PREMIER MINISTRE

Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Agent Connect

Conditions Générales d'Utilisation du service AgentConnect pour les Fournisseurs de services :

Annexe

Public

v.1.3

Propriétés du document

	Identité	Date
Rédacteur	Elodie BOUDOUIN	25/03/2021
Contrôleur	Christine BALIAN	06/05/2021
Approbateur	Nadi BOU HANNA	28/05/2021

Version du document

Version	Résumé des modifications	Modifié par	Date
v1.0	Création du document	DINUM	28/05/2021
v1.1	Mise à jour du bouton de connexion AgentConnect (cf. p5)	DINUM	21/10/2021
v1.2	Mise à jour des règles de sécurité state et nonce + correction typo AgentConnect	DINUM	10/02/2022
V1.3	Intégration des formulaires Datapass dans le processus d'implémentation	DINUM	10/06/2022

Liste de diffusion

Destinataire	Poste	Société
L'ensemble des Partenaires Fournisseurs de services au sein de la fonction publique d'Etat (administrations centrales, services déconcentrés) et des opérateurs de l'Etat présents dans les annexes générales au projet de loi de finances de l'année.		

Table des matières

1. OBJET DU DOCUMENT

La présente Annexe complète les Conditions générales d'utilisation des Fournisseurs de services du Service AgentConnect, dont elle fait intégralement partie.

2. DESCRIPTION FONCTIONNELLE D'AGENTCONNECT

AgentConnect est un dispositif d'identification et d'authentification pour les agents exerçant au sein de la fonction publique d'Etat (administrations centrales, services déconcentrés) et des opérateurs de l'Etat.

C'est un service proposé par la DINUM qui permet aux agents de se connecter à des services applicatifs métiers en ligne proposés par des Fournisseurs de services autorisés préalablement. AgentConnect s'appuie sur des comptes d'identité numérique vérifiés par ses partenaires Fournisseurs d'identité.

Ce service se matérialise par un bouton de connexion « AgentConnect » :

Les Fournisseurs de services ne peuvent demander qu'un niveau de garantie 1, soit un niveau de sécurité faible, au service AgentConnect alors que les Fournisseurs d'identité peuvent mettre à disposition les 3 niveaux d'authentification définis dans les conditions générales d'utilisation.

3. PREREQUIS A RESPECTER PAR AGENTCONNECT

3.1. Mesures de sécurité

Au regard de son rôle de client OpenID Connect vis-à-vis du Fournisseur de services, AgentConnect 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 d'impact sur la protection des données (AIPD) réalisée par la DINUM.

AgentConnect met en œuvre le protocole OpenID Connect selon les spécifications décrites sur http://openid.net/specs/openid-connect-core-1_0.html comme devant être appliquées par le Fournisseur de services.

AgentConnect 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. AgentConnect 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 de service 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.).
- Une signature robuste des données d'identité échangées entre le Fournisseur de services et le Service AgentConnect.

3.2. Gestion du SSO

La fonction de SSO (Single Sign On) n'est pas active à ce stade sur AgentConnect. Les Fournisseurs d'identités sont libres d'en posséder une.

3.3. Connaissance entre Fournisseurs d'identité et Fournisseurs de services

Lors de la cinématique d'AgentConnect, le Fournisseur d'identité connaîtra le Fournisseur de services qui souhaite disposer des données de l'agent. Le Service AgentConnect renverra également le nom du Fournisseur de services au Fournisseur d'identité.

3.4. Qualité de service

AgentConnect met en œuvre les moyens nécessaires pour assurer des performances et une disponibilité efficientes du Service AgentConnect. Cette disponibilité est dépendante de celles des Fournisseurs d'identité ainsi que du taux de disponibilité fourni par le Cloud Nubo de la DGFIP qui héberge le Service AgentConnect ; la DGFIP s'engage à hauteur de 98 % sur la plage horaire 8h-20h (jours ouvrés).

En cas d'indisponibilité du Service, AgentConnect interviendra afin d'en identifier l'origine et s'efforcera d'en tenir informés ses Partenaires dans les meilleurs délais.

Le dysfonctionnement à l'origine de l'indisponibilité peut avoir les conséquences suivantes :

- Le Fournisseur d'identité est indisponible.
- La page AgentConnect n'est pas accessible.

Outre les moyens mis en place pour garantir la disponibilité du Service AgentConnect, un suivi des incidents d'exploitation (y compris les incidents de sécurité) sera mis en place.

3.5. Données de traçabilité AgentConnect

Les traces de connexion sont conservées dans des logs de connexion qui comprennent :

- Adresse IP et port source de la connexion,
- Dates et heures de connexion au service,
- Le site du FS,
- Le FI utilisé,
- Le niveau de garantie du FI (niveau 1 : faible, niveau 2 : renforcé, niveau 3 : fort)
- SUB FI,
- SUB FS,
- Account ID.

3.6. Maintenance applicative

AgentConnect met en œuvre les moyens permettant de traiter les anomalies applicatives et les évolutions nécessaires à son fonctionnement selon l'état de l'art.

L'application AgentConnect est conçue de sorte que les maintenances et les évolutions applicatives soient opérées, dans la mesure du possible, sans interruption de service.

AgentConnect fait ses meilleurs efforts pour résoudre les anomalies critiques liées à une nouvelle mise en production dans les meilleurs délais après la prise en compte de l'anomalie.

AgentConnect n'assure pas la maintenance des applications localisées chez les Fournisseurs de services ni auprès des agents utilisateurs.

3.7. Exploitation technique

AgentConnect met en œuvre les moyens permettant le maintien en condition opérationnelle, le maintien en condition de sécurité et la supervision applicative et technique de la plateforme sur laquelle repose le Service et ce, conformément aux conditions fixées à la présente Annexe.

La plateforme AgentConnect est conçue de sorte que les opérations de maintenances soient réalisées avec un minimum d'interruption de service.

3.8. Support mis à disposition des Fournisseurs de services

Le Support DINUM mis à disposition des Fournisseurs de services regroupe :

- Le niveau 2 : ensemble des demandes qui ne concernent pas des problématiques techniques (enrôlement, …)
- Le niveau 3 : résolution des incidents techniques qui nécessitent l'intervention d'un développeur.

Le Support AgentConnect n'a pas vocation à avoir contact avec l'agent utilisateur puisque c'est de la responsabilité du Fournisseur de services.

Le Support AgentConnect mis à disposition des Fournisseurs de services est assuré du lundi au vendredi de 9h30 à 18h00 (hors jours fériés).

A chaque demande d'assistance, le Fournisseur de services doit écrire à : support.partenaires@agentconnect.gouv.fr.

Dès réception, la demande est référencée dans la base de ticketing. Le Support AgentConnect s'engage à la traiter dans les 48 heures ouvrées.

L'analyse du ticket permet d'y associer un niveau de priorité. Après affectation du niveau de priorité, l'équipe Support AgentConnect s'engage à traiter l'incident dans un temps imparti. Néanmoins, chaque niveau de priorité possède une échéance qui donnera lieu à une escalade si le problème n'est toujours pas résolu.

La DINUM s'engage à informer le Fournisseur de services à chaque évènement de niveau critique ou majeur impactant celui-ci.

NIVEAU DE PRIORITE	DESCRIPTION	DUREE TOTALE DE TRAITEMENT EN JOURS OUVRES	RESPONSABLE DINUM
1 (Critique)	- Le système ne fonctionne plus. - Le service n'est plus assuré. - Le service ne peut être relancé sans la résolution complète et définitive du problème. - Un problème de sécurité.	2 jours	Responsable de la production, Responsable produit AgentConnect
2 (Majeure)	- Le système est opérationnel mais ne fonctionne que grâce aux dispositifs des systèmes de secours. - Les temps de réponse sont fortement affectés.	2 jours	Responsable produit AgentConnect, Responsable produit AgentConnect
3 (Normal)	- Le service est opérationnel mais présente des réductions de fonctionnalités ou des dysfonctionnements. - Les temps de réponse sont fortement dégradés.	5 jours	Responsable produit AgentConnect
4 (Mineure)	- Les fonctionnalités majeures du service ne sont pas touchées. - Aucun dysfonctionnement critique n'existe mais les temps de réponse peuvent être partiellement affectés avec des fonctionnalités pouvant apparaître de façon réduite au vu de l'agent utilisateur.	5 jours	Responsable des relations partenaires, Responsable produit AgentConnect
5 (Info)	- Le service fonctionne parfaitement. - La question ne concerne pas un dysfonctionnement de l'application AgentConnect. - Il s'agit simplement d'une demande d'information de la part d'un fournisseur (de service ou d'identité)).	8 jours	Responsable des relations partenaires

Figure 1 : Durée de traitement d'un incident en fonction de sa priorité et identification des personnes responsables DINUM

Les conditions de fermeture d'un ticket sont les suivantes :

- Une demande d'assistance (ticket) sera fermée par le service Support AgentConnect si celle-ci est résolue avec la confirmation verbale ou écrite du Fournisseur de services.
- Un ticket pour un objet non résolu sera fermé si les deux parties en conviennent.
- Un ticket sera fermé par le service Support AgentConnect en cas d'absence de réactivité ou de non-collaboration du Fournisseur de service à fournir les informations nécessaires permettant sa résolution.

- Un ticket sera fermé par la DINUM lorsque celui-ci sera résolu par la DINUM, notifié au Fournisseur de services.

3.9. Protection des communications de serveur à serveur

AgentConnect doit fournir au Fournisseur de services un identifiant client (Client ID OpenIDConnect) et un secret (Client Secret OpenIDConnect) pour l'authentifier. L'identifiant client et le secret sont communiqués au Fournisseur de services sur des canaux différents et de manière sécurisée.

Le secret doit avoir une complexité équivalente à une entropie au minimum de 256 bits et renouvelé tous les trois ans.

4. PREREQUIS A RESPECTER PAR LE FOURNISSEUR DE SERVICES

4.1. Protocole technique et sécurité

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 256 bits (32 octets avec un alphabet de 256 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 256 bits (32 octets avec un alphabet de 256 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 AgentConnect 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 AgentConnect,
    - Le paramètre « acr » doit contenir le niveau de garantie (faible, renforcé, élevé) 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.

4.2. 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 le Service AgentConnect. En cas d'attaque de sécurité en lien avec le Service AgentConnect, il s'engage à alerter AgentConnect dans les plus brefs délais.

Le Fournisseur de services forme et sensibilise les acteurs sous son autorité à la sécurité et aux enjeux d'AgentConnect (notamment les développeurs et à la cible les agents utilisant AgentConnect).

4.3. Recommandations globales d'implémentation sécurisée

Les Fournisseurs de services peuvent 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 quelle 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).

4.4. Fonction Support du Fournisseurs de services

Le Fournisseur de services met à disposition un support accessible à ses agents utilisateurs.

4.5. Confidentialité des échanges

La sécurité du protocole OpenID Connect est basée sur la confidentialité des échanges entre le Service AgentConnect et le Fournisseur de services.

Pour cela, le Fournisseur de services doit :

- Utiliser la version de TLS préconisée par AgentConnect pour les communications chiffrées ;
- Configurer les suites cryptographiques robustes selon les règles du Référentiel Général de Sécurité ;

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

4.6.1 Codes d'autorisation

OPEN ID recommande que le code d'autorisation transmis aux fournisseurs de services par le Service AgentConnect soit généré de manière non prédictible soit au moins 32 octets à l'aide d'un générateur (avec un CSPR) aléatoire cryptographique et haché à l'aide d'une fonction de hachage respectant le Référentiel Général de Sécurité tel que SHA-256.

Le Service AgentConnect vérifie lors de la récupération du jeton d'accès que le code d'autorisation appartient bien au Fournisseur de services.

Le Fournisseur de services doit sécuriser le stockage des codes d'autorisation fournis par le Service AgentConnect. En cas de compromission de ces codes, il doit prévenir la DINUM dans les plus brefs délais. La DINUM procèdera alors à la révocation des codes d'autorisation compromis et en génèrera de nouveaux pour le Fournisseur de services concerné.

4.6.2 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 de services doit implémenter les mesures de sécurité adéquates pour 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).

Le Service AgentConnect vérifie systématiquement le jeton d'accès envoyé par le Fournisseur de services lors de chaque demande d'accès à des ressources proposées par le Service AgentConnect ou des tiers habilités.

Les jetons d'accès fournis par le Service AgentConnect au Fournisseur de service ne doivent en aucun cas être communiqués à un tiers non habilité. En cas de compromission de ces jetons, le Fournisseur de services doit les révoquer en utilisant le service de révocation mis à disposition par le Service AgentConnect, dans les plus brefs délais.

4.6.3 Session utilisateur et déconnexion

La durée de session utilisateur et la déconnexion sont définies par le fournisseur d'identité.

5. CONDITIONS D'IMPLEMENTATION DU SERVICE AGENTCONNECT

Le Fournisseur de services suit le processus d'implémentation temporaire[1] suivant :

- Le Fournisseur de services sollicite la DINUM pour un échange sur le produit AgentConnect (par téléphone ou par email).
- La DINUM vérifie alors avec le Fournisseur de services si ce dernier respecte les prérequis techniques et fonctionnels définis dans la documentation technique : https://github.com/france-connect/Documentation-AgentConnect.
- Si tel est le cas, le Fournisseur de services renseigne la demande d'habilitation à partir du formulaire « DATAPASS » disponible ici : https://datapass.api.gouv.fr/agent-connect-fs.
- La DINUM étudie ladite demande dans un délai moyen de 5 jours ouvrés.
- Si la demande est complète et que tous les critères d'habilitation sont respectés, la DINUM valide la demande d'habilitation.
- Une fois la demande validée, un membre de l'équipe AgentConnect en informe par email le Responsable Technique (déclaré dans la demande Datapass) et lui demande l'ensemble des informations nécessaires à l'enrôlement du Fournisseur de services sur la plateforme de tests.
- Une fois le Fournisseur de services enrôlé, l'équipe AgentConnect communiquera par email au Responsable Technique les éléments permettant d'accéder aux ressources de développement et de tests.
- Si l'implémentation est validée par notre équipe, le Fournisseur de Services demande la mise en production du service par email à support.partenaires@agentconnect.gouv.fr.
- La DINUM envoie alors les secrets (par email et SMS) au Responsable Technique pour passer en production.
- Avant la mise en production :
    - la DINUM organise un rendez-vous technique pour vérifier le fonctionnement de la cinématique en production.
    - la DINUM communique au Fournisseur de Services les éléments relatifs à la politique de sécurité et de gestion des mots de passe des Fournisseurs d'identité pour que le Fournisseur de services indique à la DINUM le ou les Fournisseurs d'identité qu'il autorise à accéder à son service.

[1] *Dans l'attente de la mise en place de l'espace partenaires dédié à AgentConnect.*

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

20 Avenue de Ségur
TSA 30719
75334 Paris CEDEX 7