ANNEXE TECHNIQUE - RACCORDEMENT / PROCESSUS IMPLÉMENTATION DE FRANCECONNECT PAR LE FOURNISSEUR DE SERVICE

SOMMAIRE

1. OBJET

La présente annexe a pour objectif de définir les modalités de mise en oeuvre de FranceConnect par le fournisseur de services en environnement d'intégration et de production.

2. PROCESSUS DE MISE EN OEUVRE DE FRANCECONNECT

Étapes	Engagements
Inscription à FranceConnect et validation des CGU	Obligatoire
Intégrer et configurer un client OpenID Connect	Obligatoire
Intégration d'un bouton d'action FranceConnect	Obligatoire
Intégration du "Kit FranceConnect"	Facultatif
Implémentation de la déconnexion	Obligatoire
Réconciliation et dissociation de compte	Facultatif
Gestion des erreurs entre FranceConnect et le fournisseur de service	Obligatoire

Expiration des données	Obligatoire
Respect de la charte	Obligatoire
Information auprès de la CNIL	Obligatoire
Recette et mise en production	Obligatoire

3. INSCRIPTION A FRANCECONNECT ET VALIDATION DES CGU

Le fournisseur de service doit s'inscrire à FranceConnect via le formulaire d'enregistrement mis à sa disposition sur le portail développeur FranceConnect.

Dans le cadre de la mise en oeuvre le fournisseur de service se doit de s'enregistrer en précisant les informations suivantes :

Nom du service	Obligatoire
Email de contact	Obligatoire
Logo du service	Recommandé
Urls de callback*	Obligatoire - en y indiquant une par ligne
Quel est votre cas d'usage ?	Obligatoire

*** Informations complémentaires concernant les URLs de callback :**

- L'URL peut avoir une profondeur quelconque de sous domaines
- Le fournisseur de service peut utiliser des ports spécifiques
- Le fournisseur de service peut utiliser une IP plutôt qu'un FQDN
- Le "search" de l'URL peut être d'une taille arbitraire
- Le fournisseur de service peut utiliser "localhost"

Afin de valider son enregistrement le fournisseur de service doit **valider les conditions générales d'utilisation** du service FranceConnect au moment de l'envoi de ses informations.

4. INTÉGRER ET CONFIGURER UN CLIENT OPENID CONNECT

4.1. Introduction

FranceConnect suit l'implémentation standard d'OpenID Connect. Le protocole OpenID Connect est une surcouche d'identification au protocole OAuth 2.0. Il permet à un fournisseur de service d'accéder à l'identité pivot (voir annexe identité pivot) des usagers

(utilisateurs finaux) transmise par un fournisseur d'identité via l'intermédiaire de FranceConnect.

- Le fournisseur de service est client OpenID Connect pour FranceConnect
- FranceConnect est fournisseur OpenID Connect pour le fournisseur de service

*** Informations complémentaires concernant OIDC :**

- Spécification du protocole : http://openid.net/connect/.
- Référence d'implémentation OpenID Connect : http://openid.net/specs/openid-connect-core-1_0.html

4.2. Intégration

Le fournisseur de service doit implémenter et configurer un client OpenID connect afin de communiquer avec FranceConnect (considéré comme fournisseur OIDC).

*** Liste non exhaustive de clients OpenID Connect :**

http://openid.net/developers/libraries/

4.3. Configuration

Le protocole OpenID Connect définit 3 appels REST et 1 endpoint par le client OIDC (3 endpoints du côté fournisseur)

Les endpoints disponibles en environnement d'intégration en https sont les suivants :

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

4.3.1. Mise en place de la cinématique

Le fournisseur de service dans sa mise en oeuvre doit suivre la cinématique suivante :

1. L'usager clique sur le bouton d'authentification du client.

2. Le client fait une redirection vers le "authorization endpoint" du provider avec son client id et son url de callback.

<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 -> Cible :	FS -> FC
	Type d'appel :	redirection navigateur
Requête	**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
Réponse	**/**	

3. Le provider redirige alors l'usager vers sa mire d'authentification. Si l'internaute se loggue correctement, le provider renvoie un code d'autorisation au client.

<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 -> Cible :	FC -> FS
	Type d'appel :	redirection navigateur
Requête	**URL :**	**<FS_URL>**/<URL_CALLBACK>?code=**<AUTHZ_CODE>**&state=**<STATE>**
	Méthode :	GET
Réponse	**/**	

4. Le client fait un appel Web service vers le "token endpoint" du provider avec le code d'autorisation reçu (**<AUTHZ_CODE>)**, 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), un id token (sous la forme d'un Json Web Token, voir https://developer.atlassian.com/static/connect/docs/concepts/understanding-jwt.html)

<FC_URL>/api/v1/token [WEB SERVICE]

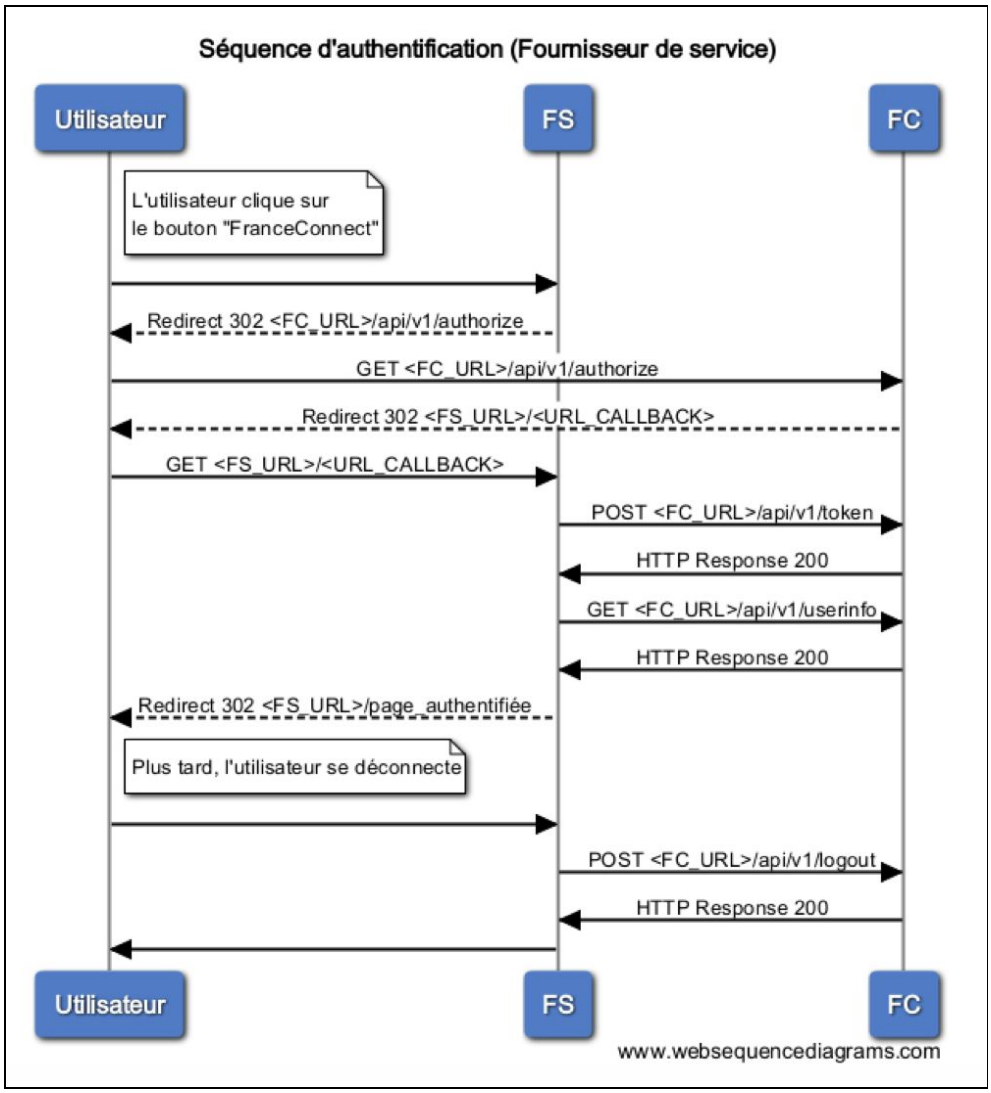
Description	**Contexte :**	Le FS a récupéré un authorization code. Il veut maintenant récupérer un access token et un id token.
	Origine -> Cible :	FS -> FC
	Type d'appel :	appel de Web service
Requête	**URL :**	**<FC_URL>**/api/v1/token
	Méthode :	POST
	Corps HTTP :	'grant_type': 'authorization_code', 'redirect_uri': '**<FS_URL>**/<URL_CALLBACK>', 'client_id': '**<CLIENT_ID>**', 'client_secret': '**<CLIENT_SECRET>**', 'code': '**<AUTHZ_CODE>**'
Réponse	**Corps HTTP :**	{ 'access_token': **<ACCESS_TOKEN>**, 'token_type': 'Bearer', 'expires_in': 3600, 'id_token': **<ID_TOKEN>** }

5. Le client fait un appel Web service vers le "userInfo endpoint" du provider avec l'access token reçu

<FC_URL>/api/v1/userinfo [WEB SERVICE]		
Description	**Contexte :**	Le FS a récupéré un access token. Il veut maintenant récupérer les USER INFO.
	Origine -> Cible :	FS -> FC
	Type d'appel :	appel de Web service
Requête	**URL :**	**<FC_URL>**/api/v1/userinfo?schema=openid
	Méthode :	GET
	Entêtes HTTP :	Authorization = 'Bearer **<ACCESS_TOKEN>**'
Réponse	**Corps HTTP :**	**<USER_INFO>**

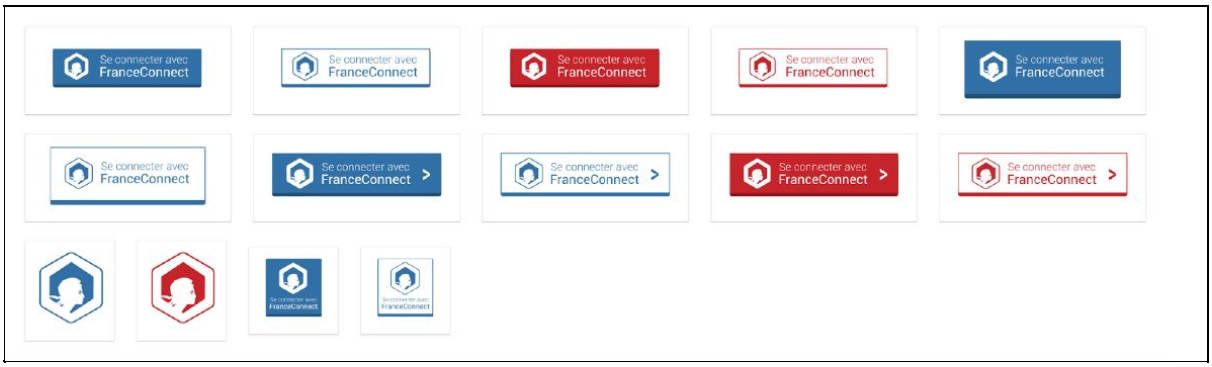
6. Le provider renvoie les informations de l'usager au client (le FS). La description des informations transmises est définie dans l'échange de données

4.3.2. Diagramme des flux



5. INTÉGRATION D'UN BOUTON D'ACTION FRANCECONNECT

Les boutons d'action FranceConnect sont primordiaux dans l'usage du service. Contrairement au logo, ils ne sont pas représentatifs mais actifs. Afin d'accéder au service, il est **obligatoire** d'utiliser l'un des boutons proposé par la charte et aucun autre visuel. (le détail des possibilités de mise en place est détaillé plus loin). Ces boutons sont disponibles sur le portail développeur.



Les boutons sont toujours accompagnés d'un texte expliquant la connexion ("Se connecter avec FranceConnect"). S'ils sont utilisés sans, il est impératif de rajouter ce texte soi même, ces symboles ne pouvant pas être utilisés seuls.

Quel que soit le bouton d'action que choisi par le fournisseur de service pour proposer la connexion à **FranceConnect**, il doit obligatoirement s'accompagner d'un lien précisant «qu'est-ce que FranceConnect ?» pointant vers l'url suivante pour l'intégration : https://fcp.integ01.dev-franceconnect.fr/a-propos (une url de production sera fournie dès validation de la recette).

Dans le choix de bouton, le fournisseur de service prendra garde à ne pas utiliser :

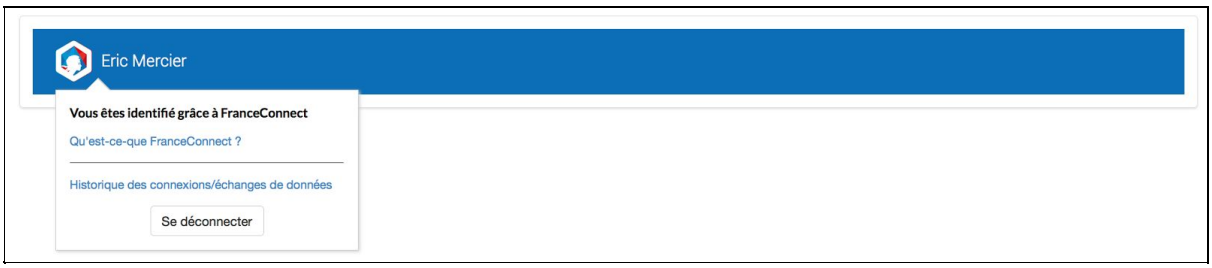
- Des couleurs de boutons qui soient les même que celles du fond utilisé
- Des couleurs de boutons qui soient foncées avec un fond foncé sur votre site
- Des liens vers «Qu'est-ce que FranceConnect ?» qui soient également trop proches de la couleur de fond.

6. INTÉGRATION DU KIT FRANCECONNECT

Le "Kit FranceConnect" est le script qu'il est possible d'inclure pour le fournisseur de service afin de disposer du **bouton de déconnexion** ainsi que du lien vers les **traces**. Le kit

propose un menu présentant divers liens liés à FranceConnect (aujourd'hui le bouton de déconnexion et l'accès à la page "traces").

Il est nécessaire que l'utilisateur soit connecté à FranceConnect pour afficher ce bloc.



Le SGMAP recommande l'intégration du kit FranceConnect tel proposé en :

1. Incluant la librarie javascript FranceConnect en bas de page :

```
<script src="http://fcp.integ01.dev-franceconnect.fr/js/franceconnect.js"></script>
```

2. Insérant dans le code HTML la structure suivante :

```
<div id="fconnect-profile" data-fc-logout-url="/lien-deconnexion">
   <a href="#"> le nom de l'utilisateur connecté* </a>
</div>
```

3. Paramétrant les variables suivantes :

Variables	**Valeurs**
data-fc-logout-url	Mettre le lien de déconnexion
Utilisateur	Remplacer par le nom de l'utilisateur connecté

En fonction des contraintes du fournisseur de service, il est possible que ce dernier veuille intégrer le kit manuellement. Dans ce cas, le fournisseur de service se doit de mettre en place :

- un lien vers l'historique des connexions et des échanges de données (traces)

Environnement	**URLs**
Intégration	https://fcp.integ01.dev-franceconnect.fr/traces

- la déconnexion FranceConnect (Section 4 de la présente annexe)

- Un lien vers la page qu'est ce que FranceConnect?

Environnement	URLs
Intégration	https://fcp.integ01.dev-franceconnect.fr/a-propos

7. IMPLEMENTATION DE LA DÉCONNEXION

FranceConnect implémente la section sur la déconnexion en cours de spécification dans la norme OpenID Connect :
http://openid.net/specs/openid-connect-session-1_0-15.html#RPLogout

Le fournisseur de service doit proposer la déconnexion de FranceConnect à son utilisateur et l'implémenter la cinématique suivante :

1. L'utilisateur clique sur un lien de déconnexion présenté par le fournisseur de service. Il est a noté que le bouton de déconnexion est présent dans le kit d'intégration FranceConnect.

2. Le fournisseur doit **déconnecter** l'utilisateur de son application, puis le rediriger vers la page de déconnexion de FC : ***<FC_URL>/api/v1/logout***. Selon le choix de l'utilisateur, il est éventuellement déconnecté du service FranceConnect

3. L'utilisateur est redirigé vers la page de retour spécifiée par le fournisseur de service

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 OIDC

<FC_URL>/api/v1/logout [REDIRECTION]		
Requête :	**URL :**	**<FC_URL>**/api/v1/logout?id_token_hint=**<ID_TOKEN_HINT>**&state=**<STATE>**&post_logout_redirect_uri=**<POST_LOGOUT_REDIRECT_URI>**
	Méthode :	GET

8. RÉCONCILIATION ET DISSOCIATION DE COMPTE

Le SGMAP recommande de mettre en oeuvre la réconciliation et la dissociation des comptes existants des usagers du fournisseur de service. L'implémentation est propre au fournisseur de service en fonction de son S.I.

9. GESTION DES ERREURS ENTRE FRANCECONNECT ET LE FOURNISSEUR DE SERVICE

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))

10. EXPIRATION DES DONNEES

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 :

Type	**Usage**	**Durée**
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)	20 minutes
Authorization code	Code fourni lors du début de la démarche d'authentification, il sert ensuite à récupérer l'access token	5 minutes

11. RESPECT DE LA CHARTE

11.1. Orthographe

FranceConnect s'écrit avec les deux caractéristiques immuables suivantes :

- Tout attaché et sans le moindre espace FranceConnect se compose de 13 caractères
- FranceConnect a deux Capitales et onze bas-de-casses :
    - le F initial est une Majuscule ainsi que le C
    - les autres caractères sont en minuscules

Il n'y a que dans le logo que les deux parties du mot FranceConnect sont détachées comme ici :

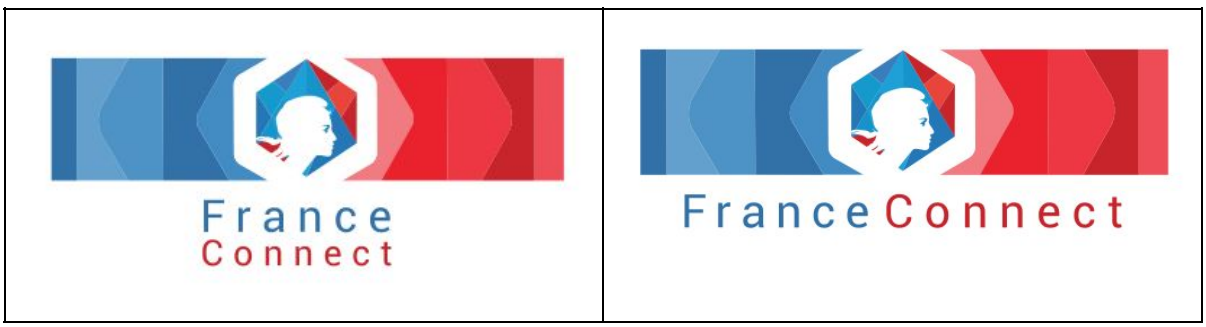
11.2. Le logo

Le Logotype FranceConnect se compose d'un symbole hexagonal à facettes bleu, blanc et rouge. L'hexagone représente la france, son unité.
il est utilisé :

- Uniquement à des fins de représentation
- Le choix se fait librement parmi les logos disponibles dans la charte

il n'est jamais utilisé :

- Comme bouton d'action de connection
- partiellement ou juste en sigle s'il s'agit de représenter FranceConnect



11.3. Les couleurs

Si ces couleurs sont utilisées avec la police par défaut «Roboto» en blanc (R255 V255 B255, #FFFFFF), le résultat est valide au test d'accessibilité AA

11.3.1. Les couleurs primaires

	bleu	R 52 V 113 B 169	hexa #3471A9
	rouge	R 201 V 19 B 31	hexa #C9131F
	gris	R 128 V 129 B 132	hexa #808184

11.3.2. Les couleurs secondaires

	bleu	R 34 V 81 B 123	hexa #23507A
	rouge	R 149 V 29 B 35	hexa #951D22

11.3.3. La police

«Roboto» est la police utilisée par FranceConnect. Elle est disponible sur Google fonts

- La police GoogleFont gratuite et disponible aux formats TrueType et OpenTrueType
- Elle est la police du logo

12. INFORMATION AUPRES DE LA CNIL

Dans le cadre de l'implémentation de FranceConnect pour une démarche en ligne, une déclaration simple sur le site de CNIL (https://www.declaration.cnil.fr/declarations/declaration/declarant.display.action;jsessionid=E874E414F2603828AB7E9AD278B4D3AA) devra être réalisée.

13. RECETTE ET MISE EN PRODUCTION

Dès souhait de mettre FranceConnect en production, le fournisseur de service devra informer par email (support@dev-franceconnect.fr) le SGMAP afin de réaliser une recette du dispositif et d'être informé de la date de mise en production souhaité par le fournisseur de service. Le SGMAP pourra également demander un audit sur la partie du système d'information concernée.

Dès la recette validée, l'équipe support contactera par téléphone le fournisseur de service afin de lui transmettre ses clients id / secret de production ainsi que les urls de production suivantes :

- authorize
- token
- userInfo
- logout
- A propos de FranceConnect

14. SUPPORT

FranceConnect met à disposition de ses partenaires fournisseur de service l'adresse électronique suivante : support@dev-franceconnect.fr pour tout besoin relatif à la mise en oeuvre de FranceConnect

15. GLOSSAIRE

FC_URL	URL de FranceConnect
FS_URL	Votre URL, en tant que fournisseur de service
CALLBACK_URL_DATA	le callback du FS, communiqué lors de son inscription auprès de FC
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 (dans l'URL) 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 formatOpenIDConnect ● 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 : facultatif, si disponible, renvoie l'adresse e-mail de la personne ● address : facultatif, si disponible, renvoie l'adresse postale de la personne ● phone : facultatif, si disponible, renvoie le numéro de téléphone de la personne Cette liste de scopes est définie par la norme OpenIDConnect L'identité pivot complète se récupère par 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	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 cinq clés : aud,exp,iat,iss,sub. Exemple : {'aud':'895fae591ccae777094931e269e46447', 'exp':1412953984, 'iat':1412950384, 'iss':http://franceconnect.gouv.fr, 'sub':YWxhY3JpdMOp, 'idp':'dgfip', '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 /authorization. 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 ● idp : spécifique à FranceConnect. Fournit l'identifiant du fournisseur d'identité utilisé par l'utilisateur courant (exemple: 'dgfip' si l'utilisation a choisi d'utiliser son compte des Finances Publiques). 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 l'annexe échange de données
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).