PREMIER MINISTRE

Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Agent Connect

Conditions d'adhésion des Fournisseurs d'identité au service AgentConnect

Annexe

Public

v.1.2

Propriétés du document

	Identité	Date
Rédacteur	Elodie BOUDOUIN	26/04/2021
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	Intégration des formulaires Datapass dans le processus d'implémentation	DINUM	08/06/2022

Liste de diffusion

Destinataire	Poste	Société
L'ensemble des Partenaires Fournisseurs d'identité 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 d'adhésion des Fournisseurs d'identité au Service AgentConnect, dont elle fait intégralement partie.

2. DESCRIPTION FONCTIONNELLE D'AGENTCONNECT

AgentConnect est un dispositif facultatif d'identification et d'authentification pour les agents exerçant au sein de la fonction publique d'Etat (administrations centrales, services déconcentrés) y compris les 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 service 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 service 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 d'adhésion.

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 d'identité, 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 d'identité.

Le Fournisseur d'identité doit réaliser les développements nécessaires à son intégration en tant que fournisseur Open ID Connect dans le Service AgentConnect. Il s'appuie pour cela sur les exigences formalisées par AgentConnect sur le portail mis à la disposition des Partenaires ainsi que sur les exigences en termes de sécurité Référentiel Général de Sécurité.

L'annexe de sécurité s'appuie sur les documents de référence suivants :

- Référentiel Général de Sécurité – Version 2.0 du 13 juin 2014, il s'applique aux systèmes d'information mis en œuvre par les autorités administratives dans leurs relations entre elles et avec les usagers, il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes ;
- Guide d'Hygiène Informatique de l'ANSSI, il comporte les mesures pour renforcer la sécurité de son système d'information ;
- Sécuriser un site web, le document comporte les recommandations pour la sécurisation des sites web rédigé par l'ANSSI ;
- Le site de l'OWASP https://owasp.org/ comporte le document « OWASP secure coding practices quick reference guide » et les différentes itérations des « Top 10 » sont des sources d'information extrêmement appréciables pour les développeurs web

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 désactivation d'un Fournisseur d'identité 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 d'identité et le Service AgentConnect.

3.2. Gestion du SSO

La fonction de SSO (Single Sign On) n'est pas active à ce stade.

3.3. Connaissance des Fournisseurs d'identité et des 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. 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. Traces de connexion 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 d'identité 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. Fonction Support AgentConnect

Le Support DINUM mis à disposition des Fournisseurs d'identité 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 d'identité.

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

A chaque demande d'assistance, le Fournisseur d'identité 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 d'identité 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 d'identité.
- 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 d'identité 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 d'identité.

4. PREREQUIS A RESPECTER PAR LE FOURNISSEUR D'IDENTITE

4.1. Transmission des données obligatoires au service AgentConnect

Le Fournisseur d'identité collecte, vérifie, et met à jour les données suivantes relatives à l'agent utilisateur :

- Les informations relatives à son état-civil :
  - Le(s) prénom(s) utilisé(s) par l'agent dans le cadre de ses fonctions,
  - Le nom utilisé par l'agent dans le cadre de ses fonctions (nom de naissance, nom d'usage).
- L'adresse de courrier électronique professionnelle.

Le Fournisseur d'identité s'engage à fournir au Service AgentConnect l'ensemble de ces données dites obligatoires.

Le Fournisseur d'identité s'engage à respecter le protocole OpenID Connect et fournit à chaque transaction :

- Les clés de fédération ou « alias » générés par le système à la connexion de l'usager, comprenant notamment l'identifiant technique propre au fournisseur d'identité ;
- Un alias technique unique propre au système.

4.2. Conformité RGS

Le Fournisseur d'identité doit être homologué en application du Référentiel Général de Sécurité (RGS) ou en cours d'homologation ; cette homologation constitue un prérequis avant son activation dans le Service AgentConnect.

La décision d'homologation RGS portant a minima sur le périmètre du service de gestion des identités proposé au travers du service AgentConnect devra être communiquée à la DINUM.

En cas de renouvellement ou de changement de périmètre, le Fournisseur d'identité homologué RGS s'engage à fournir à la DINUM la nouvelle décision d'homologation RGS. En cas de suspension ou de perte de cette homologation, le Fournisseur d'identité s'engage à prévenir la DINUM dans les plus brefs délais. La DINUM se réserve alors le droit de le désactiver.

Le Fournisseur d'identité met à disposition de la DINUM tout document lui permettant d'apprécier les mesures prises pour assurer la sécurité des Données d'identité tels que notamment les analyses d'impact détaillées, les certifications de sécurité, les audits,

processus de conservation des identités, tests d'intrusion, processus de transmissions des données, la décision d'homologation RGS lorsqu'elle existe…

4.3. Fonction Support du Fournisseur d'identité

Le Fournisseur d'identité met à disposition un support accessible à ses agents utilisateurs.

4.4. Veille et sensibilisation

Le Fournisseur d'identité 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 d'identité 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).

4.5. Protection des communications de serveur à serveur

Le Fournisseur d'identité doit fournir à AgentConnect un identifiant client (Client ID OpenID Connect) et un secret (Client Secret OpenIDConnect). L'identifiant client et le secret sont communiqués sur des canaux différents et de manière sécurisée.

Le secret doit avoir une complexité équivalente à une entropie au minimum de 128 bits et renouvelé tous les trois ans.

4.6. Règles de sécurisation des identités des agents utilisateurs du Fournisseur d'identité

Le Fournisseur d'identité doit :

- Imposer à ses utilisateurs, un mot de passe avec une bonne complexité, équivalente au minimum à une entropie de 128 bits (cf. l'annexe B3 du Référentiel Général de Sécurité) ;
- Implémenter des mécanismes de blocage des utilisateurs 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.

4.7. Confidentialité des échanges

La sécurité du protocole OpenId Connect est basée sur la confidentialité des échanges entre le Service AgentConnect et le Fournisseur d'identité.

Pour cela, le Fournisseur d'identité 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.

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

4.8.1 Codes d'autorisation

Le code d'autorisation fourni par le Fournisseur d'Identité à AgentConnect doit être généré par le Fournisseur d'identité de manière non prédictible avec au moins 32 octets à l'aide d'un générateur aléatoire cryptographique.

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

Afin de limiter l'impact en cas de vol, par exemple à la suite d'une attaque par injection sur la base stockant les codes d'autorisation, il est recommandé aux Founisseurs d'identité 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 ;
- 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 d'attaque par rejeu, il est recommandé aux fournisseurs d'identités de :

- Limiter dans le temps la durée de vie du code d'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 les attaques par force brute ou dictionnaire, le Fournisseur d'identité doit mettre en place des mécanismes de sécurité adaptés et les communiquer à la DINUM.

4.8.2 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).

Le serveur de jeton d'accès du Fournisseur d'identité vérifie systématiquement le mot de passe envoyé par AgentConnect.

AgentConnect recommande que le jeton d'accès soit :

- 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 ;
- 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.

4.8.3 Session utilisateur et déconnexion

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

5. PROCESSUS D'IMPLEMENTATION DU SERVICE AGENTCONNECT

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

- Le Fournisseur d'identité sollicite la DINUM pour un échange sur le produit AgentConnect (par téléphone ou par email).
- La DINUM vérifie alors avec le Fournisseur d'identité 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 d'identité renseigne la demande d'habilitation à partir du formulaire « DATAPASS » disponible ici : https://datapass.api.gouv.fr/agent-connect-fi
- 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 d'identité sur la plateforme de tests.
- Une fois le Fournisseur d'identité 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 d'identité demande la mise en production du service par email à agentconnect.supportpartenaires@modernisation.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 vérifie avec le Fournisseur d'identité la liste des Fournisseurs de service qu'il autorise à utiliser les données transmises par AgentConnect pour procéder à l'authentification de leurs agents utilisateurs.

[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