PREMIER MINISTRE
Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Téléservice FranceConnect/FranceConnect +
Conditions d'adhésion
(Fournisseurs d'identité)

Annexe
Fonctionnement de FranceConnect/FranceConnect + pour les Fournisseurs d'identité

Public

Version V1 Mai 2021

Table des matières

1. OBJET DU DOCUMENT

La présente Annexe décrit les modalités opérationnelles et fonctionnelles du Téléservice auquel adhère le Fournisseur d'identité en devenant partenaire de FranceConnect ou FranceConnect+.

La présente annexe complète les Conditions d'adhésion des Fournisseurs d'identité au Téléservice FranceConnect/FranceConnect+, dont elle fait intégralement partie.

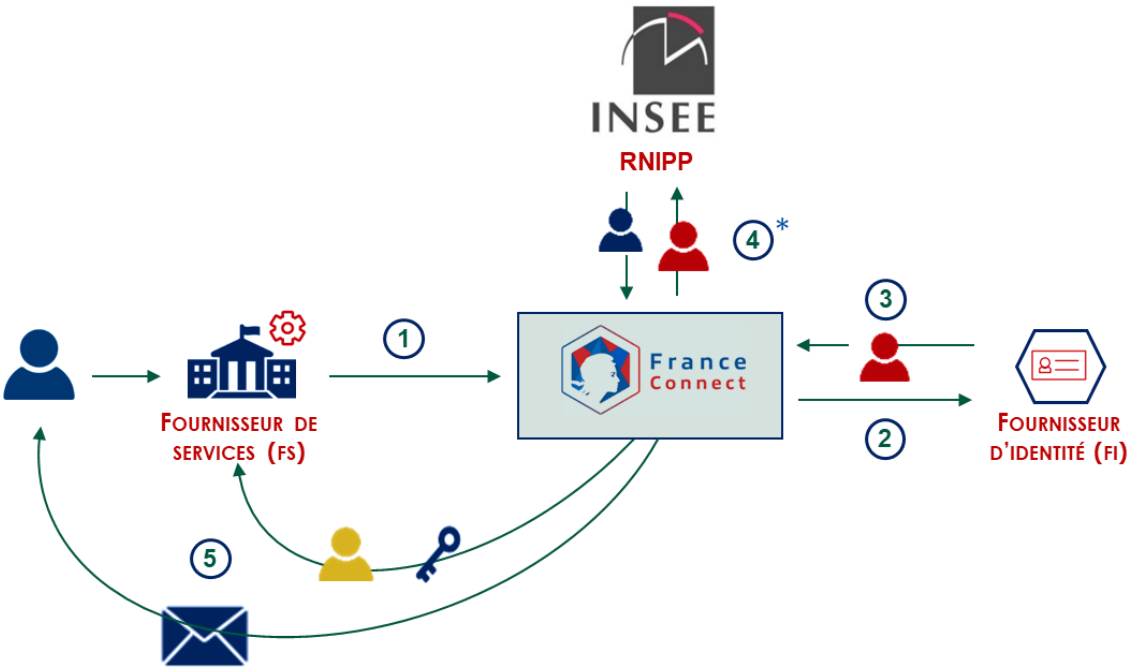
2. PRESENTATION GENERALE DU FONCTIONNEMENT DU TELESERVICE

Le Téléservice FranceConnect/FranceConnect+ mis en œuvre par l'État français propose un dispositif d'identification et d'authentification électroniques des personnes physiques.
Ce Téléservice permet à ses Utilisateurs de se connecter aux services en ligne de Fournisseurs de service habilités en tant que Partenaires de FranceConnect et/ou FranceConnect+.
Le Téléservice s'appuie sur les services d'identité électronique fournis par ses Partenaires Fournisseurs d'identité qui peuvent proposer des Niveaux faible, substantiel ou élevé au sens du Règlement eIDAS.

Etapes de fonctionnement du Téléservice :

- Etape 1 : L'Utilisateur initie son identification/authentification en cliquant sur le bouton FranceConnect ou FranceConnect+ présent sur le site du Fournisseur de Service (FS) afin de réaliser sa démarche en ligne ;
- Etape 2 : L'Utilisateur sélectionne parmi les Fournisseurs d'identité (FI) proposés dans la fenêtre de choix des FI, celui auprès duquel il possède un compte et souhaite s'identifier/authentifier.
- Etape 3 : Suite à l'identification/authentification réussie de l'Utilisateur auprès du FI, ce dernier envoie au Téléservice les données d'identité (nom de naissance, prénoms, date et lieu de naissance, sexe) ainsi que les données complémentaires de l'Utilisateur (nom d'usage, adresse courriel).
- Etape 4 : le Téléservice interroge le RNIPP (INSEE) pour vérifier que l'Utilisateur existe, qu'il n'est pas décédé et qu'il n'existe pas d'homonyme.
  - Si la vérification est validée par le RNIPP, le Téléservice affiche les catégories de données de l'Utilisateur dans la limite de celles sélectionnées par le Fournisseur de service dans sa demande d'habilitation. Cet affichage se fait dans une fenêtre du Téléservice ;
  - Si la vérification n'est pas validée par le RNIPP, le Téléservice interrompt la démarche de l'Utilisateur.
- Etape 5 : l'Utilisateur accepte de passer à l'étape suivante en cliquant sur le bouton proposé par le Téléservice. Le Téléservice transmet au Fournisseur de service les données de l'Utilisateur ainsi que l'identifiant SUB de l'Utilisateur (tel que décrit au 3.1.2. de la présente Annexe). L'Utilisateur est alors connecté au service en ligne du FS. Le Téléservice notifie par mail l'Utilisateur de sa connexion via FranceConnect/FranceConnect+ au service du FS, en précisant les date et heure de connexion.

Le schéma ci-dessous synthétise le fonctionnement du Téléservice FranceConnect/FranceConnect+ :



Identité pivot (nom de naissance*, sexe*, date de naissance*, code INSEE du pays de naissance*, code INSEE de la commune de naissance* (si l'usager est né en France)) + données complémentaires (nom d'usage, adresse e-mail*, adresse postale, numéro de téléphone) de l'utilisateur provenant du FI (*: informations obligatoires)

Identité pivot provenant du RNIPP (redressée)

- Pour un FS de niveau de garantie e-IDAS faible : scope de l'identité pivot reçue du RNIPP conforme à la demande d'habilitation du FS
- Pour un FS de niveau de garantie substantiel ou élevé : scope de l'identité pivot reçue du FI conforme à la demande d'habilitation du FS

Identifiant unique (SUB)

Notification de connexion par mail

3. MESURES DE SECURITE

3.1. Protocole technique et sécurité du Téléservice

3.1.1 Sécurité générale et spécifications OpenID Connect

Au regard de son rôle de client OpenID Connect vis-à-vis du Fournisseur d'identité, la DINUM met en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin de protéger les données traitées et stockées dans le cadre du Téléservice, 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.

Le Téléservice met en œuvre le protocole OpenID Connect selon les spécifications décrites sur http://openid.net/specs/openid-connect-core-1_0.html qui doivent être appliquées par le Fournisseur de service.

Le Fournisseur d'identité doit réaliser les développements nécessaires à son intégration en tant que fournisseur Open ID Connect dans le Téléservice. Il s'appuie pour cela sur les exigences formalisées sur le portail Partenaire https://partenaires.franceconnect.gouv.fr ainsi que sur les exigences en terme 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

Le Fournisseur d'identité

Par la suite, il appartient au Fournisseur d'identité de s'adapter aux évolutions éventuelles du Téléservice, que celles-ci soient liées à des exigences législatives ou réglementaires ou au bon fonctionnement du Téléservice FranceConnect/FranceConnect +.

3.1.2 Génération et gestion du SUB Fournisseur de service

A chaque usage de FranceConnect/FranceConnect+, le Téléservice génère un identifiant unique de l'Utilisateur (dénommé SUB), spécifique au Fournisseur de service (FS) quel que soit le Fournisseur d'identité utilisé.

Ce SUB est systématiquement calculé sur la base des données d'identité du RNIPP. Le RNIPP est un instrument de vérification de l'état civil des personnes, maintenu et hébergé par l'Institut National de la Statistique et des Etudes Economiques (INSEE).

En cas de différences minimes entre les données d'identité fournies par le Fournisseur d'identité et celles du RNIPP (exemples : accent, tiret entre prénom composé) :

- Pour un usage FranceConnect, ce sont les données du RNIPP, éventuellement corrigées, qui sont transmises au Fournisseur de service.

- Pour un usage FranceConnect+, ce sont les données issues du Fournisseur d'identité qui sont transmises au Fournisseur de service.

3.1.3 Gestion du SSO (Single Sign On)

Le Téléservice FranceConnect intègre automatiquement une fonction de SSO qui permet à un utilisateur d'accéder à plusieurs Fournisseurs de service en ne procédant qu'à une seule authentification FranceConnect.
Cette fonction de SSO a une durée équivalente à la durée de session du Téléservice FranceConnect.
Cette fonction de SSO n'est active que pour FranceConnect (niveau eIDAS faible).
Cette fonction n'est pas autorisée sur des usages nécessitant FranceConnect+ (niveaux eIDAS substantiel et élevé).

3.1.4 Protection des communications de serveur à serveur

Afin de réduire les risques d'usurpation d'identité, une authentification mutuelle doit être mise en œuvre entre le Fournisseur d'identité et le client Téléservice FranceConnect ou FranceConnect+.

Le Fournisseur d'Identité doit fournir au Téléservice un identifiant client (client ID OpenIDConnect) et un secret (Client Secret OpenIDConnect) pour l'authentifier. L'identifiant client et le secret doivent être communiqués au Téléservice 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.
Le processus de renouvellement du secret fera l'objet d'une communication distincte avec un préavis de mise en œuvre associé. Ce processus de renouvellement nécessitera une coordination entre le Fournisseur d'identité et le client Téléservice afin de minimiser la durée d'interruption de service pour les Utilisateurs.

3.2. Protocole technique et sécurité du côté du Fournisseur d'identité

3.2.1 Mesures générales et sécurité du protocole OpenId Connect

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 mise en place de mesures afin de prévenir la fuite des données ci-dessus en cas d'intrusion ;
- La confidentialité et l'intégrité des secrets échangés (mots de passe : client ID et client secret, clés cryptographiques).

De plus, la sécurité du protocole OpenId Connect est basée sur la confidentialité des échanges entre le Téléservice et le Fournisseur d'identité.
Pour cela, le Fournisseur d'identité doit :

- Mettre en œuvre les mesures de sécurité nécessaires afin d'assurer le stockage sécurisé du secret permettant l'authentification du client OpenID Connect et

respecter les spécifications décrites sur http://openid.net/specs/openid-connect-core-1_0.html lors de l'utilisation du Téléservice ;
- Utiliser la version de TLS préconisée par le Téléservice pour les communications chiffrées ;
- Configurer les suites cryptographiques robustes selon les règles du Référentiel Général de Sécurité ;
- Utiliser des certificats serveurs RGS 1* conformes au Référentiel Général de Sécurité.

3.2.2 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 Téléservice.

Le Fournisseur d'identité forme et sensibilise les acteurs sous son autorité à la sécurité et aux enjeux du Téléservice (notamment les développeurs et à la cible les agents utilisant FranceConnect et/ou FranceConnect+).

3.2.3 Recommandations globales d'implémentation sécurisée

Les Fournisseurs d'identité 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 quel que soit leur provenance.
- Mettre en place des mécanismes permettant de s'assurer de la légitimité de la requête.
- 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.

3.3. Conformité du Fournisseur d'identité

Lorsque le Fournisseur d'identité doit être homologué en application du Référentiel Général de Sécurité (RGS), cette homologation constitue un prérequis avant son activation dans le Téléservice. La décision d'homologation RGS portant a minima sur le périmètre du service de gestion des

identités proposé au travers du Téléservice 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, la décision de première qualification ou de renouvellement de qualification aux Niveaux eIDAS, les certifications de sécurité, les audits, process de conservation des identités, tests d'intrusion, process de transmissions des données, la décision d'homologation RGS lorsqu'elle existe,...

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

3.4.1 Codes d'autorisation

Le code d'autorisation fourni par le Fournisseur d'identité 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 ou FranceConnect+.

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

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 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 ;
- 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 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.

3.4.2 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 FranceConnect ou FranceConnect+.

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 ou FranceConnect+ ;
- 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.

3.4.3 Durée de vie de la session et déconnexion

La durée de la session Utilisateur chez le Fournisseur d'identité ne doit pas excéder **deux minutes**.
Le Fournisseur d'identité doit permettre au Téléservice de demander la déconnexion d'un utilisateur et ainsi mettre fin à la session chez le Fournisseur d'identité.

4. ORGANISATION FONCTIONNELLE DU TELESERVICE

4.1. Qualité de service

La DINUM met en œuvre les moyens nécessaires pour assurer des performances et une disponibilité efficientes du Téléservice FranceConnect et FranceConnect+. Cette disponibilité est dépendante de celles des Fournisseurs d'identité et du RNIPP.

En cas d'indisponibilité du Téléservice, les équipes compétentes de FranceConnect ou FranceConnect+ interviendront afin d'en identifier l'origine et s'efforceront d'en tenir informés les Partenaires dans les meilleurs délais.

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

- le Téléservice n'affiche pas la mire de choix des Fournisseurs d'identité.
- le Téléservice n'est pas en mesure de renvoyer les données d'identité demandées par le Fournisseur de service même si l'authentification a réussi chez le Fournisseur d'identité.
- Tous les Fournisseurs d'identité sont indisponibles alors même que le Téléservice ne présente aucun dysfonctionnement.

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

4.2. Données d'identité et de contact collectées par le Fournisseur d'identité

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

- Genre
- Nom de naissance
- Prénoms
- Date de naissance
- Ville de naissance
- Pays de naissance
- L'adresse @mail

Cas particulier du « nom d'usage » : Dans le cas où la donnée « nom d'usage » de l'Utilisateur existe et a été collectée par le Fournisseur d'identité, celle-ci doit également être transmise au Téléservice si elle est demandée par le Fournisseur de service.

En cas d'Identification et d'Authentification réussies de l'Utilisateur, le Fournisseur d'identité s'engage à fournir au Téléservice l'ensemble des données demandées.

Le Fournisseur d'identité s'engage à respecter le protocole OpenID Connect et fournit à chaque transaction un identifiant (SUB) FI unique par Utilisateur du Téléservice réalisée avec des Données d'identification personnelle qu'il a authentifiées.

4.3. Données de suivi du fonctionnement du Téléservice

Le Téléservice communique mensuellement au Fournisseur d'identité les éléments permettant le suivi du fonctionnement de FranceConnect+ :

- Pour un Fournisseur d'identité donné, par Fournisseur de service et par niveau eIDAS substantiel ou élevé :
    1. Le nombre d'identités numériques uniques utilisées (Un utilisateur avec au moins une Authentification réussie jusqu'au Fournisseur de Service)
    2. Le détail des données fournies (celles sélectionnées par le Fournisseur de service dans sa demande d'habilitation)
    3. Le nombre d'identités numériques uniques utilisées par Fournisseur de service (Un Utilisateur avec au moins une Authentification réussie jusqu'au Fournisseur de service)
    4. Le nombre d'Authentifications réussies (abouties jusqu'au Fournisseur de service)
    5. Le nombre d'Authentifications échouées (non abouties chez le Fournisseur de service) : différence entre le nombre de clics sur le bouton du Fournisseur d'identité et le nombre d'authentifications abouties chez le Fournisseur de service. Elles peuvent concerner les cas suivants :
        - Utilisateur désactivé par le Téléservice
        - Réponse RNIPP ne permettant pas de finaliser la cinématique (Utilisateur décédé, en doublon, non trouvé, …)
        - Fournisseur d'identité répondant hors délai :
            - soit du temps de session du Téléservice
            - soit du temps de session du Fournisseur de service
        - Réponse du Téléservice dépassant le temps de session du Fournisseur d'identité
        - Indisponibilité du Téléservice en cours de cinématique
        - Indisponibilité du Fournisseur de service en cours de cinématique
        - Abandon du parcours par l'Utilisateur
        - Pas de réponse du Fournisseur d'identité.

4.4. Dossier de preuve du Téléservice

Le dossier de preuves contient les données de traçabilité sont conservées dans des logs horodatés de connexion qui comprennent :

- L'adresse IP de l'Utilisateur ;
- les dates et heures de connexions de l'Utilisateur à FranceConnect ou FranceConnect+ ;
- l'identifiant technique de l'Utilisateur chez le Fournisseur de service (SUB Fournisseur de service) ;
- l'identifiant technique de l'Utilisateur chez le Fournisseur d'identité (SUB Fournisseur d'identité) à chaque transaction lors de la période demandée ;
- Le nom et les coordonnées du Fournisseur d'identité concerné par l'utilisation du Téléservice ;

- Le nom et les coordonnées du Fournisseur de service concerné par l'utilisation du Téléservice ;
- le niveau eIDAS de chaque transaction de l'Utilisateur lors de la période demandée.

5. SUPPORTS UTILISATEURS ET PARTENAIRES

5.1. Gestion du Support du Téléservice

Pour assurer le support du Téléservice, un processus organisationnel ainsi qu'un outil permettant de tracer et suivre les incidents rencontrés par les Partenaires et les Utilisateurs du Téléservice sont mis en œuvre par la DINUM. Il s'agit du service du Support.
Le service de Support notifiera aux personnes en charge du service de support du Fournisseur de service chaque évènement de niveau critique ou majeur impactant celui-ci.
Dès réception, la demande est référencée dans la base de ticketing et le Support s'engage à la traiter dans les 48 heures ouvrées.
L'analyse du ticket permet d'y associer un niveau de priorité, conformément aux niveaux de criticité définis dans la partie Gestion des incidents de la présente Annexe.

5.1.1 Processus Support du Téléservice

Le schéma ci-dessous illustre le processus global du support du Téléservice mis en œuvre d'une part avec les Fournisseurs de service et d'autre part avec les Utilisateurs.

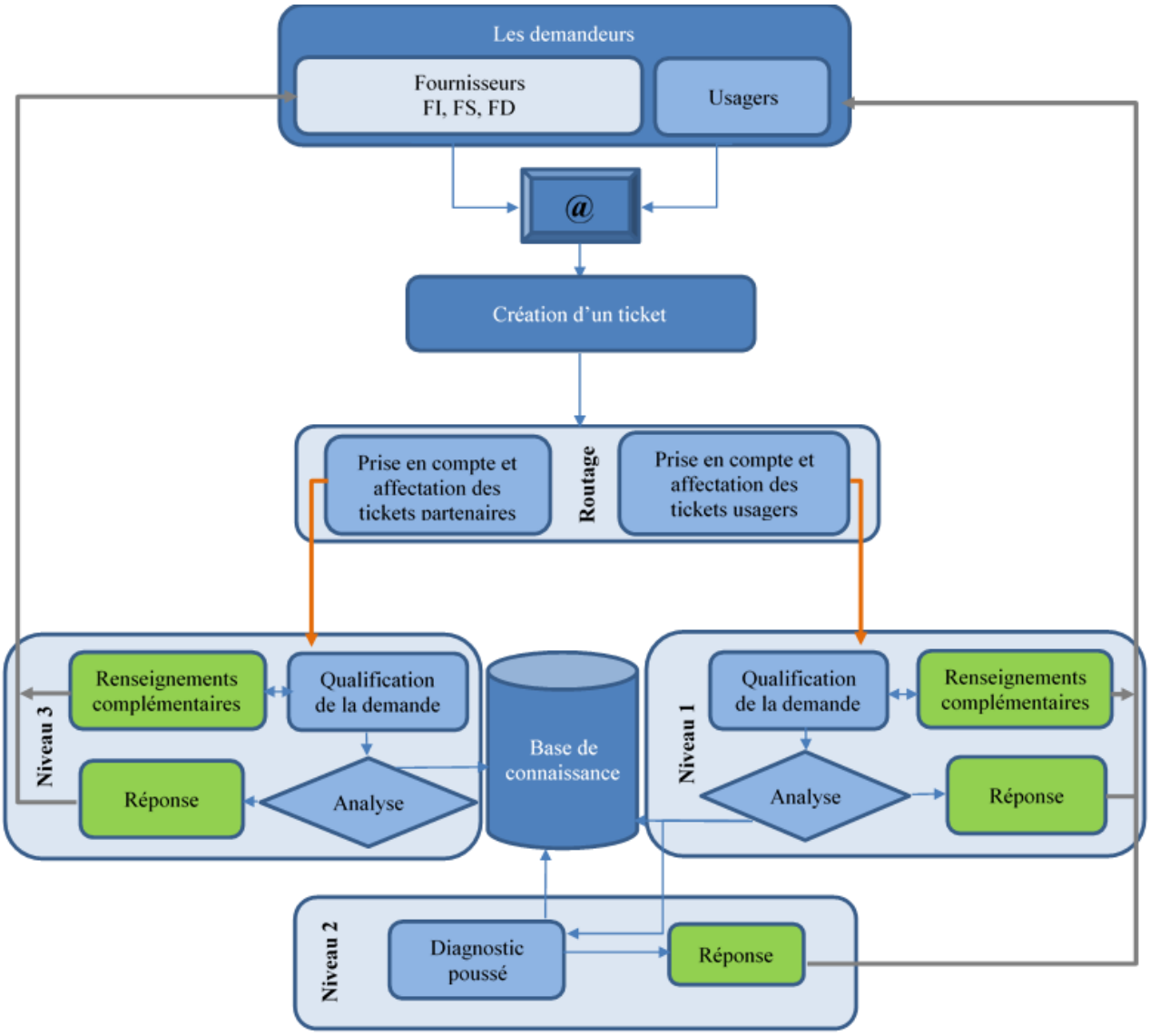


Figure 1 - Processus global du support du Téléservice FranceConnect/FranceConnect+

Les Partenaires ont la possibilité de solliciter le support du Téléservice pour l'ouverture d'un ticket de deux manières différentes :

- Par mail à l'attention de : support.partenaires@franceconnect.gouv.fr. Dans ce cas, les échanges se feront uniquement par mail.
- Par téléphone de 9h00 à 18h00 : les contacts nécessaires figurent en Annexe Fiche contact FranceConnect/FranceConnect+.Pour rappel, l'usage du téléphone entre les parties est à réserver aux situations d'urgence.

Concernant l'Utilisateur, ce dernier n'a qu'une seule possibilité pour contacter le Support du Téléservice :

- Par mail à l'attention de : support.usagers@franceconnect.gouv.fr. Dans ce cas, les échanges se feront uniquement par mail.

5.1.2 Outil Support du Téléservice

L'outil Support du Téléservice permet de tracer et suivre les incidents rencontrés par les Partenaires (en production ou en cours d'intégration) et les Utilisateurs du Téléservice. C'est l'outil sur lequel s'appuie le processus support du Téléservice.

5.1.3 Assistance aux Partenaires

L'outil Support du Téléservice offre un service d'assistance aux Partenaires. En effet, c'est via cet outil que les Partenaires peuvent principalement :

- Pour les Fournisseurs de service :
  - Demander leurs identifiants suite à leur implémentation au Téléservice ;
  - Demander le renouvellement de leur Client Secret ;
  - Demander leur désactivation / réactivation suite par exemple, à un problème critique ou de sécurité ;
  - Demander leurs statistiques ;
  - Demander de l'aide lors de leur phase d'intégration au Téléservice ;
- Pour les Fournisseurs d'Identité :
  - Demander la mise à jour de leur Client Secret ;
  - Demander la mise à jour de leur niveau eIDAS ;
  - Demander leur masquage / affichage dans la mire du Téléservice et des Fournisseurs de service concernés, le cas échéant ;
  - Demander leur désactivation / réactivation dans la mire du Téléservice et des Fournisseurs de service concernés, le cas échéant ;
  - Demander de l'aide lors de leur phase d'intégration dans le Téléservice ;
  - Demander leurs statistiques.

5.1.4 Assistance aux Utilisateurs

L'outil Support du Téléservice offre également un service d'assistance aux Utilisateurs. En effet, c'est via cet outil que les Utilisateurs peuvent principalement :

- Poser des questions en cas de problème rencontré ;
- Signaler une usurpation d'identité ;
- Demander la désactivation / réactivation de l'utilisation du Téléservice ;
- Signaler une divergence entre les données contenues dans le RNIPP et leurs données.

5.2. Fonction support chez le Fournisseur d'identité

Le Fournisseur d'identité assure un dispositif de support accessible aux utilisateurs 24h/24 7 jours sur 7.

Une base de connaissance est maintenue à jour par le Fournisseur d'identité et doit être mise à disposition de l'Utilisateur afin de l'aider lors de ses demandes de connexion ou dans la résolution de ses problèmes. Lorsque l'Utilisateur ne trouve pas la réponse à sa demande, il pourra contacter le support du Fournisseur d'identité.

Le Fournisseur d'identité s'engage à informer, sans délai, les Utilisateurs de tout incident de sécurité dont ils seraient victimes et qui engendrerait un dysfonctionnement et/ou un risque concernant leur relation avec les Fournisseurs de service référencés dans le Téléservice sur https://franceconnect.gouv.fr/nos-services.

Le Fournisseur d'identité s'engage à informer le Support, sur simple demande, de tout incident de sécurité notifié aux autorités compétentes, survenu dans le service d'identité qu'il met en œuvre.

6. GESTION DES CHANGEMENTS

6.1. Information et suivi des changements

Le suivi des changements concerne tout changement programmé qui pourrait impacter le Téléservice, ses Partenaires et/ou Utilisateurs. Sont ainsi concernées notamment les opérations de maintenance évolutives ou correctives.

Il n'y a pas d'outil partagé entre la DINUM et les Partenaires sur le suivi des changements. Ce partage est assuré obligatoirement :

- Par des réunions présentielles ou en ligne,
- Par la mise en place d'un calendrier prévisionnel des changements et des plages de maintenance programmées,
- Par une communication écrite par courriel.

L'usage du téléphone entre les parties est à réserver aux changements urgents.

Les changements doivent être annoncés avant le jour J de leur application :

- En conditions nominales : 6 mois à l'avance avec un rappel à 1 mois.
- En conditions d'urgences : 14 jours ouvrés à l'avance avec un rappel à 5 jours ouvrés.

Si des changements opportuns n'impactent pas les Partenaires ou le Téléservice, ils peuvent ne pas être contraints par ces délais.

Les contacts nécessaires figurent en Annexe Fiche contact FranceConnect/FranceConnect+. Les deux parties s'engagent à ne pas communiquer ces points de contact aux Utilisateurs.

6.2. Suivi des changements du Téléservice seul

Lors de tout changement du Téléservice et en l'absence d'outil dédié, la DINUM respectera les règles associées au suivi des changements décrites au paragraphe 5.1 **Erreur ! Source du renvoi introuvable.**.

6.3. Suivi des changements exclusivement chez le Partenaire

Lors de tout changement chez le Partenaire pouvant impacter le Téléservice, et/ou ses utilisateurs et/ou les autres Partenaires, et en l'absence d'outil dédié, le Partenaire s'engage à respecter les règles associées au suivi des changements décrites au paragraphe **Erreur ! Source du renvoi introuvable. Erreur ! Source du renvoi introuvable.**.

7. GESTION DES USURPATIONS D'IDENTITE

7.1. Suivi des usurpations d'identité

Le suivi des usurpations d'identité concerne toute usurpation d'identité d'un Partenaire ou d'un Utilisateur. L'outil utilisé par la DINUM permet la communication, la traçabilité et le suivi des usurpations d'identité rencontrées par un Partenaire ou un Utilisateur dans l'écosystème du Téléservice. Le dispositif de gestion des incidents du Téléservice est celui décrit au point 7 de la présente Annexe.

7.2. Usurpation d'identité d'un Partenaire

Lors d'une usurpation d'identité d'un Partenaire, le Partenaire et la DINUM s'engagent à respecter les règles associées au suivi des usurpations d'identité décrites au paragraphe 6.1 Suivi des usurpations d'identité.

7.2.1 Usurpation détectée par le Partenaire

En cas d'usurpation d'identité détectée par le Partenaire, le Partenaire s'engage également à :

- Alerter par téléphone la DINUM. Les contacts habilités à prévenir la Dinum doivent figurer en Annexe Fiche contact FranceConnect/FranceConnect+; En complément de l'alerte téléphonique, un courriel doit être envoyé à la Dinum et l'équipe support du Téléservice (support.securite@franceconnect.gouv.fr) par une personne habilitée figurant dans l'Annexe contact du partenaire.
-
- Alerter par courriel la DINUM et l'équipe support du Téléservice (support.securite@franceconnect.gouv.fr) en cas d'usurpation d'identité en précisant dans son mail envoyé au support la personne à contacter qui devra confirmer l'usurpation à la DINUM. Dans le cas d'un Partenaire, la personne à contacter doit être un des contacts figurant dans l'Annexe Fiche contact FranceConnect/FranceConnect+);
- Fournir à la DINUM l'URL ou le Client ID du Fournisseur d'identité à désactiver.

En cas d'usurpation d'identité détectée par le Partenaire, la DINUM s'engage également à :

- Appeler par téléphone un contact du Partenaire qui devra confirmer l'usurpation à la DINUM ;
- Désactiver le Partenaire en cas d'usurpation d'identité avérée ou confirmée à partir de l'URL ou le Client ID du Fournisseur d'identité transmis ;
- Récupérer les traces / logs associées à l'usurpation d'identité du Partenaire ;
- Mettre à jour le ticket ouvert lors de l'usurpation d'identité en traçant au fil de l'eau les différents échanges entre la DINUM et le Partenaire.

Note : *l'article 226-4-1 du code pénal réprime le délit d'usurpation d'identité en sanctionnant d'un an de prison et de 15 000 euros d'amende : " Le fait d'usurper l'identité*

d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ».

7.2.2 Usurpation détectée par la DINUM

En cas d'usurpation d'identité détectée par la DINUM, la DINUM s'engage également à :

- Alerter par téléphone le Partenaire. Les contacts nécessaires figurent en Annexe Fiche contact FranceConnect/FranceConnect+;
- Alerter par courriel le Partenaire. Les contacts nécessaires figurent en Annexe Fiche contact FranceConnect/FranceConnect+;
- Désactiver le Partenaire en cas d'usurpation d'identité confirmée ou avérée par le Partenaire ;
- Notifier le Partenaire de sa désactivation en précisant l'URL ou le Client ID du Fournisseur d'identité désactivé ;
- Récupérer les traces / logs associées à l'usurpation d'identité du Partenaire ;
- Mettre à jour le ticket ouvert lors de l'usurpation d'identité en traçant au fil de l'eau les différents échanges entre la DINUM et le Partenaire.

Note : *l'article 226-4-1 du code pénal réprime le délit d'usurpation d'identité en sanctionnant d'un an de prison et de 15 000 euros d'amende : " Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* ».

7.3. Usurpation d'identité d'un Utilisateur

Lors d'une usurpation d'identité d'un Utilisateur, le Partenaire et la DINUM s'engagent à respecter les règles associées au suivi des usurpations d'identité décrites au paragraphe 7.1 Suivi des usurpations d'identité.

En cas d'usurpation d'identité détectée par un Utilisateur et remontée à la DINUM via le support, la DINUM s'engage également à :

- Echanger par courriel (voire téléphone) avec l'Utilisateur pour confirmer / infirmer la suspicion d'usurpation d'identité ;
- Demander à l'Utilisateur de lui transférer le mail de notification d'utilisation du Téléservice qu'il a reçu ;
- Demander à l'Utilisateur de lui envoyer par mail une demande de désactivation de son accès via le Téléservice, s'il le souhaite ;
- Désactiver l'accès via le Téléservice pour l'Utilisateur suite à la réception des 2 prérequis ci-dessus ;
- Notifier l'Utilisateur pour :
    - L'informer de la désactivation de son accès via le Téléservice ;
    - Lui demander de conserver ce mail de notification qui lui sera demandé lors de la demande de réactivation de son accès via le Téléservice ;
    - Lui indiquer qu'il a la possibilité de déposer :

  - Soit une plainte pénale auprès du commissariat de police ou de la brigade de gendarmerie de son domicile, ou auprès du procureur de la République ;
  - Soit une pré-plainte en ligne qu'il devra signer auprès d'une unité de gendarmerie ou d'un service de police de son choix afin qu'elle soit enregistrée comme une plainte.
- Signaler l'usurpation d'identité au Fournisseur d'Identité et au Fournisseur de service en leur demandant de conserver les traces / logs associées à l'usurpation d'identité de l'Utilisateur ;
- Récupérer les traces / logs associées à l'usurpation d'identité de l'Utilisateur auprès du Téléservice ;
- Mettre à jour le ticket ouvert lors de l'usurpation d'identité en traçant au fil de l'eau les différents échanges entre la DINUM, l'Utilisateur et les Partenaires impactés.

Note : *l'article 226-4-1 du code pénal réprime le délit d'usurpation d'identité en sanctionnant d'un an de prison et de 15 000 euros d'amende : " Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ».*

8. GESTION DES INCIDENTS

8.1. Suivi des incidents

Le suivi des incidents concerne tout incident qui pourrait impacter le Téléservice et ses Partenaires. L'outil partagé entre la DINUM et ses Partenaires pour le suivi des incidents est l'outil Support Téléservice mis en place par la DINUM. Les modalités de son utilisation sont celles décrites au point 9 de la présente Annexe.

L'usage du téléphone entre les parties est à réserver aux incidents critiques ou de sécurité.

Les contacts nécessaires figurent en Annexe Fiche contact FranceConnect/FranceConnect+. Les deux parties s'engagent à ne pas communiquer ces points de contact aux Utilisateurs.

8.2. Niveaux des incidents

Les niveaux des incidents sont définis conformément au tableau suivant :

Niveaux de priorité des incidents			Priorité
Périmètre Impact	Dysfonctionnement concernant l'ensemble des Fournisseurs d'identité utilisant FranceConnect ou FranceConnect+	Entreprise	1 (Critique)
	Dysfonctionnement concernant un Fournisseur d'identité utilisant FranceConnect ou FranceConnect+	Site	2 (Majeure)
	Dysfonctionnement touchant plusieurs Utilisateurs	Plusieurs Utilisateurs	3 (Normal)
	Dysfonctionnement ne touchant qu'un Utilisateur	Utilisateurs	4 (Mineure)
	Demande d'information autour du fonctionnement de FranceConnect ou FranceConnect+	Informations	5 (Info)

Figure 1 : Niveaux de priorité d'un incident

8.3. Traitement des incidents

Après affectation du niveau de priorité, l'équipe Support 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.

Dans le cas d'un dysfonctionnement impactant la disponibilité du service du Fournisseur d'identité, ce dernier sera désactivé jusqu'à la résolution complète de l'incident pour permettre à l'Utilisateur de disposer d'un parcours fluide.

Niveau de priorite	Description	Escalade apres	Duree totale de traitement en heures ouvrees	Escalade vers
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.	1 h	2 h	Responsable de la production
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 h	4 h	Équipe Support de niveau 3
3 (Normal)	- Le service est opérationnel mais présente des réductions de fonctionnalités ou des dysfonctionnements. - Les temps de réponse sont fortement dégradés.	8 h	12 h	Équipe Support de niveau 2
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 du Client.	16 h	24 h	Équipe Support de niveau 1
5 (Info)	- Le service fonctionne parfaitement. - La question ne concerne pas un dysfonctionnement de l'application FranceConnect ou FranceConnect+. - Il s'agit simplement d'une demande d'information de la part d'un Utilisateur, ou de la part d'un fournisseur (services, identités ou données).	16 h	24 h	Équipe Support de niveau 1

Figure 2 : Escalade et temps imparti au traitement d'un incident en fonction de sa priorité

8.4. Conditions de fermeture d'un ticket d'incident

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

- Une demande d'assistance (ticket) sera fermée par le service Support 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, dans un délai de 2 semaines après la réponse de la DINUM, 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.

9. GESTION OPERATIONNELLE DES RELATIONS FOURNISSEURS D'IDENTITE ET FOURNISSEURS DE SERVICE DANS LE CADRE DU TELESERVICE

9.1. Confidentialité entre Fournisseurs d'identité et Fournisseurs de service

Le Téléservice ne permet pas à un Fournisseur d'identité de savoir pour quel service et dans quelle finalité il est sollicité. De même, le Fournisseur de service ne sait pas quel Fournisseur d'identité a été utilisé par l'Utilisateur du Téléservice pour accéder au service en ligne qu'il propose.

9.2. Gestion de l'affichage des Fournisseurs d'identité

Le Téléservice gère une matrice d'affichage dynamique des Fournisseurs d'identité par Fournisseur de service.

La présentation des Fournisseurs d'identité dans le Téléservice se fait par niveau eIDAS et par ordre chronologique d'implémentation des Fournisseurs d'identité.

10. CONDITIONS D'IMPLEMENTATION DU TELESERVICE FRANCECONNECT ET/OU FRANCECONNECT+

Le Fournisseur d'identité suit le processus d'implémentation suivant :

- Envoi par courrier à l'attention du directeur de la DINUM d'une demande d'adhésion contenant :
  - un dossier décrivant les processus de collecte, de vérification d'identité (Identification) et de parcours d'Authentification, ainsi que les éléments précisés sur le lien suivant https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-identite;
  - la liste des sous-traitants du Fournisseur d'identité intervenant dans le service d'identification ou d'authentification de celui-ci ;
  - la liste de contacts intégrant a minima le responsable de traitement ou son représentant, le RSSI, le DPD et le responsable de production, joignables à tout moment en cas d'incident de disponibilité ou de sécurité du Fournisseur d'identité ou du Téléservice. Le Fournisseur d'identité doit mettre à jour ladite liste dès qu'un changement intervient. La liste et toutes mises à jour doivent être communiquées à la DINUM par mail, à l'adresse support.partenaires@franceconnect.gouv.fr .
- La DINUM procède à l'analyse du dossier de demande du Fournisseur d'identité pour intégrer FranceConnect ou FranceConnect+. Cette étude est réalisée en tenant compte du ou des niveaux du service d'identité proposé par le prestataire d'identité. Sont également analysés selon la demande d'habilitation déposée : son respect des exigences posées par les textes législatifs et réglementaires applicables à son service ainsi que son respect des conditions et modalités imposées dans les conditions d'adhésion des Fournisseurs d'identité du Téléservice FranceConnect ou FranceConnect+, en ce compris la présente Annexe et la documentation à laquelle il est renvoyé.
- En cas d'acceptation de son dossier, la DINUM donne accès au Fournisseur d'identité aux ressources de développement et de tests.
- Avant l'ouverture du service, doit compléter la fiche contact (cf. Annexe Fiche contact FranceConnect/FranceConnect+) et la transmettre à l'adresse mail support.partenaires@franceconnect.gouv.fr. Le Fournisseur de service doit mettre à jour ladite liste dès qu'un changement intervient et la communiquer à l'adresse mail support.partenaires@franceconnect.gouv.fr.
- Lors de la 1ère mise en production la DINUM valide l'ensemble des prérequis de la documentation technique, puis fournit le jeton de production.
- Avant toute mise à jour réalisée par le Fournisseur d'identité, ce dernier s'engage à avoir effectué des tests préalables sur un environnement de test mis à disposition par la DINUM, afin de s'assurer que l'ensemble des prérequis de la documentation technique du Téléservice FranceConnect ou FranceConnect+ sont respectés selon la demande d'habilitation déposée.

PREMIER
MINISTRE

Liberté
Égalité
Fraternité

20 Avenue de Ségur
TSA 30719
75334 Paris CEDEX 7

www.franceconnect.gouv.fr