

SSI

Connexion


Interfacer une application avec CrousConnect

Document technique



SDN

Publié le 19/06/2024

	SSI	Interfacer une application avec CrousConnect	
	Connexion	Document technique	
SDN	SDN	VO.2	Publié le 19/06/2024 Etat du document : Valide

1 Table des matières

1 Introduction

Ce document constitue la spécification de mise en œuvre du fournisseur d'identité nommé **CrousConnect** permettant la connexion au travers du protocole **OIDC** pour les **Crous** et le **Cnous**.

Le CNOUS a défini un modèle appelé « CrousConnect » qui s'inspire du modèle étatique FranceConnect & AgentConnect.

C'est un service qui permet aux agents de se connecter à des services applicatifs métiers en ligne proposés par des fournisseurs de services autorisés préalable. CrousConnect s'appuie sur des comptes d'identité numériques vérifiés par le fournisseurs d'identité.

- Le chapitre 2 décrit le principe général de l'utilisation du fournisseur d'identité
- Le chapitre 3 décrit le bouton « CrousConnect ».
- Le chapitre 4 décrit les attributs disponibles en retour de l'authentification.
- Le chapitre 5 décrit le fonctionnement de l'authentification.

2 Principe général

1. L'utilisateur déclenche une demande d'authentification depuis une application (fournisseur de service) en utilisant le bouton « **CrousConnect** » au travers du protocole **OIDC**.
2. L'utilisateur est renvoyé vers la page de choix d'authentification du fournisseur d'identité : connect.lescrous.fr.
3. L'utilisateur saisit ses identifiants.
4. Si l'authentification réussit, l'utilisateur est redirigé vers l'application appelante.
5. Le fournisseur de service récupère les attributs pour en faire une session locale à l'utilisateur

3 Le Bouton « CrousConnect »

Le bouton « CrousConnect » est fourni par le Cnous.



Sa charte graphique est prédéfinie (forme, couleur, ...) et ne peut être modifiée par le fournisseur de service qui utilise le FI.

L'ensemble sera précisé en mission 1.

4 Quelles sont les étapes pour devenir Fournisseur de Services

- Faire une demande d'enrôlement de Fournisseur de Services.
- Intégration en reproduction :
Une fois le fournisseur de services enrôlé la SDN transmet un ClientID et un Client Secret ainsi que la documentation technique permettant de commencer la phase de développement et de tests.
- Implémentation
- Tokens de production :
Une fois le fournisseur de services enrôlé la SDN transmet un ClientID et un Client Secret

5 Description des attributs

Attributs disponibles en retour de l'authentification :

Nom Attribut	Utilisation			Valeurs possibles
given_name	les prénoms séparés par des espaces (standard OpenIDConnect)	oui	UTF-8	1 ^{er} prénom
usual_name	Nom de famille d'usage	oui	UTF-8	= sn selon la configuration CrousAD Nom usuel ou par défaut le nom de naissance
email	l'adresse courriel (standard OpenIDConnect)	oui	UTF-8	Adresse mail
UID	Identifiant unique auprès du FI	oui	String	= eppn + nom de domaine du crous (à construire) = UPN
display_name	Nom complet avec accents	oui	UTF-8	Nom usuel + + prénom (selon les règles CrousAD) CN
matricule Claim custom	matricule	oui	string	Matricule de Pléiades ou matricule généré au besoin (employeeNumber selon la configuration CrousAD)
nickname	identifiant	oui	string	SamAccountName selon la configuration CrousAD
adressLocality	Valeur par défaut 0	non	string	Valeur par défaut 0 (selon la configuration CrousAD)
chorusdt	Entité ministérielle/Matricule agent	non	string	string Chorusdt :matricule ; chorusdt :société Compagny/employeeNumber
Organizational_unit	Ministère/Direction/Service d'affectation	non	UTF8	businessCategory dans CrousAD

Belonging_population	Population d'appartenance	non	String	Agent, prestataire, partenaire, stagiaire EmployeeType dans crousAD : employee par défaut		
phone	Téléphone de contact	non		Format non normé Telephonenumber ou mobile dans la CrousAD		
Crous Claim custom	Cours de rattachement de l'agent	oui	string	Code		
				CNOUS001	Cnous	
				CROUS013	CROUS AIX-MARSEILLE-AVIGNON	
				CROUS080	CROUS AMIENS - PICARDIE	
				CROUS 971	CROUS ANTILLES-GUYANE	
				CROUS 971	Crous des Antilles et de la Guyane	
				CROUS 015	CROUS BOURGOGNE FRANCHE-COMTÉ	
				CROUS 033	CROUS BORDEAUX - AQUITAINE	
				CAL	NOUVELLE CALEDONIE	
				CROUS 063	CROUS CLERMONT - AUVERGNE	
				CROUS 020	CROUS CORSE	
				CROUS 094	CROUS CRÉTEIL	
				CROUS 038	CROUS GRENOBLE - ALPES	
				CROUS 059	CROUS LILLE - NORD-PAS-DE-CALAIS	
				CROUS 087	CROUS LIMOGES	
				CROUS 069	CROUS LYON	
				CROUS 034	CROUS MONTPELLIER - OCCITANIE	
				CROUS 044	CROUS NANTES - PAYS DE LA LOIRE	
				CROUS 054	CROUS LORRAINE	
				CROUS 006	CROUS NICE - TOULON	
				CROUS 090	CROUS NORMANDIE	
				CROUS 045	CROUS ORLÉANS - TOURS	
				CROUS 075	CROUS PARIS	
				CROUS 086	CROUS POITIERS	
				POL	POLYNESIE	
				CROUS 051	CROUS REIMS	
				CROUS 035	CROUS RENNES - BRETAGNE	
				CROUS 974	CROUS LA RÉUNION ET MAYOTTE : LA RÉUNION	
				CROUS 067	CROUS STRASBOURG	
				CROUS 031	CROUS TOULOUSE - OCCITANIE	
				CROUS 078	CROUS VERSAILLES	
SIRET	Identifiant d'établissement	non	String 9 chiffres sans espaces	01	Crous	18004401800026
				05	Crous de Bordeaux - Aquitaine	18330008600091
				06	Crous de Nice - Toulon	18060004100289
				13	Crous d'Aix - Marseille - Avignon	18130008800661
				15	Crous de Bourgogne-Franche-Comté	13002443300018

				20	Crous de Corse	18202010700013
				31	Crous de Toulouse - Occitanie	18310007200259
				34	Crous de Montpellier - Occitanie	18340008400012
				35	Crous de Rennes - Bretagne	18350003200010
				38	Crous de Grenoble - Alpes	18380156200723
				44	Crous de Nantes - Pays de la Loire	18440132100015
				45	Crous d'Orléans - Tours	18450021300014
				51	Crous de Reims	18510200100327
				54	Crous de Lorraine	18542210200011
				59	Crous de Lille - Nord-Pas-de-Calais	18591150000014
				63	Crous de Clermont - Auvergne	18630697300014
				67	Crous de Strasbourg	18670644600017
				69	Crous de Lyon	18690156700013
				75	Crous de Paris	18750006100010
				78	Crous de Versailles	18780008100486
				80	Crous d'Amiens - Picardie	18800200000134
				86	Crous de Poitiers	18860005000143
				87	Crous de Limoges	18871900900014
				90	Crous de Normandie	13002442500014
				94	Crous de Créteil	18940004700016
				971	Crous des Antilles et de la Guyane	18971002300012
				974	Crous de La Réunion et de Mayotte	18974001200019
SIREN	Identifiant d'entreprise	non	String, 14 chiffres sans espaces	01	Crous	180044018
				05	Crous de Bordeaux - Aquitaine	183300086
				6	Crous de Nice - Toulon	180600041
				13	Crous d'Aix - Marseille - Avignon	181300088
				15	Crous de Bourgogne-Franche-Comté	130024433
				20	Crous de Corse	182020107
				31	Crous de Toulouse - Occitanie	183100072
				34	Crous de Montpellier - Occitanie	183400084
				35	Crous de Rennes - Bretagne	183500032
				38	Crous de Grenoble - Alpes	183801562
				44	Crous de Nantes - Pays de la Loire	184401321
				45	Crous d'Orléans - Tours	184500213
				51	Crous de Reims	185102001
				54	Crous de Lorraine	185422102
				59	Crous de Lille - Nord-Pas-de-Calais	185911500
				63	Crous de Clermont - Auvergne	186306973
				67	Crous de Strasbourg	186706446
				69	Crous de Lyon	186901567

				75	Crous de Paris	187500061
				78	Crous de Versailles	187800081
				80	Crous d'Amiens - Picardie	188002000
				86	Crous de Poitiers	188600050
				87	Crous de Limoges	188719009
				90	Crous de Normandie	130024425
				94	Crous de Créteil	189400047
				971	Crous des Antilles et de la Guyane	189710023
				974	Crous de La Réunion et de Mayotte	189740012

6 Méthodes d'authentification OIDC

6.1 Principe de fonctionnement

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

Le fournisseur d'identité reçoit cette demande et en atteste l'origine.

L'utilisateur s'authentifie.

Le fournisseur d'identité atteste l'origine et renvoie les informations utilisateurs :

given_name, usual_name, email, display_name, matricule, crous et l

L'application récupère les champs d'en-têtes http pour en faire une session locale à l'utilisateur.

Exemple d'entête récupérée par `apache_request_headers()`

A venir

Pour pouvoir être éligible à CrousConnect, il faut respecter certaines règles :

Contenu des « ID-Tokens » limité aux claims suivants :

Sub :

aud : client_id du fournisseur de données qui a effectué la demande, cela correspond généralement à l'ID client de votre application.

iss : entityID, (indique la plateforme émettrice (<https://sso.lescrous.fr/auth>) du jeton d'accès

auth_time : L'heure à laquelle l'utilisateur s'est authentifié

iat : L'heure à laquelle l'ID token a été émis

exp : L'heure à laquelle l'ID token expire (au format UNIX timestamp)

exp : auth_time + 15 minutes,

nonce : une valeur aléatoire incluse dans la demande d'authentification pour éviter les attaques de replay

jti : qui identifie de manière unique le token. Il est utilisé pour éviter les attaques de replay, car chaque token doit avoir un JTI différent.

given_name : given_name

usual-name : sn

email : mail

display_name : display-name

chorsdt : matricule

matricule : employeeNumber

crous : code crous : à construire si pas dans l'annuaire

l : 0 par défaut sinon 1

=> attention au paramètre « op.authz.feedSubjectSessionClaimsIntoIDToken=true »

- Durée de vie des « Access-Tokens » : 15 minutes (access token : jeton qui permet de valider l'accès à une ressource. La durée de validité de ce jeton est limitée et généralement de l'ordre de quelques minutes;

- Durée de vie des « ID-Tokens » : entre 16 et 20 minutes maxi

- Durée de vie des « Refresh-Tokens » : 4 heures, avec stockage encrypté sur IDP + transit via TLS (*efresh token* : jeton qui permet de renouveler l'autorisation sans la demander à nouveau au propriétaire de la ressource. Il permet de récupérer un nouvel *access token*. La durée de validité de ce jeton est généralement de plusieurs jours voir de plusieurs mois. Ce jeton doit être stocké de manière sécurisé par le client)

- Type de tokens utilisés pour transporter des éléments d'identification de type JWT

- Les réponses sont apportées sous forme d'objet JSON, exemple avec une requête « UserInfo » :

Toutes les informations concernant le protocole OpenID Connect sont sur :

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

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

https://github.com/france-connect/Documentation-AgentConnect/blob/main/doc_fs.md

[Documentation-AgentConnect/README.md at main · france-connect/Documentation-AgentConnect · GitHub](#)

[Documentation-AgentConnect/doc_fs/technique fca/technique fca oidc.md at main · france-connect/Documentation-AgentConnect · GitHub](#)

6.2 Configuration

Les configurations nécessaires pour une connexion pour le fournisseur de services:

Endpoint OIDC	Url de préproduction (*)
---------------	--------------------------

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

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

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

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

Information à fournir à xxx par les partenaires :

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

6.2.1 Connexion

Initialisation de l'authentification :

Endpoint OIDC	Authorization
Méthode	GET
Réponse	TokenID

Paramètres de requête	Valeurs admises
client_id	client_id fourni
scope	'openid profile email'
response_type	'code'
approval_prompt	'auto'
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

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

```
https://xxx /auth/oauth2/auth?
nonce=c12ce09dd61179ef9cb85905681797d5e7c0d2065ac9
&scope=openid%20profile%20email
&state=abcc2f5d56a951cd9e4c5ae5ad4b6539
&response_type=code
&approval_prompt=auto
&redirect_uri=https%3A%2F%2F%2Fenvole%2Foauth2%2Fcallback
&client_id=xxxx
```

6.2.2 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.)

****Exemple de requête de déconnexion en PREPROD****

https://xxx/auth/oauth2/sessions/logout?

id_token_hint=eyJhbGciOiJSUzI1NiIsImtpZCI6InB1YmxpYzpoeWRyYS5vc[...]

&post_logout_redirect_uri=https%3A%2F%2Fpp.messervices.etudiant.gouv.fr%2Fenvole%2Flogout-success

6.3 Intégration du fournisseur d'identité

L'intégration du fournisseur d'identité est réalisée sous le contrôle de la sous-direction du numérique du Cnous (SDN).

Le fournisseur d'identité a accès à la plateforme de pré production pour réaliser les tests.

Quand le fournisseur de service a fini son intégration du fournisseur d'identité, une phase de qualification conjoint avec la SDN peut commencer.

La mise en production est réalisée après prononcé de la vérification de service régulier par la SDN.