ANNEXE TECHNIQUE - ÉCHANGE DE DONNÉES ENTRE FRANCECONNECT ET LE FOURNISSEUR DE SERVICE

Ce document définit les données échangées entre FranceConnect et le fournisseur de service et la manière dont celles-ci sont traitées.

1. Définition

L'identité pivot d'un usager est définit par un ensemble de données demandé par FranceConnect auprès d'un fournisseur d'identité et retransmise au fournisseur de service par l'intermédiaire de FranceConnect lors d'une connexion d'un usager au dispositif.

Le fournisseur de service s'engage à ce que l'ensemble des données d'identité transmises par FranceConnect ne puissent être modifiées dans le cadre des démarches si ces données ont été au préalable enregistrées dans le S.I. du fournisseur de service.

2. Constitution de l'identité pivot

Chaque donnée constituant l'identité pivot d'un usager est appelée **scopes**. Des **alias** sont également à disposition du fournisseur de service lui permettant de récupérer un ensemble de scopes.

Le scope **<openid>** doit obligatoirement être récupéré par le fournisseur de service.
Le fournisseur de service à libre arbitre de récupérer les autres scopes en fonction des informations dont il a besoin. Le fournisseur de service doit récupérer uniquement les informations nécessaires au cadre des démarches proposées.

Certains scopes sont "optionnels" : Ils ne seront pas obligatoirement transmis bien que le fournisseur de service en ait fait la demande. En effet, ces données sont transmises par le fournisseur d'identité que si ce dernier possèdent ces informations.

Les données vérifiées (en opposition avec les données déclaratives) sont les données qui ont été redressés par interrogation au Répertoire national d'identification des personnes physiques (RNIPP) par FranceConnect.

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

Alias	Scopes	Format	Description	Type	Standard OIDC

	openid	string	l'identifiant technique (sub) de l'utilisateur au format OpenID Connect	Obligatoirement demandé par le FS Non vérifié	OUI
profile	**given_name**	string	les prénoms de la personne Les prénoms sont séparés par des espaces selon le standard OpenIDConnect	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI
	family_name	string	le nom de naissance de la personne	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI
	preferred_username	string	le nom d'usage de la personne	Optionnellement demandé par le FS Optionnellement transmis par le FI Vérifiée auprès du RNIPP	OUI
	gender	string	le sexe de la personne **Valeurs possibles :** - male - female	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI
	birthdate	string	la date de naissance de la personne La date de naissance au format YYYY-MM-DD	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI

birth	**birthcountry**	string	le pays de naissance de la personne **<u>Valeurs possibles :</u>** - le code INSEE du pays de naissance	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI
	birthplace	string	la ville de naissance de la personne **<u>Valeurs possibles :</u>** - le code INSEE du lieu de naissance ou - chaîne vide si la personne est née à l'étranger	Optionnellement demandé par le FS Obligatoirement transmis par le FI Vérifiée auprès du RNIPP	OUI
	email	string	l'adresse e-mail de la personne	Optionnellement demandé par le FS Obligatoirement transmis par le FI Non vérifié	OUI
	address	string	l'adresse postale de la personne	Optionnellement demandé par le FS Optionnellement transmis par le FI Non vérifié	OUI
	phone	string	le numéro de téléphone de la personne	Optionnellement demandé par le FS Optionnellement transmis par le FI Non vérifié	OUI

3. Récupération de l'identité pivot

Le fournisseur de service après avoir récupéré un accès token (**Annexe Processus d'implémentation**) va récupérer les USER_INFO de l'usager en faisant un appel de webservice **<FC_URL>/api/v1/userinfo** à FranceConnect.

Url de la requête :

<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>

FranceConnect va alors faire un appel de webservice similaire au fournisseur d'identité afin de récupérer de son côté les USER_INFO de l'usager.

3.1 Transfert des données pivot du fournisseur d'identité à FranceConnect

Une fois récupération des USER_INFO provenant du fournisseur d'identité, FranceConnect fait un appel au RNIPP afin de contrôler l'identité de l'usager. Les informations sont éventuellement redressées si nécessaire avant transmission au fournisseur de service.

3.1.1 Contrôle de l'identité pivot par le RNIPP

Le RNIPP est un instrument de vérification de l'état civil des personnes. Sa consultation permet entre autre de préciser si une personne est en vie ou décédée. Le RNIPP permet également la certification de l'état civil.

Les traitements de retour du RNIPP dans FranceConnect sont les suivants :

- Le RNIPP renvoit une identité
- Le RNIPP ne renvoit pas d'identité

3.1.1.1 Le RNIPP renvoit une identité

Si l'INSEE renvoit une identité, alors on corrige l'identité avec celle du RNIPP. Tous les champs suivant sont susceptibles d'être corrigés :

- le(s) prénom(s)
- le(s) nom(s)
- la date de naissance
- le lieu de naissance
- le sexe

Le seul champ de l'identité pivot qui n'est pas corrigé par le RNIPP est le preferred_username (qui doit désigner le nom d'usage) : l'INSEE ne renvoie pas le nom d'usage, mais seulement le nom de naissance (En revanche le RNIPP est capable de retrouver une identité à partir d'un nom d'usage).

Si l'identité renvoyée indique que la personne est décédée, L'authentification est rejetée et tracée.

3.1.1.2 Le RNIPP ne renvoit pas d'identité

Dans ce cas, l'authentification est bloquée : FranceConnect n'est pas en capacité de contrôler l'identité

Les erreurs possibles :

demande identifiée sans divergence d'état civil
demande identifiée avec divergence(s) d'état civil ou NIR
demande non identifiée mais existence d'un seul écho
demande non identifiée mais existence de plus d'un écho
demande identifiée avec le nom d'usage uniquement
demande non identifiée sans écho
demande rejetée au contrôle en raison d'erreurs de syntaxe

L'appel au RNIPP et ses résultats sont bloquants pour tous les fournisseurs d'identité. Si l'identité a été contrôlée ou validée par le RNIPP, alors l'identité de l'INSEE sera utilisé à la place de l'identité renvoyée par le fournisseur d'identité.

Les erreurs renvoyées par le RNIPP sont bloquantes (personne non trouvée, identité non redressée, personne décédée) : l'usager est renvoyé vers la mire d'authentification, avec un message d'erreur l'invitant à se connecter avec un autre fournisseur d'identité.

3.3 Génération de la clé de hachage

FranceConnect se sert des données redressées **(USER_INFO)** pour générer une clé de hachage unique par l'usager. Cette clé de hachage générée via un algorithme SHA-256 est stockée en base de donnée chez FranceConnect.

FranceConnect va également générer un sub aléatoire. Ce sub correspond au scope **<openid>** transmis au fournisseur de service pour création ou réconciliation de compte. France connect va également associer le couple sub généré / client_id du fournisseur de service à cette clé de hachage.

Un sub est unique par usager pour un fournisseur de service donné.

4. Durée de conservation des données

Les données constituant l'identité pivot ne sont pas stockées en base de données par FranceConnect, ces données sont sauvés en session côté serveur pendant une durée de 30 minutes.
Les données sont récupérés par FranceConnect à chaque connexion de l'usager.

FranceConnect conserve les trente-six mois d'historique de connexion de l'usager dans un fichier de logs et indexé via un moteur elasticsearch.
Il n'y a aucune limite de conservation des données stockées en base (clé de hachage, couples client_id/sub)