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 ii – Annexe technique – Echange de données entre le FI et FranceConnect Particuliers

Août 2018

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

Cette annexe définit les données échangées entre FranceConnect Particuliers et le Fournisseur d'Identité et la manière dont celles-ci sont traitées. 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. DEFINITION DE L'IDENTITE PIVOT

Le dispositif FranceConnect Particuliers permet aux Usagers d'utiliser les télé-services offerts par des Fournisseurs de Services après s'être identifiés et authentifiés auprès d'un Fournisseur d'identité.

FranceConnect Particuliers met en œuvre pour ce faire la cinématique du protocole OpenID Connect dite par « code autorisation » qui permet la vérification de l'identité de l'Usager, son authentification et l'échange des données qui constituent cette identité.

L'ensemble de ces données d'identité est dénommé « Identité pivot ». Cette identité est transmise par FranceConnect Particuliers au Fournisseur de Services, après vérification de son existence et de son unicité auprès du Répertoire National d'Identification des Personnes Physiques (RNIPP).

Le Fournisseur d'Identité doit renvoyer le corps HTTP <USER_INFO> d'un Usager lorsque FranceConnect Particuliers appelle le web service <FI_URL>/api/user. Les informations attendues doivent être sous la forme d'un hash (clé/valeur) au format JSON.

3. DONNEES TRANSMISES PAR LE FOURNISSEUR D'IDENTITE

3.1. Données obligatoirement transmises par le Fournisseur d'Identité

Les données à transmettre obligatoirement par le Fournisseur d'Identité sont les suivantes :

CLES (SCOPE)	FORMAT	DESCRIPTION	STANDARD OIDC
openid	string	Identifiant technique (sub) de l'utilisateur au format OpenID Connect	OUI
given_name	string	Prénoms de la personne, séparés par des espaces selon le standard OpenID Connect	OUI
family_name	string	Nom de naissance de la personne	OUI
gender	string	Sexe de la personne, male / female	OUI
birthcountry	string	Pays de naissance de la personne, au format code INSEE	NON
birthdate	string	Date de naissance de la personne, au format YYYY-MM-DD	OUI
birthplace	string	Ville de naissance de la personne, code INSEE du lieu de naissance ou chaîne vide si la personne est née à l'étranger	NON
email	string	Adresse e-mail de la personne	OUI

3.2. Autres données pouvant être transmises par le Fournisseur d'Identité

Dans le cas où les données suivantes sont à la disposition du Fournisseur d'Identité, celles-ci doivent également être transmises :

CLES (SCOPE)	FORMAT	DESCRIPTION
preferred_username	string	Nom d'usage de la personne
address	string	Adresse postale de la personne
phone	string	Numéro de téléphone de la personne

4. TRANSFERT DES DONNEES PIVOT DU FOURNISSEUR D'IDENTITE A FRANCECONNECT PARTICULIERS

1. Après récupération des USER_INFO auprès du Fournisseur d'Identité, FranceConnect Particuliers effectue un appel au RNIPP afin de vérifier l'identité de l'Usager transmise par le Fournisseur d'Identité. Le RNIPP est un instrument de vérification de l'état civil des personnes maintenu par l'Institut National de la Statistique et des Etudes Economiques (INSEE[1]).

2. FranceConnect Particuliers peut ensuite ajustés les attributs de l'identité reçue du Fournisseur d'Identité afin de les aligner avec l'identité retournée par le RNIPP avant leur transmission au Fournisseur de Services.
    - Si l'appel au RNIPP renvoie une identité, alors celle-ci est utilisée par FranceConnect Particuliers afin de corriger les attributs d'identité transmis par le Fournisseur d'Identité en cas de valeurs divergentes. Tous les champs suivants 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 suite à l'appel au RNIPP est le « preferred_username » (nom d'usage). L'INSEE ne renvoie pas le nom d'usage, mais seulement le nom de naissance. Cependant, 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.
      En cas de doublon (deux Usagers ayant la même identité pivot), l'Usager ne pourra pas se connecter du fait de l'impossibilité d'obtenir l'unicité de son identité pivot.
    - Si l'appel au RNIPP ne renvoie pas d'identité, l'authentification est bloquée : FranceConnect Particuliers n'est pas en capacité de contrôler l'identité.

Remarques :

- Les codes retour transmis par l'INSEE suite à un appel au RNIPP :
    - 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 utilisée 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.

[1] http://www.insee.fr/fr/themes/detail.asp?ref_id=fd-etatcivil2010&page=fichiers_detail/etatcivil2010/presentation.htm

5. GENERATION DE LA CLE DE HACHAGE

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

FranceConnect Particuliers génère également un sub aléatoire. Ce sub correspond au scope **<openid>** transmis au Fournisseur de Services pour la création ou réconciliation de compte.
FranceConnect Particuliers associe également le couple sub généré / client_id du Fournisseur de Services à cette clé de hachage. Un sub est unique par Usager pour un Fournisseur de Services donné.

6. DUREE DE CONSERVATION DES DONNEES

Les données constituant l'identité pivot ne sont pas stockées en base de données par FranceConnect Particuliers, ces données sont sauvées en session côté serveur pendant une durée de 30 minutes.

Les données sont récupérées par FranceConnect Particuliers à chaque connexion de l'Usager.

FranceConnect Particuliers conserve les trente-six mois d'historique de connexion de l'Usager dans un fichier de logs et indexé via un moteur ElasticSearch.

En l'absence de connexion de l'usager pendant une durée de trente-six mois, les données stockées en base (clé de hachage, couples client_id/sub) sont supprimées.

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