CAREERPRO - FEDERAL LEARNING ACCOUNT

REST-API-Kanal erstellen

17.09.2024

Ein Service von

Sigedis VoG Place Victor Horta 11(P3) 1060 Brüssel T +32 (0)2 791 50 00 M info@sigedis.fgov.be www.sigedis.be

Geschichte des Dokuments		
Datum	**Beschreibung**	**Betroffene Seite**
01/04/2024	Erstveröffentlichung des Dokuments	
17/09/2024	Präzision auf die Einzigartigkeit des SFTP-Kanals nach Qualität Hinzufügung der Qualität „Schulungsanbieter“.	

Inhalt

1. Einführung

Für die Plattform FLA wurden diverse Kanäle entwickelt, die eine möglichst einfache Übertragung von FLA-Fortbildungsdaten durch Arbeitgebende ermöglichen sollen.

Großunternehmen, die ihre Fortbildungsdaten auf digitalen Plattformen speichern, können die Daten mit Batch-Files oder mit einem Webservice (Onlinekanal, REST-API) übermitteln. Kleine und mittlere Unternehmen, die ihre Fortbildungsdaten noch nicht auf einer digitalen Plattform speichern, können die Onlineanwendung CareerProFLA von careerpro.be verwenden.

1.1. Ziel des vorliegenden Dokuments

Die nachfolgenden Dokumente beschreiben die einzelnen Schritte zur Einrichtung der Verbindung zwischen den IT-Systemen der Arbeitgebenden und der FLA-Plattform (über das Portal der Sozialen Sicherheit) für den Webservice „CareerProFLA API“.

Das vorliegende Dokument ist Teil der Dokumente, die Arbeitgebenden und ihren Bevollmächtigten zur Verfügung gestellt werden:

Dokument	Beschreibung
Handbuch für den Batchkanal	Das Dokument beschreibt die einzelnen Schritte, die für die Übermittlung von FLA-Daten über den Batchkanal erforderlich sind.
Handbuch für den API-Kanal	Das Dokument beschreibt die einzelnen Schritte, die für die Übermittlung von FLA-Daten über den API-Kanal erforderlich sind.
Handbuch der Onlineanwendung	Das Dokument beschreibt die einzelnen Schritte, die für die Eingabe der FLA-daten in der Onlineanwendung erforderlich sind.
Fehlermeldungen	Liste aller Fehlermeldungen und (Warn-)Hinweise bei der Meldung von FLA-Daten
Glossar	Technische Dokumentation zur Beschreibung der Datenblöcke und Datenbereiche des Batchs und der API
XSD	Schema, in dem die Batch-Struktur definiert wird
SWAGGER	Schema, in dem die API-Struktur definiert wird
Batchkanal erstellen	Das Dokument beschreibt die einzelnen Schritte, die für die Konfigurierung des Batchkanals auf dem Portal der Sozialen Sicherheit erforderlich sind.
API-Kanal erstellen	Das Dokument beschreibt die einzelnen Schritte, die für die Konfigurierung des Webservice-Kanals (API) auf dem Portal der Sozialen Sicherheit erforderlich sind.
Einrichtung eines Zugangs zur Onlineanwendung	Das Dokument beschreibt die einzelnen Schritte, mit denen ein Zugang zur Onlineanwendung *CareerPro Federal Learning Account* für einen Benutzer eingerichtet wird.

2. Art der Benutzung des API-Kanals

2.1. Allgemeine Benutzung

Da die Benutzer (Arbeitgebende und ihre Bevollmächtigten) oder die Fortbildungsanbieter viele Meldungen im *Federal Learning Account (FLA)* vornehmen müssen, können sie die Daten mit dem Webservice-Aufruf REST-API schicken. REST-API-Aufrufe nutzen den Webservice der Sozialen Sicherheit.

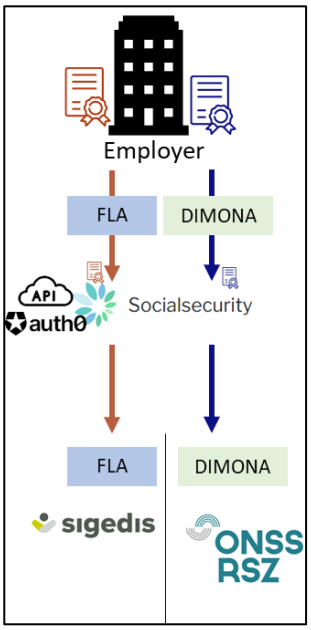
Für eine bestimmte Eigenschaft (Arbeitgeber, Dienstleister, Sozialsekretariat, Fortbildungsanbieter), der Benutzer kann

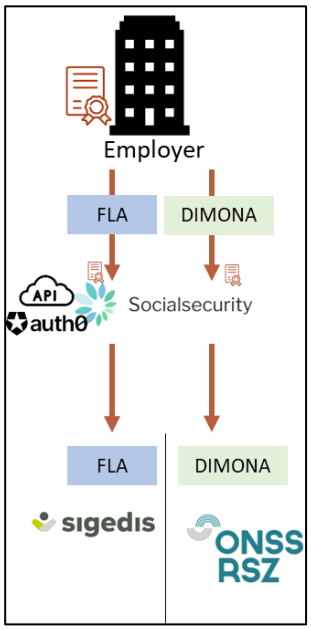
- entweder einen Webservice-Account für jede Art von Datenaustausch erstellen. Er kann zum Beispiel einen Account für Dimona-Daten und einen anderen Account für *Federal Learning Account*-Daten erstellen. Jeder Account kann ein eigenes Sicherheitszertifikat haben.

- oder einen gemeinsamen Webservice-Account für alle Datenströme erstellen. In diesem Fall ist das Sicherheitszertifikat für alle Datenströme gleich.

Beispiel 1:
Links: Der Arbeitgeber verwendet gesonderte Webservice-Accounts für beide Meldungen (FLA und Dimona).

Rechts: Der Arbeitgeber verwendet einen gemeinsamen Webservice-Account für beide Meldungen.





2.2. Sonderfall: Bevollmächtigte

Der Arbeitgeber kann ein oder mehrere Unternehmen (Dienstleister oder Sozialsekretariat) mit der Verwaltung seiner Personalangelegenheiten, der Abgabe der Meldungen und der Erledigung sonstiger Verwaltungsvorgänge betrauen.

Ein Arbeitgeber kann zum Beispiel ein Unternehmen zum Versand seiner Dimona-Daten und *Federal Learning Account*-Daten in seinem Namen ermächtigen. In diesem Fall schickt der Bevollmächtigte (= Dienstleister oder Sozialsekretariat) die Daten mit der Unternehmensnummer des Vollmachtgebers (Arbeitgeber). Damit der Versand vom System angenommen wird, muss der Vollmachtgeber dem Bevollmächtigten eine offizielle Vollmacht für die jeweilige Datenart erteilen.

2.2.1. Erteilung der Vollmacht

In diesem Fall muss eine Vollmacht für den gewünschten Dienst, in unserem Fall „*Federal Learning Account*“, erteilt werden. Die Vollmacht ist für den Vollmachtgeber (Arbeitgeber) und den Bevollmächtigten (Dienstleister/Sozialsekretariat) bindend. Die Erteilung einer Vollmacht kann mithilfe des Onlinedienstes Mahis der Sozialen Sicherheit erfolgen. Dieser Dienst steht Ihnen zur Verfügung unter:

www.socialSecurity.be → Unternehmen → Onlinedienste → Mahis

Anmerkungen

- Es müssen bestimmte Bedingungen erfüllt sein, damit ein Unternehmen Bevollmächtigter sein kann. Diese Bedingungen finden Sie ebenfalls auf der Seite von Mahis (Dokument „*Handlungsanweisungen für Dienstleister" (auf Französisch)*).
- Arbeitgebende dürfen nur einen Bevollmächtigten für den *Federal Learning Account* in Anspruch nehmen. Dieser Bevollmächtigte kann jedoch ein anderer sein als der bzw. die, die für die anderen Dienste der Sozialen Sicherheit ermächtigt wurde(n).

2.2.2. Nutzung des Kanals

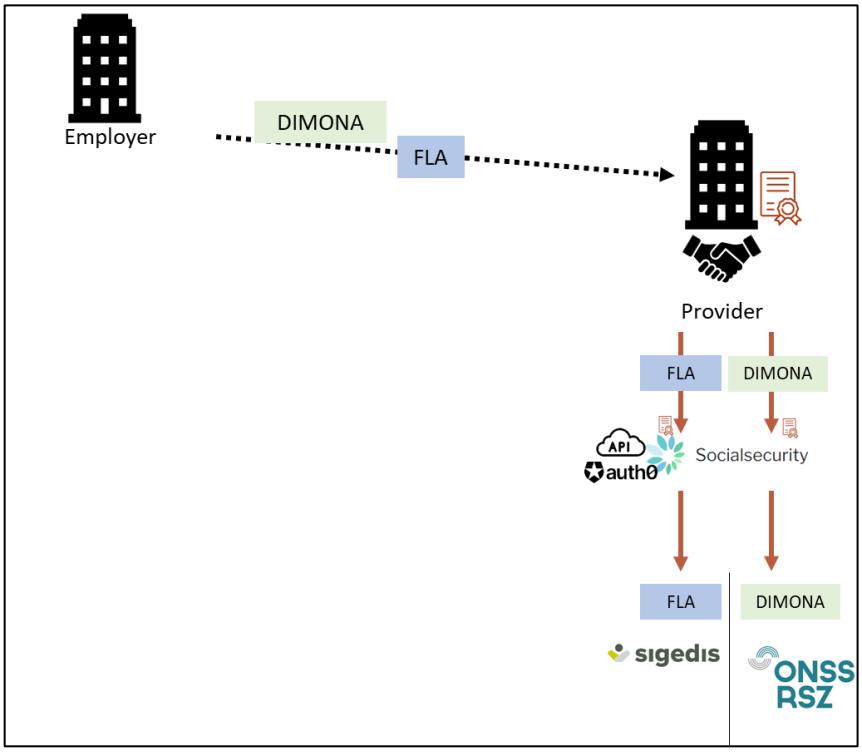
Nachdem die Vollmacht freigegeben wurde, kann der Datenversand für den *Federal Learning Account* durch den Bevollmächtigten beginnen.

Konkret stellt der Arbeitgeber seinem Bevollmächtigten die erforderlichen Informationen bereit, damit dieser die Daten beim *Federal Learning Account* melden kann. Diese Datenübertragung kann in unterschiedlicher Form erfolgen, je nachdem, welchen Vertrag Vollmachtgeber und Bevollmächtigter geschlossen haben. Sie können zum Beispiel vom Arbeitgeber in einer Anwendung des Bevollmächtigten erfasst werden.

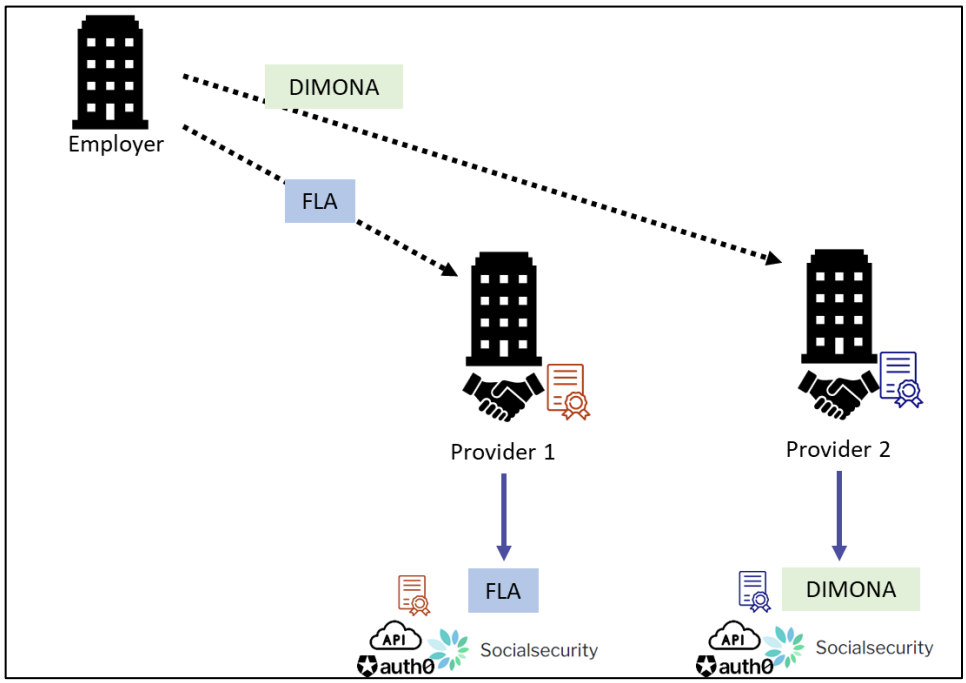
Anschließend schickt der Bevollmächtigte die *Federal Learning Account*-Daten seiner Kunden (Arbeitgebenden) mithilfe seines (zuvor konfigurierten) Webservice-Accounts als Bevollmächtigter für derartige Daten. Konkret bedeutet dies:

- Der Bevollmächtigte schickt die Daten all seiner Kunden (Arbeitgebenden) mit demselben Webservice-Account (dem mit dem *Federal Learning Account*-Dienst). Es wird also das gleiche Sicherheitszertifikat verwendet.
- Die Arbeitgebenden benötigen dann keinen eigenen Webservice-Account.
- Der Arbeitgeber kann für den *Federal Learning Account* einen anderen Bevollmächtigten in Anspruch nehmen als für die anderen Dienste (Dimona etc.).

Beispiel 2: Ein Arbeitgeber nutzt für alle Dienste (FLA und Dimona) denselben Bevollmächtigten (sog. Provider). Der Bevollmächtigte hat in diesem Fall nur einen Webservice-Account.

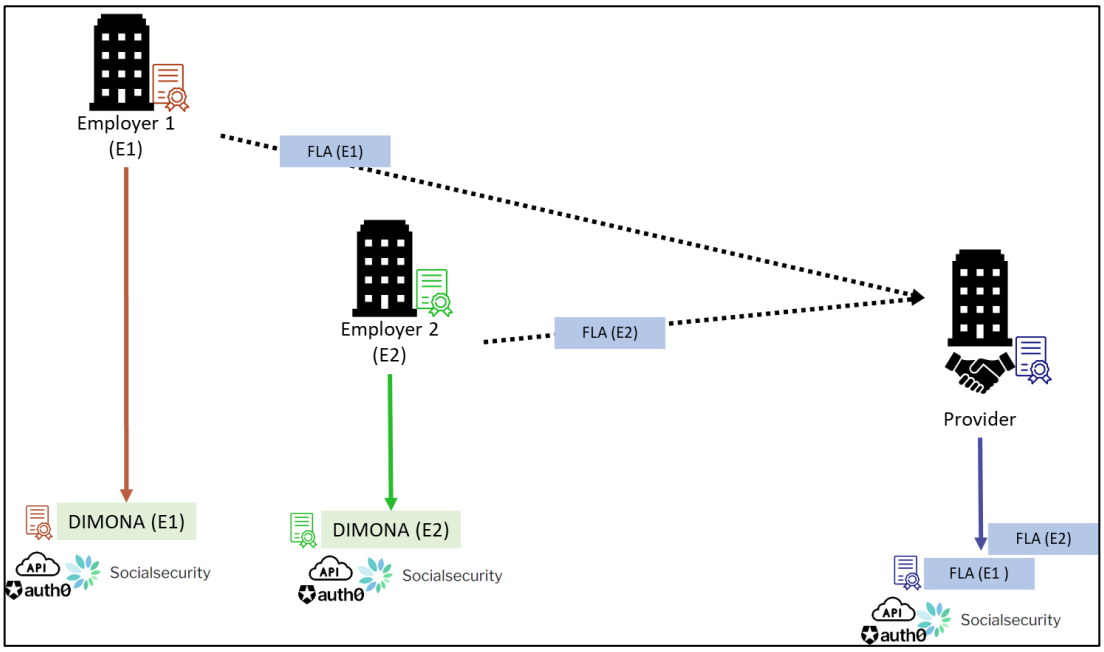


Beispiel 3: Der Arbeitgeber hat einen speziellen Bevollmächtigten (sog. Provider) für die Daten des *Federal Learning Account*.



Auch Mischkonstellationen sind denkbar: Ein Teil der Dienste eines Arbeitgebers wird von einem Bevollmächtigten abgewickelt, ein anderer nicht.

Beispiel 4: Zwei Arbeitgebende schicken ihre Dimona-Daten selbst, nehmen aber denselben Bevollmächtigten für die *Federal Learning Account*-Daten in Anspruch.

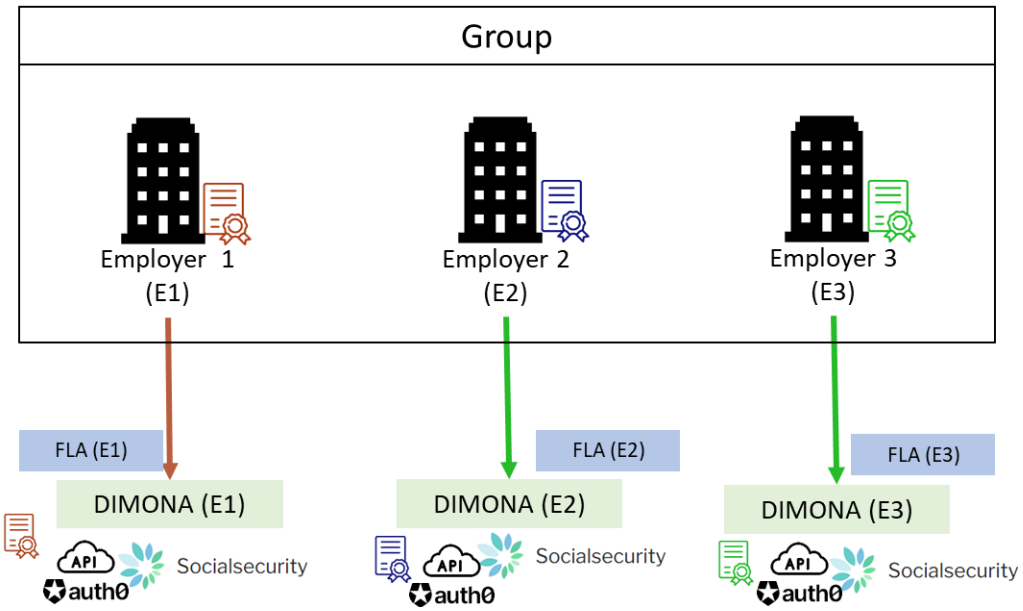


2.3. Sonderfall: Unternehmensgruppen

Wenn Gesellschaften mit unterschiedlicher Unternehmensnummer (ZDU-Nummer) miteinander verbunden sind (z. B. Holding/Tochtergesellschaft, Konsortium usw.), haben sie zwei Möglichkeiten für die Übermittlung der Daten des *Federal Learning Account*:

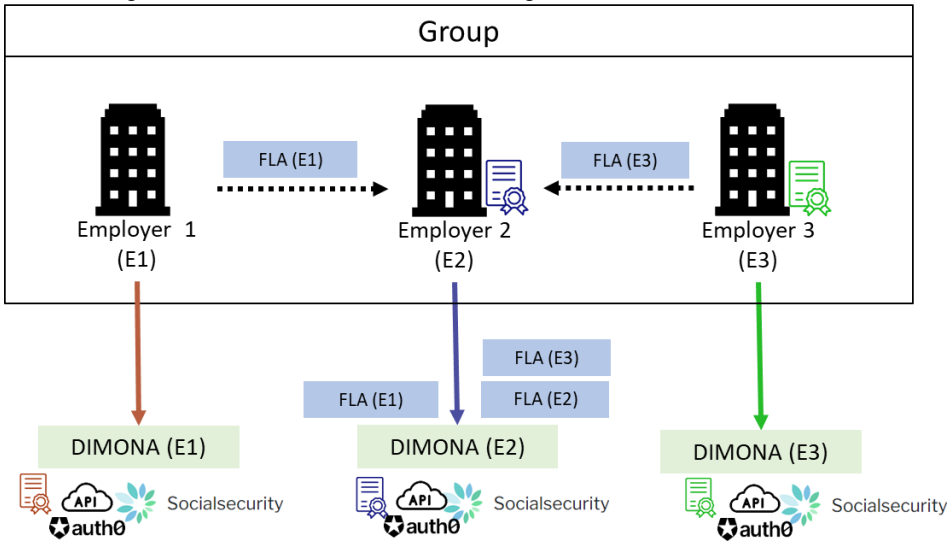
1) Jedes Unternehmen meldet die Daten der eigenen Arbeitnehmenden und nutzt dabei seinen eigenen Kanal. In diesem Fall ist für jede ZDU-Nummer ein Webservice-Account zu erstellen (und für jede ZDU-Nummer wird ein Zertifikat benötigt).

   Beispiel 5: Angenommen, ein Konzern besteht aus drei Unternehmen. Jedes der drei Unternehmen meldet die Daten seiner eigenen Arbeitnehmenden selbst (ein einziger Webservice-Account pro Unternehmen).



2) Ein Unternehmen wird Bevollmächtigter für alle anderen Konzernunternehmen für die *Federal Learning Account*-Daten. In diesem Fall gilt das Gleiche wie bei Bevollmächtigten.

   Beispiel 6: Angenommen, ein Konzern besteht aus drei Unternehmen. Unternehmen 2 wird von den beiden anderen Unternehmen mit der Bereitstellung der Daten des *Federal Learning Account* für den gesamten Konzern bevollmächtigt. Unternehmen 2 erstellt einen einzigen Webservice-Account für FLA und Dimona.



Anmerkung

Die *Federal Learning Account*-Daten eines Arbeitnehmenden müssen immer für die ZDU-Nummer des Unternehmens gesendet werden, das für ihn auch die Dimona- und die DmfA-Erklärung abgibt. Dieses Unternehmen kann die Körperschaft sein, die das Konsortium vertritt.

2.4. Sonderfall: Softwareanbieter

Wenn ein Unternehmen Arbeitgebenden eine Software bereitstellt, mit der die Daten des *Federal Learning Account* verschickt werden können, hängt die Art der Verwendung des Webservice-Kanals von der jeweiligen Situation ab.

1) Handelt es sich um eine zentrale Software beim Softwareanbieter oder hat dieser einen Vertrag über den Versand der FLA-Daten im Namen des Arbeitgebers geschlossen, gilt die Regelung für Bevollmächtigte (vgl. 2.2 Sonderfall: Bevollmächtigte). Der Softwareanbieter schickt die Datenfiles seiner Arbeitgebenden selbst.
2) Läuft die Software eigenständig oder hat der Softwareanbieter keinen Vertrag mit den Arbeitgebenden geschlossen, gilt die allgemeine Regelung: Jeder Arbeitgeber erstellt seinen eigenen Kanal bzw. Webservice-Account und schickt die Daten an die REST-API (mit der oder ohne die Anwendung des Softwareanbieters).

2.5. Spezifität der Schulungsanbieter

Ein Unternehmen in der Eigenschaft als „Fortbildungsanbieter“ ist ein Unternehmen, das Arbeitgebern Fortbildungsdienstleistungen anbietet. Sie ist diejenige, die die Fortbildungen für die Teilnehmer organisiert und durchführt.

Um Arbeitgebern die Codierungsaufgabe zu erleichtern, kann ein „Fortbildungsanbieter“-Unternehmen der FLA-Plattform Daten zu den von ihm organisierten Fortbildungen zur Verfügung stellen. Dabei nutzt das Unternehmen den technischen Kanal BATCH/API mit der Eigenschaft „Fortbildungsanbieter“.

Der Fortbildungsanbieter versendet die Fortbildungsdaten im eigenen Namen, also mit eigener ZDU-Nummer. Die von einem Fortbildungsanbieter bereitgestellten Daten können möglicherweise Informationen für den Arbeitgeber eines Teilnehmers liefern. Auch wenn in den Daten der Arbeitgeber eines Teilnehmers angegeben ist, ist kein Mandat zwischen dem Fortbildungsanbieter und diesem Arbeitgeber erforderlich.

3. Konfigurierung des API-Kanals

Der IT-Dienst des Unternehmens (Arbeitgeber oder Bevollmächtigter, je nach Situation im Einzelfall) bzw. der Softwareanbieter bindet diese API in ein bestehendes (oder neues) Datensystem ein.

Nutzt das Unternehmen noch keinen REST-Webservice der Sozialen Sicherheit und/oder hat sich das Unternehmen nicht vorab auf dem Portal der Sozialen Sicherheit angemeldet, muss dieser erst konfiguriert werden.

Abhängig von der geschilderten Situation sind im Einzelfall einige bzw. die meisten der im vorliegenden Handbuch erläuterten Schritte bereits als abgeschlossen zu betrachten.

4. Schritt-für-Schritt-Plan des Geschäftsführers des Unternehmens

Bevor der REST-FLA-Service genutzt werden kann, muss der REST-Webdienst der Sozialen Sicherheit konfiguriert werden. Zur Erstellung eines Profils und Gewährleistung der Sicherheit muss der Kunde (Arbeitgeber) wie folgt vorgehen:

4.1. Schritt 1: Identifizieren Sie sich als Arbeitgeber auf dem Portal der Sozialen Sicherheit.

Wenn Sie bereits als Arbeitgeber bei der Sozialen Sicherheit gemeldet sind, können Sie diesen Schritt als erledigt betrachten.

Für die Nutzung der Onlinedienste der Sozialen Sicherheit muss das Unternehmen auf dem Portal der Sozialen Sicherheit als Arbeitgeber gemeldet sein. Bitte gehen Sie wie folgt vor, falls dies noch nicht der Fall ist: https://www.socialsecurity.be/site_de/general/first_visit/access/register-as-employer.htm

4.2. Schritt 2: Melden Sie sich als Arbeitgeber auf dem Portal der Sozialen Sicherheit an.

Wenn Sie bereits auf dem Portal angemeldet sind, können Sie diesen Schritt als abgeschlossen betrachten.

Wenn Sie bei der Sozialen Sicherheit als LSS-Arbeitgeber bekannt sind, müssen Sie angeben, ob Sie die Verwaltung und Benutzung der gesicherten Zugänge in Ihrem Unternehmen behalten oder auslagern möchten.

Sie können sich mit folgendem Link auf dem Portal anmelden:

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

4.3. Schritt 3: Zugang zum Onlinedienst „Chaman“

Die Konfigurierung eines technischen Kanals (Batch oder API) kann nur durch einen Benutzer vorgenommen werden, der bereits Zugang zur Anwendung Chaman der Sozialen Sicherheit hat.

Zugang zu Chaman haben:

- der „**lokale Verwalter**“ als LSS-Arbeitgeber (oder Dienstleister, Sozialsekretariat, Fortbildungsanbieter). Dieser wird bei der Anmeldung des Unternehmens auf dem Portal bestimmt.
- Jeder Benutzer, der vom lokalen Verwalter einen Zugang erhalten hat. Der lokale Verwalter kann als LSS-Arbeitgeber (oder Dienstleister, Sozialsekretariat, Fortbildungsanbieter) mithilfe des Onlinedienstes „Zugangsverwaltung“ der Sozialen Sicherheit Zugang zum Onlinedienst Chaman gewähren (socialsecurity.be).

  Falls Sie keinen Zugang zu Chaman haben, können Sie bei Ihrem lokalen Verwalter beantragen, dass Ihnen die „Verwaltung der technischen Kanäle“ im Onlinedienst „Zugangsverwaltung“ zugewiesen wird.

4.4. Schritt 4: Ein REST-Webservice-Account aktivieren

Wenn Ihr Unternehmen im Rahmen einer anderen Sozialversicherungsanwendung (DmfA, Dimona usw.) bereits ein REST-Webservice-Account für die Eigenschaft erstellt hat, die Sie betrifft (Arbeitgeber, Sozialsekretariat, Dienstleister oder Fortbildungsanbieter), ist die auch möglich für das FLA-Framework. Befolgen Sie in diesem Fall bitte „Schritt 4b: Ändern eines vorhandenen REST-Webservice-Account“.

Andernfalls befolgen Sie bitte „Schritt 4a: Erstellen Sie ein REST-Webservice-Account“.

Anmerkung

Für einige Unternehmen ist es möglich, dass die FLA-Plattform in mehreren unterschiedlichen Eigenschaften genutzt wird:

- Eigenschaft “Arbeitgeber”, um dem Unternehmen die Übermittlung der FLA-Daten seiner eigenen Arbeitnehmer zu ermöglichen
- Eigenschaft “Bevollmächtigten“ (Dienstleister oder Sozialsekretariat), um dem Unternehmen die Übermittlung der FLA-Daten der Arbeitnehmer seiner Kunden zu ermöglichen
- Eigenschaft Fortbildungsanbieter, damit das Unternehmen Schulungsdaten senden kann, die es für Arbeitgeber organisiert hat

In diesem Fall müssen mehrere REST-Webservice-Account erstellt werden: mindestens eines pro Qualität.

4.4.1. Schritt 4a: Erstellen eines REST-Webservice-Account

Dieser Schritt ist erforderlich, wenn Ihr Unternehmen noch keinen REST-Webservice-Account hat oder wenn Sie einen Account speziell für die Anwendung CareerPro Federal Learning Account erstellen möchten. Ist dies nicht der Fall, fahren Sie mit Schritt 4b fort.

Vorbedingungen:

Für die Erstellung eines neuen REST-Webservice-Accounts benötigen Sie ein qualifiziertes digitales Zertifikat,1 das als CER-Datei exportiert wurde.

Sie haben mehrere Möglichkeiten::

- Sie können das Zertifikat bei einer anerkannten Zertifizierungsstelle bestellen. Hier ist eine Liste der derzeit unterstützten Zertifizierungsstellen:

Zertifizierungs-stelle	Zertifikatstyp	Link
GlobalSign	PersonalSign 3 Pro	https://shop.globalsign.com/en/belgian-government-services

- Sie können ein selbstsigniertes Zertifikat auf den Namen Ihres Unternehmens verwenden. Das Verfahren zur Erstellung eines solchen Zertifikats wird hier derzeit nicht beschrieben. Normalerweise wird die Erstellung eines solchen Zertifikats von der IT-Abteilung Ihres Unternehmens durch die Verwendung eines Tools wie OpenSSL unterstützt. Bitte beachten Sie die folgenden Einschränkungen bei der Erstellung Ihres selbstsignierten Zertifikats:

Zu respektierende Kriterien	Zulässige Werte
Algorithmus zur Erzeugung des Schlüsselpaares	RSA oder EC
Schlüsselgröße (Bits)	Für RSA : 2048, 3072 oder 4096
Für EC : P-384 oder P-521	
Digest-Algorithmus, der mit der Signatur des Zertifikats verbunden ist	SHA-256, SHA-384 oder SHA-512
Key Usage des Zertifikats	Digital Signature

Dieses Zertifikat wird benötigt:

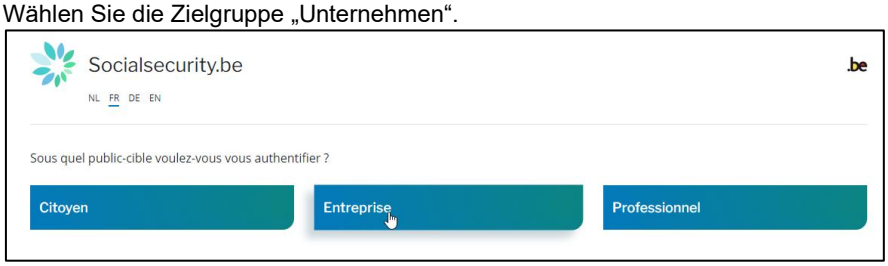
- für die Erstellung des Webservice-Accounts
- für die Authentifizierung Ihres IT-Systems auf dem Portal mit dem Sicherheitsprotokoll OAuth, also für den Erhalt des erforderlichen Sicherheitstokens beim Aufruf der REST-API FLA.

Schritte

1. Der Benutzer (mit Zugang zu Chaman) loggt sich in der Anwendung „Chaman“ ein.

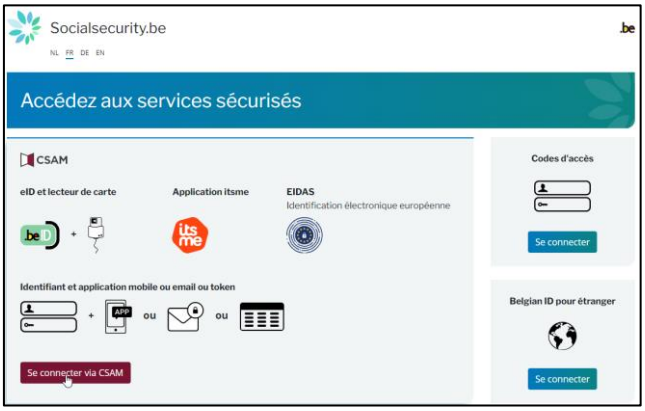
   www.socialSecurity.be → Unternehmen → Onlinedienste → Chaman → Verwaltung technischer Kanäle

2. Wählen Sie die Zielgruppe „Unternehmen“.



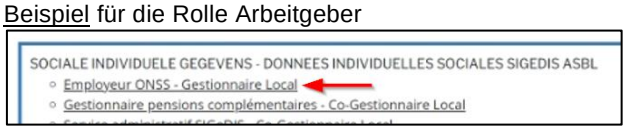
3. Melden Sie sich mit CSAM an und folgen Sie den Anweisungen für die Verwendung der beabsichtigten Methode (eID, itsme usw.).

[1] Siehe „6.3.2 Zertifikat öffnen“



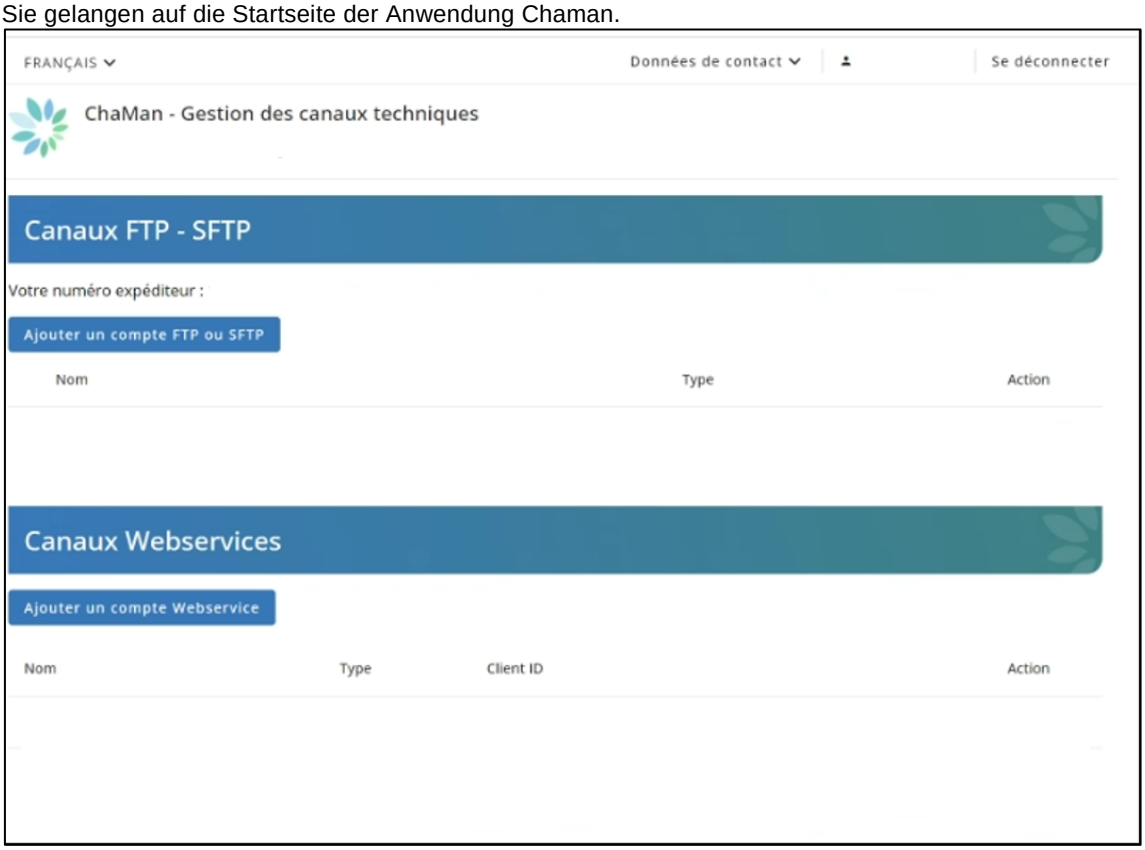
4. Wenn Ihr Unternehmen unterschiedliche Rollen hat, wählen Sie die Eigenschaft:
   - „LSS-Arbeitgeber“ bei Verwendung des Batchkanals für einen Arbeitgeber ohne Bevollmächtigten
   - „Sozialsekretariat“ oder „Dienstleister“ bei Verwendung des API-kanals durch einen Bevollmächtigten
   - „Fortbildungsanbieter“ im Falle der Nutzung des API-Kanals zur Übermittlung von Fortbildungsdaten, den das Unternehmen für Arbeitgeber organisiert hat

   Beispiel für die Rolle Arbeitgeber



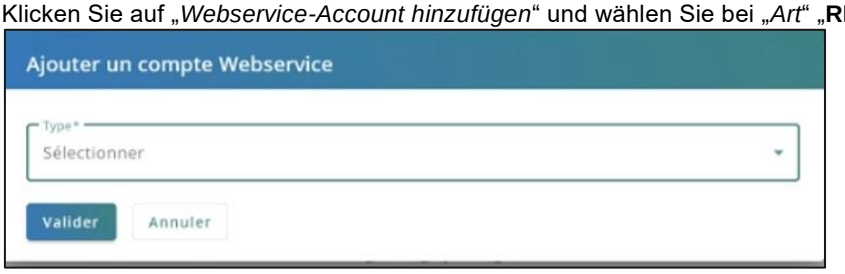
   Anmerkung
   Steht die beabsichtigte Rolle nicht zur Verfügung, muss sie Ihr Hauptverwalter im Tool „Zugangsverwaltung“ anlegen. Mit den anderen Rollen kann kein API-kanal für den Federal Learning Account erstellt werden.

5. Sie gelangen auf die Startseite der Anwendung Chaman.

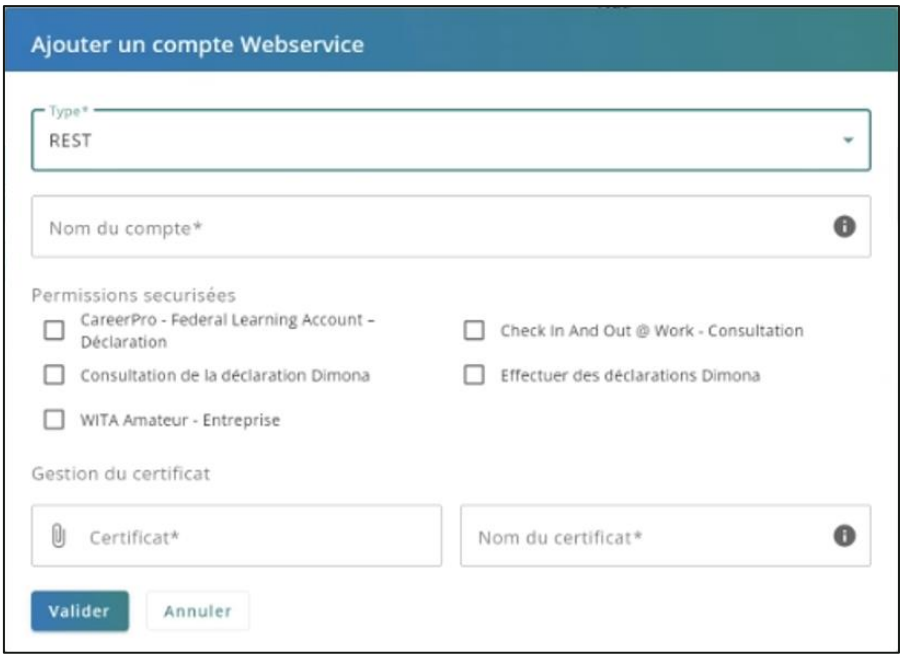


Anmerkung: Wenn Sie die Fehlermeldung „Zugang verweigert“ erhalten, wenden Sie sich an Ihren lokalen Verwalter, der Ihnen einen Zugang zu Chaman zuweist.

6. Klicken Sie auf „*Webservice-Account hinzufügen*“ und wählen Sie bei „*Art*“ „**REST**“.



7. Füllen Sie das Formular aus.



- Accountname: Hier können Sie frei einen beliebigen Namen vergeben.
- Bei „Permissions“ kreuzen Sie „CareerPro – Federal Learning Account“ an.
- Zertifikat: Laden Sie den öffentlichen Schlüssel (CER) Ihres Zertifikats in dieses Feld (siehe Vorbedingungen).
- Zertifikatname: Geben Sie Ihrem Zertifikat einen Namen

8. „Bestätigen“

Die Client-ID wird in der Zeile des REST-Webservice-Accounts angezeigt, den Sie soeben erstellt haben. Wir empfehlen Ihnen, diese Angaben gut aufzubewahren, denn Sie benötigen Sie später noch (= OAuth-ClientId).

4.4.2. Schritt 4b: Änderung eines bestehenden REST-Webservice-Accounts

Dieser Schritt ist erforderlich, wenn Ihr Unternehmen bereits einen REST-Webservice-Account in der gewünschten Eigenschaft hat und Sie ihn für die Anwendung CareerPro Federal Learning Account benutzen möchten. Ist dies nicht der Fall, fahren Sie bitte mit Schritt 4a fort.

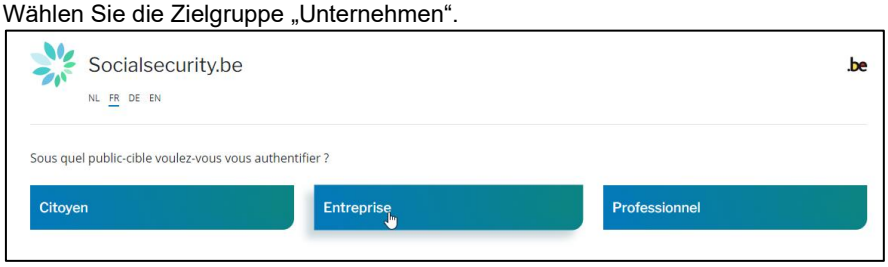
Besitzen Sie bereits einen aktiven REST-Webservice-Kanal in der gewünschten Eigenschaft das Sie auch für den „CareerPro - Federal Learning Account“ (wieder)verwenden möchten, wird kein neues Zertifikat benötigt. Es wird das vorhandene Zertifikat benutzt.

Schritte

1. Der Benutzer (mit Zugang zu Chaman) loggt sich in der Anwendung „Chaman“ ein.

   www.socialSecurity.be → Unternehmen → Onlinedienste → Chaman → Verwaltung technischer Kanäle

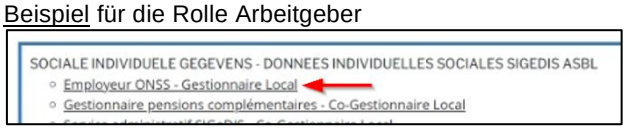
2. Wählen Sie die Zielgruppe „Unternehmen“.



3. Melden Sie sich mit CSAM an und folgen Sie den Anweisungen für die Verwendung von eID oder itsme.

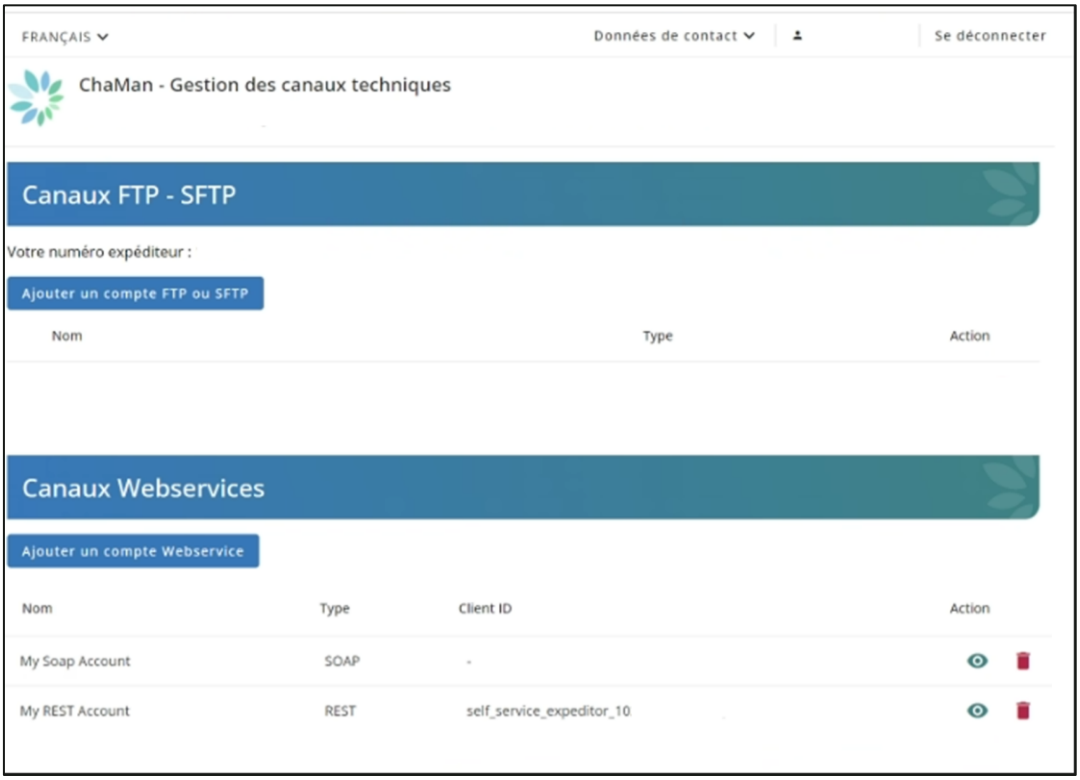
   Wenn Ihr Unternehmen unterschiedliche Rollen hat, wählen Sie die Eigenschaft:
   - „LSS-Arbeitgeber“ bei Verwendung des API-kanals für einen Arbeitgeber ohne Bevollmächtigten
   - „Sozialsekretariat“ oder „Dienstleister“ bei Verwendung des API-kanals durch einen Bevollmächtigten
   - „Fortbildungsanbieter“ im Falle der Nutzung des API-Kanals zur Übermittlung von Fortbildungsdaten, den das Unternehmen für Arbeitgeber organisiert hat

   Beispiel für die Rolle Arbeitgeber

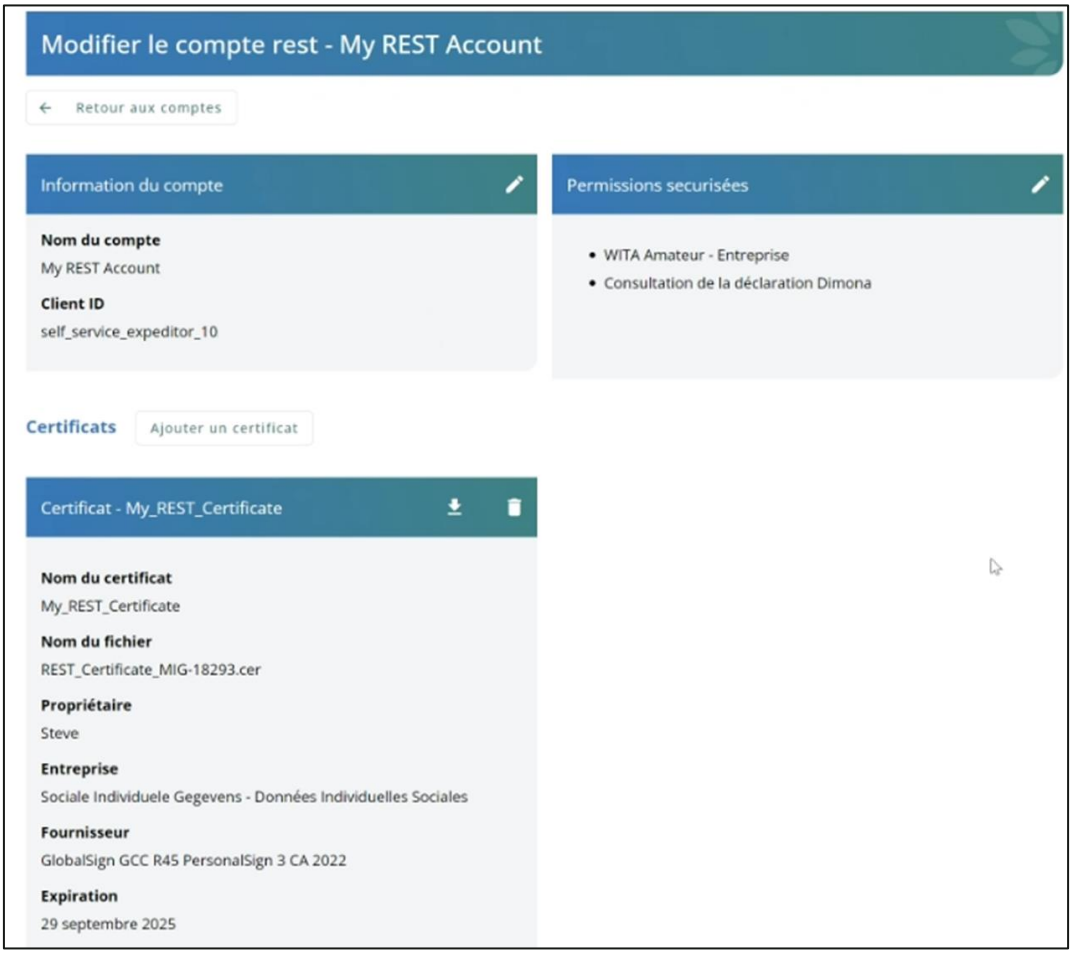


   Anmerkung
   Steht die beabsichtigte Rolle nicht zur Verfügung, muss sie Ihr Hauptverwalter im Tool „Zugangsverwaltung“ anlegen. Mit den anderen Rollen kann kein API-kanal für den Federal Learning Account erstellt werden.

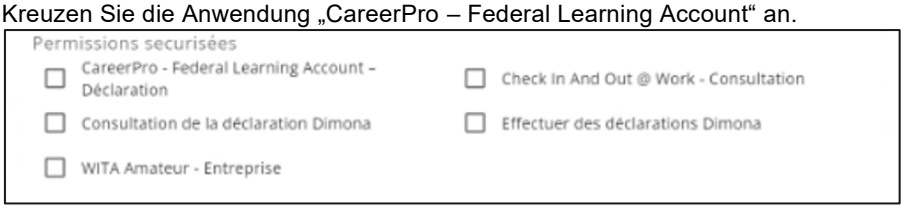
4. Sie gelangen auf die Startseite der Anwendung Chaman.



5. Zum Anschauen des REST-Webservice, den Sie verwenden möchten, klicken Sie auf  .



6. Klicken Sie in **Permissions sécurisées** an.
7. Kreuzen Sie die Anwendung „CareerPro – Federal Learning Account“ an.



8. „Bestätigen“

Die Client-ID wird angezeigt. Wir empfehlen Ihnen, diese Angaben gut aufzubewahren, denn Sie benötigen Sie später wieder (= OAuth-ClientId).

5. Schritt-für-Schritt-Plan für Anwendungsentwickler

5.1. Schritt 1: Implementierung der Sicherheit OAuth

Der Webservice REST-API des Federal Learning Account ist gesichert indem er dem OAUTH-Protokoll folgt. Bevor Sie ihn benutzen können, müssen Sie dieses Sicherheitsprotokoll OAuth implementieren. Mit dieser Implementierung erhält Ihr Client des Webservice ein Sicherheitstoken vom OAuth-Server. Dieses Token muss bei Aufrufen der REST-API des Federal Learning Account verwendet werden.

Mit anderen Worten: Ihre Anwendung muss zunächst den OAuth-Server der sozialen Sicherheit mit den Parametern aufrufen, die es Ihnen ermöglichen, anzugeben, „wer Sie sind“ (Client-ID, Zertifikat, Umfang usw.). Im Gegenzug erhalten Sie einen Sicherheitstoken, der bescheinigt, dass OAUTH Sie korrekt identifiziert hat und Sie Zugriff auf die FLA-API haben. Dieser Token läuft ab und muss regelmäßig erneuert werden. Dieses Token sollte in alle Ihre Aufrufe der FLA-API integriert werden. Ohne diesen Token wird Ihr Anruf von der Sozialversicherung abgelehnt.

Bitte beachten Sie diesbezüglich die nachfolgende Dokumentation.

Oauth2 Integration Client Credential: https://www.socialsecurity.be/site_de/general/helpcentre/rest/documents/pdf/doc_portal_oauth2_client_credential_DE.pdf
Beispielcode zur Implementierung der OAUTH-Sicherheit: Siehe Anhang 6.2

Folgende Parameter sind bei der Anforderung des OAuth-Tokens anzugeben:

Grant type	client_credentials
Scope	Der Wert des Bereichs hängt von der Eigenschaft ab, mit der Sie das REST-Webservice-Konto auf CHAMAN erstellt haben. Eigenschaft Arbeitgeber: → Scope = “scope:sigedis:gestion:careerpro-federal-learning-account:employer” Eigenschaft Bevollmächtigte (Sozialsekretariat oder Dienstleister): → Scope = “scope:sigedis:gestion:careerpro-federal-learning-account:provider” Eigenschaft Fortbildungsanbieter: → Scope =
ClientId	Die OAuth-ClientID, die bei der Freischaltung des Kanals vergeben wurde (siehe vorheriger Abschnitt)
Zertifikat	Das Zertifikat, das bei der Freischaltung des Kanals verwendet wurde (siehe vorheriger Abschnitt)
Token Endpoint	https://services.socialsecurity.be/REST/oauth/v5/token
Audience URL	https://services.socialsecurity.be/REST/oauth/v5/token

Sie erhalten dann ein Access Token.

5.2. Schritt 2: Aufrufen der REST-API CareerPro FLA

Zum Aufrufen der REST-API FLA muss Ihr Client des Webservice das Access Token verwenden, das er beim letzten Schritt erhalten hat.

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	to be defined

5.3. Testumgebung

Es ist möglich, die FLA-API in einer TEST-Umgebung zu testen. Diese Umgebung ist vollständig von der Produktionsumgebung getrennt. In dieser Umgebung muss ein Kanal erstellt werden.

Nachfolgend finden Sie die Liste der URLs, die für die Testumgebung verwendet werden sollen.

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	to be defined

BITTE BEACHTEN SIE, dass diese TEST-Umgebung standardmäßig nicht für Unternehmen zugänglich ist. Wir müssen Ihr Unternehmen in dieses Umfeld integrieren. Dazu müssen Sie eine Zugriffsanfrage an ContactCenter@support.eranova.fgov.be senden

6. Anhang

6.1. Ermittlung des lokalen Zugangsverwalters

Für Unternehmen, die bereits auf dem Portal der Sozialen Sicherheit angemeldet sind, ist es nicht immer einfach herauszufinden, wer der **lokale Verwalter** ist. Wenn Sie bereits eine Anwendung auf dem Portal benutzen, können Sie diese Information herausfinden, indem Sie sich in die Anwendung „Zugangsverwaltung“ auf dem Portal einloggen.

www.socialSecurity.be → Unternehmen → Onlinedienste → Zugangsverwaltung → Zugangsverwaltung.

Der Name des **lokalen Verwalters** steht auf der Seite „**Vos responsables**“ unter „LSS-Arbeitgeber“ (bzw. bei Bevollmächtigten als „Dienstleister“ oder „Sozialsekretariat“).

6.2. OAuth-Beispiel

```
/*
  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());

    }
```

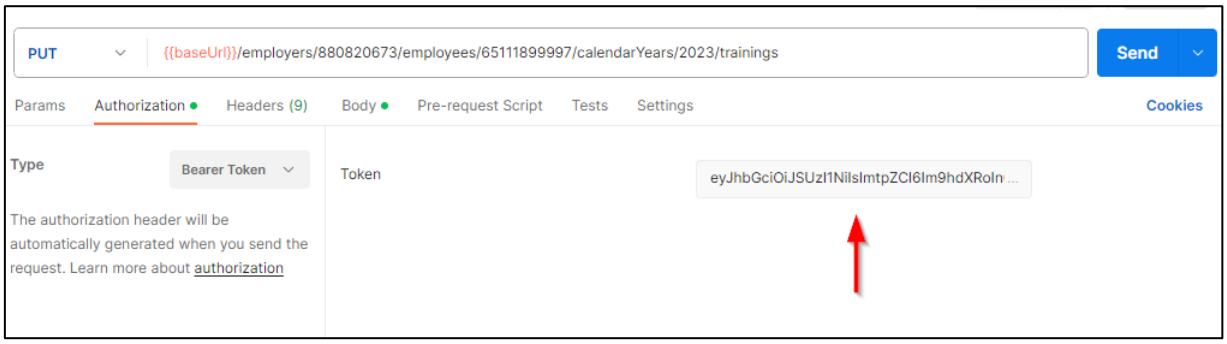
6.3. Tools

6.3.1. Aufruf an der REST-API mit PostMan

Es gibt Anwendungen, mit denen eine REST-API manuell ohne Entwickler aufgerufen werden kann (PostMan, Insomnia usw.). Diese Anwendungen sind mit den Token OAuth kompatibel und können verwendet werden, um die API besser zu verstehen, bevor Sie Ihre Entwicklungen starten.

In der Anwendung „PostMan“ zum Beispiel können Aufrufe der REST-API FLA durch Hinzufügen des im letzten Schritt erhaltenen Tokens erfolgen.

Zum Hinzufügen des Tokens gehen Sie in die Registerkarte „Authorization“, wählen Sie „Bearer Token“ und fügen Sie den Wert des Tokens im entsprechenden Feld hinzu.

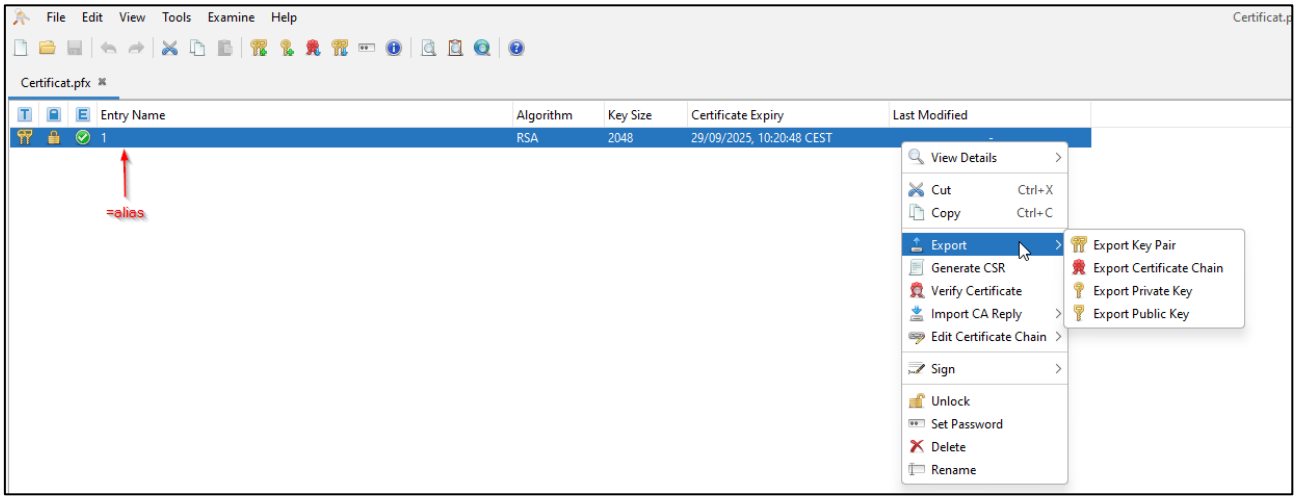


6.3.2. Zertifikat öffnen

Bei qualifizierten Zertifikaten handelt es sich normalerweise um eine PFX-Datei. Es gibt Anwendungen, mit denen dieser Dateityp geöffnet und bestimmte Informationen wie der Alias, der öffentliche Schlüssel, der private Schlüssel oder das CER-Zertifikat extrahiert werden können.

Beispiel mit dem Tool „Key Store Explorer“

In diesem Beispiel ist der Alias des Zertifikats „1“. Mit einem Rechtsklick kann das Zertifikat in der bei der Konfigurierung des Kanals verlangten Form als CER-Datei exportiert werden.


File
Edit
View
Tools
Examine
Help
Certificat.pfx
Entry Name
Algorithm
Key Size
Certificate Expiry
Last Modified
1
RSA
2048
29/09/2025, 10:20:48 CEST
=alias
View Details
Cut Ctrl+X
Copy Ctrl+C
Export
Generate CSR
Verify Certificate
Import CA Reply
Edit Certificate Chain
Sign
Unlock
Set Password
Delete
Rename
Export Key Pair
Export Certificate Chain
Export Private Key
Export Public Key