PREMIER MINISTRE
Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Téléservice FranceConnect/FranceConnect +
Conditions générales d'utilisation
(Fournisseurs de services)

Annexe
Fonctionnement de FranceConnect/FranceConnect + pour les Fournisseurs de service

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 de service en devenant partenaire de FranceConnect ou FranceConnect+.

Cette Annexe complète les Conditions générales d'utilisation des Fournisseurs de service du Téléservice FranceConnect/FranceConnect+, dont elle fait intégralement partie.

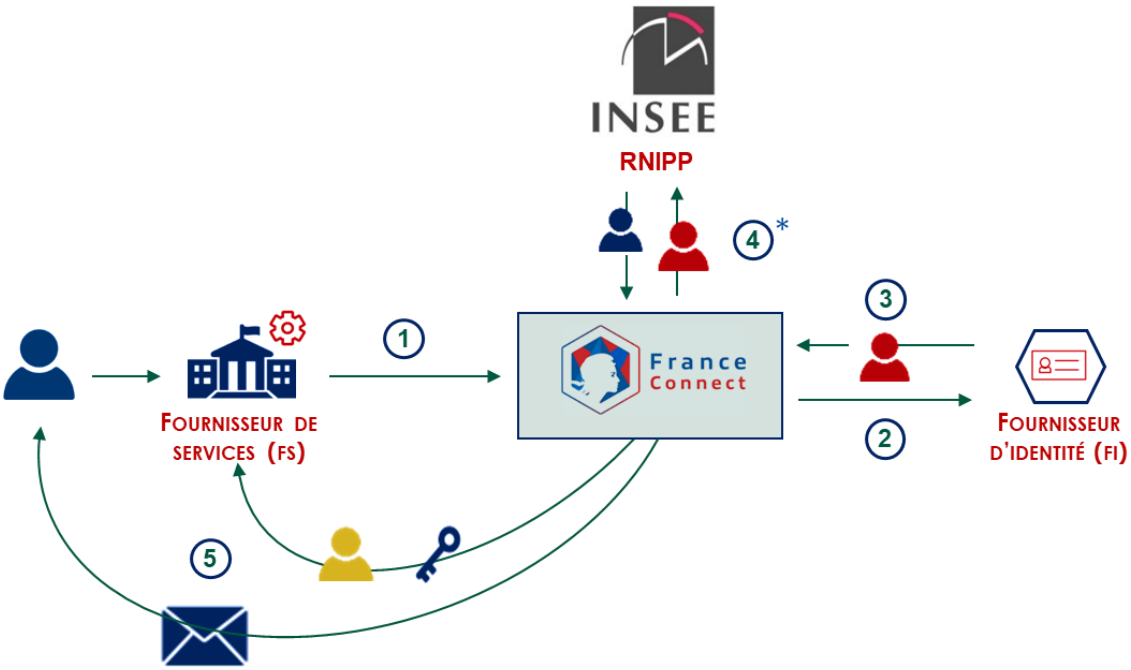
2. PRESENTATION GENERALE DU FONCTIONNEMENT DU TELESERVICE

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, 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 Répertoire National d'Identification des personnes physiques (RNIPP) de l'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 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

Le Téléservice met en œuvre le protocole OpenID Connect selon les spécifications décrites sur http://openid.net/specs/openid-connect-core-1_0.html. Dans ce cadre, le Téléservice doit être regardé comme client OpenID Connect vis-à-vis du Fournisseur d'identité.

Le Téléservice 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 des risques de sécurité (AIPD). Ces mesures concernent en particulier :

- Le contrôle systématique de tous les paramètres en entrée des requêtes afin de réduire le risque d'injection. Le Téléservice 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 (client secret, jetons d'accès, clefs de chiffrement et signature), 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 service et le Téléservice.
- Une authentification du Fournisseur de service par certificat RGS 1* auprès du Téléservice.

3.1.2 Génération et gestion du SUB

A chaque usage 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, le Téléservice doit authentifier le client Fournisseur de service implémentant OpenId Connect à l'aide d'un certificat RGS 1* conforme au Référentiel Général de Sécurité.

Le Téléservice doit fournir au Fournisseur de service 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 service 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.

3.2. Protocole technique et sécurité du côté du Fournisseur de service

3.2.1 Mesures générales et sécurité du protocole OpenId Connect

Le Fournisseur de service met en œuvre les mesures de sécurité techniques et organisationnelles nécessaires afin d'assurer, sur son périmètre :

- La non divulgation des données fonctionnelles et techniques échangées dans le cadre du protocole à un tiers non autorisé ;
- La mise en place de mesures 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 de service.
Pour cela, le Fournisseur de service 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.

Le Fournisseur de service doit par ailleurs répondre aux exigences suivantes :

- Générer le paramètre *state* aléatoirement en utilisant une fonction de génération de caractères aléatoires sécurisée et avec une entropie équivalente à 100 bits (minimum 16 caractères avec un alphabet de 70 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 100 bits (minimum 16 caractères avec un alphabet de 70 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 le Téleservice 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 France Connect,
    - Le paramètre « acr » doit contenir le niveau eIDAS précédemment fourni lors de la requête d'authentification et conservé avec la session de l'utilisateur.

3.2.2 Veille et sensibilisation

Le Fournisseur de Service 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 de Service 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 le Téléservice).

3.2.3 Recommandations globales d'implémentation sécurisée

Les Fournisseurs de Service 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 (l'inclusion des pages dans des « iframe » est proscrite).

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

3.3.1 Codes d'autorisation

Le code d'autorisation fourni par le Téléservice doit :

- Être 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 ;
- Être lié à l'identifiant client OpenId Connect du Fournisseur de service fourni par le Téléservice.

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

Le Fournisseur de service doit sécuriser le stockage des codes d'autorisation fournis par le Téléservice. 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 service concerné.

3.3.2 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 service 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 Téléservice vérifie systématiquement le jeton d'accès envoyé par le Fournisseur de service lors de chaque demande d'accès à des ressources proposées par le Téléservice ou des tiers habilités.

Les jetons d'accès fournis par le Téléservice 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 service doit les révoquer en utilisant le service de révocation mis à disposition par le Téléservice, dans les plus brefs délais.

3.3.3 Déconnexion

Le Fournisseur de service doit mettre à disposition de ses utilisateurs un moyen explicite de se déconnecter de son service (un bouton « déconnexion » par exemple) ou un moyen

implicite de se déconnecter (sur un bouton d'action de type « étape suivante »). Lors de la déconnexion de l'Utilisateur au service du Fournisseur de service, ce dernier doit envoyer une requête de déconnexion de l'Utilisateur au Téléservice, afin de mettre fin à la session du Téléservice.

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/FranceConnect+. Cette disponibilité est dépendante de celles des Fournisseurs d'identité et du RNIPP.

En cas d'indisponibilité du Téléservice, les équipes FranceConnect/FranceConnect+ interviendront afin d'en identifier l'origine et s'efforceront d'en tenir informés les Partenaires concernés 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 de suivi du fonctionnement du Téléservice

Le Téléservice met à disposition du Fournisseur de service un espace partenaires sécurisé, dans lequel il peut notamment consulter des éléments statistiques de connexion.

Pour les niveaux eIDAS substantiel et élevé, FranceConnect+ communique mensuellement aux Fournisseurs de service ayant implémenté ces niveaux les éléments suivants : pour un Fournisseur de service donné, par Fournisseur d'identité 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 sollicité (FranceConnect ou FranceConnect+) 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.

4.3. Dossier de preuves du Téléservice

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

- 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.

4.4. Résultat fourni par le Téléservice

Ce résultat est fourni uniquement dans les cas où l'Utilisateur n'abandonne pas en cours de démarche ou qu'il est impossible d'identifier le Fournisseur de service

Ensemble d'informations transmis par le Téléservice au Fournisseur de service et comprenant :

- le verdict (succès ou échec) de l'authentification ou de l'identification,
  - Dans le cas d'un échec : motif de l'erreur
  - En cas de succès :
    - les données d'identité et de contact telles que sélectionnées dans la demande d'habilitation du Fournisseur de service,
    - l'identifiant technique unique de l'Utilisateur pour ce Fournisseur de service,
    - le niveau de garantie eIDAS soit :
      - Dans le cas de FranceConnect : eIDAS 1 systématiquement
      - Dans le cas de FranceConnect+ : celui utilisé par l'Utilisateur,

5. GESTION DES CHANGEMENTS

5.1. 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.

5.2. 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 ci-dessus.

5.3. 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 5.1 ci-dessus.

6. SUPPORTS UTILISATEURS ET PARTENAIRES

6.1. 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 de 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.

6.1.1 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.

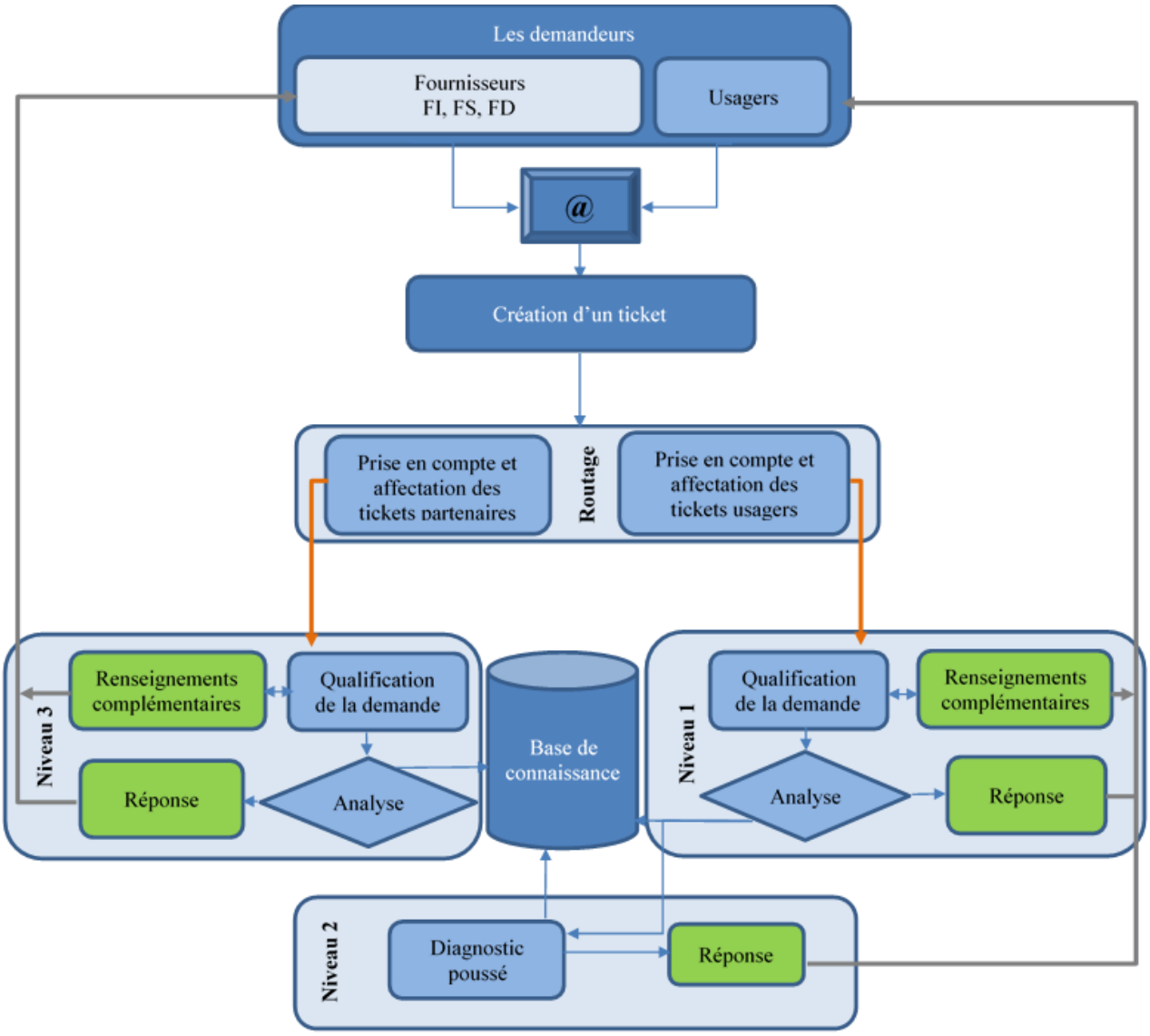


Figure 1 - Processus global du support du Téléservice FranceConnect/FranceConnect+

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 et doit systématiquement faire l'objet de l'envoi d'un courriel de confirmation à support.partenaires@franceconnect.gouv.fr par un contact habilité figurant dans la liste des contacts de l'Annexe Contacts du Fournisseur de service.

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.

6.1.2 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.

6.1.3 Assistance aux Partenaires Fournisseurs de service

Le support du Téléservice offre un service d'assistance aux Partenaires. Via l'outil de support, les Partenaires Fournisseurs de services peuvent principalement :

- Demander de l'aide lors de leur phase d'intégration au Téléservice ;
- 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 ;
- Poser des questions techniques ou fonctionnelles ;
- Gérer les usurpations/tentatives d'usurpation d'identité (cf. chapitre 6) ;
- Gérer les incidents (cf. chapitre 7).

6.1.4 Assistance aux Utilisateurs

Le Support du Téléservice offre également un service d'assistance aux Utilisateurs. Via l'outil de support 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.

6.2. Fonction Support chez le Fournisseur de service

Dans la mesure du possible, le Fournisseur de service met à disposition un support accessible aux utilisateurs. Par ailleurs, le Fournisseur de service est libre d'intégrer des messages pédagogiques adaptés aux spécificités de son service, incitant ses utilisateurs à utiliser le Téléservice.

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 de Service 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 de service 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 de service 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 applications du Fournisseur de Services utilisant FranceConnect et/ou FranceConnect+	Entreprise	1 (Critique)
	Dysfonctionnement concernant une seule application du Fournisseur de Services utilisant FranceConnect et/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 et/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.

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 heure	2 heures	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.	2,5 heures	4 heures	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 heures	12 heures	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 de l'Utilisateur.	15 heures	24 heures	Équipe Support de niveau 1
5 (Info)	- Le service fonctionne parfaitement. - La question ne concerne pas un dysfonctionnement de l'application FranceConnect et/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).	15 heures	24 heures	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 de service.
- 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 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 service.

9. GESTION OPERATIONNELLE DES RELATIONS FOURNISSEURS D'IDENTITE ET FOURNISSEURS DE SERVICES 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 de service suit le processus d'implémentation suivant :

- Demande d'habilitation à réaliser par le Fournisseur de service via le lien : https://franceconnect.gouv.fr/partenaires.
- Étude de la demande par la DINUM.
- Si la demande est complète et que tous les critères d'habilitation sont respectés, la DINUM valide la demande d'habilitation.
- Selon la demande d'implémentation, le Fournisseur de service reçoit alors ses accès à l'espace partenaires FranceConnect ou FranceConnect+, aux ressources de développement et à l'outil de Support partenaires.
- Lorsque le Fournisseur de service a finalisé l'implémentation du Téléservice FranceConnect ou FranceConnect+ sur son service, il communique à la DINUM, par l'envoi d'un mail à support.partenaires@franceconnect.gouv.fr, un accès à son environnement de test, afin de lui permettre de vérifier que les prérequis techniques, sécurité, parcours, pédagogie ont bien été respectés.
- Si la DINUM valide l'implémentation testée, le Fournisseur peut alors demander la mise en production de son service, sur son espace partenaire FranceConnect ou FranceConnect+.
- Le Fournisseur de 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.
- La DINUM lui communique alors ses jetons d'accès et code d'autorisation.
- Le Fournisseur de service intègre les jetons d'accès et code d'autorisation et passe alors en production.