webservice, you need a qualified certificate, exported under the form « .cer ». If you don't have a certificate yet, please follow these steps:

https://www.socialsecurity.be/site_nl/general/helpcentre/soa/local_manager_certificate.htm

This certificate will be used:

- To create the webservice account
- To authenticate your IT system on the portal via the oAuth security protocol, i.e. to obtain the security token required for calls to the REST API.

Steps

1. The user (who has access to Chaman) login to the "Chaman" application
   www.socialSecurity.be → onderneming → Naar alle onlinediensten → ChaMan → Beheer uw technische kanalen (NL)
   www.socialSecurity.be → entreprise → service en ligne → Chaman → gérer vos canaux techniques (FR)
   (the screenshots below are from the Dutch-language 'Chaman' online service).

2. Choose the target audience 'Enterprise'
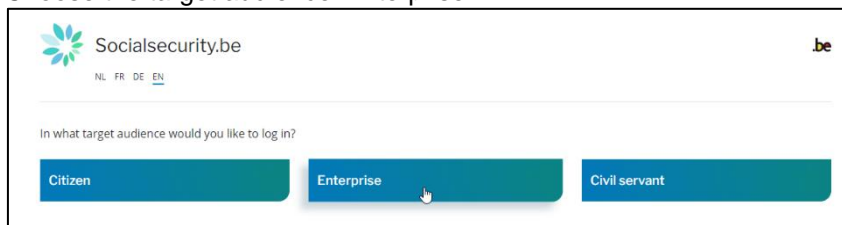
3. Log in via CSAM and follow the instructions for the selected method (eID, itsme, ...)
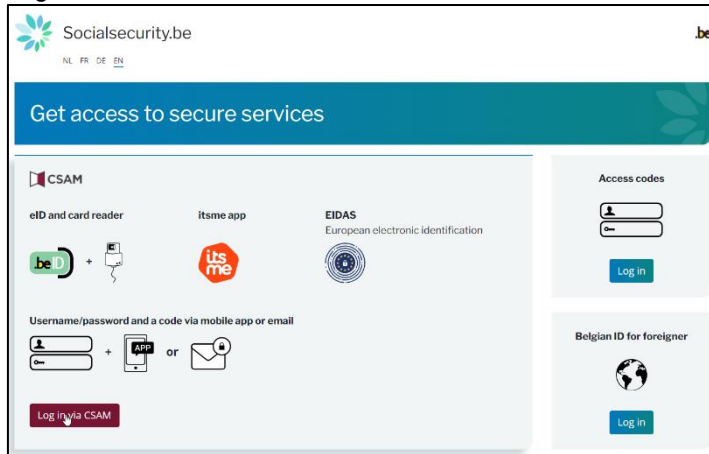
4. If your enterprise has several qualities, you must choose one:
   o "NOSS Employer" in case of use of the BATCH channel by an employer without the intervention of a authorized representative.
   o "Social Secretariat" or "Service provider" when using the BATCH channel by an authorized representative
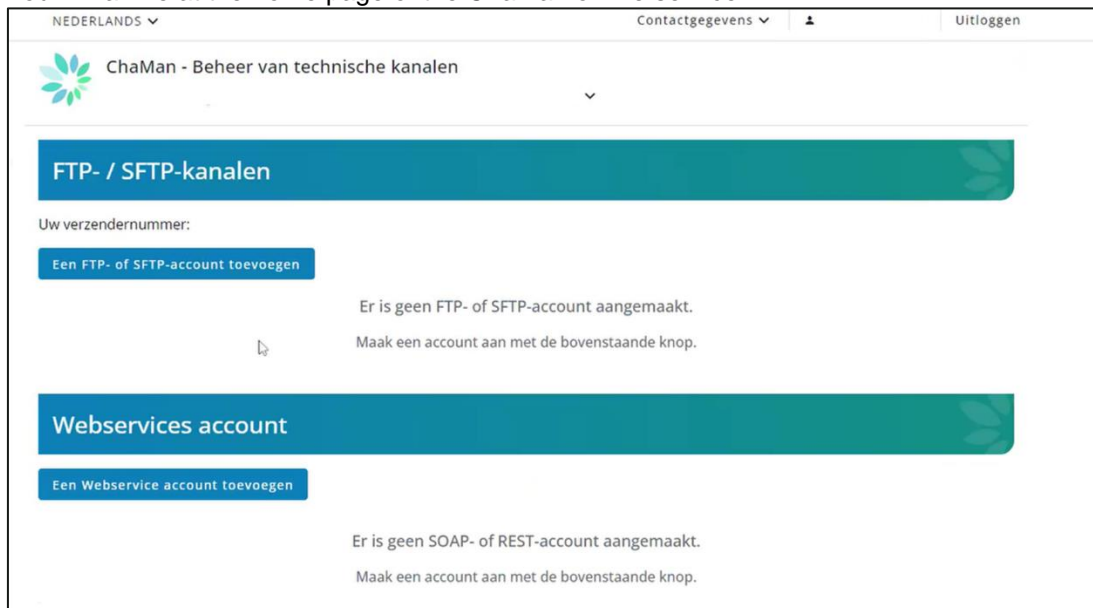
   Example of employers quality
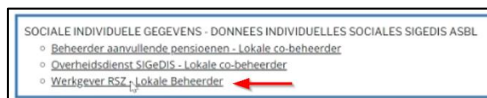
   Note:
   If the desired quality is not available, your main access manager must create it in the "access management" tool. Other qualities do not allow you to create a BATCH channel for the Federal Learning Account.

5. You will arrive at the home page of the Chaman online service..

   Note:
   If you see a "no access" message, the local manager still needs to give you access to Chaman.

6. Click on 'Add a webservice account'. In the zone 'Type', select 'REST'

7. Complete the form :

- Accountnaam: Free choice (internal choice)
- Authorisations: check 'CareerPro – Federal Learning Account'.
- Certificate : upload the public key (.cer file) of your certificate (see requirements).
- Certificate name: Free choice (internal choice)

8. Select 'Confirm'.

The 'Client ID' is shown for the webservice account REST that was just created. This 'Client ID' will later be used for the oAuth (= clientId oauth). So it is recommended to keep it close at hand.

### 4.5. Step 4b: Modify existing webservice account REST

Step to follow if the company already has a webservice account REST and wants to (re)use it for the 'CareerPro Federal Learning Account'. Otherwise, please follow Step 4a.

If there is a webservice account REST already active for the enterprise, that you also want to (re)use for 'CareerPro Federal Learning Account', then it is not necessary to request a new certificate. The existing certificate will be used.

<u>Steps</u>

1. The user (who has access to Chaman) login to the "Chaman" application
   www.socialSecurity.be → onderneming → Naar alle onlinediensten → ChaMan → Beheer uw technische kanalen (NL)
   www.socialSecurity.be → entreprise → service en ligne → Chaman → gérer vos canaux techniques (FR)

2. Choose the target audience 'Enterprise'
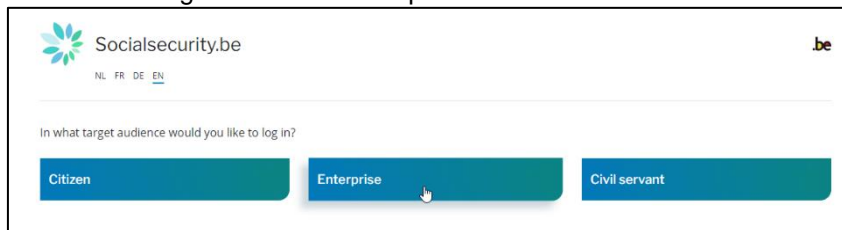
3. Log in via CSAM and follow the instructions for the selected method (eID, itsme, ...)
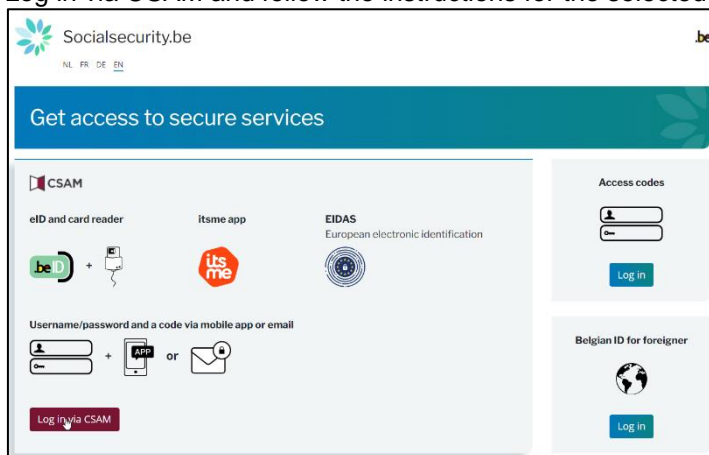
9. If your enterprise has several qualities, you must choose one:
   o "NOSS Employer" in case of use of the BATCH channel by an employer without the intervention of a authorized representative.
   o "Social Secretariat" or "Service provider" when using the BATCH channel by an authorized representative

   Example of employers quality
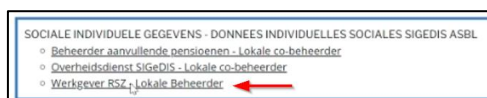
   Note:
   If the desired quality is not available, your main access manager must create it in the "access management" tool. Other qualities do not allow you to create a BATCH channel for the Federal Learning Account.

4. You will arrive at the home page of the Chaman online service.

5. Consult the webservice account REST that you want to use by clicking on 👁

6. Click on in 'secured authorizations'
7. Check the application 'CareerPro - Federal Learning Account'

Beveiligde machtigingen	
☐ CareerPro - Federal Learning Account – Aangifte	☐ Check In And Out @ Work - Consultatie
☐ Consultatie van de Dimona-aangifte	☐ Dimona-aangiftes verrichten
☐ WITA Amateur - Werkgever	

8. Click on 'Confirm'

Account wijzigen rest - My REST Account

← Terug naar overzicht kanalen

Account Informatie ✎

Accountnaam
My REST Account

Client ID
self_service_expeditor_10

The 'Client ID' is shown for the webservice account REST that was just modified. This 'Client ID' will later be used for the oAuth (= clientId oauth).

5. Step-by-step plan developer: developing a client

5.1. Step 1: setting up OAUTH security

The REST API web service of the Federal Learning Account is secured. Before being able to use it, you are to implement the OAuth security protocol. This implementation should allow your web service client to obtain a security token from the OAUTH server. This token will be used when calling the REST API of the Federal Learning Account.

In this respect we refer to the following documentation:

Oauth2 Integration Client Credential: https://www.socialsecurity.be/site_nl/general/helpcentre/rest/documents/pdf/doc_portal_oauth2_client_credential_NL.pdf (NL)   https://www.socialsecurity.be/site_fr/general/helpcentre/rest/documents/pdf/doc_portal_oauth2_client_credential_FR.pdf (FR)
Oauth example: See annex 6.2

The parameters to apply for an OAUTH token are:

Grant type	client_credentials
Scope	For employers: "scope:sigedis:gestion:careerpro-federal-learning-account:employer" For authorized representatives: "scope:sigedis:gestion:careerpro-federal-learning-account:provider"
ClientId	The clientID OAUTH obtained upon activating the channel (cf. previous paragraph)
Certificate	The certificate used when activating the channel (cf. previous paragraph)
Token endpoint	https://services.socialsecurity.be/REST/oauth/v5/token
Audience url	https://services.socialsecurity.be/REST/oauth/v5/token

and you will receive an access token.

5.2. Step 2: calling the REST API CareerPro Fla

In order to call the REST API FLA your web service client must use the access token obtained in the previous step.

URL PROD RestAPI FLA	https://services.socialsecurity.be/REST/federalLearningAccount/v1

6. Annex

6.1. Identifying your local manager

For the NOSS employers which have already been registered on the social security portal, it is not always obvious to know who was appointed "**local manager**". If you already use a portal application, it is possible to retrieve that information by logging into the "**access management**" application of the portal.

www.socialSecurity.be → onderneming → Naar alle onlinediensten → ChaMan → Beheer uw technische kanalen (NL)

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

The name of the "**local manager**" can be found on the " **Uw verantwoordelijken** " page under quality "NOSS Employer" (or in case of authorized representatives, providers or social secretariat).

6.2. Oauth example

```
/*

  This example 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());


}
```

6.3. Tools

6.3.1. restAPI call with PostMan

There are applications that allow you to manually call a REST API without any development involved (PostMan, Insomnia, etc.). These applications are compatible with the oauth tokens and can be used to get to know the API better before starting development.

For example, in the "PostMan" application, the calls to the REST API FLA can be made by adding the token obtained in the previous step.

To add the token, you need to go to the "Authorization" tab, choose the type "Bearer Token" and add the value of the token in the field provided.
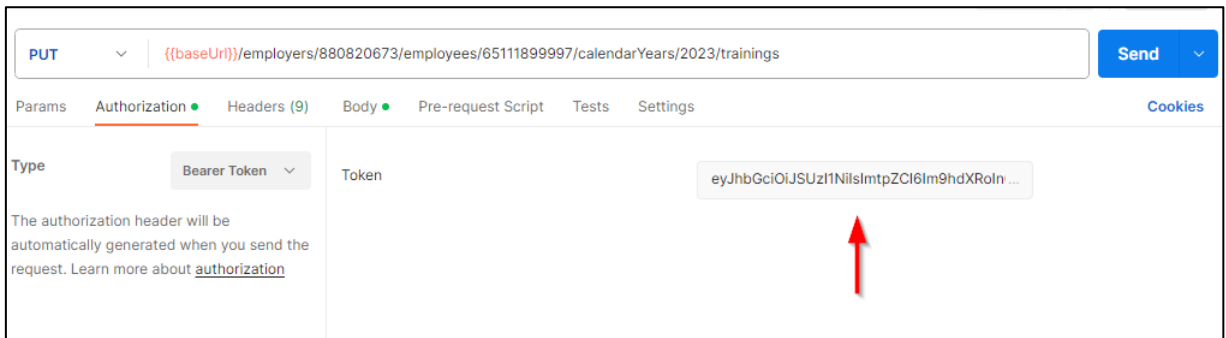
6.3.2. Open a certificate

Qualified certificates are usually of the ".PFX" type. There are applications that allow you to open these types of files and extract certain information such as the alias, the public key, the private key or the ".cer" certificate.

An example with the tool « Key store explorer »

In this example, the alias of the certificate is "1". By right clicking you can export the certificate in the format requested during the channel configuration: « .cer » file.