Direction interministérielle du numérique et du système d'information et de communication de l'Etat

Conditions générales d'utilisation du service FranceConnect Particuliers par les Fournisseurs de Services

Annexe sécurité

Février 2019

Table des matières

1. OBJET DE LA PRESENTE ANNEXE

La présente annexe a pour objet de décrire les exigences et recommandations de sécurité relatives aux échanges entre FranceConnect Particuliers et les Fournisseurs de Services, tous deux désignés comme « les Parties » dans la suite du document.

Elle rappelle en outre les engagements attendus en matière de protection des données à caractère personnel, de confidentialité et de respect du Référentiel Général de Sécurité (RGS).

Elle s'inscrit en complément des Conditions Générales d'Utilisation du service FranceConnect Particuliers par les Fournisseurs de Services et ne saurait être prise isolément.

2. EXIGENCES RELATIVES AU FOURNISSEUR DE SERVICES

2.1. Exigences de sécurité relatives au protocole OpenID Connect

Le Fournisseur de Services met en œuvre les mesures de sécurité techniques et organisationnelles nécessaires afin d'assurer, sur son périmètre :

- La non divulgation des données fonctionnelles et techniques échangées dans le cadre du protocole à un tiers non autorisé ;
- La mise en place de mesures afin de prévenir leur fuite en cas d'intrusion ;
- La confidentialité et l'intégrité des secrets échangés (mots de passe, clés cryptographiques).

Le Fournisseur de Services répond par ailleurs aux exigences suivantes :

- Mettre en œuvre les mesures de sécurité nécessaires afin d'assurer le stockage sécurisé du secret permettant l'authentification du client OpenID Connect.
- Générer le paramètre *state* aléatoirement en utilisant une fonction de génération de caractères aléatoires sécurisée et avec une entropie équivalente à 100 bits (minimum 16 caractères avec un alphabet de 70 caractères différents). Le paramètre *state* transmis dans la requête de demande d'autorisation est obligatoire afin de contrer les attaques CSRF. Il est retransmis dans les paramètres de l'URL de retour et sa concordance doit être vérifiée avec la valeur stockée dans la session de l'utilisateur.
- Valider systématiquement toutes les données en entrée, si possible par l'utilisation de listes blanches, pour empêcher par exemple leur manipulation en insérant des caractères spécifiques, en particulier, valider les codes d'autorisation, les jetons d'accès et le contenu de l'identité pivot (user_info).
- Générer le paramètre *nonce* aléatoirement en utilisant une fonction de génération de caractères aléatoires sécurisée et une entropie équivalente à 100 bits (minimum 16 caractères avec un alphabet de 70 caractères différents). Le paramètre *nonce* transmis dans la requête de demande d'autorisation est obligatoire afin de contrer le rejeu de requête. Il est retransmis dans le jeton nommé token_id retourné par FranceConnect Particuliers lors de la récupération du jeton d'accès. Sa concordance doit être vérifiée avec la valeur stockée dans la session de l'utilisateur.
- Vérifier le haché d'authentification grâce au secret du jeton d'authentification token_id et les informations qu'il contient :
    - Le paramètre « aud » doit contenir le client_id,
    - Le paramètre « exp » correspondant à l'expiration de l'authentification ne doit pas être expiré,
    - Le paramètre « nonce » doit correspondre à celui fourni dans la requête de demande d'authentification,
    - Le paramètre « iss » doit contenir le nom de domaine de France Connect,
    - Le paramètre « acr » doit contenir le niveau eIDAS précédemment fourni lors de la requête d'authentification et conservé avec la session de l'utilisateur.
- Vérifier le nom de domaine du serveur retourné avec celui utilisé pour l'appel serveur à serveur (appel FS ←→ FD).

2.2. Veille et sensibilisation

Le Fournisseur de Services met en œuvre sur son périmètre une veille avancée afin de détecter les velléités d'attaques cyber criminelles sur les services en lien avec FranceConnect Particuliers (FCP). En cas d'attaque, il s'engage à alerter FranceConnect Particuliers et l'ensemble des partenaires de la chaîne de sécurité.

Le Fournisseur de Services forme et sensibilise les acteurs sous son autorité à la sécurité et aux enjeux de FranceConnect Particuliers (notamment les développeurs et à la cible les agents utilisant FCP).

2.3. Recommandations globales quant à l'implémentation sécurisée des services numériques

Il est recommandé au Fournisseur de Services de s'appuyer sur les recommandations ANSSI pour la sécurisation des applications web (note technique No DAT-NT-009/ANSSI/SDE/NP), en particulier :

- Appliquer les principes de défense en profondeur aux architectures logicielles et matérielles des applications. La mise en œuvre de ses principes par des mesures adéquates est à étudier dès l'étape de conception, au vu des risques et menaces auxquels sera exposée l'application.
- Sécuriser le processus d'administration via des protocoles sécurisés et restreindre les tâches d'administration aux seuls postes d'administration dûment authentifiés et habilités.
- Appliquer le principe du moindre privilège à l'ensemble des éléments du système (« tout ce qui n'est pas autorisé explicitement est par défaut interdit »).
- Contrôler systématiquement les données en entrée des requêtes, qu'elles soient fonctionnelles ou techniques et quel que soit leur provenance.
- Mettre en place des mécanismes permettant de s'assurer de la légitimité de la requête (l'inclusion des pages dans des « iframe » est proscrite).

3. EXIGENCES RELATIVES A FRANCECONNECT PARTICULIERS

3.1. Conformité réglementaire

Le service FranceConnect Particuliers a fait l'objet d'une déclaration auprès de la CNIL (Délibération 2015-254 du 16 juillet 2015). Une extension du champ d'application et des destinataires a été validée par la CNIL (Délibération 2018-164 du 24 mai 2018).
Parallèlement, la DINSIC poursuit sa démarche d'homologation RGS et mène un système de management de la sécurité de l'information sur le téléservice.

3.2. Mesures de sécurité

FranceConnect Particuliers met en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin de protéger les données traitées et stockées dans le cadre du service, et ce au regard des objectifs de sécurité identifiés suite à l'analyse des risques de sécurité. Ces mesures concernent en particulier :

- Le contrôle systématique de tous les paramètres en entrée des requêtes afin de réduire le risque d'injection. FranceConnect Particuliers met en œuvre des mécanismes de blocage des clients en cas d'échecs répétés afin d'éviter les attaques par force brute. Cette mesure peut aller jusqu'à la déconnexion d'un fournisseur en cas de menace critique.
- La robustesse des secrets, leur stockage et leur transmission sécurisés.
- De manière générale : l'application des principes de défense en profondeur, notamment en matière de gestion des droits d'accès aux différents composants du système (reverse proxies, serveurs d'application et de données, etc.).

3.3. Gestion des incidents

FranceConnect Particuliers offre aux Fournisseurs de Services un support en cas d'incident, conformément à l'Annexe qualité de service et chaîne de support.

4. GLOSSAIRE

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
DINSIC	Direction Interministérielle du Numérique et des Systèmes d'Information et de Communication
FCP	FranceConnect Particuliers
FD	Fournisseur de Données
FI	Fournisseur d'Identité
FS	Fournisseur de services
RGS	Référentiel Général de Sécurité
SSI	Sécurité des Systèmes d'Information

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Direction interministérielle du numérique et du système d'information et de communication de l'État

Direction interministérielle du numérique et du système d'information et de communication de l'Etat

20 Avenue de Ségur
TSA 30719
75334 Paris CEDEX 7

www.franceconnect.gouv.fr