ANNEXE SECURITE DES CONDITIONS GÉNÉRALES D'UTILISATION DU SERVICE FRANCECONNECT PAR LES FOURNISSEURS DE SERVICE

1. Objet de la présente annexe

La présente annexe a pour objet de décrire les exigences et recommandations de sécurité relatives aux échanges entre FranceConnect et les fournisseurs de service, 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).

2. Engagements du Fournisseur de Service

Les obligations en matière de sécurité et de confidentialité des données à caractère personnel le cas échéant devront être répercutées aux éventuels prestataires ou sous-traitants des Parties ayant accès à ces données dans le cadre de l'administration, la maintenance et l'exploitation de FranceConnect Particulier Sphère Publique.

Il appartient au Fournisseur de Service de mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment dans le cadre de la transmission de ces données au travers d'un réseau non sécurisé, ainsi que contre toute autre forme de traitement illicite.

a. Exigences de sécurité relatives au protocole OpenID Connect

Le Fournisseur de Service 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 prévenir leur fuite en cas d'intrusion,
- la confidentialité et l'intégrité des secrets échangés (mots de passe, clés cryptographiques).

Le Fournisseur de Service répond par ailleurs aux exigences suivantes :

- Mettre en œuvre les mesures de sécurité nécessaires afin d'assurer le stockage sécurisé du client secret et du client Open Id Connect,
- 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 : vérifier le format des jetons d'autorisation et d'accès (token_Id),
- vérifier le paramètre *nonce* du jeton d'accès. Ce dernier est rendu obligatoire lors de l'appel à FranceConnect afin d'éviter le rejeu des requêtes,
- vérifier la date d'expiration du jeton d'accès,
- vérifier le nom de domaine du serveur retourné avec celui utilisé pour l'appel serveur à serveur (appel FS <->FD)

Il relève de la responsabilité du Fournisseur de Service de réaliser régulièrement des revues de code et des tests d'intrusion sur ses applications afin de détecter les failles potentielles.

b. <u>Veille et sensibilisation</u>

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

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

c. <u>Recommandations globales quant à l'implémentation sécurisée des services numériques</u>

Il est recommandé au Fournisseur de Service 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

3. Engagements de FranceConnect

a. Mesures de sécurité

FranceConnect 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 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 ainsi que leur renouvellement régulier
- 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.)