

SI-MesServices.etudiant.gouv.fr

Interfacer une application avec le MSE

[Résumé]



SDN

SDN

Publié le [Date de publication]

	SI-MesServices.etudiant.gouv.fr	Interfacer une application avec le MSE	
	-	[Résumé]	
SDN	SDN	V5.0	Publié le [Date de publication] Etat du document : Valide

Version	Historique du document	Auteur	Publication
V4.0	Précisions : §2, §3, §4.2.1 Mises à jour infra MSE : §4.1.3, §4.2.2, §4.2.3, §4.2.4, §5.1.1, §6	SDN	05/06/2024
V4.1	Ajout §4.2.4	Cadoles	05/07/2024
V4.2	Modification §4.1.3.1, §4.1.3.2	Cadoles	02/10/2024
V4.3		Cadoles	18/03/2025
V5.0	Ajout §5 et Modification §6	Cadoles	31/03/2025
V5.1	Ajout propriété name au token_id et typo §3 et §4.1.2	Cadoles	28/04/2025
V5.1.1	Typo §2.6	Cadoles	27/05/2025
V5.2	Ajout nouveau process de SingleSignOn	Cadoles	06/01/2026

1 Table des matières

1	Introduction.....	4
2	Principe général.....	4
3	Description des attributs.....	5
4	Méthodes d'authentification.....	8
4.1	Authentification MSE sur reverse proxy « OIDC ».....	8
4.1.1	Principe de fonctionnement.....	8
4.1.2	Adaptation d'une application accédée depuis le MSE	8
4.1.3	Urls à utiliser	10
4.2	Authentification OIDC (connexion/déconnexion depuis applicatif).....	11
4.2.1	Principe de fonctionnement.....	11
4.2.2	Configuration.....	11
4.2.3	Connexion.....	12
4.2.4	Utiliser la fonctionnalité de SSO	13
4.2.5	Récupération Information utilisateur	14
4.2.6	Déconnexion.....	14
4.2.7	Applicatif mobile	15
5	Récupération des données complètes d'un étudiant par API REST.....	16
5.1	Exigences et contraintes de l'échange	16

5.2	Demandes d'accès et droits d'utilisation	16
5.3	Description détaillée des données échangées	17
5.3.1	Authentification et jeton JWT	17
5.3.2	Documentation API DOC	17
5.3.3	Récupérer les données complètes d'un étudiant.....	17
6	<i>Récupération des données complètes d'un étudiant par Webservice SOAP</i>	18
6.1.1	Exigences et contraintes de l'échange	19
6.1.2	Exigences et contraintes de Sécurité.....	19
6.1.3	Description détaillée des données échangées	19
7	<i>URLS du MSE</i>	27
8	<i>Accompagnement technique.....</i>	27
9	<i>Documents applicables et de référence (A/R)</i>	28
10	<i>Glossaire</i>	28

1 Introduction

Ce document constitue la spécification de l'interfaçage entre le MSE (Portail MesServices.etudiant.gouv.fr) et une **application** qui doit être accessible via ce portail comme LOKAVIZ, JOBAVIZ, CITE'U, TROUVERUNLOGEMENT, CVEC, DEMANDE DE DSE ...

- Le chapitre 2 décrit le principe général de l'utilisation du MSE pour accéder à une **application**.
- Le chapitre 3 décrit les attributs de session du MSE qui sont utilisés.
- Le chapitre 4 décrit le fonctionnement de l'authentification via OIDC.
- Le chapitre 5 décrit l'utilisation de l'API Rest.
- Le chapitre 6 recense les URLS à utiliser.

2 Principe général

1. L'utilisateur déclenche une demande d'authentification soit depuis le MSE (1) soit depuis une application (2).
2. L'utilisateur est renvoyé vers la page de choix d'authentification du fournisseur d'identité : FranceConnect ou MesServices.etudiant.gouv.fr
3. L'utilisateur choisit son fournisseur d'identité :
 - 3.1. MesServices.etudiant.gouv.fr
 - 3.1.1. L'utilisateur est renvoyé vers la page d'authentification du fournisseur d'identité-du MSE.
 - 3.1.2. L'utilisateur saisit son identifiant et son mot de passe habituel.
 - 3.2. FranceConnect
 - 3.2.1. L'utilisateur est renvoyé vers la page d'authentification du fournisseur d'identité FranceConnect.
 - 3.2.2. L'utilisateur saisit son compte et son mot de passe.
4. Si l'authentification réussit, l'utilisateur est redirigé soit vers la page d'accueil du portail MSE (1) soit vers l'application appelante (2).
5. Le MSE (1) et l'application appelante (2) récupèrent les attributs dans le jeton d'authentification OIDC pour en faire une session locale à l'utilisateur : **given_name, family_name, email, ine, display_name, idpve, ayantdroitdse et crous** en OPENID
 - 5.1. Si idPVE vide ou inexistant, l'étudiant n'a pas de compte sur MesServices ou possède un compte bloqué sur MesServices : **mettre un message d'erreur invitant à se connecter/s'inscrire depuis MesServices (cf. 4.2.1.).**

A noter : L'idPVE sera toujours renseigné pour les services derrière le reverse proxy MesServices. (cf. 4.1)
6. Si idPVE renseigné, et que l'application appelante possède les droits, elle peut faire un appel API REST du MSE vers la ressource `/mse/v1/etudiant/{typeid}/{id}`, afin de récupérer les données complètes auxquelles l'application appelante a les droits de lecture.

3 Description des attributs

Attributs disponibles avec le protocole OIDC :

Nom Attribut	Utilisation	Valeurs possibles	
given_name	les prénoms séparés par des espaces (standard OpenIDConnect)	Tous les prénoms si connexion avec FranceConnect 1 ^{er} prénom si connexion avec MesServices	
family_name	le nom de naissance (standard OpenIDConnect)	le nom de naissance	
email	l'adresse courriel (standard OpenIDConnect)		
ine	Identifiant National Etudiant (INE)	INE référent courant	
display_name	Nom complet avec accents	prenom1 + espace + nom de famille	
name	Nom complet avec accents	prenom1 + espace + nom de famille	
idpve	Identifiant institutionnel unique dans MesServices	Si idPVE vide ou inexistant, l'étudiant n'a pas de compte sur MesServices ou possède un compte bloqué sur MesServices : mettre un message d'erreur invitant à se connecter/s'inscrire depuis MesServices (cf. 4.2.1.) A noter : L'idPVE sera toujours renseigné pour les services derrière le reverse proxy MesServices. (cf. 4.1)	
ayantdroitdse	Indique si l'étudiant est un ayant droit au DSE	O = ayant droit à un DSE N = non ayant droit à un DSE U = non définit	
crous	Cours de rattachement de l'étudiant Cette donnée peut être vide	Code	Nom MSE
			Pas de crous de rattachement défini
		AIX	CROUS AIX-MARSEILLE-AVIGNON
		AMI	CROUS AMIENS - PICARDIE
		ANT	CROUS ANTILLES-GUYANE
		BFC	CROUS BOURGOGNE FRANCHE-COMTÉ
		BOR	CROUS BORDEAUX - AQUITAINE
		CAL	NOUVELLE CALEDONIE
		CLE	CROUS CLERMONT - AUVERGNE
		COR	CROUS CORSE
		CRE	CROUS CRÉTEIL
		GRE	CROUS GRENOBLE - ALPES
		LIL	CROUS LILLE - NORD-PAS-DE-CALAIS
		LIM	CROUS LIMOGES
		LYO	CROUS LYON
		MAY	CROUS LA RÉUNION ET MAYOTTE : MAYOTTE
		MON	CROUS MONTPELLIER - OCCITANIE
		NAN	CROUS NANTES - PAYS DE LA LOIRE
		NCY	CROUS LORRAINE
NIC	CROUS NICE - TOULON		

		NOR	CROUS NORMANDIE
		ORL	CROUS ORLÉANS - TOURS
		PAR	CROUS PARIS
		POI	CROUS POITIERS
		POL	POLYNESIE
		REI	CROUS REIMS
		REN	CROUS RENNES - BRETAGNE
		REU	CROUS LA RÉUNION ET MAYOTTE : LA RÉUNION
		STR	CROUS STRASBOURG
		TOU	CROUS TOULOUSE - OCCITANIE
		VER	CROUS VERSAILLES

Exemples de contenu du token OIDC :

- Pour une connexion avec MesServices :

```
{
  "appId": "sql",
  "at_hash": "oYJJt0z-Nz2Oog9A7I6pFQ",
  "aud": [
    "mse-demo"
  ],
  "auth_time": 1681992632,
  "cn": "sta test",
  "crous": "POI",
  "display_name": "sta test",
  "name": "sta test",
  "email": "teststa@yopmail.com",
  "eppa": null,
  "exp": 1681996235,
  "family_name": "test",
  "given_name": "sta",
  "iat": 1681992635,
  "idpve": 4709925,
  "ine": "22222222LL",
  "iss": "https://messervices.etudiant.gouv.fr/auth/",
  "jti": "9e116edc-8465-49e3-8044-960c24f61f1f",
  "nonce": "CFwgMx9DrDrrlDG1",
  "rat": 1681992604,
  "sid": "d9f1a714-e134-4917-9f5c-898ba87ed179",
  "sub": "4709925@portail-vie-etudiante.fr"
}
```

- Pour une connexion avec FranceConnect :

```
{
  "appId": "france-connect",
  "at_hash": "5Y2ibBSUCEjKJECHPWVKEw",
  "aud": [
    "mse-demo"
  ],
  "auth_time": 1680859974,
  "birthcountry": "99100",
  "birthdate": "1962-08-24",
  "birthplace": "75107",
  "crous": "BFC",
  "display_name": "Angela DUBOIS",
  "name": "Angela DUBOIS",
  "email": "wossewodda-3728@yopmail.com",
  "exp": 1680863577,
  "family_name": "DUBOIS",
  "gender": "female",
  "given_name": "Angela Claire Louise",
  "iat": 1680859977,
  "idpve": 1140,
  "ine": "660042144AC",
  "iss": "https://msedev.crous-toulouse.fr/auth/",
  "jti": "ea8c448c-8e53-4194-b15a-d5f5e7e2900b",
  "nonce": "Tu5Y94AQM0slVr9V",
  "preferred_username": "",
  "rat": 1680859969,
  "sid": "9107578f-eae5-4727-8d50-99a66414754c",
  "sub": "dc45ee4d92bc1e3889b442209ec032231c27b4b92ba9ca6ed680adeec25105e7v1"
}
```

4 Méthodes d'authentification

4.1 Authentification MSE sur reverse proxy « OIDC »

Un reverse proxy "OIDC", mis en frontal d'une application, permet de localiser au niveau du reverse proxy la phase d'authentification.

ATTENTION : Pour utiliser ce type d'authentification il faut que l'application soit capable de fonctionner derrière un reverse proxy

Si l'application possède sa propre gestion d'authentification, il faudra la supprimer tout en conservant la notion éventuelle et existante de session/jeton/ticket.

4.1.1 Principe de fonctionnement

1. L'url de l'application qui est accédée via le reverse proxy est appelée ;
2. La requête est interceptée le reverse proxy MSE et le processus OIDC s'enclenche.
3. Le reverse proxy transfère alors la requête vers le serveur hébergeant l'application, avec les champs d'en-têtes HTTP, notamment ceux positionnés par le SP MSE (**ine, display_name, name, given_name, family_name, email, idpve, ayantdroidse, crous**) ;
4. Sinon, l'application récupère ces champs d'en-têtes http pour en faire une session locale à l'utilisateur.

4.1.2 Adaptation d'une application accédée depuis le MSE

Une application accédée par le MSE récupérera les attributs OIDC via l'entête http.

Ex en PHP :

```
$arh=apache_request_headers();  
$arh['OIDC_CLAIM_ine'] pour récupérer l'attribut ine.  
$arh['OIDC_CLAIM_family_name'] pour récupérer l'attribut family_name  
$arh['OIDC_CLAIM_given_name'] pour récupérer l'attribut given_name  
$arh['OIDC_CLAIM_display_name'] pour récupérer l'attribut display_name  
$arh['OIDC_CLAIM_name'] pour récupérer l'attribut name  
$arh['OIDC_CLAIM_email'] pour récupérer l'attribut email  
$arh['OIDC_CLAIM_idpve'] pour récupérer l'attribut idpve  
$arh['OIDC_CLAIM_ayantdroidse'] pour récupérer l'attribut ayantdroidse  
$arh['OIDC_CLAIM_crous'] pour récupérer l'attribut crous
```

Exemple d'entête récupérée par `apache_request_headers()` en **préproduction** :

```
array(38) {  
  ["Host"]=> string(24) "messervices-pp.lescrous.fr"  
  ["Cache-Control"]=> string(9) "max-age=0"  
  ["Upgrade-Insecure-Requests"]=> string(1) "1"  
  ["User-Agent"]=> string(114) "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36"  
  ["Accept"]=> string(85) "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8"  
  ["Referer"]=> string(125) "https://messervices-pp.lescrous.fr/xxxxxxxxxxxxx"  
  ["Accept-Encoding"]=> string(17) "gzip, deflate, br"  
  ["Accept-Language"]=> string(35) "fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7"  
  ["Cookie"]=> string(155) "xxxxxxxxxxxxx"  
  ["X-Forwarded-Port"]=> string(3) "443"  
  ["X-Forwarded-Proto"]=> string(5) "https"  
  ["X-Forwarded-For"]=> string(14) "xx.xxx.xxx.xxx"  
  ["Connection"]=> string(5) "close"  
  ["OIDC_CLAIM_idpve"]=> string(26) "6"  
  ["OIDC_CLAIM_ine"]=> string(11) "9916D00003F"  
  ["OIDC_CLAIM_cn"]=> string(12) "testetu test"  
  ["OIDC_CLAIM_family_name"]=> string(4) "test"  
  ["OIDC_CLAIM_email"]=> string(19) "testetu@yopmail.com"  
  ["OIDC_CLAIM_given_name"]=> string(7) "testetu"  
  ["OIDC_CLAIM_display_name"]=> string(12) "testetu test"  
  ["OIDC_CLAIM_name"]=> string(12) "testetu test"  
  ["OIDC_CLAIM_crous"]=> string(3) "AIX"  
  ["OIDC_CLAIM_ayantdroidse"]=> string(1) "O"  
  ["OIDC_CLAIM_sub"]=> string(26) "xxxxxxxxxxxxx"  
}
```

4.1.3 Urls à utiliser

4.1.3.1 En préproduction

Pour déclencher l'authentification depuis l'application :

<https://messervices-pp.lescrous.fr/oauth2/login?redirect=/<application>/>

- <application> : entrée du reverse proxy qui permet la redirection vers l'url réelle de l'application.
- Ex : <https://messervices.etudiant.gouv.fr/oauth2/login?redirect=/depot/>
après l'authentification, l'utilisateur sera redirigé vers la demande DSE

Pour déclencher la déconnexion depuis une application :

<https://messervices-pp.lescrous.fr/auth/oauth2/sessions/logout>

(*) les URL de production seront fournies après les premiers tests de qualification.

4.2 Authentification OIDC (connexion/déconnexion depuis applicatif)

4.2.1 Principe de fonctionnement

Une demande d'authentification est faite par l'utilisateur.

Le SSO MSE reçoit cette demande et en atteste l'origine.

Le SSO MSE propose à l'utilisateur les sources d'authentifications disponibles (RP)

L'utilisateur s'authentifie

Le SSO MSE atteste l'origine et renvoie les informations utilisateurs.

Si idPVE vide ou inexistant, l'étudiant n'a pas de compte sur MesServices ou possède un compte bloqué sur MesServices : mettre un message d'erreur invitant à se connecter/s'inscrire depuis MesServices.

Voici la phrase à indiquer dans le cas où l'idPVE est vide en session dans chaque applicatif.

« **Votre session ne permet pas de vous connecter à ce service.**

Veuillez au préalable vous connecter directement au portail MesServices.etudiant.gouv.fr via l'URL : <https://messervices.etudiant.gouv.fr> »

Toutes les informations concernant le protocole OpenID Connect sont sur :

<https://openid.net/connect/>

https://openid.net/specs/openid-connect-core-1_0.html

4.2.2 Configuration

Les configurations nécessaires pour une connexion par MesServices en **pré-production** :

Endpoint OIDC	Url
Discovery Url	https://messervices-pp.lescrous.fr/auth/.well-known/openid-configuration
Authorization	https://messervices-pp.lescrous.fr/auth/oauth2/auth
Token	https://messervices-pp.lescrous.fr/auth/oauth2/token
Userinfo	https://messervices-pp.lescrous.fr/auth/userinfo
Logout	https://messervices-pp.lescrous.fr/auth/oauth2/sessions/logout

(*) les URL de production seront fournies après les premiers tests de qualification.

Informations de connexion délivrées par MSE, uniques à chaque partenaire :

- Client ID : **client_id**
- Client Secret : **client_secret**

Information à fournir à MSE par les partenaires :

- Urls de callback de connexion **redirect_uri**
- Urls de redirection après déconnexion **post_logout_redirect_uri**

- A noter : possibilité de déclarer plusieurs sous-domaines.
- Pas d'impact lors du changement d'infrastructure MSE.

Attention :

- les Urls 'redirect_uri' et 'post_logout_redirect_uri' doivent partager le même nom de domaine.
- chaque URI de logout doit correspondre à au moins une des URIs de redirection (même domaine, port et protocole).
Ex : <https://test.exemple.fr/in> et <https://test.exemple.fr/out>
- Le protocole OIDC impose de lister toutes les URIs. Il n'est pas possible d'ajouter une seule URI pour englober plusieurs URIs.
Ex : <https://test.exemple.fr/> ne peut substituer <https://test.exemple.fr/a> <https://test.exemple.fr/b> etc...

4.2.3 Connexion

Endpoint OIDC	Authorization
Méthode	GET
Réponse	TokenID

Paramètres de requête	Valeurs admises
client_id	client_id fourni lors par MSE (cf. paragraphe précédent)
scope	'openid profile email'
response_type	'code'
prompt	'login' ou 'none'
redirect_url	Url de Callback redirect_uri
nonce	Valeur aléatoire, devant être identique et vérifiée à la fin de connexion de 24 caractères minimum
state	Valeur aléatoire de 24 caractères minimum, différent du nonce
acr_values	Optionnel : - non défini pour avoir le choix d'authentification avec MesServices ou FranceConnect - 'sql' pour forcer la méthode d'authentification uniquement avec MesServices

****Exemple de requête d'authentification en préproduction ****

```
https://messervices-pp.lescrous.fr/auth/oauth2/auth?
nonce=c12ce09dd61179ef9cb85905681797d5e7c0d2065ac9
&scope=openid%20profile%20email
&state=abcc2f5d56a951cd9e4c5ae5ad4b6539
&response_type=code
&prompt=login
&redirect_uri=https%3A%2F%2Fmesservices-pp.lescrous.fr%2Foauth2%2Fcallback
```

&client_id=mse

4.2.4 Utiliser la fonctionnalité de SSO

Le paramètre **prompt** permet de contrôler le comportement de l'autorisation et de l'authentification. Il est utile pour optimiser l'expérience utilisateur, et ainsi bénéficier du mécanisme de *Single Sign On*, où l'objectif est de réutiliser une session existante sans interaction utilisateur.

Côté client :

Le client envoie une requête d'autorisation avec `prompt=none`.

```
https://messervices-pp.lescrous.fr/auth/oauth2/auth?  
nonce=c12ce09dd61179ef9cb85905681797d5e7c0d2065ac9  
&scope=openid%20profile%20email  
&state=abcc2f5d56a951cd9e4c5ae5ad4b6539  
&response_type=code  
&prompt=none  
&redirect_uri=https%3A%2F%2Fmesservices-pp.lescrous.fr%2Foauth2%2Fcallback  
&client_id=mse
```

Si une session valide existe :

MSE renvoie un code d'autorisation ou un token.

Si aucune session valide n'existe :

MSE redirige vers le `redirect_uri` avec une erreur OIDC (typiquement `login_required`, `consent_required`, `selected_app_id_not_found` ou `interaction_required`)

Le client doit interpréter le code d'erreur et relancer une requête d'autorisation avec un `prompt` approprié :

- Exemple : `prompt=login` pour demander la connexion.

4.2.5 Récupération Information utilisateur

Endpoint OIDC	Token
Méthode	POST
Réponse	AccessToken et TokenID
Auth Méthode	client_secret_basic

Pour la méthode **client_secret_basic**, l'en-tête Authorization doit être au format

Authorization: Basic encodedString

où `encodedString` est le résultat de l'encodage Base64 de `clientId:clientSecret` du client Oauth.

Paramètres de requête	Valeurs admises
code	client_id fourni lors par MSE (cf. paragraphe précédent)
grant_type	'authorization_code'

****Exemple de requête de en PREPROD avec curl****

```
curl -X POST https://messervices-pp.lescroux.fr/auth/oauth2/token \
--header 'Authorization: BASIC YzNyc3BkN[...]S0tOEZZw==' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-raw "grant_type=authorization_code&code=Xs01spaDxxx"
```

4.2.6 Déconnexion

Requête de déconnexion :

Endpoint OIDC	Logout
Méthode	GET

Paramètres de requête	Valeurs admises
id_token_hint	TokenID récupéré en réponse à la connexion (cf. paragraphe 5.2.1)
post_logout_redirect_uri	Url de déconnexion post_logout_redirect_uri (cf. paragraphe 5.2.)
state	Valeur aléatoire de 24 caractères minimum

Recommandé : Si aucun paramètre n'est transmis à la requête, une déconnexion sera initié par l'IDP, et l'utilisateur sera redirigé sur le portail MSE.

****Exemple de requête de déconnexion côté IDP en **préproduction** avec redirection MSE ****

<https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout>

****Exemple de requête de déconnexion côté Relying Party en **préproduction** ****

[https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout?](https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout?state=abcc2f5d56a951cd9e4c5ae5ad4b6539&id_token_hint=eyJhbGciOiJIUzI1NiIsImtpZCI6InB1YmtpYzpoZWY5S5vc[...]&post_logout_redirect_uri=https%3A%2F%2Fmesservices-pp.lescroux.fr%2Flogout-success)

[state=abcc2f5d56a951cd9e4c5ae5ad4b6539](https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout?state=abcc2f5d56a951cd9e4c5ae5ad4b6539&id_token_hint=eyJhbGciOiJIUzI1NiIsImtpZCI6InB1YmtpYzpoZWY5S5vc[...]&post_logout_redirect_uri=https%3A%2F%2Fmesservices-pp.lescroux.fr%2Flogout-success)

[&id_token_hint=eyJhbGciOiJIUzI1NiIsImtpZCI6InB1YmtpYzpoZWY5S5vc\[...\]](https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout?state=abcc2f5d56a951cd9e4c5ae5ad4b6539&id_token_hint=eyJhbGciOiJIUzI1NiIsImtpZCI6InB1YmtpYzpoZWY5S5vc[...]&post_logout_redirect_uri=https%3A%2F%2Fmesservices-pp.lescroux.fr%2Flogout-success)

[&post_logout_redirect_uri=https%3A%2F%2Fmesservices-pp.lescroux.fr%2Flogout-success](https://messervices-pp.lescroux.fr/auth/oauth2/sessions/logout?state=abcc2f5d56a951cd9e4c5ae5ad4b6539&id_token_hint=eyJhbGciOiJIUzI1NiIsImtpZCI6InB1YmtpYzpoZWY5S5vc[...]&post_logout_redirect_uri=https%3A%2F%2Fmesservices-pp.lescroux.fr%2Flogout-success)

4.2.7 Applicatif mobile

Fournisseur d'identité uniquement par MesServices (pas de choix de fournisseur d'identité car la connexion avec FranceConnect ne doit pas être utilisée).

Dans les paramètres de la requête de connexion, l'attribut `acr_values` devra être défini avec `saml` pour forcer la méthode d'authentification uniquement avec MesServices.

5 Récupération des données complètes d'un étudiant par API REST

5.1 Exigences et contraintes de l'échange

L'API REST pour la gestion des données étudiantes utilise le protocole HTTP pour permettre la communication et l'échange de données entre les applications distantes. Voici les exigences et contraintes à respecter lors de l'utilisation de cette API :

Authentification : Chaque requête doit inclure un en-tête d'autorisation valide avec une clé API (`apiKey`) pour accéder aux ressources protégées.

Format des données : Les données échangées doivent être au format JSON.

Types d'identifiants : Les identifiants des étudiants peuvent être de type `ine` (Identifiant National Étudiant) ou `idpve` (Identifiant Portail Vie Étudiante).

Gestion des erreurs : Les erreurs sont renvoyées avec des codes HTTP appropriés et des messages descriptifs.

5.2 Demandes d'accès et droits d'utilisation

Il est nécessaire de disposer d'un compte sur <https://developers.lescroux.fr/> et de faire une demande d'accès à l'API MSE.

Il est également nécessaire de se rapprocher des services MSE afin de réaliser une demande d'APIKey et de droits d'accès aux informations étudiantes.

5.3 Description détaillée des données échangées

5.3.1 Authentification et jeton JWT

L'utilisation des ressources REST est soumise à une authentification via jeton JWT.

Pour récupérer votre jeton JWT, vous devez réaliser une requête d'authentification.

Exemple de requête d'authentification :

```
curl -v -d "grant_type=client_credentials" -d "env=PPD" -H "Authorization: $(echo -n
VOTRE_APP_ID:VOTRE_APP_SECRET_PPD_SAUVEGARDE | base64 -w 0)" -H "Content-Type: application/x-www-form-
urlencoded" https://api-pp.nuonet.fr/v1/token
```

5.3.2 Documentation API DOC

PRODUCTION	https://api.lescrous.fr/mse/swagger
PRE-PRODUCTION	https://api-pp.nuonet.fr/mse/swagger

5.3.3 Récupérer les données complètes d'un étudiant

5.3.3.1 Paramètres de la requête

Endpoint OIDC	/mse/v1/etudiant/{typeid}/{id}
Méthode	GET
Réponse	JSON
Auth Méthode	Jeton JWT & APIKey
API Doc	/mse/swagger

Paramètres de requête	Valeurs admises
Jeton JWT (Authorization Header, obligatoire)	Jeton JWT émis par la demande d'authentification sur api.lescrous.fr
apikey (query, obligatoire)	Clé API de l'auteur de la requête (cf. paragraphe 5.2.1)
typeid (path, obligatoire)	Type d'identifiant de l'étudiant (ine ou idpve).
Id (path, obligatoire)	INE ou IDPve de l'étudiant, en fonction du type précédent

Exemple de requête :

HTTP GET https://api-pp-nuonet.fr/mse/v1/etudiant/idpve/607?apiKey=aabbccddeeff

5.3.3.2 Réponses possibles

200 OK : Retourne les données de l'étudiant basées sur les rôles liés à votre `ApiKey`.

401 Unauthorized : Autorisation invalide ou échec de la validation du jeton.

404 Not Found : Étudiant non trouvé.

Exemple de données en réponse avec des droits de lecture de l'identité de l'étudiant:

```
{  
  "idpve": "1234567890",  
  "INE": "9876543210",  
  "nom": "Dupont",  
  "prenom": "Jean",  
  "dateNaissance": "01/01/2000",  
  "courriel": "jean.dupont@example.com",  
  "telephoneFixe": "0123456789",  
  "telephonePortable": "0698765432",  
  "adresseVoie": "1 rue de la Paix",  
  "adresseCodePostal": "75001",  
  "adresseCodePays": "FRA"  
}
```

6 Récupération des données complètes d'un étudiant par WebService SOAP

Obsolète

Les échanges via API Rest sont à privilégier.

Les échanges via SOAP décrits ci-dessous sont à usage informatif

Pour récupérer les données complètes d'un étudiant, l'application doit utiliser la méthode `lireDonneesEtudiant` du WebService exposé par le MSE en passant les paramètres **idPVE** l'**INE** et/ou le **nom**, tous transmis lors de l'authentification.

- Cf. 3 Description des attributs
- Cf. 6.1.3.4 Cinématique de l'échange

6.1.1 Exigences et contraintes de l'échange

L'appel du WebService utilise le protocole SOAP 1.1 sur HTTP. Le protocole de communication est défini dans la signature du service exposé (WSDL).

Le WSDL du WebService est accessible via les URLs suivantes :

En production : <https://messervices.etudiant.gouv.fr/soap/common>

<https://www.messervices.etudiant.gouv.fr/envole/soap/common>

En préproduction : <https://messervices-pp.lescrous.fr/soap/common>

<https://pp.messervices.etudiant.gouv.fr/envole/soap/common>

A noter : L'appel du WebService avec le protocole REST est à venir.

6.1.1.1 Encodage des caractères

Le MSE utilise la norme UTF-8.

6.1.2 Exigences et contraintes de Sécurité

- Le MSE utilise le mécanisme de reverse proxy : Intermédiaire de sécurité.

Le reverse proxy protège un serveur Web des attaques provenant de l'extérieur. La réécriture programmable des URL permet de masquer et de contrôler, par exemple, l'architecture d'un site web interne. Mais cette architecture permet surtout le filtrage en un point unique des accès aux ressources Web.

- Les adresses IP de l'applicatif en PREPROD et en PROD qui appellent le WS MSE devront être transmises pour autorisation.

6.1.3 Description détaillée des données échangées

6.1.3.1 Structure des données échangées

6.1.3.1.1 Données du contexte pour l'appel du web service.

Nom	Libelle	Type	Valeurs possibles
systemeID	Nom de l'application cliente	String	
mdp	Mot de passe pour l'accès au service	String	NA

6.1.3.2 Données pour l'appel du web service.

Nom	Libelle	Type
idPVE	Identifiant unique de l'utilisateur du MSE	String : 11 caractères maximum
INE	INE de l'étudiant	String : 11 caractères
nom	Nom patronymique de l'utilisateur	String : 100 caractères (minuscules accentuées, majuscules non accentuées)

6.1.3.3 Données retournées par le web service

Nom	Libelle	Type	Valeurs possibles
codeRetour	Code de retour du web service	String	Cf. Codes retours
nom	Nom patronymique de l'utilisateur	String : 100 caractères maximum	NA
prenom	Prénom de l'utilisateur	String : 100 caractères maximum	NA
prenom2	Prénom 2 de l'utilisateur	String : 100 caractères maximum	NA
prenom3	Prénom 3 de l'utilisateur	String : 100 caractères maximum	NA
dateNaissance	Date de naissance de l'utilisateur	String : "jj/mm/aaaa"	NA
courriel	Adresse de messagerie électronique de l'utilisateur	String : 100 caractères maximum	NA
civilite	Titre de civilité de l'utilisateur	String : 1 caractère	Nomenclature N_CIVILITE.code
dateCreation	Date de création de l'utilisateur	String : "jj/mm/aaaa"	NA
codeProfil	Code du profil de l'utilisateur	String : 1 caractère	Nomenclature N_PROFIL.code
libelleProfil	Libelle du profil de l'utilisateur	String : 20 caractères maximum	Nomenclature N_PROFIL.libelleCourt
statutProfil	Code du statut du profil de l'utilisateur	String : 1 caractère	Nomenclature N_STATUT_PROFIL.code
libelleStatutProfil	Libelle du statut profil de l'utilisateur	String : 20 caractères maximum	Nomenclature N_STATUT_PROFIL.libelleCourt
inscrit	Indique si l'étudiant est inscrit actuellement dans un établissement	String : 1 caractère	'O' ou 'N'
telephone1	Téléphone fixe de l'utilisateur	String : 20 caractères maximum	NA
telephone2	Téléphone portable de l'utilisateur	String : 20 caractères maximum	NA
adresseVoie	Voie de l'adresse de l'utilisateur	String : 50 caractères maximum	NA
adresseComplement1	Complément de l'adresse de l'utilisateur	String : 50 caractères maximum	NA
adresseComplement2	Complément de l'adresse de l'utilisateur	String : 50 caractères maximum	NA
adresseLocalite	Localité de l'adresse de l'utilisateur	String : 50 caractères maximum	NA
adresseCodePostal	Code postal de l'adresse de l'utilisateur	String : 10 caractères maximum	NA
adresseCodePays	Code pays de l'adresse de l'utilisateur	String : 3 caractères	Nomenclature : N_PAYS.codeBCN
dateDerniereModif	Date de dernière modification du profil de l'utilisateur dans le MSE	String : "jj/mm/aaaa"	NA
dateDernierAcces	Date de dernier accès au MSE par l'utilisateur	String : "jj/mm/aaaa"	NA
dernierINE	Dernier INE de l'étudiant	String : 11 caractères	
listeINE	Liste des INE de l'étudiant triés par date de mise à jour de l'ine, du plus récent au plus ancien		Séparées par des virgules
situationFamille	Situation de famille de l'étudiant	String : 1 caractère	Nomenclature : N_SITUATION_FAMILLE.code
civiliteContactFamial1	Titre de civilité du contact familial 1	String : 1 caractère	Nomenclature N_CIVILITE.code
nomContactFamial1	Nom patronymique du contact familial 1	String : 50 caractères maximum	NA
prenomContactFamial1	Prénom du contact familial 1	String : 50 caractères maximum	NA
telephone1ContactFamial1	Téléphone 1 du contact familial 1	String : 20 caractères maximum	NA
telephone2ContactFamial1	Téléphone 2 du contact familial 1	String : 20 caractères maximum	NA

courrielContactFamial1	Adresse de messagerie électronique du contact familial 1	String : 100 caractères maximum	NA
adresseVoieContactFamial1	Voie de l'adresse du contact familial 1	String : 50 caractères maximum	NA
adresseComplement1ContactFamial1	Complément de l'adresse du contact familial 1	String : 50 caractères maximum	NA
adresseComplement2ContactFamial1	Complément de l'adresse du contact familial 1	String : 50 caractères maximum	NA
adresseLocaliteContactFamial1	Localité de l'adresse du contact familial 1	String : 50 caractères maximum	NA
adresseCodePostalContactFamial1	Code postal de l'adresse du contact familial 1	String : 10 caractères maximum	NA
adresseCodePaysContactFamial1	Code pays de l'adresse du contact familial 1	String : 3 caractères	Nomenclature : N_PAYS.codeBCN
civiliteContactFamial2	Titre de civilité du contact familial 2	String : 1 caractère	Nomenclature N_CIVILITE.code
nomContactFamial2	Nom patronymique du contact familial 2	String : 50 caractères maximum	NA
prenomContactFamial2	Prénom du contact familial 2	String : 50 caractères maximum	NA
telephone1ContactFamial2	Téléphone 1 du contact familial 2	String : 20 caractères maximum	NA
telephone2ContactFamial2	Téléphone 2 du contact familial 2	String : 20 caractères maximum	NA
courrielContactFamial2	Adresse de messagerie électronique du contact familial 2	String : 100 caractères maximum	NA
adresseVoieContactFamial2	Voie de l'adresse du contact familial 1	String : 50 caractères maximum	NA
adresseComplement1ContactFamial2	Complément de l'adresse du contact familial 2	String : 50 caractères maximum	NA
adresseComplement2ContactFamial2	Complément de l'adresse du contact familial 2	String : 50 caractères maximum	NA
adresseLocaliteContactFamial2	Localité de l'adresse du contact familial 2	String : 50 caractères maximum	NA
adresseCodePostalContactFamial2	Code postal de l'adresse du contact familial 2	String : 10 caractères maximum	NA
adresseCodePaysContactFamial2	Code pays de l'adresse du contact familial 2	String : 3 caractères	Nomenclature : N_PAYS.codeBCN
uaiEtabOrigineAVenir	Code UAI de l'établissement d'origine ou à venir de l'étudiant	String : 8 caractères	Nomenclature : N_ETABLISSEMENT.uai

6.1.3.3.1 Codes retours

Ce tableau présente la raison du rejet et le code retourné à l'application.

Id rejet	Description	Code retour	Champs concernés
PVE_FL01_R01	OK	OK	
PVE_FL01_R02	Connexion refusée	ConnexionErreur	
PVE_FL01_R03	Un élément du contexte est vide ou ne correspond pas aux valeurs autorisées	ContextErreur	contexte
PVE_FL01_R04	idPVE non connu du portail MSE.	UsagerErreur	idPVE
PVE_FL01_R05	L'INE fait plus de 11 caractères, ou est inconnu pour cet idPVE.	IneErreur	INE

PVE_FL01_R06	Le nom fait plus de 100 caractères, ou est inconnu pour cet idPVE.	NomErreur	nom
--------------	--	-----------	-----

6.1.3.3.2 Sémantique

Ce paragraphe précise les entités métier / attributs du MSE pour les attributs échangés à travers les flux.

Les entités et attributs référencées pour le MSE se trouvent dans le modèle de domaine détaillé du projet MSE. (cf. [R1])

Libelle	MSE			Id transformation
	Entité	Attribut		
		Code	Type	
Identifiant unique de l’usager du MSE	Usager	idPVE	11 car maximum (identifiant technique incrémental)	
Nom patronymique de l’usager	Usager	nom	100 car maximum	
Prénom de l’usager	Usager	prenom	100 car maximum	
Prénom2 de l’usager	Usager	prenom2	100 car maximum	
Prénom3 de l’usager	Usager	prenom3	100 car maximum	
Date de naissance de l’usager	Usager	dateNaissance	date : (jj/mm/aaaa)	
Email de l’usager	Usager	mail	100 car maximum	
Civilité de l’usager	Usager	codeCivilite	1 car : Nomenclature N_CIVILITE.code	
Téléphone1 (fixe) de l’usager	Usager	telephoneFixe	20 car maximum	
Téléphone2 (portable) de l’usager	Usager	telephonePortable	20 car maximum	
Voie de l’adresse de l’usager	Usager	adresseVoie	50 car maximum	
Adresse Complément 1 de l’usager	Usager	adresseComplement1	50 car maximum	
Adresse Complément 2 de l’usager	Usager	adresseComplement2	50 car maximum	
Localité de l’adresse de l’usager	Usager	adresseLocalite	50 car maximum	
Code postal de l’adresse de l’usager	Usager	adresseCodePostal	10 car maximum	
Code pays de l’adresse de l’usager	Usager	adresseCodePays	3 car : Nomenclature N_PAYS.codeBCN	
Date de dernière modification du profil de l’usager dans le MSE	Usager	dateDerniereModif	date : (jj/mm/aaaa)	
Date de dernier accès au MSE par l’usager	Usager	dateDernierAcces	date : (jj/mm/aaaa)	
Code du profil de l’usager	Usager	profil	1 car : Nomenclature N_PROFIL.code	

Libelle du profil de l'utilisateur	N_PROFIL	libelleCourt	20 car maximum	
Code du statut du profil de l'utilisateur	Usager	statutProfil	entier : Nomenclature N_STATUT_PROFIL.code	
Libelle du statut profil de l'utilisateur	N_STATUT_PROFIL	libelleCourt	20 car maximum	
Dernier INE de l'étudiant	INE_Etudiant	Ine	11 car	PVE_FL00_T01
Liste des INE	INE_Etudiant	Ine	Liste des INE de 11 car	PVE_FL00_T02
Situation de famille de l'étudiant	Etudiant	codeSituationFamille	1 car : Nomenclature N_SITUATION_FAMILLE.code	
Code UAI de l'établissement d'origine ou à venir de l'étudiant	Etudiant	origineEtablissement	8 car : Nomenclature N_ETABLISSEMENT.uai	
Civilite du contact familial 1	Contact_familial de Etudiant.idContact1	codeCivilite	1 car : Nomenclature N_CIVILITE.code	
Nom du contact familial 1	Contact_familial de Etudiant.idContact1	nom	50 car maximum	
Prenom du contact familial 1	Contact_familial de Etudiant.idContact1	prenom	50 car maximum	
Téléphone 1 du contact familial 1	Contact_familial de Etudiant.idContact1	telephone1	20 car maximum	
Téléphone 2 du contact familial 1	Contact_familial de Etudiant.idContact1	telephone2	20 car maximum	
Email du contact familial 1	Contact_familial de Etudiant.idContact1	mail	100 car maximum	
Voie de l'adresse du contact familial 1	Contact_familial de Etudiant.idContact1	adresseVoie	50 car maximum	
Adresse Complément 1 voie du contact familial 1	Contact_familial de Etudiant.idContact1	adresseComplement1	50 car maximum	
Adresse Complément 2 voie du contact familial 1	Contact_familial de Etudiant.idContact1	adresseComplement1	50 car maximum	
Localité de l'adresse contact familial 1	Contact_familial de Etudiant.idContact1	adresseLocalite	50 car maximum	
Code postal de l'adresse du contact familial 1	Contact_familial de Etudiant.idContact1	adresseCodePostal	10 car maximum	
Code pays de l'adresse du contact familial 1	Contact_familial de Etudiant.idContact1	adresseCodePays	3 car : Nomenclature N_PAYS.codeBCN	
Civilite du contact familial 2	Contact_familial de Etudiant.idContact2	codeCivilite	1 car : Nomenclature N_CIVILITE.code	
Nom du contact familial 2	Contact_familial de Etudiant.idContact2	nom	50 car maximum	
Prenom du contact familial 2	Contact_familial de Etudiant.idContact2	prenom	50 car maximum	
Téléphone 1 du contact familial 2	Contact_familial de Etudiant.idContact2	telephone1	20 car maximum	
Téléphone 2 du contact familial 2	Contact_familial de Etudiant.idContact2	telephone2	20 car maximum	
Email du contact familial 2	Contact_familial de Etudiant.idContact2	mail	100 car maximum	
Voie de l'adresse du contact familial 2	Contact_familial de Etudiant.idContact2	adresseVoie	50 car maximum	

Adresse Complément 1 du contact familial 2	Contact_familial de Etudiant.idContact2	adresseComplement1	50 car maximum	
Adresse Complément 2 du contact familial 2	Contact_familial de Etudiant.idContact2	adresseComplement2	50 car maximum	
Localité de l’adresse contact familial 2	Contact_familial de Etudiant.idContact2	adresseLocalite	50 car maximum	
Code postal de l’adresse du contact familial 2	Contact_familial de Etudiant.idContact2	adresseCodePostal	10 car maximum	
Code pays de l’adresse du contact familial 2	Contact_familial de Etudiant.idContact2	adresseCodePays	3 car Nomenclature N_PAYS.codeBCN	

Ce tableau présente les règles de transformation des entités et attributs.

Id transformation		Description
PVE_FL00_T01		Le MSE fournira l'INE courant pour l'étudiant.
PVE_FL00_T02		Le MSE fournira la liste des INE retrouvés dans la table INE_ETUDIANT pour l'idPVE de l'Etudiant, triés par date de mise à jour de l'ine du plus récent au plus ancien.

6.1.3.4 Cinématique de l'échange

L'application interroge le WebService exposé par le MSE (méthode lireProfilPVE) en passant en paramètre :

- l'identifiant technique de l'utilisateur (**idPVE**)
- le paramètre l'INE (**ine**) pour un étudiant
- le nom (**family_name**) de l'utilisateur (case sensitive)

INE ou nom : l'un des deux doit être fourni obligatoirement (en plus de idPVE).

Le MSE répond de manière synchrone en retournant le profil de l'utilisateur, ou un code erreur si la demande n'a pas pu être traitée.

Pour une meilleure sécurité, si un INE est en paramètre d'appel du service, le MSE comparera l'INE envoyé et la liste d'INE enregistrée dans le profil correspondant à l'idPVE avant de renvoyer le profil, afin de croiser 2 sources de données distinctes.

Si l'INE n'est pas trouvé, un code retour « PVE_FL01_R05 » sera retourné à l'application.

Si un nom est en paramètre d'appel du service, le MSE comparera ce nom envoyé et le nom enregistré dans le profil correspondant à l'idPVE avant de renvoyer le profil, afin de croiser 2 sources de données distinctes.

Si le nom n'est pas trouvé, un code retour « PVE_FL01_R06 » sera retourné à l'application

7 URLS du MSE

Pour accéder au MSE de production : <https://messervices.etudiant.gouv.fr>

Pour accéder au MSE de préproduction : <https://messervices-pp.lescrous.fr/>

- Protégé par BasicAuth

8 Accompagnement technique

Les partenaires de MSE peuvent contacter par mail support-partenaires-mse@crous.fr pour les questions techniques concernant l'authentification.

9 Documents applicables et de référence (A/R)

A/R	Référence	Titre
[R1]	SFD-CRO-001_PVE_Cas_dUtilisation	Cas d'Utilisation MSE
[R2]	SFD-CRO-001_PVE_Nomenclatures	Nomenclatures MSE

10 Glossaire

Terme	Définition
MSE	Portail Messervices.etudiant.gouv.fr
URL	Adresse d'un site sur internet
Web service	Programme informatique qui permet la communication et l'échange de données entre des applications distantes à travers le réseau internet (protocole HTTP)
INE	Identifiant National Etudiant
SOAP	Simple Object Access Protocol
WSDL	Web Services Description Language
OIDC	OpenID Connect