Mon projet

Documentation

Fournisseur de service Particulier

Démo

FOURNISSEUR DE SERVICE

DOCUMENTATION

Docs

EXEMPLES DE CODE

Références

FranceConnect v1 sera décommissionné en septembre 2025.
Nous vous accompagnons dans la migration sur FranceConnect v2 avec la documentation partenaire.

FAQ

Concepts de base

Le protocole OpenID Connect

Connexion S'incrire

INTRODUCTION

Le protocole OpenID Connect est au cœur du fonctionnement de FC. C'est une surcouche d'identification au protocole OAuth 2.0. Il permet à des Clients (ici, les FS) d'accéder à l'identité des Utilisateurs finaux (les internautes) par l'intermédiaire d'un serveur d'autorisation (ici, les FIs).

Mon projet Démo Docs Références FAQ

Les FS doivent donc être des clients OpenID Connect (aussi appelés relying parties), et les FIs doivent être des fournisseurs OpenID Connect (aussi appelés providers).

La spécification du protocole se trouve sur http://openid.net/connect/.

- Connexion

Pour une référence d'implémentation OpenID Connect voici le lien : http://openid.net/specs/openid-connect-core-1_0.html

S'inscrire

LES FLUX STANDARDS

Le protocole OpenID Connect définit **3 appels REST** faits par le client, et **4 endpoints** (un du côté client, et trois du côté provider).

En amont, le client s'inscrit (en général manuellement) auprès du provider. Il lui fournit une URL de callback (l'URL du client vers lequel l'internaute est redirigé une fois authentifié), aussi appelée "callback endpoint". En retour le provider donne au client un client ID et un client secret.

Lorsque l'internaute clique sur le bouton d'authentification du client, le flux est le suivant :

- Le client fait une redirection vers le "authorization endpoint" du provider avec son client id et son url de callback. Le provider redirige alors l'internaute vers sa mire d'authentification. Si l'internaute se loggue correctement, le provider renvoie un code d'autorisation au client.
- Le client fait un appel Web service vers le "token endpoint" du provider avec le code d'autorisation reçu, et authentifie cette requête avec son client id et son client secret. Le provider retourne un access token (une chaîne de caractères encodée en base64) et un id token (sous la forme d'un Json Web Token).
- Le client fait un appel Web service vers le "userInfo endpoint" du provider avec l'access token reçu, et le provider renvoie les informations de l'internaute au client.

DANS LE CADRE DE FRANCECONNECT

Les flux FranceConnect implémentent les flux standards d'OpenID Connect. Les fournisseurs de service doivent être clients OpenID Connect, et les fournisseurs d'identité doivent être fournisseurs OpenID Connect. FranceConnect est une brique intermédiaire qui est à la fois fournisseur (du point de vue des FS) et client (du point de vue des FI).

Les données usagers

Les données usagers sont fournies par les Fournisseurs d'Identité aux Fournisseurs de Service, via FranceConnect Particuliers, conformément à l'habilitation obtenue.

FranceConnect transmet systématiquement au Fournisseur de Service un identifiant unique pour chaque utilisateur.

L'identité pivot permet d'identifier un utilisateur particulier.

- Nom de naissance
- Prénoms
- Sexe
- Date de naissance
- Code géographique INSEE de la ville de naissance
- Code géographique INSEE du pays de naissance

En complément, il est possible d'obtenir le nom d'usage. Cependant cette donnée n'est pas obligatoirement connue dans tous les Fournisseurs d'Identité.

Vous pouvez avoir accès également à l'adresse email. Cette donnée de contact qui peut différer selon le Fournisseur d'Identité choisi par l'usager.

Je veux identifier/authentifier des utilisateurs via FC

Ci-dessous une clé d'intégration à usage public afin de vous permettre de découvrir l'application et de commencer vos tests sans attendre la validation de votre dossier.

Cette clé est à usage limité et ne bénéficie d'aucun support par notre équipe.
La clé (client id, client secret) proposée en accès libre et configurée avec des URLs de callback en localhost ne peut être utilisée que sur la plateforme Franceconnect appelée plateforme d'intégration : https://fsp1-legacy.integ01.fcp.fournisseur-de-service.fr/.

- CLIENT ID : '211286433e39cce01db448d80181bdfd005554b19cd51b3fe7943f6b3b86ab6e'
- CLIENT SECRET : '2791a731e6a59f56b6b4dd0d08c9b1f593b5f3658b9fd731cb24248e2669af4b'

LES URLS DE CALLBACK DE CONNEXION CONFIGURÉES SONT LES SUIVANTES :

- http://localhost:4242/callback
- http://localhost:8080/callback
- http://localhost:1337/callback
- http://localhost:3000/callback
- http://localhost:1337/login-callback
- http://localhost:4242/login-callback
- http://localhost:8080/login-callback
- http://localhost:3000/login-callback
- http://localhost:1337/data-callback
- http://localhost:4242/data-callback
- http://localhost:8080/data-callback
- http://localhost:3000/data-callback

LES URLS DE CALLBACK DE DÉCONNEXION CONFIGURÉES SONT LES SUIVANTES :

- http://localhost:4242/logout
- http://localhost:8080/logout
- http://localhost:1337/logout
- http://localhost:3000/logout
- http://localhost:4242/logout-callback
- http://localhost:8080/logout-callback
- http://localhost:1337/logout-callback
- http://localhost:3000/logout-callback

Le code est disponible à l'adresse https://github.com/france-connect/service-provider-example.

Afin d'implémenter FranceConnect, il vous faut obtenir une habilitation pour votre démarche sur la plateforme : https://franceconnect.gouv.fr/partenaires.
Une fois votre cas d'usage validé, vous recevrez une invitation pour accéder au Portail Partenaire et commencer vos tests d'intégration.

Sur notre environnement d'intégration, vous pouvez utiliser le fournisseur d'identité "Démonstration" dont les données sont modifiables ici : https://github.com/france-connect/identity-provider-example/blob/master/database.csv

Vous pouvez proposer de nouvelles identités de tests directement sur ce fichier.

Nos Endpoints

INTÉGRATION

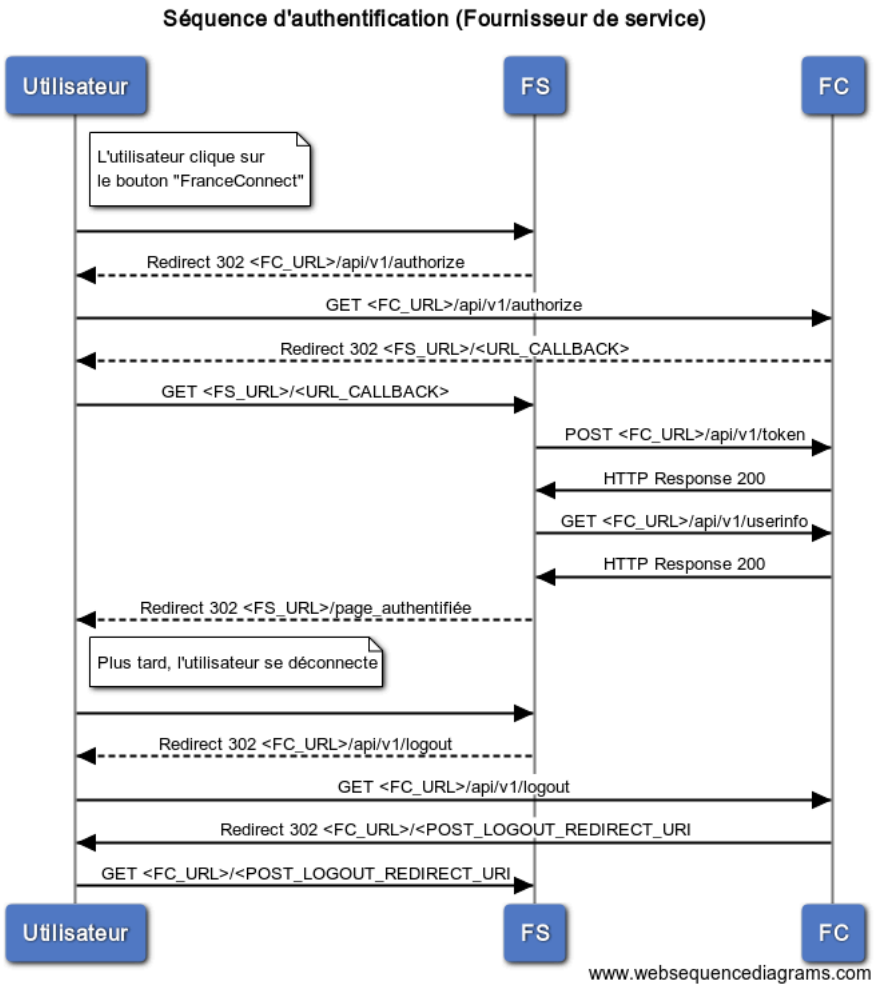
En environnement d'intégration de FranceConnect , les endpoints sont disponibles en HTTPS.

Authorization	https://fcp.integ01.dev-franceconnect.fr/api/v1/authorize
Token	https://fcp.integ01.dev-franceconnect.fr/api/v1/token
UserInfo	https://fcp.integ01.dev-franceconnect.fr/api/v1/userinfo
Logout	https://fcp.integ01.dev-franceconnect.fr/api/v1/logout

PRODUCTION

Authorization	https://app.franceconnect.gouv.fr/api/v1/authorize
Token	https://app.franceconnect.gouv.fr/api/v1/token
UserInfo	https://app.franceconnect.gouv.fr/api/v1/userinfo
Logout	https://app.franceconnect.gouv.fr/api/v1/logout

Détail du fonctionnement



La récupération de l'identité pivot doit être faite dans la suite immédiate des appels précédents (authentification et récupération du code). Le fait d'appeler ce Web service plus tard n'est aujourd'hui pas proposé.

Détail des flux

<FC_URL>/api/v1/authorize [Redirection]

DESCRIPTION

Contexte : Le FS redirige depuis la requête précédente vers /api/v1/authorize pour engager la cinématique d'authentification.
Origine : FS
Cible : FC
Type d'appel : redirection navigateur

Note : il est possible d'ajouter des paramètres supplémentaires via la redirect_uri, à passer après ? sous la forme clé=valeur. Ils seront renvoyés tels quels lors du retour vers le FS. Ces paramètres ne peuvent être dynamiques et doivent respecter l'ordre dans lequel ils ont été définis. (cf. RFC6749 section 3.1.2 et RFC3986 section 4.3)
Exemple :
si vous redirigez vers l'URL https://fcp.integ01.dev-franceconnect.fr/api/v1/authorize?response_type=[...]&client_id=[...]&redirect_uri=https%3A%2F%2Ffs.fr%2Foidc_callback**%3Ftestkey%3Dtestvalue**&state=[...]&nonce=[...]&scope=[...]
alors FC redirigera vers le FS à l'URL https://fs.fr/oidc_callback**?testkey=testvalue**&[...]
Cela permet de conserver un état quand le site de départ et le site d'arrivée ne partagent pas leurs sessions Web.

REQUETE

URL:

```
<FC_URL>/api/v1/authorize?response_type=code&client_id=<CLIENT_ID>&redirect_uri=<FS_URL>%2F<URL_CALLBACK>&scope=<SCOPES>&state=><STATE>&nonce=<NONCE>
```

Méthode : GET

REPONSE

/

<FS_URL>/<URL_CALLBACK> [Redirection]

DESCRIPTION

Contexte : L'internaute s'est identifié sur le FI, FranceConnect redirige vers le callback du FS, avec un Authorization code dans l'URL.
Origine : FC
Cible : FS
Type d'appel : redirection navigateur

REQUETE

URL:

```
<FS_URL>/<URL_CALLBACK>?code=<AUTHZ_CODE>&state=<STATE>
```

Méthode : GET

<FC_URL>/api/v1/token [Web Service]

DESCRIPTION

Contexte : Le FS a récupéré un authorization code. Il veut maintenant récupérer un access token et un id token.
Origine : FS
Cible : FC
Type d'appel : appel de Web service

REQUETE

URL:

```
<FC_URL>/api/v1/token
```

Méthode : POST
Corps HTTP :

- 'grant_type': 'authorization_code',
- 'redirect_uri': '**<FS_URL>**/<URL_CALLBACK>',
- 'client_id': '**<CLIENT_ID>**',
- 'client_secret': '**<CLIENT_SECRET>**',
- 'code': '**<AUTHZ_CODE>**'

REPONSE

Corps HTTP:

```
{
  'access_token': <ACCESS_TOKEN>,
  'token_type': 'Bearer',
  'expires_in': 60,
  'id_token': <ID_TOKEN>
}
```

<FC_URL>/api/v1/userinfo [Web Service]

DESCRIPTION

Contexte : Le FS a récupéré un access token. Il veut maintenant récupérer les USER INFO.
Origine : FS
Cible : FC
Type d'appel : appel de Web service

REQUETE

URL:

```
<FC_URL>/api/v1/userinfo?schema=openid
```

Méthode : GET
Entêtes HTTP : Authorization = 'Bearer **<ACCESS_TOKEN>**'

REPONSE

Corps HTTP:

```
<USER_INFO>
```

Données usager

LISTE DES SCOPES DISPONIBLES LORS DE L'ÉTAPE D'AUTHENTIFICATION FRANCECONNECT

FranceConnect a étendu le mécanisme de scopes pour qu'il soit plus modulaire.

- Un seul scope est obligatoire : *openid*. Il permet de récupérer le sub (identifiant unique technique) de l'utilisateur.
- Il est possible de récupérer individuellement chaque propriété de l'identité pivot en utilisant leurs scopes dédiés
- Il est possible de combiner plusieurs scopes de son choix pour récupérer seulement les informations dont a besoin le FS

Champs	Type	Description	Pattern
openid	string	identifiant technique (sub) de l'utilisateur au format OpenIDConnect(standard OpenIDConnect)	n'excède pas 255 caractères ASCII
given_name	string	les prénoms séparés par des espaces (standard OpenIDConnect)	[A-Za-zÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸàâäçéèêëîïôöùûüÿÆŒæœ -'] - [Details]
family_name	string	le nom de naissance (standard OpenIDConnect)	[A-ZÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸÆŒ \-'] - [Details]
birthdate	string	la date de naissance (standard OpenIDConnect)	• [YYYY-01-01] - (\d{4})-01-01 - (Présumé mois) • [YYYY-MM-01] - (\d{4})-(\d{2})-01 - (Présumé jours) • [YYYY-MM-DD] - (\d{4})-(\d{2})-(\d{2}) [Details]
idp_birthdate	string	la date de naissance telle que fournie par le fournisseur d'identité (sans tranformation)	• [YYYY-00-00] - (\d{4}) - (Présumé mois) • [YYYY-MM-00] - (\d{4})-(\d{2}) - (Présumé jours) • [YYYY-MM-DD] - (\d{4})-(\d{2})-(\d{2}) [Details]
gender	string	"male" ou "female" (standard OpenIDConnect)	• female: pour genre féminin • male: pour genre masculin

birthplace	string	le code INSEE du lieu de naissance	• Si né en France (Taille de 5)
			  • [(([0-8][0-9AB])|(9[0-8AB]))[0-9]{3}] - [Details] - [Liste]
			• En cas de pays étranger
			  • En cas de pays étranger : Champs vide

birthcountry	string	le code INSEE du pays de naissance	• Pour les pays étrangers (Taille de 5)
			  • [99[0-9]{3}] - [Details]
			• Pour la France
			  • 99100

email	string	l'adresse courriel (standard OpenIDConnect)	RFC 5322 - [Details]
preferred_username	string	le nom d'usage (standard OpenIDConnect)	[A-ZÀÂÄÇÉÈÊËÎÏÔÖÙÛÜŸÆŒ \-'] - [Details]

Les "alias"

- **profile** : Regroupe les scopes **given_name**, **family_name**, **birthdate** et **gender**. Si disponible, renvoie aussi **preferred_username**
- **birth** : Regroupe les scopes **birthplace** et **birthcountry**. Permet de récupérer la ville et le département de naissance de la personne.
- **identite_pivot** : Regroupe les scopes **profile** et **birth**. Permet de récupérer l'identité pivot complète plus le nom d'usage si disponible.

Cette liste de scopes est définie par la norme OpenIDConnect : http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims

Recommandation

Afin de garantir un fonctionnement nominal pour la gestion des utilisateurs, il est fortement préconisé aux fournisseurs de service d'adopter la cinématique suivante :

- **1er accès de l'utilisateur au FS :** le traitement du FS collecte les données identité pivot et l'identifiant technique SUB
- **Pour les accès suivants de l'utilisateur à ce même FS :** le traitement du FS identifie l'utilisateur en s'appuyant uniquement sur le SUB et non sur les données d'identité pivot

Intégration d'un bouton FranceConnect

Les boutons d'action FranceConnect sont primordiaux dans l'usage du service. Il est obligatoire d'utiliser l'un des boutons proposé et aucun autre visuel pour la connexion des usagers.

Pour les boutons en svg, lors de l'utilisation d'une image veuillez preciser la taille du bouton.

Téléchargements :

- Pack boutons

Utiliser les niveaux eIDAS en tant que FS

EIDAS est un nouveau standard européen visant à normaliser et à améliorer la sécurité de l'identification sur Internet. Il propose notamment 3 niveaux de garantie sur les moyens utilisés pour l'identification. Vous pouvez, en tant que FS, **utiliser les niveaux eIDAS pour que FC filtre les FIs réputés compatibles** avec un niveau eIDAS précis.

Comme la norme ne prévoit pas aujourd'hui de mesures techniques particulières pour préciser le niveau souhaité, **FranceConnect utilise le claim optionnel "acr"** (http://openid.net/specs/openid-connect-basic-1_0.html#RequestParameters) de la norme OpenID Connect. Pour le FS, cela veut dire remplir le claim optionnel *acr_values* lors de la demande d'authentification (appel à l'endpoint /api/v1/authorize).

Au sujet du claim acr_values, on notera que c'est, selon la norme, un "*voluntary claim*" qui théoriquement traduit une préférence et non une exigence. Le fait de fournir ce claim va faire filtrer à FranceConnect les FIs réputés répondre à la demande qui est faite et le FI renverra, par le biais de FranceConnect le niveau eIDAS avec lequel l'authentification a eu lieu. Le FS pourra donc vérifier le niveau eIDAS utilisé.

Exemple d'appel précisant un niveau eIDAS minimum :

```
https://fcp.integ01.dev-franceconnect.fr/api/v1/authorize?response_type=code&client_id=123456&redirect_uri=https%3A%2F%2Ffournisseur-de-service.dev-franceconnect.fr%2Flogin-callback&scope=openid%20profile%20email%20address%20phone%20preferred_username%20email%20address%20phone%20preferred_username&acr_values=eidas1&state=
```

Afin d'y arriver, il faut spécifier une ou plusieurs valeurs parmi les suivantes :

- eidas1 : niveau standard (exemple : authentification par identifiant / mot de passe)
- eidas2 : niveau substantiel (exemple : second facteur. Homologué eIDAS)
- eidas3 : niveau fort (exemple : utilisation de certificats, lecteurs de cartes, ... Homologué eIDAS)

Si le **claim** *acr* n'est **pas précisé**, le niveau par défaut est fixé à eidas3, le plus sécurisé.
Si le **claim est précisé**, FranceConnect ne proposera à l'utilisateur que les fournisseurs d'identité de niveau supérieur ou égal. Sinon, FranceConnect ne proposera à l'utilisateur que les Fournisseurs d'Identité de niveau élevé.
Si plusieurs niveaux sont précisés, FranceConnect considère que le **claim n'est pas valide**.
Si le claim est considéré par FranceConnect comme n'étant pas valide, le niveau par défaut est utilisé.

Le **niveau eIDAS utilisé pour l'authentification est retourné par le fournisseur d'identité** (cf la documentation du FI), par le biais de FranceConnect (qui le transmet sans le modifier) et du **claim *acr* dans l'ID Token** retourné au Fournisseur de Service.
Il est de la responsabilité du Fournisseur de service de s'assurer que le niveau retourné est au moins égal ou supérieur à celui demandé (si eidas2 est demandé, eidas3 doit être accepté tout comme eidas2, mais pas eidas1).

Je veux déconnecter l'utilisateur de FranceConnect

FranceConnect implémente la section sur la déconnexion en cours de spécification dans la norme OpenID Connect :http://openid.net/specs/openid-connect-session-1_0.html#RPLogout

FranceConnect ne gère pas la déconnexion de l'usager au service FranceConnect à la fermeture du navigateur.

Le FS doit pouvoir déconnecter l'utilisateur de sa session FranceConnect. La cinématique globale est celle-ci :

- L' utilisateur clique sur un lien de déconnexion présenté par le FS.
- Le FS doit **déconnecter** l'utilisateur de son application et de sa session FranceConnect.
- L' utilisateur est redirigé vers la page de retour spécifiée par le FS.

Le FS doit préciser l'URL où l'on doit rediriger l'utilisateur une fois qu'il a choisi de se déconnecter ou non de FranceConnect via le paramètre ***post_logout_redirect_uri***, ainsi que passer l'id_token récupéré lors de l'authentification de l'utilisateur via le paramètre **id_token_hint**.

Il est obligatoire de renseigner les différentes urls de redirections de déconnexion dans les paramètres client

<FC_URL>/api/v1/logout [Redirection]

REQUETE

URL:

```
<FC_URL>/api/v1/logout?id_token_hint=<ID_TOKEN_HINT>&state=<STATE>&post_logout_redirect_uri=<POST_LOGOUT_REDIRECT_URI>
```

Méthode : GET

Je veux récupérer des ressources auprès d'un FD qui utilise FranceConnect

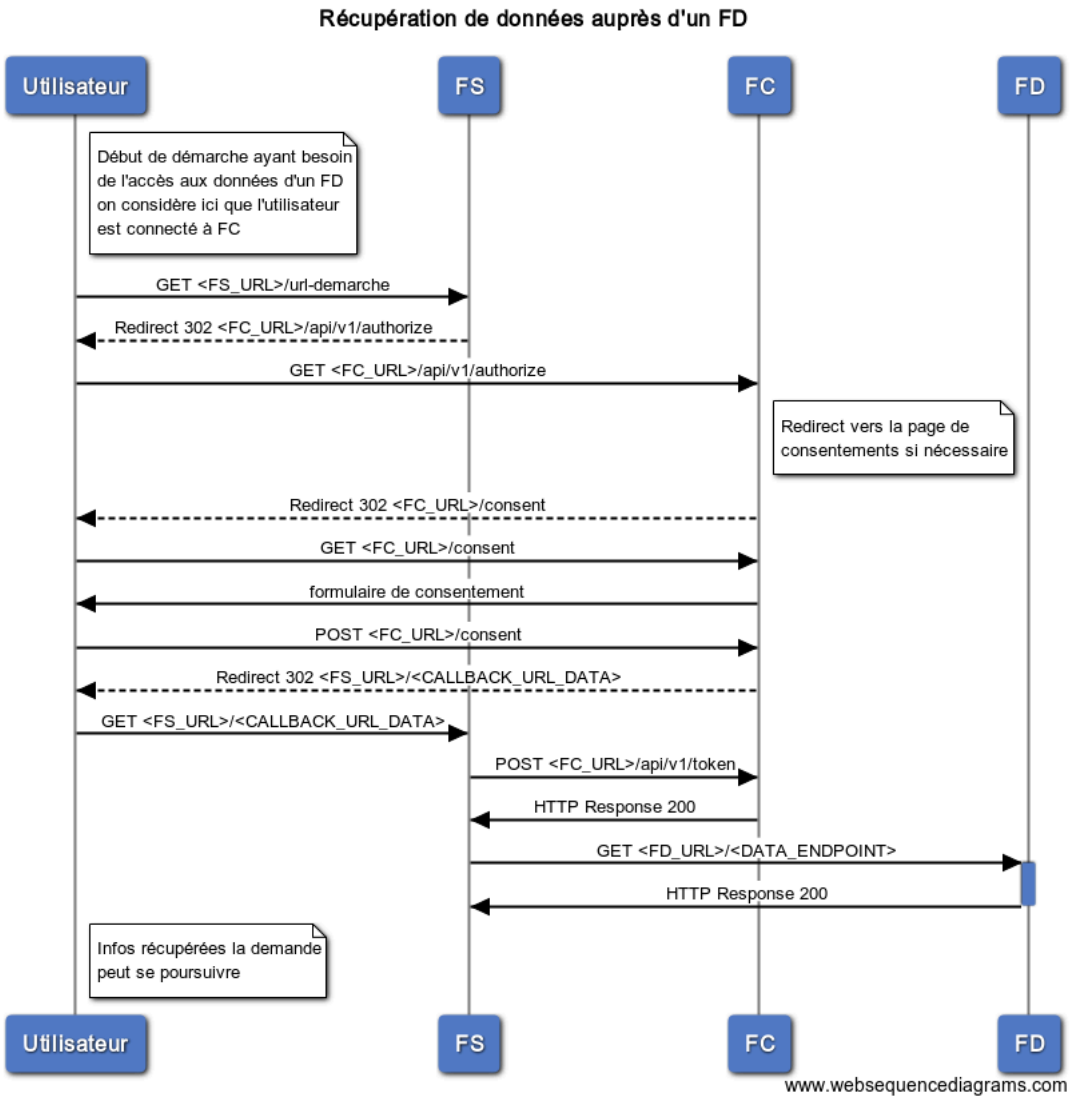
Un fournisseur de service de démo est mis à votre disposition sur https://fournisseur-de-service.dev-franceconnect.fr

Celui propose également d'appeler un fournisseur de données "FranceConnecté", simulant actuellement un échange de données avec la DGFIP.

Tous les liens importants (documentation, code source, etc) sont dans le footer du site d'exemple.

Authorization	https://app.franceconnect.gouv.fr/api/v1/authorize
Token	https://app.franceconnect.gouv.fr/api/v1/token

Détail du fonctionnement



Vous devez pouvoir à la fois communiquer avec FranceConnect et avec le FD de votre choix. Il faut donc veiller à ce que les flux entre les machines ne soient pas bloqués (pour FC, les ports 80 et 443).

Détail des flux

<FS_URL>/<url-demarche> [Redirection]

DESCRIPTION

Contexte : L'internaute accède à la page lui permettant d'effectuer une démarche en ligne via FranceConnect.
Origine : FS
Cible : FS
Type d'appel : Redirection navigateur

REQUETE

URL :

```
<FS_URL>/<url-demarche>
```

Méthode : GET

REPONSE

/

<FC_URL>/api/v1/authorize [Redirection]

DESCRIPTION

Contexte : L'internaute a besoin d'accéder à une ressource mise à disposition par un FD. Il commence donc par demander un jeton à FC. FS doit le rediriger vers le /api/v1/authorize de FC.
Origine : FS
Cible : FC
Type d'appel : Redirection navigateur

REQUETE

URL :

```
<FC_URL>/api/v1/authorize?response_type=code&client_id=<CLIENT_ID>&redirect_uri=<FS_URL>%2F<CALLBACK_URL_DATA>&scope=<SCOPES>&state=<STATE>&nonce=
<NONCE>
```

Méthode : GET

REPONSE

/

<FC_URL>/consent (GET) [Redirection]

DESCRIPTION

Contexte : Le FS a fait la requête d'autorisation, mais l'utilisateur n'a pas encore donné son consentement. FC redirige vers sa page de consentement.
Origine : FC
Cible : FC
Type d'appel : Redirection navigateur

REQUETE

URL :

```
<FC_URL>/consent?
return_url=%2Fuser%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D<CLIENT_ID>%26scope%3D<SCOPES>%26redirect_uri%3D<CALLBACK_URL_DATA>
```

Méthode : GET

REPONSE

Page HTML, formulaire de consentement

<FC_URL>/consent (POST) [Redirection]

DESCRIPTION

Contexte : L'utilisateur donne son consentement à la transmission de ses données sur la page de consentement, en cliquant sur le bouton "Accepter". FC soumet le formulaire puis redirige vers le CALLBACK_URL_DATA du FS.
Origine : FC
Cible : FC
Type d'appel : Redirection navigateur

REQUETE

URL :

```
<FC_URL>/consent?
return_url=%2Fuser%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D<CLIENT_ID>%26scope%3D<SCOPES>%26redirect_uri%3D<CALLBACK_URL_DATA>
```

Méthode : POST

REPONSE

HTTP 302 - Redirection vers <FS_URL>?code=xxx

<FS_URL>/<CALLBACK_URL_DATA> [Redirection]

DESCRIPTION

Contexte : L'utilisateur a accepté la transmission de ses données sur la page de consentement, FC appelle le callback du FS avec un code d'autorisation dans l'URL.
Origine : FC
Cible : FS
Type d'appel : redirection navigateur

REQUETE

URL :

```
<CALLBACK_URL_DATA>?code=<AUTHZ_CODE>"&state=<STATE>
```

Méthode : GET

REPONSE

/

<FC_URL>/api/v1/token [Web Service]

DESCRIPTION

Contexte : Le FS a reçu le code d'autorisation. Il doit maintenant demander un access token à FC.
Origine : FS
Cible : FC
Type d'appel : appel de web service

REQUETE

URL :

```
<FC_URL>/api/v1/token
```

Méthode : POST Corps HTTP :

- 'grant_type': 'authorization_code',
- 'redirect_uri': '**<FS_URL>**/<CALLBACK_URL_DATA>',
- 'client_id': '**<CLIENT_ID>**',
- 'client_secret': '**<CLIENT_SECRET>**',
- 'code': '**<AUTHZ_CODE>**'

REPONSE

Corps HTTP:

```
{
  'access_token': <ACCESS_TOKEN>,
  'token_type': 'Bearer',
  'expires_in': 60,
  'id_token': <ID_TOKEN>
}
```

<FD_URL>/<DATA_ENDPOINT> [Web Service]

DESCRIPTION

Contexte : Le FS interroge le FD selon les conventions définies avec lui (headers, query http ...).
Origine : FS
Cible : FD
Type d'appel : appel de web service

REQUETE

URL :

```
<FD_URL>/<DATA_ENDPOINT>
```

Méthode : <dépend du FD>. Cependant, il faut lui passer dans cet appel l'**access token** reçu dans la requête précédente. La transmission du token JWT 'access_token' **DOIT** se faire dans le header **Authorization : Bearer <Token>**.

REPONSE

Corps HTTP:

les données demandées (dépend du formatage des données par le FD)

Gestion d'erreurs entre FranceConnect et le FS

En tant qu'OpenID Connect provider, FranceConnect peut renvoyer toutes sortes d'erreurs à une application cliente. Pour se faire, FranceConnect passe par le mécanisme de retour d'erreurs d'un fournisseur d'identité openid connect tel que décrit dans la norme (http://openid.net/specs/openid-connect-core-1_0.html#AuthError, en particulier les sections 3.1.2.6 (authentification), 3.1.3.4 (jeton d'accès), 5.3.3 (service d'informations utilisateur))

Système de codes d'erreurs "Usagers" FranceConnect

Afin de rendre plus simple la détection et la gestion de bugs, FranceConnect possède un système de codes d'erreurs.

Core

Code	Description
E000000	Cette erreur n'est déclenchée qu'en dernier recours, elle correspond à une exception mal ou non gérée. Il est impératif de remonter cette erreur aux développeurs car elle nécessite une investigation plus poussée dans le code.
E000001	Compte désactivé, connexion impossible via FranceConnect à moins de réactiver le compte.

Code	Description
E000009	Cette erreur intervient si le paramètre "redirect_uri" est présent et différent des valeurs autorisées en base de donnée. Ajouter l'url dans la liste des adresses de redirection.
E000035	Connexion désactivée par l'usager pour le fournisseur d'identité actuel.

RNIPP

Code	Description
E010000	Cette erreur n'est déclenchée qu'en dernier recours, elle correspond à une exception mal ou non gérée. Il est impératif de remonter cette erreur aux développeurs car elle nécessite une investigation plus poussée dans le code.
E010004	Demande non identifiée mais existence d'un seul écho. Un écho est le nombre d'occurences d'identité proches de celle recherchée mais pas similaires lors de la vérification auprès du RNIPP
E010006	Demande non identifiée mais existence de plus d'un écho.
E010007	Demande identifiée avec le nom d'usage uniquement.
E010008	Demande non identifiée sans écho.
E010009	Demande rejetée au contrôle en raison d'erreurs de syntaxe.
E010011	Ce code se déclenche principalement lorsque le RNIPP met trop de temps à répondre, voir ne répond pas du tout. L'IP avec lequel vous essayez de contacter le RNIPP n'est pas whitelisté par l'insee.
E010012	On a appelé le RNIPP mais celui-ci renvoie un mauvais format, qui n'est pas du XML (par ex. : à cause d'une opération de maintenance). Généralement c'est une page HTML qui est renvoyée avec le code HTTP correspondant (400, ..., 500, ...).
E010013	La réponse du RNIPP est un XML bien formaté mais il manque des informations dans l'identité renvoyée (ex. : il manque la ville pour les personnes nées à l'étranger).
E010014	Actuellement déclenchée quand le RNIPP redresse une personne mais que la date de naissance envoyée par le FI ainsi que celle renvoyée par le RNIPP diffèrent. Cette erreur concerne bien le RNIPP qui redresse une identité alors qu'il devrait probablement la bloquer par prudence. Peut nécessiter la correction de l'identité soit sur le FI, soit sur le RNIPP, voire sur les deux.
E010015	Ce code erreur correspond au RNIPP qui renvoie l'information "décédée" pour la personne dont l'identité est actuellement redressée.

Fournisseur d'Identité

Code	Description
E020000	Cette erreur n'est déclenchée qu'en dernier recours, elle correspond à une exception mal ou non gérée. Il est impératif de remonter cette erreur aux développeurs car elle nécessite une investigation plus poussée dans le code.
E020001	Cette erreur se déclenche sur un 404 du FI qui ne nous renvoie pas l'utilisateur car il le considère souvent incomplet ou non certifié. Très souvent il s'agit de la DGFIP.
E020002	Informations personnelles, fournies incomplètes, et ne permettent pas de certifier l'identité.
E020003	Cette erreur se déclenche si un des champs reçu du FI n'est pas au format attendu / contient des caractères non supportés.
E020004	Cette erreur se déclenche si le FI n'a pas envoyé d'e-mail pour l'usager qui se connecte. Dans le cadre de l'interopérabilité eIDAS, l'e-mail ne sera pas envoyé la majorité du temps car non obligatoire.
E020005	Cette erreur se déclenche si le champ "sub" n'est pas présent dans l'objet renvoyé par le FI.
E020006	Cette erreur se déclenche si il a été impossible d'enregistrer en base le "compte" de l'usager. Il est nécessaire de contacter le support et de voir avec les devs.
E020007	Cette erreur se déclenche quand le FI nous renvoie autre chose qu'un JSON valable. Il est impossible de parser la réponse et donc de la traiter. Vient très probablement d'une indisponibilité du FI.
E020008	Cette erreur se déclenche lorsqu'il y a un code 401 - refus d'autorisation, pour indisponibilité du FI.
E020009	Cette erreur se déclenche en cas de code 500 du FI, qui est indisponible.
E020010	Cette erreur se déclenche en cas de code 502 du FI, pour indisponibilité.
E020011	Cette erreur se déclenche en cas de code 503 du FI, pour maintenance ou des problèmes de capacité.
E020012	Cette erreur se déclenche si le FI fourni dans la requête un niveau eIDAS supérieur à celui déclaré.
E020017	Cette erreur se déclenche quand on appelle un fournisseur d'identité qui n'est pas activé.

Code	Description
E020018	Cette erreur se déclenche quand on appelle un fournisseur d'identité qui ne répond pas pour le moment.
E020019	Cette erreur est déclenchée lorsque le FI n'est pas présent dans la base de données de FC.
E020020	Cette erreur se déclenche quand l'appel à la route /oidc_callback est faite sans contexte (comprenez hors cinématique de connexion).
E020021	Cette erreur est déclenchée s'il manque des paramètres à la route /oidc_callback (code et/ou state). Cela provient en général d'une mauvaise implémentation du FI.
E020022	Erreur retournée si le paramètre "state" n'est pas valide.

Interopérabilité eIDAS

Code	Description
E050000	Cette erreur n'est déclenchée qu'en dernier recours, elle correspond à une exception mal ou non gérée. Il est impératif de remonter cette erreur aux développeurs car elle nécessite une investigation plus poussée dans le code. Erreur internationale, en anglais.
E050001	Dans la majorité des cas cela vient d'un lien qui a été réutilisé ou rafraîchi trop tard sur la page "choix du pays". Les cookies peuvent aussi avoir été désactivés sur le navigateur de l'usager.
E050002	Cette erreur est déclenché lorsqu'on arrive pas à comprendre la réponse SAML du FS (ou du FI ?).

Les données de FranceConnect qui expirent

FranceConnect gère plusieurs types de données "périssables" lors du déroulé d'une authentification par OpenID Connect ou de la fourniture d'un jeton d'accès à une ressource protégée (cinématique OAuth2 classique). Chacune de ces données possède une durée de vie qui lui est propre au delà de laquelle elle doit être régénérée. En voici le détail :

Type	Utilisé lors de ...	Durée de vie
Session Web	A chaque authentification et pour maintenir la session côté FranceConnect	30 minutes sans action
Access Token	Récupération d'informations (phase 3 cinématique d'authentification / cinématique OAuth2)	60 secondes
Authorization code	Code fourni lors du début de la démarche d'authentification, il sert ensuite à récupérer l'access token	30 secondes
Consentement	Consentement donné par l'utilisateur pour l'accès à une ressource protégée (associée à un scope au sens OAuth2)	5 secondes

Recette d'intégration de FranceConnect

Ci-dessous les éléments permettant une recette technique. En ce qui concerne la recette fonctionnelle, l'équipe FranceConnect a mis en place une démarche pour demander la qualification de votre service. Nous vous prions de bien vouloir y déposer votre demande afin qu'elle puisse être étudiée et traitée. Cette démarche est disponible à l'adresse suivante : https://www.demarches-simplifiees.fr/commencer/demande-qualification-fs

CONNEXION / CREATION DE COMPTE

- **Afin de pouvoir** réaliser des démarches chez un fournisseur de service
- **En tant qu'** internaute
- **Je veux** pouvoir créer un compte FranceConnect

Affichage de la mire FranceConnect (Cas passant)

- **Sachant que** je suis sur la page d'inscription du fournisseur de service
- **Et** que je vois le bouton FranceConnect
- **Quand** je clique sur le bouton FranceConnect
- **Alors** je dois voir la mire FranceConnect apparaître

Affichage de la mire d'authentification d'un fournisseur d'identité (Cas passant)

- **Sachant que** je suis sur la mire FranceConnect
- **Et** que je vois un logo d'un fournisseur d'identité
- **Quand** je clique sur le logo d'un fournisseur d'identité
- **Alors** je dois être redirigé vers la page d'authentification du fournisseur d'identitié

Authentification/identification via un fournisseur d'identité adéquat (Cas passant)

- **Sachant** que je suis sur la page d'authentification d'un fournisseur d'identité ayant le niveau de confiance eIDAS adéquat
- **Et** que j'indique mon login dans le champ correspondant
- **Et** que j'indique mon mot de passe dans le champ mot de passe
- **Quand** je clique sur le bouton "valider"
- **Alors** je dois être redirigé vers la page d'accueil du fournisseur de service

- **Et** je dois voir mon nom
- **Et** je dois voir mon prénom
- **Et** je ne dois plus voir le bouton FranceConnect

Authentification/identification via un fournisseur d'identité avec un niveau de confiance inférieur à celui exigé (Cas non passant)

- **Sachant** que je suis sur la page d'authentification d'un fournisseur d'identité ayant un niveau de confiance eIDAS insuffisant (si eidas2 est demandé, sélectionner un niveau eidas1)
- **Et** que j'indique mon login dans le champ correspondant
- **Et** que j'indique mon mot de passe dans le champ mot de passe
- **Quand** je clique sur le bouton valider
- **Alors** je ne dois pas être redirigé vers la page d'accueil du fournisseur de service
- **Et** je dois être redirigé vers la page d'erreur **E020023**

Authentification/identification via un fournisseur d'identité avec un mauvais mot de passe (Cas non passant)

- **Sachant que** je suis sur la page d'authentification d'un fournisseur d'identité
- **Et** que j'indique mon login dans le champ correspondant
- **Et** que j'indique un mauvais mot de passe dans le champ mot de passe
- **Quand** je clique sur le bouton valider
- **Alors** je ne dois pas être redirigé vers la page d'accueil du fournisseur de service
- **Et** je dois rester sur la page d'authentification du fournisseur d'identité

DECONNEXION

- **Afin de** pouvoir être l'unique utilisateur de mon compte
- **En tant qu'** utilisateur connecté
- **Je veux** pouvoir me déconnecter du fournisseur de service et de ma session FranceConnect

Déconnexion du fournisseur de service et de FranceConnect (Cas passant)

- **Sachant que** je suis connecté au fournisseur de service via FranceConnect
- **Quand** je clique sur le bouton "Se déconnecter"
- **Alors** je dois être déconnecté de ma session FranceConnect ainsi que celle du fournisseur de service
- **Je suis** redirigé vers l'URL de callback de déconnexion du fournisseur de service

DONNEES USAGERS

- **Afin de pouvoir** gagner du temps
- **En tant qu'** internaute
- **Je veux** que FranceConnect transmette mes informations pivot au fournisseur de service dans le cadre d'une démarche

Utilisation des données pivot dans le cadre d'une démarche sans consentement (Cas passant)

- **Sachant que** je suis connecté à un fournisseur de service avec mon compte FranceConnect
- **Et** que je commence ma démarche
- **Si** ma démarche nécessite mon "nom"
- **Alors** le champ doit indiquer mon "nom"
- **Et** je ne peux pas modifier la valeur du champ "nom"
- **Si** ma démarche nécessite mes "prénoms"
- **Alors** le champ doit indiquer mes "prénoms"
- **Et** je ne peux pas modifier la valeur du champ "prénoms"
- **Si** ma démarche nécessite ma "date de naissance"
- **Alors** le champ doit indiquer ma "date de naissance"
- **Et** je ne peux pas modifier la valeur du champ "date de naissance"
- **Si** ma démarche nécessite ma "civilité"
- **Alors** le champ doit indiquer ma "civilité"
- **Et** je ne peux pas modifier la valeur du champ "civilité"
- **Si** ma démarche nécessite mon "pays de naissance"
- **Alors** le champ doit indiquer mon "pays de naissance"
- **Et** je ne peux pas modifier la valeur du champ "pays de naissance"
- **Si** ma démarche nécessite ma "ville de naissance"
- **Alors** le champ doit indiquer ma "ville de naissance"
- **Et** je ne peux pas modifier la valeur du champ "ville de naissance"
- **Si** ma démarche nécessite mon "adresse email"
- **Alors** le champ doit indiquer mon "adresse email" si je dispose de cette information
- **Et** je peux modifier la valeur du champ "adresse email" même si elle provient de FranceConnect

CONSENTEMENT

- **Afin de pouvoir** donner mon accord concernant la transmission de données
- **En tant qu'** internaute
- **Je veux** que FranceConnect me donne le choix d'accepter cette transmission de données

Glossaire

FC_URL	URL de FranceConnect
FS_URL	Votre URL, en tant que fournisseur de service

FD_URL	URL du fournisseur de données
CALLBACK_URL_DATA	le callback du FS, communiqué lors de son inscription auprès de FC
DATA_ENDPOINT	Endpoint sur lequel le FD expose sa ressource. Il doit être communiqué par le FD
POST_LOGOUT_REDIRECT_URI	L'URL de redirection après la demande de déconnexion FC
CLIENT_ID	Identifiant du FS, communiqué lors de son inscription auprès de FC
CLIENT_SECRET	Le secret du FS, communiqué lors de son inscription auprès de FC
AUTHZ_CODE	Code retourné (dans l'URL) par FC au FS lorsque ce dernier fait un appel sur le endpoint FC_URL/api/v1/authorize. Il est ensuite passé (dans le corps de la requête HTTP POST) lors de l'appel sur le endpoint FC_URL/api/v1/token
ACCESS_TOKEN	Token retourné (dans le corps HTTP) par l'appel au endpoint FC_URL/api/v1/token. Il est ensuite passé lors de l'appel au endpoint FC_URL/api/v1/userinfo
SCOPES	Liste des scopes demandés séparés par des espaces (donc par %20 au format unicode dans l'URL). Voici la liste supportée par FranceConnect • openid : **obligatoire**, permet de demander l'identifiant technique de l'utilisateur au format OpenIDConnect • profile : **obligatoire**, permet de récupérer l'essentiel de l'identité pivot. Si disponible, renvoie aussi le preferred_username • birth : **obligatoire**, permet de récupérer la ville et le département de naissance de la personne (identité pivot) • email : **obligatoire**, permet de récupérer l'adresse électronique de la personne Cette liste de scopes est définie par la norme OpenIDConnect L'identité pivot complète se récupère soit par le scope identite_pivot, soit en cumulant deux scopes différents (profile + birth) car les informations de ville et de département de naissance de la personne ne font pas partie des données pouvant être renvoyées en soumettant le scope 'profile' seul. Le découpage est fait ici dans un souci de se conformer à la norme.
ID_TOKEN	Objet JWT retourné par l'appel au endpoint FC_URL/api/v1/token. L'objet JWT est un objet JSON formatté et signé. Le JSON doit contenir ces six clés : aud,exp,iat,iss,sub et nonce. Exemple : `{ 'aud':'895fae591ccae777094931e269e46447', 'exp':1412953984, 'iat':1412950384, 'iss':http://franceconnect.gouv.fr, 'sub':YWxhY3JpdMOp, 'idp':'FC', 'nonce':'12344354597459' }` Détail des champs : • **aud, exp, iat, iss, sub** : ce sont des champs obligatoires de la norme OpenIDConnect • **nonce** : paramètre obligatoirement envoyé lors de l'appel à /authorize. Le FS doit impérativement vérifier que la valeur correspond bien à celle qu'il a envoyée, et qui doit être liée à la session de l'utilisateur Si vous utilisez une librairie pour transformer le json en JWT, il génèrera une chaîne de caractères constitué de 3 chaînes base64 séparées par un point. Pour vérifier la signature, il faut utiliser le secret partagé avec FranceConnect (qui vous a été attribué lors de votre provisioning côté FC)
ID_TOKEN_HINT	Objet JWT identique au format ID_TOKEN qui a été reçu lors de l'échange avec l'appel à FC_URL/api/v1/token et doit être passé en paramètre lors de l'appel à FC_URL/api/v1/logout
USER_INFO	Voir la section identité pivot
STATE	Champ obligatoire, généré aléatoirement par le FS, que FC renvoie tel quel dans la redirection qui suit l'authentification, pour être ensuite vérifié par le FS. Il est utilisé afin d'empêcher l'exploitation de failles CSRF
NONCE	Champ obligatoire, généré aléatoirement par le FS que FC renvoie tel quel dans la réponse à l'appel à /token, pour être ensuite vérifié par le FS. Il est utilisé pour empêcher les attaques par rejeu
SUB	Identifiant technique (unique et stable dans le temps pour un individu donné) fourni par FranceConnect au FS. Le sub est présent dans l'IdToken retourné au FS ainsi que dans les informations d'identité. Le sub retourné par FranceConnect est spécifique à chaque fournisseur de service (i.e: Un usager aura toujours le même sub pour un FS donné, en revanche il aura un sub différent par FS qu'il utilise).