Direction interministérielle du numérique et des systèmes d'information et de communication

Convention d'adhésion au service FranceConnect Particuliers à destination des Fournisseurs d'Identité –

Annexe i – Annexe technique – Processus d'implémentation de FranceConnect Particuliers par le FI

Août 2018

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

La présente annexe a pour objectif de définir les modalités de mise en œuvre de FranceConnect Particuliers par le Fournisseur d'Identité en environnement d'intégration et de production. Elle s'inscrit en complément de la Convention d'Adhésion au service FranceConnect Particuliers à destination des Fournisseurs d'Identité et ne saurait être prise isolément.

2. CONDITIONS D'INTEGRATION AU SERVICE FRANCECONNECT PARTICULIERS

2.1. Prérequis

Outre l'acceptation des conditions définies dans le corps juridique de la convention d'adhésion, le Fournisseur d'Identité doit préalablement à l'intégration avec FranceConnect Particuliers remplir les conditions suivantes :

- Homologation de sécurité RGS portant a minima sur le périmètre des services de gestion des identités proposés au travers de FranceConnect Particuliers (sous réserve pour les opérateurs privés) ;
- Déclarations CNIL relatives aux traitements des données à caractère personnel ;
- Validation du niveau eIDAS par l'ANSSI ;
- Publication du schéma eIDAS pour les Fournisseurs d'Identité souhaitant ouvrir leurs services d'identification aux autres pays membres de l'UE ;
- Fourniture de l'intégralité de l'Identité pivot telle que définie dans l'Annexe ii – Annexe technique – Echange de données entre le Fournisseur d'Identité et FranceConnect Particuliers.

2.2. Synthèse d'implémentation

Le Fournisseur d'Identité suivra le processus d'implémentation suivant :

1. Envoi d'une demande d'adhésion à la DINSIC avec explication de son processus de vérification d'identité ;
2. Redirection du Fournisseur d'Identité par la DINSIC vers l'ANSSI pour validation du niveau eIDAS si ce dernier est considéré éligible ;
3. En parallèle de la validation du niveau e-IDAS, le Fournisseur d'Identité contactera la DINSIC pour une réunion de planification ;
4. Début des développements - Inscription au formulaire d'enregistrement (section 3 de la présente annexe) et envoi de son certificat TLS à l'équipe support (support.partenaires@franceconnect.gouv.fr) ;
5. Communication régulière sur l'avancement ;
6. Phase de recette avec l'équipe FranceConnect Particuliers sur l'ensemble des cinématiques et vérification que toutes les données des Usagers sont correctement transmises à FranceConnect Particuliers ;
7. Envoi par le Fournisseur d'Identité de ses URLs de production, logo et certificat de production (RGS) à l'équipe support FranceConnect Particuliers ;
8. Mise en production et communication.

3. PROCESSUS DE MISE EN ŒUVRE DE FRANCECONNECT PARTICULIERS

Le processus de mise en œuvre de FranceConnect Particuliers par le Fournisseur d'Identité se décline en plusieurs étapes :

N°	Étapes	Engagements
1	**Inscription à FranceConnect Particuliers et validation des CDA**	Obligatoire
2	**Intégration et configuration d'un provider OpenID Connect**	Obligatoire
3	**Mise en place de la mire d'authentification FranceConnect Particuliers**	Obligatoire
4	**Expiration des données**	Obligatoire
5	**Gestion des erreurs entre FranceConnect Particuliers et le Fournisseur d'Identité**	Obligatoire
6	**Recette et mise en production**	Obligatoire

3.1. Etape 1 – Inscription à FranceConnect Particuliers et validation de la CDA

Le Fournisseur d'Identité doit s'inscrire à FranceConnect Particuliers via le formulaire d'enregistrement mis à sa disposition sur le portail développeur FranceConnect Particuliers.

Dans le cadre de la mise en œuvre le Fournisseur d'Identité se doit de s'enregistrer en précisant les informations suivantes :

Nom de l'entité	Obligatoire
Adresse email de contact	Obligatoire
URL du endpoint d'authentification et d'autorisation	Obligatoire
URL du endpoint de demande de token	Obligatoire
URL du endpoint de demande des informations utilisateur (identité pivot)	Obligatoire
Client ID	Obligatoire
Client secret	Obligatoire
Commentaire (qui êtes-vous ?, quel est votre cas d'usage ?)	Recommandé

Le Fournisseur d'Identité doit également fournir un logo au format svg à l'adresse suivante : support.partenaires@franceconnect.gouv.fr.

3.2. Etape 2 - Intégration et configuration d'un provider OpenID Connect

FranceConnect Particuliers suit l'implémentation standard d'OpenID Connect (OIDC).

Le protocole OpenID Connect est une surcouche d'identification au protocole OAuth 2.0. Il permet à un Fournisseur de Services d'accéder à l'identité pivot (cf. Annexe ii – Annexe technique – Echange de données entre le Fournisseur d'Identité et FranceConnect Particuliers) des usagers transmise par un Fournisseur d'Identité via l'intermédiaire de FranceConnect Particuliers.

Le Fournisseur d'Identité est fournisseur OpenID Connect pour FranceConnect Particuliers.
FranceConnect Particuliers est client OpenID Connect pour le Fournisseur d'Identité.

Des informations complémentaires concernant OIDC sont disponibles aux adresses suivantes :

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

3.2.1 Intégration

Le Fournisseur d'Identité doit implémenter et configurer un provider OpenID Connect afin de communiquer avec FranceConnect Particuliers.

Une liste non exhaustive de providers OpenID Connect est disponible à l'adresse suivante : http://openid.net/developers/libraries/.

3.2.2 Configuration

Le Fournisseur d'Identité doit enregistrer FranceConnect Particuliers comme client avec l'URL de callback suivante :

URL de callback	https://fcp.integ01.dev-franceconnect.fr/oidc_callback

Il est à noter que les « endpoints » sont uniquement disponibles en HTTPS.

Le Fournisseur d'Identité doit être à même de fournir un sub (identifiant technique) lors des appels de FranceConnect Particuliers (**<FI_URL>/user/token**) et d'apporter les modifications structurelles à son système d'information (SI) si nécessaire. Il est à noter que le sub transmis doit être différent de l'identifiant technique du SI du Fournisseur d'Identité.

3.2.3 Mise en place de la cinématique

Le Fournisseur d'Identité dans sa mise en œuvre doit suivre la cinématique suivante :

1. L'usager clique sur le Fournisseur d'Identité de son choix.

2. FranceConnect Particuliers fait une redirection vers le "authorization endpoint" du Fournisseur d'Identité avec son client id et son url de callback.

<FI_URL>/user/authorize [REDIRECTION]		
Description	**Contexte**	FranceConnect Particuliers redirige vers /user/authorize du FI.
	Origine ➔Cible	FC ➔ FI
	Type d'appel	Redirection navigateur

Requête	**URL**	**<FI_URL>**/user/authorize?response_type=code&client_id=**<CLIENT_ID>**&redirect_uri=**<FC_URL>**%2Foidc_callback&scope=**<SCOPES>**&state=**<STATE>**&nonce= **<NONCE>**
	Méthode	GET
Réponse	/	

3. Le Fournisseur d'Identité redirige vers le callback de FranceConnect Particuliers.

<FC_URL>/oidc_callback [REDIRECTION]		
Description	**Contexte**	Le FI redirige vers le callback de FranceConnect Particuliers.
	Origine ➔ Cible	FI ➔ FC
	Type d'appel	Redirection navigateur
Requête	**URL**	**<FC_URL>**/oidc_callback?code=**<AUTHZ_CODE>**&state= **<STATE>**
	Méthode	GET
Réponse	/	

4. FranceConnect Particuliers fait appel au Web service du FI.

<FI_URL>/user/token [WEB SERVICE]		
Description	**Contexte**	FranceConnect Particuliers fait un appel au FI pour récupérer un access token, un id token et un refresh token.
	Origine ➔ Cible	FC ➔ FI
	Type d'appel	Appel de Web service
Requête	**URL**	**<FI_URL>**/user/token
	Méthode	POST
	Corps HTTP	'grant_type': 'authorization_code', 'redirect_uri': '**<FC_URL>**/oidc_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, 'refresh_token': **<REFRESH_TOKEN>**, 'id_token': **<ID_TOKEN>** }

5. FranceConnect Particuliers demande les USER_INFO de l'usager au FI.

<FI_URL>/api/user [WEB SERVICE]		
Description	**Contexte**	FranceConnect Particuliers fait un appel au FI pour récupérer les USER_INFO de l'usager.
	Origine ➔ Cible	FC ➔ FI
	Type d'appel	Appel de Web service
Requête	**URL**	**<FI_URL>**/api/user?schema=openid
	Méthode	GET
	Entêtes HTTP	Authorization = 'Bearer **<ACCESS_TOKEN>**'
Réponse	**Corps HTTP**	<USER_INFO>

3.2.4 Diagramme des flux

Le schéma ci-après fournit le diagramme des flux entre l'usager, FranceConnect Particuliers et le Fournisseur d'Identité.

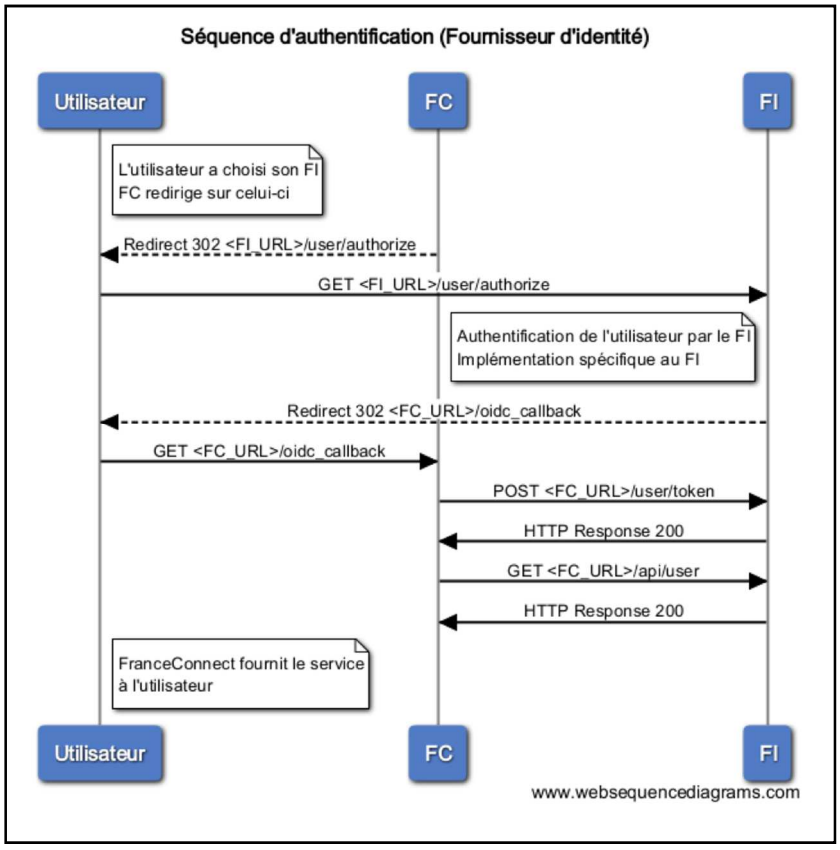

Figure 1 : Diagramme des flux « Usager ➔ FranceConnect Particuliers ➔ Fournisseur d'Identité »

3.3. Etape 3 – Mise en place de la mire d'authentification FranceConnect Particuliers

La mire d'authentification FranceConnect Particuliers redirige vers la page de connexion dédiée du Fournisseur d'Identité. Il s'agit de la redirection navigateur **<FI_URL>/user/authorize.**

Figure 2 : Page de connexion de la DGFIP

Le Fournisseur d'Identité implémente sur la page de connexion les éléments ergonomiques suivants :

Nature	Description	Statut
IHM "responsive"	IHM permettant de s'adapter à l'ensemble des supports matériels que peuvent utiliser les usagers	Obligatoire
Bouton "retour"	Bouton permettant à l'usager de retourner sur la mire d'authentification FranceConnect Particuliers proposant les différentes entités offrant le rôle de Fournisseur d'Identité	Obligatoire
Lien vers le support du Fournisseur d'Identité (mail, formulaire)	Lien permettant de faciliter les échanges en cas de problème de connexion de l'usager	Obligatoire

Figure 3 : Mire d'authentification FranceConnect Particuliers

3.4. Etape 4 – Expiration des données

Afin de garantir la déconnexion côté FranceConnect Particuliers, le Fournisseur d'Identité doit limiter la durée de sa session à deux minutes, cette durée correspondant au seuil maximal.

3.5. Etape 5 – Gestion des erreurs entre FranceConnect Particuliers et le Fournisseur d'Identité

Le Fournisseur d'Identité doit retourner les informations d'erreur à FranceConnect Particuliers par l'URL de callback fournie en utilisant le formalisme se trouvant dans la norme.

La gestion des erreurs OpenID Connect est disponible à l'adresse suivante : http://openid.net/specs/openid-connect-core-1_0.html#AuthError.

3.6. Etape 6 – Recette et mise en production

Avant toute mise en production, le Fournisseur d'Identité doit informer par email (support.partenaires@franceconnect.gouv.fr) la DINSIC de son souhait et de la date de mise en production attendue par le Fournisseur d'Identité.

La DINSIC réalise une recette du dispositif et vérifie la couverture des exigences relatives au Fournisseur d'Identité décrites dans l'annexe iii – Annexe sécurité.

Après validation de la recette, le Fournisseur d'Identité communique à l'équipe support, par deux canaux distincts obligatoirement, les informations de production suivantes :

- Par mail :
    - URL du endpoint d'authentification et d'autorisation ;
    - URL du endpoint de demande de token ;
    - URL du endpoint de demande des informations utilisateur (identité pivot) ;
    - Logo ;
    - Certificat RGS ;
    - Client ID ;
- Par SMS :
    - Client secret ;

En production, il est recommandé que le Fournisseur d'Identité renouvelle son client_secret tous les ans. Le Fournisseur d'Identité communique le nouveau client_secret à la DINSIC par téléphone.

4. SUPPORT

FranceConnect Particuliers met à disposition du Fournisseur d'Identité l'adresse électronique suivante : support.partenaires@franceconnect.gouv.fr pour tout besoin relatif à la mise en œuvre de FranceConnect Particuliers. Le détail des moyens de support et de maintenance mis en œuvre pour assurer la qualité du service est par ailleurs présenté dans l'annexe iv – Annexe qualité de service et chaîne de support.

5. GLOSSAIRE TECHNIQUE

FC_URL	URL de FranceConnect Particuliers
FI_URL	URL du Fournisseur d'Identité
CLIENT_ID	Identifiant de FC, communiqué par le FI à FC lors de son inscription
CLIENT_SECRET	Secret de FC, communiqué par le FI à FC lors de son inscription
AUTHZ_CODE	Code retourné (dans l'URL) par le FI à FC lorsque ce dernier fait un appel sur le endpoint FI_URL/user/authorize. Il est ensuite passé (dans le corps de la requête HTTP POST) lors de l'appel sur le endpoint FI_URL/user/token.
ACCESS_TOKEN	Token retourné (dans le corps HTTP) par l'appel au endpoint FI_URL/user/token. Il est ensuite passé (dans l'URL) lors de l'appel au endpoint FI_URL/api/user.
REFRESH_TOKEN	Token retourné (dans le corps HTTP) par l'appel au endpoint FI_URL/user/token. Il n'est pas utilisé par la suite.
SCOPES	Voir annexe ii
ID_TOKEN	Objet JWT retourné par l'appel au endpoint <FC_URL>/user/token. L'objet JWT est un objet JSON formaté et signé. Pour l'instant, FranceConnect Particuliers ne supporte que l'algorithme de signature HS256 (HMAC using SHA-256 hash algorithm). Le JSON doit contenir ces six clés : aus, exp, iat, iss, nonce, sub. La clé à utiliser pour la signature est le secret partagé avec FranceConnect Particuliers (que vous lui avez attribué avec un client_id lors de son provisioning en tant que client OpenID Connect du FI) Notez que le champ **nonce** est bien obligatoire et doit obligatoirement retourner la valeur fournie par FranceConnect Particuliers dans l'URL de redirection au début de la cinématique d'authentification. Exemple : {'aud':'895fae591ccae777094931e269e46447', 'exp':1412953984, 'iat':1412950384, 'iss':http://impots-franceconnect.fr, 'sub':4344343423, 'nonce':34324432468}. Si vous utilisez une librairie pour transformer le json en JWT, il génèrera une chaîne de caractères constituée de 3 chaînes base64 séparées par un point.
USER_INFO	Voir annexe ii
STATE	Champ obligatoire, généré aléatoirement par FC, que le FI renvoie tel quel dans la redirection qui suit l'authentification, pour être ensuite vérifié par FC. Il est utilisé afin d'empêcher l'exploitation de failles CSRF.
NONCE	Champ obligatoire, généré aléatoirement par FC que le FI renvoie tel quel dans la réponse à l'appel à /token, pour être ensuite vérifié par FC. Il est utilisé pour empêcher les attaques par rejeu.
SUB	Identifiant technique (unique et stable dans le temps pour un individu donné) fourni par le FI à FC. Le sub doit être présent dans l'IdToken retourné à FC ainsi que dans les informations d'identité. Pour plus d'informations sur le rôle et la description du "sub", se référer à la documentation OpenID Connect http://openid.net/specs/openid-connect-basic-1_0.html (section 2.2)

Direction interministérielle du numérique et des systèmes d'information et de communication

20 Avenue de Ségur
TSA 30719
75334 Paris CEDEX 7

www.franceconnect.gouv.fr