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

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

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 d'Identité (FI), tous deux désignés comme « les Parties » dans la suite du document.

Elle présente en outre :

- Les mesures attendues du Fournisseur d'Identité au regard des exigences du règlement e-IDAS relatives aux moyens d'identification électronique dans l'espace de l'Union Européenne,
- Les mesures de sécurités attendues de chacune des Parties dans le cadre de la mise en place de FranceConnect Particuliers.

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. ARCHITECTURE

FranceConnect Particuliers met en œuvre le protocole OpenID Connect. Celui-ci permet à des clients (applications et services), d'accéder à l'identité des utilisateurs finaux, par l'intermédiaire d'un serveur d'autorisation opéré par un tiers dit fournisseur OpenID Connect. Ainsi, FranceConnect Particuliers est client OpenID vis-à-vis du Fournisseur d'Identité qui lui-même se positionne comme fournisseur OpenID.

Il appartient au Fournisseur d'Identité de mettre en place les API et réaliser les développements nécessaires à son intégration en tant que fournisseur Open ID Connect. Il s'appuie pour cela sur les recommandations formalisées par FranceConnect Particuliers.

FranceConnect Particuliers met à disposition le portail développeur https://franceconnect.gouv.fr/ afin de fournir l'ensemble des ressources nécessaires à l'intégration du produit FranceConnect Particuliers.

Il est par la suite de la responsabilité du Fournisseur d'Identité de s'adapter aux évolutions éventuelles du dispositif FranceConnect Particuliers, que celles-ci soient liées au protocole OpenID ou non.

3. EXIGENCES RELATIVES AU FOURNISSEUR D'IDENTITE

3.1. Niveaux de garantie e-IDAS des moyens d'identification électronique du Fournisseur d'Identité

Le Fournisseur d'identité peut offrir un ou plusieurs moyens d'identification électronique correspondant chacun à un niveau de garantie donné, au sens du règlement eIDAS. Trois niveaux garantissant un degré croissant de fiabilité à l'identité d'une personne sont ainsi définis à l'article 8 du règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 : faible, substantiel et élevé.

A chacun de ces niveaux est associé, par le biais du règlement d'exécution 2015/1502 du 8 septembre 2015, un ensemble de spécifications techniques et de procédures minimales qui couvrent tout le cycle de vie des moyens d'identification électronique et dont l'objectif est de réduire plus ou moins significativement les risques d'usurpation ou d'altération de l'identité.

Sur la base des règles minimales définies dans ce règlement d'exécution 2015/1502, l'ANSSI établit les exigences applicables à chaque niveau de garantie des moyens d'identification électronique notifiés par la France. L'ANSSI contrôle le respect de ces exigences par les Fournisseurs d'Identité.
Le Fournisseur d'Identité doit s'adresser à l'ANSSI pour procéder à l'évaluation du niveau de garantie atteint par le ou les moyens d'identification électronique qu'il délivre.

Une fois l'identification et authentification de l'Usager effectuées, le Fournisseur d'Identité transmet à FranceConnect Particuliers le niveau e-IDAS du moyen d'identification / authentification utilisé (faible, substantiel, élevé) par le biais du paramètre « acr » du Token Id. FranceConnect Particuliers transmet ensuite ce paramètre sans l'altérer au Fournisseur de Services (FS).

3.2. Mesures de sécurité – Considérations générales

Le Fournisseur d'Identité 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 protection de ces données contre toute attaque, tout incident accidentel ou malveillant ;
- La confidentialité et l'intégrité des secrets échangés (mots de passe, clés cryptographiques).

Pour cela, il s'appuie sur les recommandations pour la sécurisation des sites Web de l'ANSSI (cf. bonnes pratiques ANSSI : Sécuriser un site web).

Il relève ainsi de la responsabilité du Fournisseur d'Identité de :

- Réaliser régulièrement des revues de code et des tests d'intrusion sur ses services d'identification électronique afin de détecter les failles potentielles,
- S'assurer que les mesures techniques et les procédures adéquates sont déployées afin de protéger les moyens d'identification qu'il traite et stocke, ceci durant tout leur cycle de vie : création, activation, délivrance, révocation,
- Faire appel à des prestataires qualifiés pour les audits de sécurité (PASSI).

Dans l'architecture OpenID mise en œuvre, le Fournisseur d'Identité assure le rôle de fournisseur (provider) OpenID Connect vis-à-vis de FranceConnect Particuliers qui sollicite ses serveurs d'autorisation et d'accès en tant que client OpenID.
En complément de ces mesures, le Fournisseur d'identité se reportera aux « Security Considerations[1] » relatives au protocole OpenID Connect ainsi que celles propres à OAuth 2.0 dont il dérive et les mettra en œuvre.

[1] http://openid.net/specs/openid-connect-core-1_0.html#Security

3.3. Protection relative aux redirections

Lors des redirections, le Fournisseur d'Identité vérifie la présence des paramètres suivants :

- L'identifiant client FranceConnect Particuliers ;
- L'URL de redirection ;
- Le paramètre « nonce » : caractères générés de manière non prédictible soit au moins 32 octets générés à l'aide d'un générateur aléatoire cryptographique et haché à l'aide d'une fonction de hachage respectant le Référentiel Général de Sécurité (RGS) tel que SHA-256 ;
- Le paramètre « state » : caractères générés de manière non prédictible soit au moins 32 octets à l'aide d'un générateur aléatoire cryptographique et haché à l'aide d'une fonction de hachage respectant le Référentiel Général de Sécurité tel que SHA-256.

Le Fournisseur d'Identité vérifie l'existence de l'identifiant de l'application cliente FranceConnect Particuliers ainsi que la correspondance avec l'URL de redirection qui aura été fournie lors de son enregistrement, ceci afin d'éviter des redirections vers une URL d'un site malicieux.

Toute requête non conforme est refusée.

Le paramètre « state » doit être transmis à l'application cliente FranceConnect Particuliers par le Fournisseur d'Identité lors de la redirection vers l'URL de celle-ci.
Le paramètre « nonce » doit être transmis à l'application cliente FranceConnect Particuliers par le Fournisseur d'Identité dans le jeton d'authentification généré par celui-ci.

3.4. Protection des communications serveur à serveur

Afin de réduire les risques d'usurpation d'identité, le Fournisseur d'Identité implémentant OpenId Connect doit authentifier le client FranceConnect Particuliers à l'aide d'un certificat conforme au Référentiel Général de Sécurité.

FranceConnect Particuliers envoie au Fournisseur d'Identité, lors de la demande de jeton, un paramètre client_secret OpenID Connect confidentiel, par un canal différent de la fourniture de l'identifiant client. Ce mot de passe est renouvelé tous les ans.

Le Fournisseur d'Identité doit :

- Utiliser un mot de passe avec une bonne complexité, équivalente au minimum à une entropie de 100 bits (cf. l'annexe B3 du Référentiel Général de Sécurité) ;
- Implémenter des mécanismes de blocage des clients en cas d'échecs répétés d'authentification afin d'éviter les attaques par force brute ;
- Respecter la note technique sur les recommandations de sécurité relatives aux mots de passe de l'ANSSI.

3.5. Confidentialité des échanges

La sécurité du protocole OpenId Connect est basée sur la confidentialité des échanges entre l'application cliente FranceConnect Particuliers et le Fournisseur d'Identité.
Pour cela, le Fournisseur d'Identité doit :

- Forcer l'utilisation de la version de TLS la plus récente pour les communications chiffrées ;
- Configurer les suites cryptographiques robustes selon les règles du Référentiel Général de Sécurité ;
- Utiliser des certificats serveurs conformes au Référentiel Général de Sécurité.

3.6. Protection des codes d'autorisation et d'accès

3.6.1 Codes d'autorisation

Le code d'autorisation doit :

- Etre généré de manière non prédictible soit au moins 32 octets à l'aide d'un générateur aléatoire cryptographique et haché à l'aide d'une fonction de hachage respectant le Référentiel Général de Sécurité tel que SHA-256 ;
- Etre lié à l'identifiant client OpenId Connect fourni à FranceConnect Particuliers.

Le Fournisseur d'Identité vérifie lors de la récupération du jeton d'accès que le code d'autorisation appartient bien à FranceConnect Particuliers.

Afin de limiter l'impact en cas de vol, par exemple à la suite d'une attaque par injection NoSQL ou SQL sur la base stockant les codes autorisation, il est recommandé de :

- Stocker les codes de manière sécurisée sous format haché, afin de les rendre inexploitables en employant pour ce faire un algorithme de hachage respectant le Référentiel Général de Sécurité tel que SHA-256 (ex : SHA256) ;
- De manière générale, observer les meilleures pratiques en matière de développement et d'administration, comme par exemple :
    - Appliquer le principe de moindre privilège pour tout accès à la base et prévoir des rôles distincts (administrateur, propriétaire des données, utilisateur simple, etc.) ;
    - Eviter les requêtes dynamiques ;
    - Renforcer l'accès aux fichiers de configuration des serveurs ;
    - Verrouiller l'accès aux informations de configuration du serveur de base de données.

Afin de limiter les risques de rejeu, il est recommandé de :

- Limiter dans le temps la durée de vie du code autorisation et de choisir une durée d'expiration la plus courte possible ;
- Rendre obligatoire l'utilisation du paramètre « nonce » dans les requêtes d'autorisation.

Afin de pallier aux attaques par force brute ou dictionnaire, le Fournisseur d'Identité doit limiter le nombre de codes autorisation erronés.

3.6.2 Jetons d'accès

L'interception d'un jeton d'accès par un tiers non autorisé peut permettre à ce dernier d'accéder à des ressources pour lesquelles il n'est pas habilité. Ces jetons sont donc des données confidentielles et doivent bénéficier de mesures de protection appropriées.

De même que pour les codes d'autorisation, le Fournisseur d'Identité doit implémenter les mesures de sécurité adéquates pour la génération, le stockage et l'échange sécurisés de ces jetons. Les bonnes pratiques en matière de développement et d'administration de la base de persistance des jetons s'appliquent également ici (cf. bonnes pratiques ANSSI : Sécuriser un site web).

De la même manière, le Fournisseur d'Identité doit valider tous les paramètres en entrée de la requête de demande de jeton d'accès, si possible par l'utilisation de listes blanches et d'expressions régulières. En particulier, le serveur de jeton d'accès du Fournisseur d'Identité vérifie systématiquement le mot de passe envoyé par FranceConnect Particuliers. Ce modèle de sécurité positif (liste blanche), où seules les requêtes correspondant au fonctionnement légitime de l'application sont acceptées, apporte une meilleure sécurité au prix d'une configuration plus complexe.

Le jeton d'accès doit :

- Etre généré de manière non prédictible soit au moins 32 octets à l'aide d'un générateur aléatoire cryptographique et haché à l'aide d'une fonction de hachage respectant le Référentiel Général de Sécurité tel que SHA-256 ;
- Etre lié à l'identifiant client OpenId Connect fourni à FranceConnect Particuliers ;
- Etre stocké de manière sécurisée sous format haché, afin de les rendre inexploitables en employant

pour ce faire un algorithme de hachage respectant le Référentiel Général de Sécurité tel que SHA-256 (exemple : SHA256).

3.6.3 Durée de vie de la session

La durée de la session utilisateur chez le Fournisseur d'Identité ne doit pas excéder **deux minutes**.

3.7. Protection contre les injections SQL et NoSQL

Il est recommandé que toutes les entrées (paramètres ou entêtes HTTP) manipulées par le Fournisseur d'Identité, qu'elles soient transmises dans l'URL de redirection, dans les requêtes ou réponses d'appel serveur à serveur, soient validées grâce à une liste blanche de caractères n'autorisant que ceux qui la composent.
Voici quelques exemples de validation de paramètres :

- *response_type* : uniquement les valeurs autorisées par le Fournisseur de Services soit par exemple uniquement "*code*" s'il s'agit de la seule cinématique possible ;
- *client_id* : uniquement les chiffres [0-9] et les lettres de l'alphabet [a-z] sont autorisés ;
- le code d'autorisation : par exemple encodé en hexadécimal, seuls les chiffres [0-9] et les lettres de l'alphabet [a-z] sont autorisés ;
- *state* et *nonce* : par exemple uniquement des chiffres [0-9] et des lettres de l'alphabet [a-z] sont autorisés ;
- *redirect URI* : URI encodé, donc uniquement les chiffres [0-9], les lettres de l'alphabet [a-zA-Z] et les caractères non réservés "-._~" sont autorisés ;
- *header* : autorisation contenant le jeton d'accès, uniquement les chiffres [0-9] et les lettres de l'alphabet [a-z] sont autorisés.

Les requêtes SQL doivent être paramétrées et typées, par exemple en JAVA, avec l'utilisation de la classe PreparedStatement et des méthodes setInt, setString, etc.

4. EXIGENCES RELATIVES A FRANCECONNECT PARTICULIERS

Au regard de son rôle de client OpenID Connect vis-à-vis du Fournisseur d'Identité, 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.

4.1. Mesures techniques

Dans le cadre des cinématiques impliquant le Fournisseur d'Identité, FranceConnect Particuliers met en place les mesures suivantes :

- Utilisation du paramètre « state » afin de lier les requêtes client et pallier aux attaques de types Cross-Site Request Forgery qui peuvent permettre à un attaquant de faire exécuter à un utilisateur des actions à son insu ;
- Utilisation du paramètre « nonce » dans les requêtes d'autorisation afin d'éviter les rejeux.

4.2. Gestion des incidents

FranceConnect Particuliers offre aux Fournisseurs d'Identité un support en cas d'incident ou d'alerte sécurité, conformément à l'Annexe iv - Annexe qualité de service et chaîne de support.

5. GLOSSAIRES

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information.
DINSIC	Direction Interministérielle du Numérique et des Systèmes d'Information et de Communication
FI	Fournisseur d'Identités
FS	Fournisseur de Services
RGS	Référentiel Général de Sécurité

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