

APNF – PFLAU

RECEVABILITE PFLAU :

MODE D'EMPLOI

Statu	En validation APNF
Auteur:	J. BIZART
Date:	29 October 2020
Classification:	Confidentiel
Version:	V004-02

Versions

Version no.	Version date	Status	Édité par	Validé par (le)	Modifications principales
1	11/05/2020	Validé	J. Bizart	A. Didierlaurent (12/05/2020)	Création du document
2	29/10/2020	En validation	J. Bizart	A. Didierlaurent (**/10/2020)	Refonte de la charte graphique Mise à jour des domaines "atos.net" en "pflau.fr"

TABLE DES MATIERES

Confidentiel

1	INTRODUCTION	5
1.1	OBJET DU DOCUMENT	5
1.2	RESPONSABILITES LIEES AU DOCUMENT	5
1.3	DOCUMENTS DE REFERENCE	5
1.4	ABREVIATIONS	5
1.5	LEGENDE	6
2	KIT DE RECEVABILITE	7
2.1	PRESENTATION	7
2.2	CONTENU DU KIT	7
2.3	APARTE SUR LES IHM	8
2.4	PROTOCOLE GENERAL	8
2.5	CONTRACTUALISATION	11
2.6	SUPPORT DEDIE	12
2.7	RESPONSABILITE ET EXPLOITATION	12
3	RECEVABILITE TECHNIQUE	13
3.1	PRESENTATION	13
3.2	ARCHITECTURE RESEAU	13
3.3	ACTEURS ET OUTILS	17
3.4	PROTOCOLE DE RACCORDEMENT TECHNIQUE	18
3.5	SECURISATION DES APPELS GETADDRESS :	35
3.6	SECURISATION DES APPELS TERMINAL_LOCATION-PUSH	36
4	RECEVABILITE FONCTIONNELLE	37
4.1	PRESENTATION	37
4.2	ARCHITECTURE FONCTIONNELLE	37
4.3	ACTEURS ET OUTILS	39
4.4	PROTOCOLE	40
4.5	LISTE DES SERVICES A VALIDER	41
4.6	VALIDATION DES SERVICES OPERATEUR	42
4.7	VALIDATION DES SERVICES CLASSIQUES PSAP	52

4.8	VALIDATION DES SERVICES SVH PSAP	57
5	MISE EN PRODUCTION ET APRES ?	64
5.1	MISE EN PRODUCTION	64
5.2	ET APRES ?	65

1 Introduction

1.1 Objet du document

Ce document sert de référence pour le raccordement des intervenants à la PFLAU via le kit de recevabilité. Il décrit le protocole à suivre par chaque opérateur ou intégrateur PSAP pour assurer son bon raccordement technique et fonctionnel avant d'être intégré aux flux bout en bout PFLAU.

1.2 Responsabilités liées au document

Worldline est responsable de la rédaction du mode d'emploi de la recevabilité PFLAU.
L'APNF est responsable de sa validation.

1.3 Documents de référence

N°	Version	Reference	Titre
1	09	TUM-APNF-PFLAU-E-DSF-002-XX Dossier de Conception IHM	Dossier de Conception IHM
2	28	TUM-APNF-PFLAU-E-DSF-001-XX Dossier de Conception PFLAU	Dossier de Conception PFLAU
3	2	Package WSDL PFLAU V5.zip	Package WSDL

1.4 Abréviations

Abréviation	Signification
APNF	Association pour les Plateformes de Normalisation des Flux inter-opérateurs
CGU	Conditions Générales d'Utilisation
DNS	Domain Name Server
FAQ	Foire Aux Questions
GSLB	Global Server Load Balancing
IHM	Interface Homme Machine
PFLAU	PlateForme mutualisée de Localisation des Appels d'Urgence
TTL	Time To Live
WL	Worldline
MNO	Mobile Network Operator
OPTA	Opérateurs Techniques d'Alimentation
SVH	service spécifique de Sauvegarde de la Vie Humaine

1.5 Légende

Afin de mettre en avant les informations importantes, elles seront présentées de la façon suivante :



Information particulièrement utile



Point nécessitant une attention particulière

2 Kit de recevabilité

2.1 Présentation

Le **kit de recevabilité** est un ensemble de **documents** et **outils** permettant à chaque **opérateur** ou **PSAP** de **s'interconnecter** avec la **PFLAU** en vue de sa **validation par l'APNF**.

On distingue 3 phases décrites dans les prochains paragraphes de ce mode d'emploi :

- le **raccordement technique**
- le **raccordement fonctionnel**
- l'**activation** et la **Mise En Production**

Pour rappel, la validation de la recevabilité se fera sur l'environnement cible du PSAP c'est-à-dire sur son environnement de **production**.

Une première phase de recevabilité peut être envisagée avec l'environnement de qualification de l'opérateur ou du PSAP, mais nécessitera d'en prévenir Worldline au préalable.

2.2 Contenu du kit

Le kit de recevabilité consiste en :

- ce **mode d'emploi** qui décrit les différentes étapes de la recevabilité, avec toutes les informations utiles à leurs bonnes réalisations (pourra être récupéré depuis l'IHM)
- une **IHM Web de recevabilité** permettant à l'intervenant de
 - suivre son avancement dans le processus de validation
 - consulter une FAQ pour répondre à ses éventuelles interrogations durant son intégration
 L'URL et les identifiants sont envoyés par email à chaque opérateur (cf. ci-après)
- une **fiche d'interconnexion VPN** (non applicable aux opérateurs avec Opta) qui liste
 - la configuration VPN Worldline (envoyée par mail)
 - les attendus opérateur qui seront à entrer sur l'IHM de recevabilité :
 - informations de contacts
 - configuration VPN opérateur
 - autres informations techniques utiles
- le **contrat type** : à renvoyer **par l'opérateur à Worldline, complété et signé**
- Un **package de WSDL/XSD** pour générer les classes de base de la PFLAU dont les règles métiers doivent ensuite être appliquées conformément aux règles définies dans le document « Dossier de conception PFLAU ».

	Utilisé pour les opérateurs	Utilisé pour les PSAP
mode d'emploi	✓	✓
IHM Web de recevabilité	✓	✓
fiche d'interconnexion VPN	✓	✗
contrat type	✓	✗
package de WSDL/XSD	✓	✓

2.3 Aparté sur les IHM

Afin de vous permettre de mettre en place votre recevabilité et ou d'administrer les informations présentes sur la PFLAU, vous disposez de deux IHM distinctes :

- L'IHM de recevabilité : <https://ihm-recevabilite.pflau.fr/>
- L'IHM d'administration : <https://ihm-administration.pflau.fr/>

A noter que ces deux sites, possèdent leurs propres données, ce qui est réalisé sur une IHM n'est pas répercuté automatiquement sur l'autre. Il en va de même pour les identifiants de connexion.

2.4 Protocole général

Le processus de recevabilité démarre avec la **déclaration de l'opérateur ou du PSAP par l'APNF, sur l'IHM de recevabilité**, qui fournit en particulier les informations suivantes à Worldline :

- **Adresse email de contact** pour
 - **La mise en place d'un point Kick Off de présentation du projet**
 - l'envoi du kit de recevabilité
 - la communication de l'URL de l'IHM de recevabilité et des identifiants de connexion
 - les échanges pendant le reste de la recevabilité

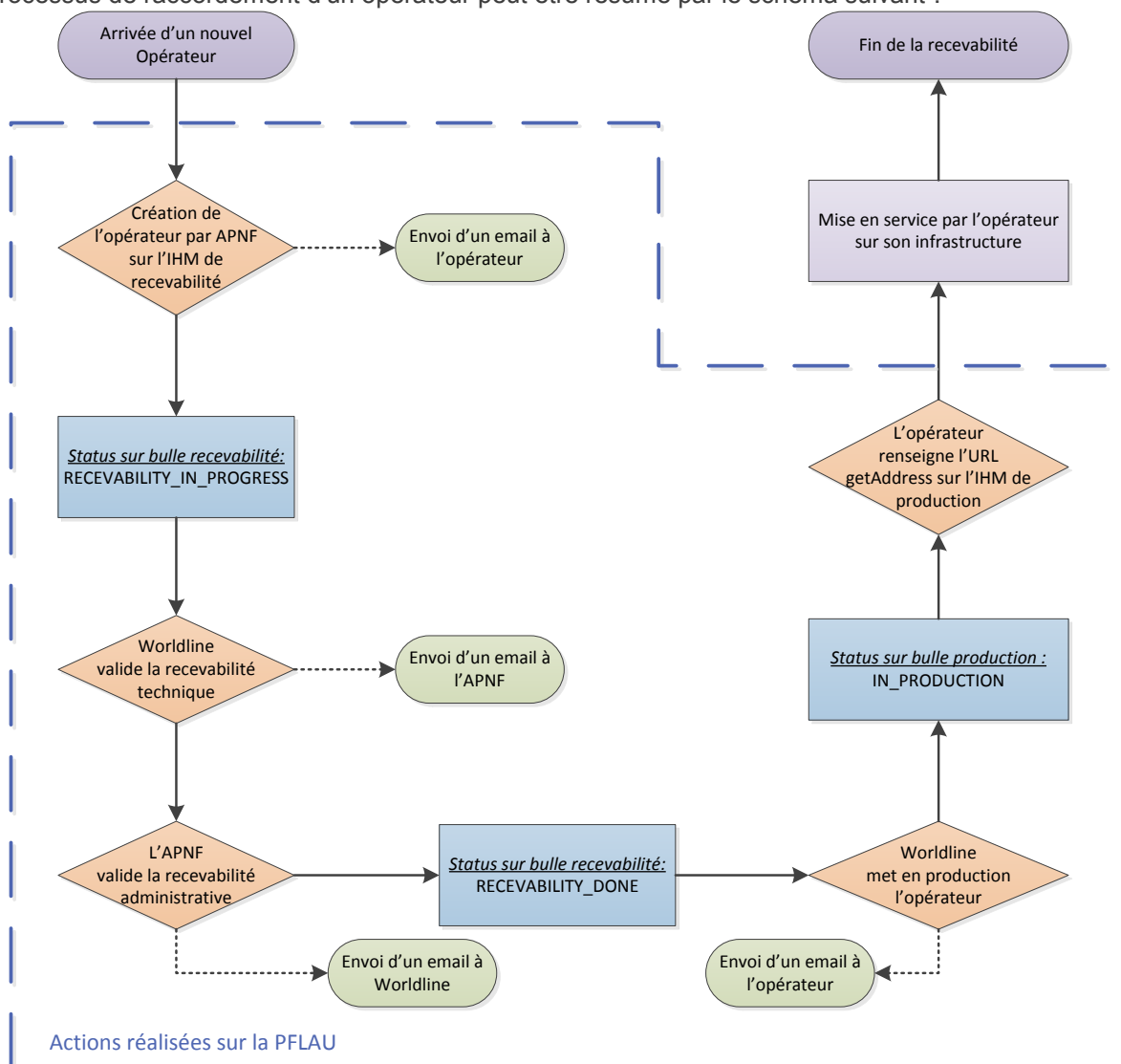
S'en suivent les recevabilités technique et fonctionnelle avant l'activation et la mise en production.



Le **PSAP** devra **obligatoirement** être présent dans l'un des fichiers CAAU précédemment intégrés sur la plateforme PFLAU.
Charge au PSAP de s'assurer de sa bonne intégration dans les fichiers de sa préfecture.
Lors du déclenchement de la recevabilité d'un PSAP, l'ensemble des idCAAU (idPSAP) non déjà rattachés à un intégrateur sera proposé dans une liste déroulante depuis l'IHM.
De même, si ce même PSAP n'est pas encore rattaché à un chef de projet ministériel, il devra le choisir via une liste déroulante depuis l'IHM.

2.4.1 Pour un opérateur

Le processus de raccordement d'un opérateur peut être résumé par le schéma suivant :



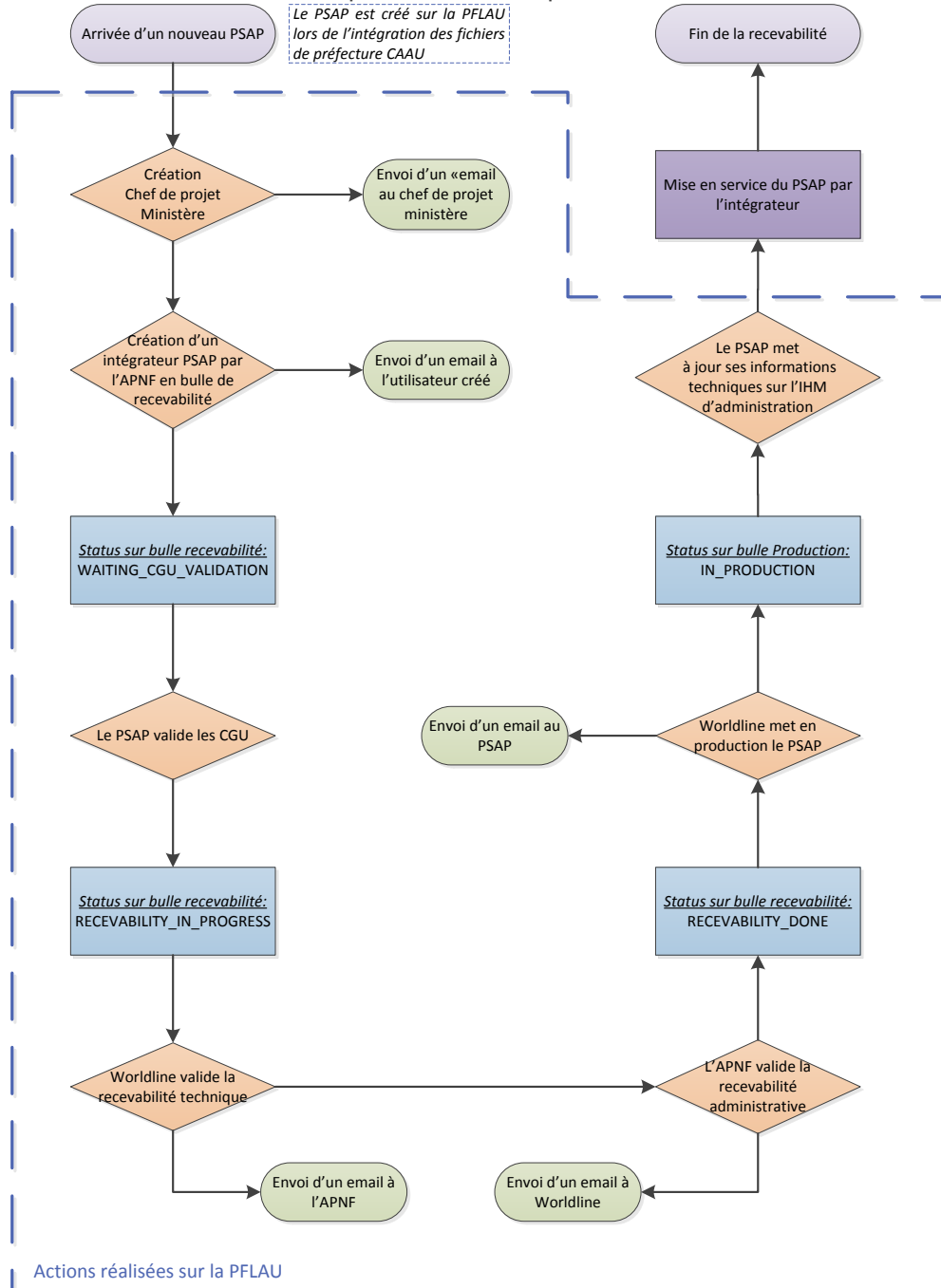
Les états de raccordement d'un opérateur sont :

- RECEVABILITY_IN_PROGRESS (cet état comprend l'ensemble des étapes déclarées dans le kit de recevabilité opérateur),
- RECEVABILITY_DONE,
- IN_PRODUCTION

Lors de la création de l'opérateur pour la recevabilité, un email est envoyé à cet opérateur détaillant les accès à l'IHM de recevabilité.

2.4.2 Pour un PSAP

Le processus de raccordement d'un PSAP peut être résumé par le schéma suivant :



Les états de raccordement d'un PSAP sont :

- WAITING_CGU_VALIDATION,
- RECEVABILITY_IN_PROGRESS (cet état comprend l'ensemble des étapes déclarées dans le kit de recevabilité PSAP),
- RECEVABILITY_DONE,
- IN_PRODUCTION

Un mécanisme de codification de ces différents états est mis en place afin de faciliter les échanges sur ces étapes du processus.

La recevabilité d'un PSAP peut démarrer dans deux cas :

- PSAP est son propre intégrateur : c'est à l'APNF de choisir ce PSAP nouvellement créé via l'intégration du CAAU et de créer le compte PSAP manager qui se voit ensuite notifié par email ses informations d'accès à l'IHM. Ensuite c'est au PSAP Manager de préciser les valeurs manquantes (nom, prénom, chef de projet ministère attaché et IP + url d'accès aux services PSAP)
- PSAP disposant d'un intégrateur : l'intégrateur se connecte et se rattache un PSAP en précisant les valeurs manquantes (nom, prénom, chef de projet ministère attaché et IP + url d'accès aux services PSAP) ; Il peut également créer le compte PSAP manager qui se voit ensuite notifié par email ses informations d'accès à l'IHM.

2.5 Contractualisation

2.5.1 Opérateur

Le raccordement VPN des opérateurs (non Opta) à la PFLAU se fait avec une **contractualisation** directement entre chaque **opérateur** et **Worldline**.

A cette fin, un **contrat type** est envoyé à l'opérateur avec le kit de recevabilité.

Charge à l'opérateur de retourner à Worldline

- le **contrat type complété et signé**,
- le ou les **bon(s) de commande** pour le règlement des coûts de raccordement Build et d'exploitation Run (CAPEX et OPEX indiqués dans le contrat type),
- Un extrait K-Bis récent,
- Ses numéros SIRET, SIREN et de TVA Intracommunautaire.



Le **démarrage de la recevabilité de l'opérateur et son intégration aux flux de production** est **conditionnée** par la bonne **réception** par Worldline **du contrat** et du **bon de commande** correspondant.

2.5.2 PSAP

Le raccordement des PSAP à la PFLAU est prévu au contrat existant entre Worldline et l'APNF. Il n'y a donc pas de contractualisation directe entre chaque PSAP et Worldline.

La facturation du raccordement est adressée à l'APNF selon les conditions prévues au contrat PFLAU.

2.6 Support dédié

La **recevabilité** est gérée **en autonomie par l'opérateur ou l'intégrateur PSAP** grâce à l'IHM de recevabilité.



Si l'intervenant le souhaite, il peut toutefois solliciter Worldline afin de **bénéficier d'un support dédié** pour faciliter son raccordement technique et/ou sa validation fonctionnelle.

Dans ce cas, un **devis spécifique** sera envoyé par Worldline à l'intervenant.

Toute demande fera l'objet d'une étude de charge et de planning par Worldline qui prendra en compte la disponibilité des ressources nécessaires au moment de la sollicitation.

2.7 Responsabilité et Exploitation.

Il est de la responsabilité des PSAP intégrateurs et des opérateurs de mettre en place les surveillances nécessaires sur leurs services pour s'assurer de leur bon fonctionnement.

La PFLAU ne fait que valider qu'il y a un flux entrant et sortant dans son ensemble.

- Si un PSAP ou un opérateur n'est plus joignable sur l'un de ses services en entrée, il peut le savoir par l'absence de flux entrant sur son service. **Aucune alerte ne sera envoyée.**
Si son trafic est nativement faible, libre à l'intervenant de mettre en place des solutions qui contrôlent la disponibilité vue de l'extérieur de son service.
- Si un PSAP ou un opérateur envoie des requêtes erronées en entrée de la PLFAU, il peut le savoir par l'analyse des réceptions de réponses avec un bloc **Bloc Status**.

Si des dérives sont constatées, Worldline peut potentiellement avertir l'APNF chaque début de mois sur la base des observations du mois précédent.

3 Recevabilité technique

3.1 Présentation

- D'un point de vue opérateur, la recevabilité technique consiste en la **mise en place** et en la **validation du lien VPN** entre l'**opérateur** et la **PFLAU**.
- D'un point de vue PSAP, la recevabilité technique consiste en la **mise en place** et en la **validation du lien SSL** entre l'**intégreteur PSAP ou un PSAP** et la **PFLAU**.

En préambule de ce chapitre, un rappel de l'architecture réseau est présenté afin de se repositionner dans le contexte général.

Nous listerons ensuite les acteurs de la recevabilité technique ainsi que les outils mis à leur disposition avant de détailler le protocole de raccordement.

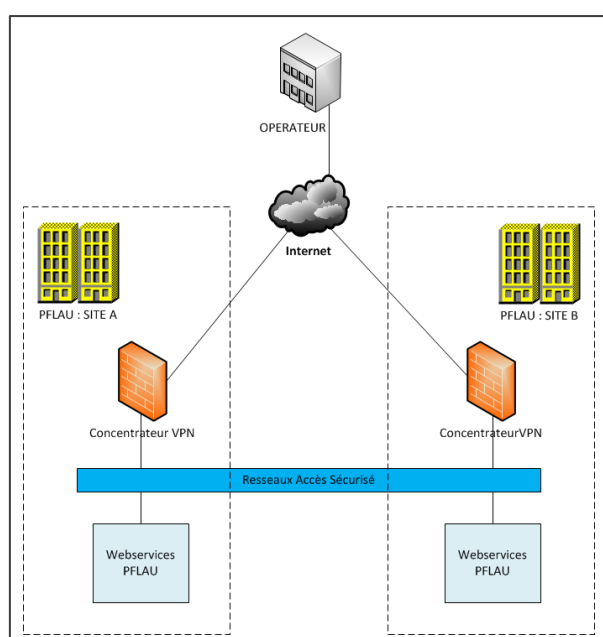
3.2 Architecture réseau

3.2.1 Raccordement bi-site actif/actif

3.2.1.1 Opérateur

L'**interconnexion** de l'opérateur avec la PFLAU se fait **au travers de réseau(x) VPN**.

Les **concentrateurs VPN PFLAU** sont dédiés, et **en bi-site actif/actif**

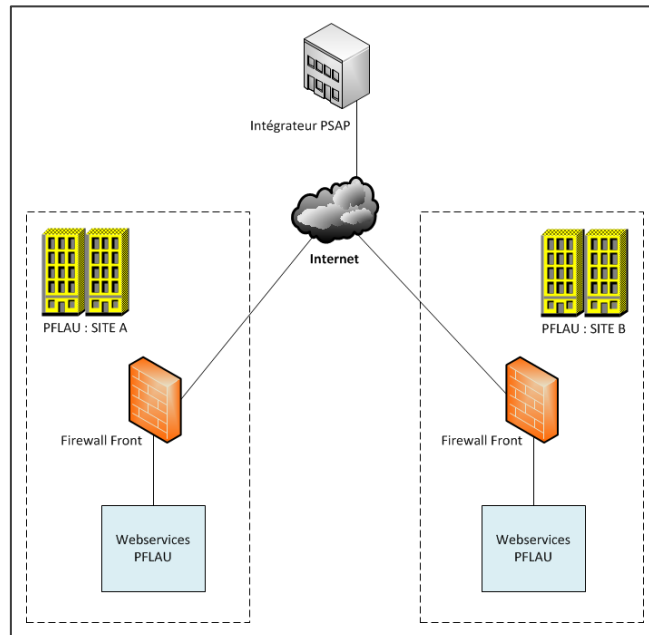


L'opérateur a la **responsabilité** de l'équipement présent chez lui (serveur VPN) ainsi que de sa connexion Internet.

3.2.1.2 PSAP

L'interconnexion avec la PFLAU se fait **en HTTPS**.

La gestion de la plateforme **PFLAU** se fait **en bi-site actif/actif**



L'intégrateur PSAP ou le PSAP a la **responsabilité** de l'équipement présent chez lui ainsi que de sa connexion Internet.

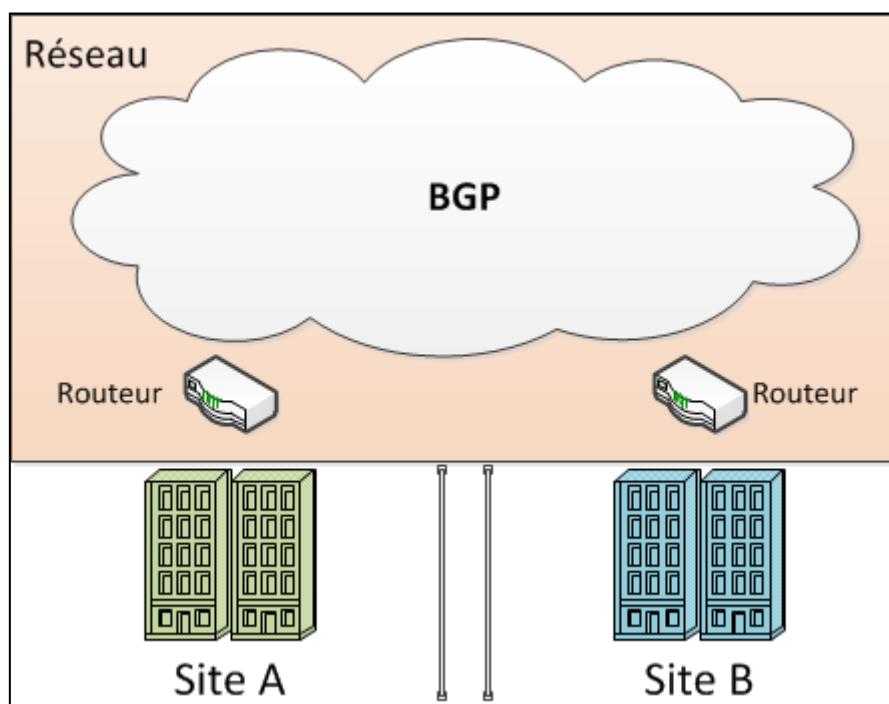
3.2.2 Particularités VPN

Les flux opérateur ↔ PFLAU étant bi-directionnels, le **VPN** est de type **Lan2Lan**.

Pour sécuriser les échanges :

- le chiffrement se fait via **tunnel IPSec**
- avec une authentification via **pre-shared key**

Pour assurer la **bascule automatique d'un site vers l'autre** en cas d'indisponibilité, les concentrateurs VPN primaire et backup sont **répartis sur chaque site** (exemple : si le primaire est indisponible sur le site A, les flux sont automatiquement repris par le concentrateur backup sur le site B).



Le processus de recevabilité prévoit le montage d'**un seul VPN par opérateur**

- **peer VPN Worldline unique** : utilisation des mêmes concentrateurs VPN Worldline pour adresser à la fois l'environnement de recevabilité et celui de production,
- **peer VPN opérateur unique** : une seule IP en entrée VPN opérateur



En cas de besoin particulier pour un opérateur (2 IP en entrées, réseaux de recevabilité et production complètement étanches), **il reste possible de monter 2 VPN, après validation des équipes techniques Worldline.**

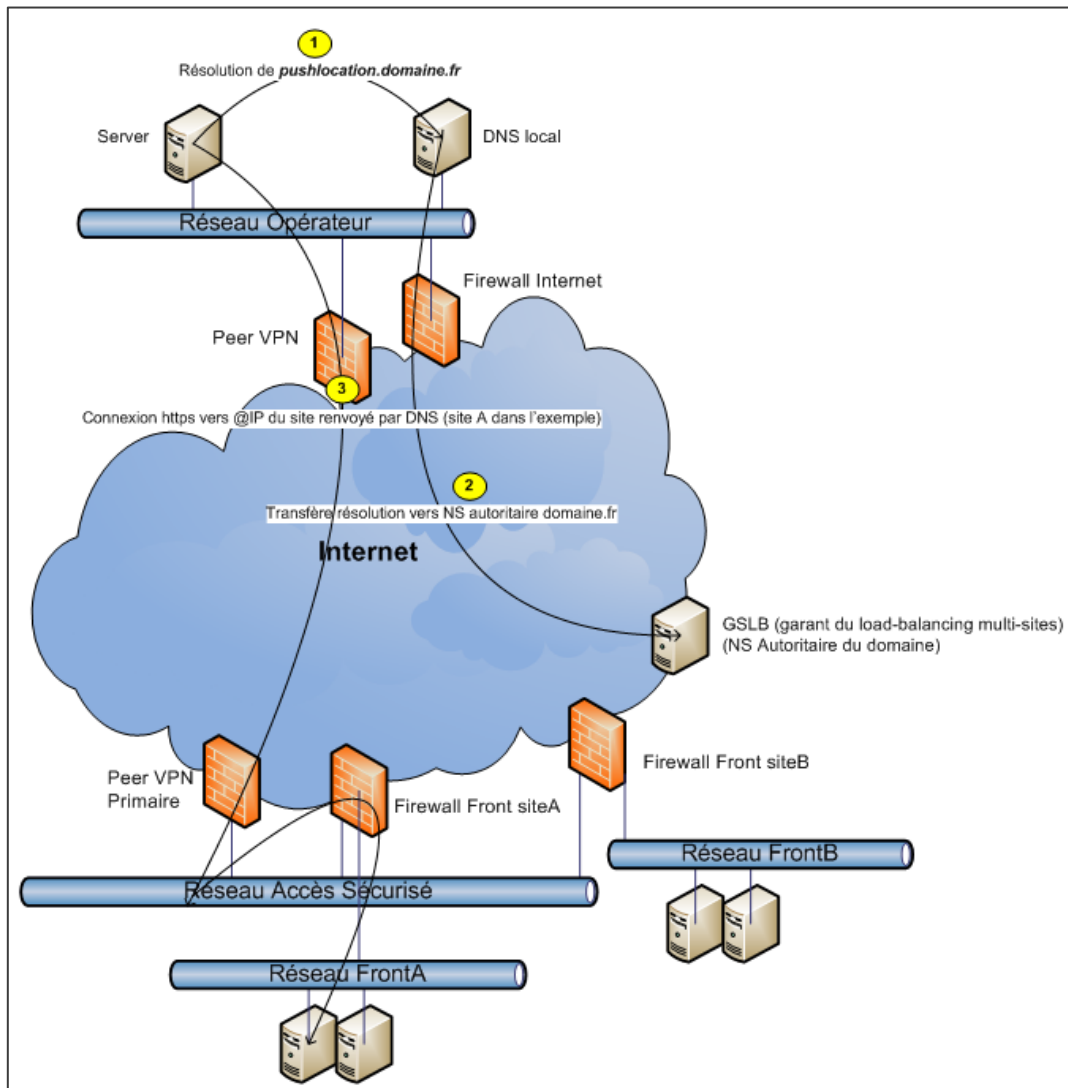
La configuration se fera alors via une *demande de support dédié* avec un **devis spécifique** envoyé par Worldline à l'opérateur.



Ce processus permet à la PFLAU de limiter l'impact en cas de perte d'un des deux sites. Si l'opérateur ne procède pas à une résolution DNS régulièrement, il prend à sa charge la responsabilité de basculer tout son flux sur le site fonctionnel puis de reprendre le trafic sur les deux sites lorsque ceux-ci sont à nouveau disponibles.

3.2.3 Loadbalancing applicatif bi-site

La **répartition de charge bi-site** est assurée par un équipement de type **GSLB** (résolution DNS dynamique) :



Worldline recommande fortement d'effectuer systématiquement la résolution DNS pour s'affranchir des problématiques de disponibilité de l'un des deux sites.

Si l'intervenant ne procède pas à une résolution DNS régulièrement, il prend à sa charge la responsabilité de basculer tout son flux sur le site fonctionnel puis à reprendre le trafic sur les deux sites lorsque ceux-ci sont à nouveau disponibles.

3.3 Acteurs et Outils

La recevabilité technique se fait via l'IHM de recevabilité : <https://ihm-recevabilite.pflau.fr/>

La recevabilité technique implique les acteurs suivants :

	Qui ?	Rôle
Pour un opérateur	Opérateur	- Montage du VPN client via le processus de recevabilité - Validation du VPN avec Worldline
	Worldline	- Montage du VPN serveur (PFLAU) - Validation du VPN avec l'opérateur
Pour un PSAP	Intégrateur PSAP / PSAP	- Autorisation d'accès à l'IP Worldline sur le SI du PSAP - Validation de l'accès SSL avec Worldline
	Worldline	- Autorisation d'accès à l'IP intégrateur PSAP / PSAP et ajout de l'autorité de certification (si pas déjà connue des serveurs) - Validation de l'accès SSL avec l'intégrateur PSAP / PSAP

Elle se fait au moyen des outils suivants :

	Qui ?	Rôle
Mode d'emploi recevabilité	Opérateur/intégrateur PSAP	- Description du protocole à suivre
IHM Web de recevabilité	Opérateur/intégrateur PSAP	- Suivi d'avancement du raccordement - Synchronisation opérateur/Worldline pour la validation VPN
Fiche d'interconnexion VPN	Opérateur	- Informations techniques Worldline nécessaires à la configuration VPN opérateur
Environnement FRONT de <u>recevabilité</u> Opérateur/Worldline	Opérateur	- Validation du VPN en <u>recevabilité</u> - URI/Pages d'accès au webservice de recevabilité : 1 côté PFLAU et l'équivalent côté opérateur pour valider les montages VPN dans les 2 sens.
Environnement FRONT de <u>production</u> Opérateur/Worldline	Opérateur	- Validation du VPN en <u>production</u> - URI/Pages d'accès au webservice de production : 1 côté PFLAU et l'équivalent côté opérateur pour valider les montages VPN dans les 2 sens
Fiche d'interconnexion SSL	Intégrateur PSAP	- Informations techniques Worldline/Intégrateur nécessaires à la configuration SSL
Environnement FRONT de <u>production</u> Intégrateur PSAP/Worldline avec une page/URL de test	Intégrateur PSAP	- Validation de l'accès SSL en <u>production</u> - 2 urls de pages de test : 1 côté PFLAU et l'équivalent côté intégrateur PSAP / PSAP pour valider l'accès dans les 2 sens

3.4 Protocole de raccordement technique

3.4.1 Opérateur

1.1.1.1 Validation des CGU

Cette étape est valable pour les deux types d'opérateurs.

La première étape consiste à la **connexion de l'opérateur à l'IHM de recevabilité** via l'URL et l'identifiant qu'il a reçu par mail suite à son inscription par l'APNF.

L'IHM affiche l'ensemble des étapes de la recevabilité. Seule la première est active et peut être modifiée par l'opérateur : la **validation des CGU**.

Administration PFLAU

Recevabilité Documentation OPER_MANAGER

Fonctionnement nominal

Recevabilité de l'opérateur OPER

1. CGU
2. INFOS VPN
3. PSK
4. CONFIG VPN
5. TEST VPN OPÉRATEUR
6. TEST VPN WORLDLINE
7. TEST PUSH
8. TEST PUSH SVH
9. TEST GET ADDRESS
10. TEST GET LOCATION SVH
11. TEST NOTIFY
12. VALIDATION WORLDLINE
13. VALIDATION APNF

1. Validation des CGU

Veuillez lire puis accepter les conditions générales d'utilisation du service avant de poursuivre.

Conditions Générales d'Utilisation

CONDITIONS GÉNÉRALES D'UTILISATION (CGU) DU SERVICE PFLAU

Objet du service « PFLAU »

1. Le service « PFLAU » (ci-après dénommé le « Service ») est un site mis en œuvre par l'Association des Plateformes de Normalisation des Flux Inter-opérateur, code SIREN 512 434 226, dont le siège social est 11-17 rue de l'Amiral Hamelin - 75116 Paris (ci-après dénommée « l'APNF ») contribuant à mutualiser les échanges entre les opérateurs de communications électroniques et les centres de réception des appels d'urgence pour répondre efficacement à l'article D95-8 du code des postes et des communications électroniques (« CPCE ») pris en application de l'art. L33-1

Règlement des litiges

23. En cas de manquement de l'une des Parties à ses obligations issues des présentes, celles-ci conviennent de se rencontrer dans les plus brefs délais afin d'y apporter une solution.

24. Les présentes CGU sont régies par la loi française. Tout différend relatif à l'application, l'exécution et l'interprétation des présentes relèvera, à défaut d'accord amiable, des juridictions compétentes du ressort du Tribunal Administratif de Paris.

Résiliation

25. En cas d'évolution législative ou réglementaire rendant obsolètes les présentes Conditions Générales d'Utilisation, l'une ou l'autre des Parties pourra résilier les présentes afin de se conformer à ses nouvelles obligations. La résiliation interviendra dans un délai compatible avec les nouvelles obligations et/ou la mise en service de solutions techniques adaptées à ces nouvelles obligations. Cette résiliation du Service ne donne droit à aucune indemnité.

26. Les parties conviennent de la possibilité de mettre fin aux présentes pour tout autre motif par lettre recommandée avec avis de réception moyennant un préavis d'1 (un) an, sauf accord des Parties sur un autre délai. Fait à le en 1 (un) exemplaire original Pour le centre de réception des appels d'urgence : Désignation du Service Nom et fonction du signataire dûment habilité aux présentes ANNEXE 1 Coordonnées du Responsable habilité pour le Service d'Urgence Désignation du Service : NOM, Prénom : Fonction : Coordonnées : (signature et tampon)

☐ Oui, je confirme avoir pris connaissance des Conditions Générales d'Utilisation du service.

Valider l'étape

Retour

En validant cette étape, l'opérateur accepte les **CGU PFLAU** consultables sur l'IHM de recevabilité et **active l'étape suivante** : la saisie des informations VPN.



A noter que cette validation de CGU ne se substitue pas à la **contractualisation** qui doit être réalisée entre les parties prenantes du projet.

3.4.1.1 Informations VPN

L'**opérateur saisit ses informations VPN** via le **formulaire** de l'IHM (type d'équipement, IP Peer, domaines d'encryptions...) **ainsi que les URL de ses 2 webservices**, en recevabilité et production, mises à disposition de Worldline pour les tests VPN.

Les informations VPN de la partie Worldline sont téléchargeables par l'opérateur directement en haut de cette page de l'IHM.

À ce jour, 2 modes sont autorisés : SHA-1 et SHA-2.

Les informations définies ci-dessous sont extraites de la version SHA1-2 qui est le standard Worldline.



Le protocole de recevabilité prévoit la configuration d'**un seul VPN**.
Si l'opérateur souhaite mettre en place **2 VPN**, il doit passer par une **prestation dédiée**.



A noter que dans le cas d'un **opérateur** déclarant utiliser un autre **opérateur défini comme Opta**, la **phase de déclaration de lien VPN n'est pas nécessaire**. Il arrive **directement sur l'étape de validation fonctionnelle**.
De plus, les **étapes de validation VPN sont également sorties des étapes de recevabilité**.



Toutes les valeurs présentées dans la colonne « *valeurs recommandées par Worldline* » sont issues des **recommandations de nos experts** sécurité réseau et ne peuvent être modifiées.
Toutes demandes de modification des valeurs indiquées par ce tableau feront l'objet d'une demande explicite impliquant une demande de validation de la part de nos experts sécurité réseau.



Tous les acteurs interconnectés via VPN à la PFLAU passent par les mêmes concentrateurs VPN et doivent donc utiliser des IP distinctes pour éviter tout conflit.
A cette fin, **le domaine d'encryption de l'opérateur doit correspondre à des plages d'IP publiques**.
Il n'y aura pas de dérogation sur ce point.



Les IP sont exclusivement des **IP v4**. **Les IP de type V6 ne sont pas autorisées**.



Dans le cas d'un opérateur souhaitant gérer les environnements de recevabilité et de production de manière distincte via **2 VPN**, l'opérateur pourra saisir les valeurs de l'environnement de production et faire **une demande** auprès de Worldline pour **intégrer le second VPN en mode projet**.



Seuls les ports **443** et **20443** sont autorisés sur la plateforme de recevabilité. Aucune demande d'ouverture sur des ports autres n'est possible.

Une fois ses informations VPN renseignées, **l'opérateur valide le formulaire**.

Confidentiel

Elles sont alors **vérifiées automatiquement** (données obligatoires, formats) :

- si elles sont valides : activation de la prochaine étape, l'échange de preShared Key
- sinon, un message d'erreur est affiché sur l'IHM indiquant les modifications nécessaires pour passer à l'étape suivante

Recevabilité de l'opérateur OPER

1. CGU

2. INFOS VPN

3. PSK

4. CONFIG VPN

5. TEST VPN OPÉRATEUR

6. TEST VPN WORLDLINE

7. TEST PUSH

8. TEST PUSH SVH

9. TEST GET ADDRESS

10. TEST GET LOCATION SVH

11. TEST NOTIFY

12. VALIDATION WORLDLINE

13. VALIDATION APNF

2. Informations VPN

Etape précédente

Veuillez renseigner les coordonnées du contact projet et du contact technique. Remplissez ensuite les informations demandées sur les caractéristiques du VPN à mettre en place. [Télécharger le fichier d'interconnexion VPN](#)

Terminez ensuite en indiquant les URL d'accès aux pages de tests puis validez le formulaire pour les envoyer à Worldline.

Coordonnées du contact projet (MOA)

Nom

Nom du contact projet

Téléphone

Téléphone du contact projet

Fax (facultatif)

-

Email

Email du contact projet

Coordonnées du contact technique

Nom

Nom du contact technique

Téléphone

Téléphone du contact technique

Fax (facultatif)

-

Email

Email du contact technique

Informations techniques

Equipement de terminaison VPN

Nom de votre équipement

Ip V4 publique du tunnel

Ip V4 publique de votre équipement

Domaine de cryptage

Domaine de cryptage

Masque de sous-domaine du cryptage

Phase 1 - Paramètres IKE

Mode d'authentification

PreSharedKey

Algorithme d'authentification

SHA-256

Algorithme de cryptage

AES-256

Groupe Diffie-Hellmann

2

Durée de validité (secondes)

86400

Méthode d'authentification

librev2

Mode de négociation

Main mode

Phase 2 - Paramètres ISAKMP

Protocole de cryptage

AES-256

Algorithme de hash

SHA-256

Algorithme d'authentification

SHA-256

Algorithme de cryptage

Algorithme de cryptage

Mode d'encapsulation

Mode tunnel

Confidentialité persistante

☒

Utiliser le groupe PFS

2

Durée de vie de la clé

28800

URL des pages de test

URL de la page de test en qualification

Indiquez le lien vers la page de test

URL de la page de test en production

Indiquez le lien vers la page de test

Instructions

Commentaires utiles

Indiquez ici tout commentaire utile

Valider l'étape

Retour

Mode d'emploi recevabilité PFLAU
© Worldline

En validation APNF | Version V004-02 | 29 October 2020 | Page 20 of 67

3.4.1.2 Echange de la preShared Key

Suite à la validation des informations VPN par Worldline, l'opérateur a la possibilité depuis l'IHM de réaliser la génération de la preShared Key.

En parallèle, Worldline valide les données VPN transmises par l'opérateur.

En cas de validation, un email est envoyé au contact technique saisi dans l'étape précédente afin de convenir d'une date et/ou heure d'appel entre **Worldline et l'opérateur** pour la réalisation de l'étape suivante : à savoir les tests VPN.

Dans le cas contraire, un autre email sera envoyé afin de demander un complément d'information et/ou demande de modification de la configuration envoyée.



Sécurité : la **preshared key** générée par Worldline aura une taille **d'au moins 20 caractères**

C'est l'opérateur qui validera l'étape sur l'IHM, une fois la preShared Key générée et communiquée.



Sécurité : l'opérateur **doit conserver** cette donnée car elle ne pourra être refournie. En cas de perte, une demande par email à Worldline devra être faite afin de repositionner l'IHM sur l'étape d'Echange de preShared Key pour relancer cette étape.

Fonctionnement nominal

Recevabilité de l'opérateur OPER

- 1. CGU
- 2. INFO'S VPN
- 3. PSK
- 4. CONFIG VPN
- 5. TEST VPN OPÉRATEUR
- 6. TEST VPN WORLDLINE
- 7. TEST PUSH
- 8. TEST PUSH SVH
- 9. TEST GET ADDRESS
- 10. TEST GET LOCATION SVH
- 11. TEST NOTIFY
- 12. VALIDATION WORLDLINE
- 13. VALIDATION APNF

3. Récupération de la PSK

Etape précédente

Générer la clé

12/\$=_5gU9OG.&D=1u,=

ATTENTION la PreSharedKey est générée de façon unique et n'est pas stockée au sein du service PFLAU. Veillez à noter et conserver cette clé. En cas de perte, nous ne pourrions pas vous la communiquer à nouveau. Une nouvelle clé pourra néanmoins être générée en contactant l'équipe technique PFLAU.

Valider l'étape

[Retour](#)

3.4.1.3 Configuration VPN

Une fois la preshared key partagée, **l'opérateur et Worldline** peuvent **mettre en place les configurations VPN** sur leurs équipements respectifs.



Les informations Worldline pour le paramétrage VPN côté opérateur sont détaillées dans les fiches d'interconnexion récupérées à l'étape de saisie des informations VPN.



Afin de faciliter les configurations, les protocoles **ping** et **telnet** sont **ouverts** sur les **ports 80 et 443** côté PFLAU.

Recevabilité de l'opérateur OPER

- 1. CGU
- 2. INFOS VPN
- 3. PSK
- 4. CONFIG VPN
- 5. TEST VPN OPÉRATEUR
- 6. TEST VPN WORLDLINE
- 7. TEST PUSH
- 8. TEST PUSH SVH
- 9. TEST GET ADDRESS
- 10. TEST GET LOCATION SVH
- 11. TEST NOTIFY
- 12. VALIDATION WORLDLINE
- 13. VALIDATION APNF

4. Configuration VPN côté Worldline

Etape précédente

Cette étape est réalisée par Worldline.
 Vos contacts technique et projet seront notifiés par mail une fois l'étape terminée.

[Retour](#)



Afin d'assurer le loadbalancing des requêtes opérateur, le réseau opérateur doit avoir un accès DNS connecté à Internet pour résoudre l'IP PFLAU à adresser **lors de chaque appel, via le serveur GSLB**.

En cas de **cache DNS**, son **TTL** ne doit pas excéder les **30 secondes**.



Sécurité :

Comme indiqué dans les configurations VPN Worldline, les **algorithmes d'authentification** et de **chiffrement** à paramétrer sont **obligatoirement** de type SHA-1 ou **SHA256**

L'étape de recevabilité suivante est effectuée par **Worldline**. Le workflow de recevabilité est mis à jour une fois **la configuration VPN opérée côté PFLAU**.

Cette action a pour effet de **notifier l'opérateur par email** (aux contacts projet et technique précédemment renseignés) afin de le prévenir qu'il peut commencer ses tests d'interconnexions.

Libre à **l'opérateur** de démarrer ses **tests VPN dès qu'il est prêt**, selon son état d'avancement de configuration VPN.

3.4.1.4 Tests VPN

Les tests VPN visent à **valider** le bon montage de **tunnels VPN dans les 2 sens** et pour adresser **chaque environnement (recevabilité et production)** :

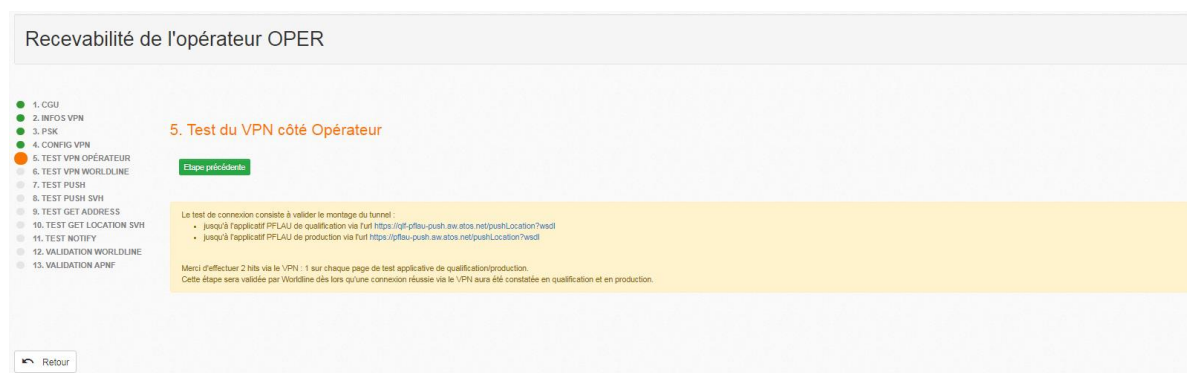
- d'abord Opérateur => PFLAU (Worldline)
- puis PFLAU (Worldline) => Opérateur

En général il peut être plus simple de réaliser ces deux étapes en convenant d'une réunion téléphonique commune entre l'ingénieur réseaux de l'opérateur et de Worldline.

Remarque : Attention, il convient de planifier **à l'avance** d'un créneau de réunion téléphonique entre Worldline et l'opérateur.

Opérateur vers Worldline

Dès que l'opérateur a validé ses tests, il l'indique à Worldline qui valide cette étape sur l'IHM de recevabilité.



Le test de connexion consiste à valider le montage du tunnel :

- jusqu'à l'appli PFLAU de recevabilité
- jusqu'à l'appli PFLAU de production

Les URL à tester sont rappelées sur cette page de l'IHM et sont :

- <https://push-recevabilite.pflau.fr/pushLocation>
- <https://push.pflau.fr/pushLocation>

Il s'agit donc pour l'opérateur d'effectuer 2 hits via le VPN : 1 sur chaque page/uri applicative de recevabilité/production.

Worldline valide l'étape dès lors qu'une **connexion réussie de l'opérateur via le VPN** a été constatée **en recevabilité et en production**.

Worldline vers Opérateur

Une fois le test opérateur validé, l'**étape suivante** est faite par Worldline qui lance les hits sur les pages/URI de recevabilité et de production de l'opérateur dès que le **tunnel VPN** n'est monté.

1. CGU
2. INFOS VPN
3. PSK
4. CONFIG VPN
5. TEST VPN OPÉRATEUR
6. TEST VPN WORLDLINE
7. TEST PUSH
8. TEST GET SVH
9. TEST GET ADDRESS
10. TEST GET LOCATION SVH
11. TEST NOTIFY
12. VALIDATION WORLDLINE
13. VALIDATION APNF

6. Test du VPN côté Worldline

Etape précédente

Worldline va désormais procéder aux tests de connexion VPN en effectuant des hits sur les pages de qualification/production de l'opérateur. Merci de vous assurer que le tunnel n'est plus monté dans le sens Opérateur vers Worldline.

Cette étape sera validée par Worldline dès lors qu'une connexion réussie via le VPN aura été constatée en qualification et en production.

Retour



Afin de permettre à Worldline de valider le montage VPN dans le sens WL=>OP, **l'opérateur doit s'assurer que le tunnel VPN n'est plus monté dans le sens OP=>WL** une fois ses tests terminés.



Le test de connexion consiste à valider le montage du tunnel jusqu'au service Web opérateur exposant la méthode *getAddress* :

- sur l'environnement de recevabilité de l'opérateur,
- sur l'environnement de production de l'opérateur.

Il s'agit donc pour l'opérateur de mettre à disposition de Worldline **une page ou uri applicative par environnement, via le VPN** (URLs renseignées précédemment lors de l'étape «*Informations VPN* » : cf. 1.1.1.1.2)

Cette **dernière étape** du raccordement VPN est alors **validée par Worldline** dès qu'un **hit** est réalisé **avec succès** sur les environnements de **recevabilité** et de **production de l'opérateur**.



Le VPN étant opérationnel, les protocoles **ping** et **telnet** sur les **ports 80** et **443** ne sont plus utiles.

Pour des raisons de sécurité, il est **vivement recommandé** à l'opérateur de supprimer ces ouvertures réseaux.

La **recevabilité technique terminée**, l'**opérateur peut démarrer sa recevabilité fonctionnelle**.

3.4.2 PSAP (flux classique)

Par défaut un PSAP a, à disposition, une URL pour dérouler sa recevabilité PFLAU. (<https://ihm-recevabilite.pflau.fr/>)

Si en plus il est habilité par l'APNF à faire des requêtes dans un cadre SVH, une deuxième URL est mise à sa disposition pour réaliser celle-ci.

Détail du Psap

Fiche Psap

Utilisateurs

Consulter la recevabilité du psap

Consulter la recevabilité SVH du psap

Identifiant	FR990PSAP
Manager	
Mail du contact	CCQA-PFLAU@golive.fr
Mail des statistiques	CCQA-PFLAU@golive.fr
Adresse	07-10
Code postal	75019
Ville	Casa
Intégrateur	Jérémie Bizart
Chef de projet Ministère	manager-RE minister
Plages IP *	
Uri de PushLocation *	
Eligible SVH	Non
Seuil Warning d'urgence	199
Seuil Alert d'urgence	999

* Champ utilisé en production

3.4.2.1 Consultation des CGU

La première étape consiste à une **connexion de l'intégrateur PSAP ou du PSAP à l'IHM de recevabilité** avec les identifiants qu'il a reçus par mail suite à son enregistrement sur la PFLAU.

L'IHM affiche l'ensemble des étapes de la recevabilité. Seule la première est active et peut être modifiée par l'intégrateur ou le PSAP : la **consultation des CGU**.

Recevabilité du Psap FR990PSAP

1. CGU
2. INFOS SSL
3. CONF SSL
4. TEST PUSH
5. TEST PULL
6. VALIDATION WORLDLINE
7. VALIDATION APNF

1. Validation des CGU

Vous devez lire puis accepter les conditions générales d'utilisation du service avant de poursuivre.

Conditions Générales d'Utilisation

CONDITIONS GÉNÉRALES D'UTILISATION (CGU) DU SERVICE PFLAU

Objet du service « PFLAU »

1. Le service « PFLAU » (ci-après dénommé le « Service ») est un site mis en œuvre par l'Association des Plateformes de Normalisation des Flux Inter-opérateur, code SIREN 512 434 226, dont le siège social est 11-17 rue de l'Amiral Hamelin – 75116 Paris (ci-après dénommée « l'APNF ») contribuant à mutualiser les échanges entre les opérateurs de communications électroniques et les centres de réception des appels d'urgence pour répondre efficacement à l'article D58-8 du code des postes et des communications électroniques (« CPCE ») pris en application de l'art. L33-1 f) du CPCE qui exige des opérateurs de communications électroniques qu'ils fournissent aux services d'urgence l'information relative à la localisation de l'appelant. Les données de localisation transmises dans le cadre du Service sont les nom, prénom, ou raison sociale et adresse de l'appelant (adresse de facturation pour le mobile, adresse d'installation ou à défaut de facturation pour le fixe), et la localisation géographique de l'appel (pour le mobile uniquement).

2. Les présentes Conditions Générales d'Utilisation ont pour objet de définir les modalités d'utilisation du service « PFLAU » par les centres de réception des appels d'urgence (ci-après dénommés « CRAU »).

Fonctionnalités du Service

3. Ce Service offre deux fonctionnalités aux CRAU : • Un compte gestionnaire unique pour administrer les comptes utilisateurs. L'utilisateur CRAU peut accéder au service pflau.apnf.fr pour mettre à jour les données administratives (adresse, contact, ...) de son centre de réception des appels d'urgence associé. • Deux webservices en HTTPS permettant la transmission des données de l'appelant : o le webservice « PostTerminalLocation » permet à l'opérateur de communications électroniques de transmettre à la « PFLAU » les données de localisation de tout appelant aux services d'urgence par un téléphone mobile. La précision et le format de localisation sont liés au type d'équipement détenu par chaque opérateur de communications électroniques. o le webservice « GetTerminalLocation » permet à la « PFLAU » d'obtenir les données d'adresse d'un numéro de téléphone (fixe ou mobile) entendues comme les nom, prénom ou raison sociale et adresse de l'appelant (adresse de facturation pour le mobile, adresse d'installation ou à défaut de facturation pour le fixe).

Modalités d'inscription et d'utilisation du Service

4. L'accès au Service est ouvert aux seuls CRAU identifiés dans les plans départementaux d'acheminement des appels d'urgence en vigueur communiqués par les représentants de l'Etat dans chaque département.

22. Les Conditions Générales d'Utilisation doivent être transmises, dûment signées et paraphées, accompagnées des coordonnées du Responsable visé à l'article 6 des présentes, en 1 (un) exemplaire à l'adresse suivante (le CRAU conservant un exemplaire) : APNF 11-17 rue de l'Amiral Hamelin – 75116 Paris

Règlement des litiges

23. En cas de manquement de l'une des Parties à ses obligations issues des présentes, celles-ci conviennent de se rencontrer dans les plus brefs délais afin d'y apporter une solution.

24. Les présentes CGU sont régies par la loi française. Tout différend relatif à l'application, l'exécution et l'interprétation des présentes relèvera, à défaut d'accord amiable, des juridictions compétentes du ressort du Tribunal Administratif de Paris.

Résiliation

25. En cas d'évolution législative ou réglementaire rendant obsolète les présentes Conditions Générales d'Utilisation, l'une ou l'autre des Parties pourra résilier les présentes afin de se conformer à ses nouvelles obligations. La résiliation interviendra dans un délai compatible avec les nouvelles obligations et/ou la mise en service de solutions techniques adaptées à ces nouvelles obligations. Cette résiliation du Service ne donne droit à aucune indemnité.

26. Les parties conviennent de la possibilité de mettre fin aux présentes pour tout autre motif par lettre recommandée avec avis de réception moyennant un préavis d'1 (un) an, sauf accord des Parties sur un autre délai. Fait à le en 1 (un) exemplaire original Pour le centre de réception des appels d'urgence : Désignation du Service Nom et fonction du signataire dûment habilité aux présentes ANNEXE 1 Coordonnées du Responsable habilité pour le Service d'Urgence Désignation du Service : NOM, Prénom : Fonction : Coordonnées : (signature et tampon)

☐ Oui, j'ai lu et j'accepte les Conditions Générales d'Utilisation du service

Valider l'étape

Retour

En validant cette étape, l'intégrateur PSAP ou le PSAP informe avoir pris connaissance des **CGU PFLAU (fichier PDF consultable et téléchargeable sur l'IHM de recevabilité via url)** et **active l'étape suivante** : la saisie des Informations SSL. L'APNF ne validera la fin de recevabilité que si elle a reçu par courrier les CGUs signées par le PSAP.

3.4.2.2 Informations SSL

Avant de poursuivre les étapes suivantes sur l'IHM de recevabilité (tests fonctionnels), l'intégrateur effectue son raccordement SSL avec le support de Worldline.

L'intégrateur **PSAP** ou le **PSAP** transmet ses informations techniques à Worldline via la **fiche d'interconnexion SSL** (autorité de certification et CN associé à son certificat, url de crt, plage IP utilisées) incluant l'**URL de son webservice de production** mises à disposition de Worldline.

Tous les acteurs interconnectés via SSL à la PFLAU doivent utiliser des IP **distinctes et publiques**.

De plus, pour permettre une optimisation dans la validation et la vérification des certificats, nous limitons les **autorités de certification** possible à la liste suivante :

- **ASIP** : services de certification pour le secteur santé-social,
- **IGC/A** : services de certification pour l'État français. Dans le cas d'un PSAP certifié par l'IGC/A, celui-ci s'engage à ce que l'autorité racine et parente du certificat reste l'IGC/A afin d'éviter les maillons intermédiaires lors de la récupération du fichier CRL,
- **Sécurité Intérieure**,
- **Entrust**,
- **Symantec** (anciennement Verisign),
- **OPENTRUST** (ex Keynectis),
- **DIGICERT**,

Worldline n'acceptera pas un certificat différent de cette liste. Aucune exception ne sera autorisée.

À la commande de votre certificat, prêtez bien attention à ce que le CN de ce certificat corresponde au DNS exposé par votre service.



Ce certificat doit également exposer la chaîne complète de certification.

Si vous faites le choix d'utiliser un certificat wildcard, vous devrez mettre en place la configuration nécessaire pour que le certificat présenté à la PFLAU affiche un CN égale au DNS exposé par votre service.

Par exemple si votre service présente l'URL <https://pflau-prod.psap.com/push> :

- CN = pflau-prod.psap.com est valide
- CN = *.psap.com **n'est pas** valide

Actuellement, seules les autorités suivantes sont proposées depuis l'IHM :

- ASIP : services de certification pour le secteur santé-social,
- Verisign-Symantec
- Sécurité Intérieure,
- Entrust,
- IGC-santé

Si votre autorité fait partie de la liste acceptée mais n'est pas présente dans celle proposé au sein de l'IHM, merci de revenir vers l'équipe PFLAU.

Dans le cas d'un intégrateur PSAP, celui-ci peut demander à l'APNF et à Worldline de disposer d'un PSAP dit « **PSAP Labo** » afin de valider sa solution avant déploiement sur la plateforme de production de leurs PSAPs.

Attention, dans ce cas de figure, cette étape doit **TOUJOURS** être suivie de la recevabilité du PSAP cible par l'intégrateur.

Recevabilité du Psap FR990PSAP

- 1. CGU
- 2. INFOS SSL
- 3. CONF SSL
- 4. TEST PUSH
- 5. TEST PULL
- 6. VALIDATION WORLDLINE
- 7. VALIDATION APNF

2. Informations SSL

Etape précédente

Coordonnées du contact projet (MOA)

Nom

Téléphone

Fax (facultatif)

Email

Coordonnées du contact technique

Nom

Téléphone

Fax (facultatif)

Email

Informations techniques

Autorité de certification

Liste des URL CRL

Common Name du certificat client PULL

Plage(s) d'Ip sources en production

URL d'accès webservice

URL de PUSH utilisé pour la recevabilité

Instructions

Commentaires utiles

Valider l'étape

[Retour](#)

Seuls les ports 443 et 20443 sont autorisés sur la plateforme de recevabilité. Aucune demande d'ouverture sur des autres ports n'est possible.

3.4.2.3 Configuration SSL

Une fois les informations de connexion partagées, **l'intégrateur PSAP ou le PSAP et Worldline** peuvent **mettre en place les configurations SSL** chacun sur leurs équipements.



Les informations Worldline pour le paramétrage SSL côté intégrateur PSAP ou PSAP sont détaillées dans la fiche d'interconnexion du kit de recevabilité disponible depuis l'IHM.



Le réseau de l'intégrateur PSAP ou PSAP doit avoir un accès DNS connecté à internet pour résoudre l'IP PFLAU à adresser lors de chaque appel, via le serveur GSLB.

En d'autres termes, toutes les requêtes faites à la PFLAU doivent passer par une résolution DNS afin d'assurer une haute disponibilité.

En cas de **cache DNS**, son **TTL** ne doit pas excéder les **30 secondes**.

Dès qu'il a validé la configuration SSL côté PFLAU, **Worldline notifie l'intégrateur PSAP ou le PSAP par mail** (contacts projet et technique précédemment renseignés) afin de le prévenir qu'il peut commencer ses tests d'interconnexions.

Recevabilité du Psap FR990PSAP

1. CGU

2. INFO S SSL

3. CONF SSL

4. TEST PUSH

5. TEST PULL

6. VALIDATION WORLDLINE

7. VALIDATION APNF

3. Configuration SSL

Etape précédente

Cette étape est réalisée par Worldline.
 Vos contacts technique et projet seront notifiés par mail une fois l'étape terminée.

Retour



Cette étape est validée au plus vite par Worldline en fonction des ressources disponibles au moment de réceptionner la notification automatique pour prévenir que vous êtes arrivé à cette étape.

Si vous avez des contraintes de réservation de ressource, il convient d'en prévenir au plus tôt Worldline pour vous assurer de notre disponibilité sur cette période.

3.4.2.4 ConfCall de validation SSL

Comme indiqué précédemment, l'intégrateur PSAP ou le PSAP est en autonomie complète pour réaliser les tests ci-dessous et la mise en place de sa configuration.

Toutefois, si celui-ci se trouve en difficulté **bloquante**, il est possible de monter une réunion téléphonique (pendant la phase de VABF) pour que Worldline et l'intégrateur PSAP ou le PSAP effectuent des tests et des contrôles pour valider le bon raccordement.

Les tests SSL visent à **valider** le bon montage des IPs d'accès **dans les 2 sens** et pour adresser **l'environnement de production** :

- d'abord intégrateur PSAP / ou PSAP => PFLAU (Worldline)
- puis PFLAU (Worldline) => Intégrateur PSAP ou PSAP

Si à la suite de cette réunion des difficultés persistent, l'intégrateur ou le PSAP peut effectuer une demande de support dédié.

3.4.2.4.1 Intégrateur PSAP vers Worldline



Le test de connexion consiste à valider l'accès SSL jusqu'à l'applicatif PFLAU de production <https://pull.pflau.fr/termLocPull>

Il s'agit donc pour l'Intégrateur PSAP ou le PSAP d'effectuer un hit via l'accès SSL sur l'accès applicatif de recevabilité et production.

Worldline valide l'étape dès lors qu'une **connexion réussie de l'Intégrateur PSAP ou le PSAP via l'accès SSL** a été constatée **en recevabilité et en production**.

3.4.2.4.2 Worldline vers Intégrateur PSAP

Une fois le test de l'Intégrateur PSAP validé, **l'étape suivante** est faite par **Worldline** qui lance les **hits** sur le webservice de **production de l'Intégrateur PSAP ou le PSAP**.



- Le test de connexion consiste à valider l'accès jusqu'au Webservice de l' **Intégrateur PSAP ou le PSAP** exposant la méthode *terminal-location-push* sur l'environnement de production de l'Intégrateur PSAP ou le PSAP.

Il s'agit donc pour l'Intégrateur PSAP ou le PSAP de mettre à disposition de Worldline une page de test applicative ou accès webservice via la liaison SSL (URLs renseignées précédemment lors de l'étape « Informations SSL » : cf. 1.1.1.1)

Cette **dernière étape** du raccordement SSL est alors **validée par l'Intégrateur PSAP ou le PSAP** dès qu'un **hit** est réalisé **avec succès** sur son environnement de **production**.

La **recevabilité technique terminée**, **l'Intégrateur PSAP (et les PSAP qui en dépendent) ou le PSAP** peuvent **démarrer leurs recevabilités fonctionnelles**.

3.4.3 PSAP (flux SVH)

Si le PSAP est habilité par l'APNF à faire des requêtes dans un cadre SVH, une deuxième URL est mise à sa disposition pour réaliser celle-ci.

Tout nouveau PSAP doit d'abord avoir réalisé sa recevabilité « classique » avant de dérouler sa recevabilité « SVH ».

Détail du Psap

Fiche Psap

Utilisateurs

Consulter la recevabilité du psap

Consulter la recevabilité SVH du psap

Identifiant	FR990PSAP
Manager	
Mail du contact	CCQA-PFLAU@golive.fr
Mail des statistiques	CCQA-PFLAU@golive.fr
Adresse	07-10
Code postal	75019
Ville	Casa
Intégrateur	Jérémie Bizart
Chef de projet Ministère	manager-RE minister
Plages IP *	
Uri de PushLocation *	
Eligible SVH	Non
Seuil Warning d'urgence	199
Seuil Alert d'urgence	999

* Champ utilisé en production

3.4.3.1 Consultation des CGU

La première étape consiste à une **connexion de l'intégrateur PSAP ou du PSAP à l'IHM de recevabilité** avec les identifiants qu'il a reçus par mail suite à son enregistrement sur la PFLAU.

L'IHM affiche l'ensemble des étapes de la recevabilité. Seule la première est active et peut être modifiée par l'intégrateur ou le PSAP : la **consultation des CGU**.

Recevabilité SVH du Psap FR990PSAP

1. CGU

2. INFOS SSL

3. DEMANDE LOCALISATION

4. TEST PUSH

5. TEST PULL

6. VALIDATION APNF

7. MISE EN PRODUCTION

1. Validation des CGU

Veuillez lire puis accepter les conditions générales d'utilisation du service avant de poursuivre.

Conditions Générales d'Utilisation

CONDITIONS GÉNÉRALES D'UTILISATION (CGU) DU SERVICE PFLAU

Objet du service « PFLAU »

1. Le service « PFLAU » (ci-après dénommé le « Service ») est un site mis en œuvre par l'Association des Plateformes de Normalisation des Flux inter-opérateur, code SIREN 512 434 226, dont le siège social est 11-17 rue de l'Amiral Hamelin – 75116 Paris (ci-après dénommée « l'APNF ») contribuant à mutualiser les échanges entre les opérateurs de communications électroniques et les centres de réception des appels d'urgences pour répondre efficacement à l'article D56-5 du code des postes et des communications électroniques (« CPCE ») pris en application de l'art. L33-11) du CPCE qui exige des opérateurs de communications électroniques qu'ils fournissent aux services d'urgence l'information relative à la localisation de l'appelant. Les données de localisation transmises dans le cadre du Service sont les nom, prénom, ou raison sociale et adresse de l'appelant (adresse de facturation pour le mobile, adresse d'installation ou à défaut de facturation pour le fixe), et la localisation géographique de l'appel (pour le mobile uniquement).

2. Les présentes Conditions Générales d'Utilisation ont pour objet de définir les modalités d'utilisation du service « PFLAU » par les centres de réception des appels d'urgence (ci-après dénommés « CRAU »).

Fonctionnalités du Service

3. Ce Service offre deux fonctionnalités aux CRAU : • Un compte gestionnaire unique pour administrer les comptes utilisateurs. L'utilisateur CRAU peut accéder au service pflau.apnf.fr pour mettre à jour les données administratives (adresse, contact, ...) de son centre de réception des appels d'urgence associé. • Deux webservices en HTTPS permettant la transmission des données de l'appelant : o le webservice « PostTerminalLocation » permet à l'opérateur de communications électroniques de transmettre à la « PFLAU » les données de localisation de tout appelant aux services d'urgence par un téléphone mobile. La précision et le format de localisation sont liés au type d'équipement détenu par chaque opérateur de communications électroniques. o le webservice « GetTerminalLocation » permet à la « PFLAU » d'obtenir les données d'adresse d'un numéro de téléphone (fixe ou mobile) entendues comme les nom, prénom ou raison sociale et adresse de l'appelant (adresse de facturation pour le mobile, adresse d'installation ou à défaut de facturation pour le fixe).

Modalités d'inscription et d'utilisation du Service

4. L'accès au Service est ouvert aux seuls CRAU identifiés dans les plans départementaux d'acheminement des appels d'urgence en vigueur communiqués par les représentants de l'Etat dans chaque département.

20. Le CRAU fera son affaire personnelle et garantit l'APNF de tout recours de sa part ou de la part de tiers du fait des modifications que le CRAU apporterait aux données de l'appelant transmises par l'APNF ou de tout usage par le CRAU des dites données de l'appelant non conforme aux termes et stipulations des présentes.

Durée

21. Les présentes Conditions Générales d'Utilisation prennent effet à compter de leur date de signature par le CRAU, pour une durée indéterminée.

22. Les Conditions Générales d'Utilisation doivent être transmises, dûment signées et paraphées, accompagnées des coordonnées du Responsable visé à l'article 6 des présentes, en 1 (un) exemplaire à l'adresse suivante (le CRAU conservant un exemplaire) : APNF 11-17 rue de l'Amiral Hamelin – 75116 Paris

Règlement des litiges

23. En cas de manquement de l'une des Parties à ses obligations issues des présentes, celles-ci conviennent de se rencontrer dans les plus brefs délais afin d'y apporter une solution.

24. Les présentes CGU sont régies par la loi française. Tout différend relatif à l'application, l'exécution et l'interprétation des présentes relèvera, à défaut d'accord amiable, des juridictions compétentes du ressort du Tribunal Administratif de Paris.

Résiliation

25. En cas d'évolution législative ou réglementaire rendant obsolète les présentes Conditions Générales d'Utilisation, l'une ou l'autre des Parties pourra résilier les présentes afin de se conformer à ses nouvelles obligations. La résiliation interviendra dans un délai compatible avec les nouvelles obligations et/ou la mise en service de solutions techniques adaptées à ces nouvelles obligations. Cette résiliation du Service ne donne droit à aucune indemnité.

26. Les parties conviennent de la possibilité de mettre fin aux présentes pour tout autre motif par lettre recommandée avec avis de réception moyennant un préavis d'1 (un) an, sauf accord des Parties sur un autre délai. Fait à le en 1 (un) exemplaire original Pour le centre de réception des appels d'urgence : Désignation du Service Nom et fonction du signataire dûment habilité aux présentes ANNEXE 1 Coordonnées du Responsable habilité pour le Service d'Urgence Désignation du Service : NOM, Prénom : Fonction : Coordonnées : (signature et tampon)

☐ Oui, j'ai lu et j'accepte les Conditions Générales d'Utilisation du service

Valider l'étape

Retour

En validant cette étape, l'intégrateur PSAP ou le PSAP informe avoir pris contact avec l'APNF pour la partie contractualisation et avoir pris connaissance des **CGU PFLAU (fichier PDF consultable et téléchargeable sur l'IHM de recevabilité via url)** et **active l'étape suivante** : la saisie des Informations SSL.

Mode d'emploi recevabilité PFLAU

© Worldline

En validation APNF | Version V004-02 | 29 October 2020 | Page 32 of 67

3.4.3.2 Informations SSL

Avant de poursuivre les étapes suivantes sur l'IHM de recevabilité (tests fonctionnels), l'intégrateur effectue son raccordement SSL avec le support de Worldline.

L'intégrateur **PSAP** ou le **PSAP** transmet ses informations techniques à Worldline via la **fiche d'interconnexion SSL** (autorité de certification et CN associé à son certificat, url de crt, plage IP utilisées) incluant l'**URL de son webservice de production** mises à disposition de Worldline.

Tous les acteurs interconnectés via SSL à la PFLAU doivent utiliser des IP **distinctes et publiques**.

De plus, pour permettre une optimisation dans la validation et la vérification des certificats, nous limitons les **autorités de certification** possible à la liste suivante :

- **ASIP** : services de certification pour le secteur santé-social,
- **IGC/A** : services de certification pour l'État français. Dans le cas d'un PSAP certifié par l'IGC/A, celui-ci s'engage à ce que l'autorité racine et parente du certificat reste l'IGC/A afin d'éviter les maillons intermédiaires lors de la récupération du fichier CRL,
- **Sécurité Intérieure**,
- **Entrust**,
- **Symantec** (anciennement Verisign),
- **OPENTRUST** (ex Keynectis),
- **DIGICERT**.

Worldline n'acceptera pas un certificat différent de cette liste. Aucune exception ne sera autorisée.

À la commande de votre certificat, prêtez bien attention à ce que le CN de ce certificat corresponde au DNS exposé par votre service.



Ce certificat doit également exposer la chaîne complète de certification.

Si vous faites le choix d'utiliser un certificat wildcard, vous devrez mettre en place la configuration nécessaire pour que le certificat présenté à la PFLAU affiche un CN égale au DNS exposé par votre service.

Par exemple si votre service présente l'URL <https://pflau-prod.psap.com/push> :

- CN = pflau-prod.psap.com est valide
- CN = *.psap.com **n'est pas** valide

Actuellement, seules les autorités suivantes sont proposées depuis l'IHM :

- ASIP : services de certification pour le secteur santé-social,
- Verisign-Symantec,
- Sécurité Intérieure,
- Entrust,
- IGC-santé.

Si votre autorité fait partie de la liste acceptée mais n'est pas présente dans celle proposé au sein de l'IHM, merci de revenir vers l'équipe PFLAU.

Dans le cas d'un intégrateur PSAP, celui-ci peut demander à l'APNF et à Worldline de disposer d'un PSAP dit « **PSAP Labo** » afin de valider sa solution avant déploiement sur la plateforme de production de leurs PSAPs.

Attention, dans ce cas de figure, cette étape doit **TOUJOURS** être suivie de la

recevabilité du PSAP cible par l'intégrateur.

1. CGU

2. INFOS SSL

3. DEMANDE LOCALISATION

4. TEST PUSH

5. TEST PULL

6. VALIDATION APNF

7. MISE EN PRODUCTION

2. Informations SSL

Coordonnées du contact projet (MOA)

Nom

Nom du contact projet

Téléphone

Téléphone du contact projet

Fax (facultatif)

Fax du contact projet

Email

Email du contact projet

Coordonnées du contact technique

Nom

Nom du contact technique

Téléphone

Téléphone du contact technique

Fax (facultatif)

Fax du contact technique

Email

Email du contact technique

Informations techniques

Autorité de certification

Liste des URL CRL

Ajouter une URL

Common Name du certificat client PULL

Plage(s) d'ip sources en production

Plage(s) d'ip sources en production

URL d'accès webservice

URL de PUSH utilisé pour la recevabilité

Indiquez le lien vers la page de test

Instructions

Commentaires utiles

Indiquez ici tout commentaires utiles

Retour



Seuls les ports 443 et 20443 sont autorisés sur la plateforme de recevabilité. Aucune demande d'ouverture sur des ports autres n'est possible.

Un contrôle automatique est en place pour valider l'interconnexion entre la PFLAU et le PSAP. Si tous est opérationnel, en cliquant sur valider pour basculerez dans la phase de recevabilité fonctionnelle des services SVH.

3.5 Sécurisation des appels getAddress :

Dans chaque appel getAddress, la PFLAU joint un certificat pour signer la requête.

Charge à l'opérateur de mettre en place un contrôle de ce certificat, le choix du niveau de contrôle appliqué est à définir en autonomie par l'opérateur en fonction de ses pratiques internes.

Ce contrôle se fait grâce au certificat qui doit en général être présent dans un truststore sur la plateforme de l'opérateur qui héberge de webservice getAddress.

Les CRT sont fournis suite au Kick off.

En cas de besoin lors de la phase de recevabilité, il est possible de redemander les certificats suivants auprès de la PFLAU :

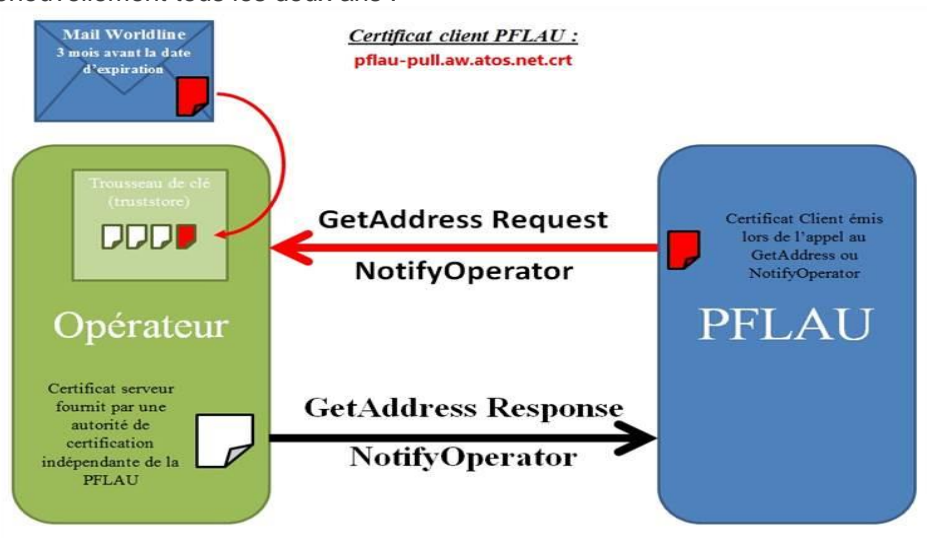
Recevabilité	Production
client-pull-recevabilite.pflau.fr	client-pull.pflau.fr

La demande se fait par mail avec les informations suivantes :

Destinataire :	dl-wl-apnf-pflau@worldline.com
Objet du mail :	[PFLAU] Demande de récupération du certificat avantage pull
Corps	<p>Bonjour,</p> <p>Pouvez-vous nous fournir les certificats Avantage de recevabilité et de production pour la validation de réception de vos appels getAddress au contact suivant :</p> <p>nom.prénom@domaine.yyy</p> <p>Cordialement,</p>

Le contact fourni doit être une personne unique (ou une mailing liste très restreinte) pour éviter la diffusion trop large de ce certificat.

Procédure de renouvellement tous les deux ans :



3.6 Sécurisation des appels Terminal_Location-Push

Dans chaque appel Terminal_Location-Push, la PFLAU joint un certificat pour signer la requête. Charge au PSAP intégrateur de mettre en place un contrôle de ce certificat, le choix du niveau de contrôle appliqué est à définir en autonomie par l'intégrateur PSAP en fonction de ses pratiques internes. Ce contrôle se fait grâce au certificat qui doit, en général, être présent dans un truststore sur la plateforme hébergeant le webservice Terminal_Location-Push.

Lors de votre phase de recevabilité, vous devrez demander les certificats suivants auprès de la PFLAU :

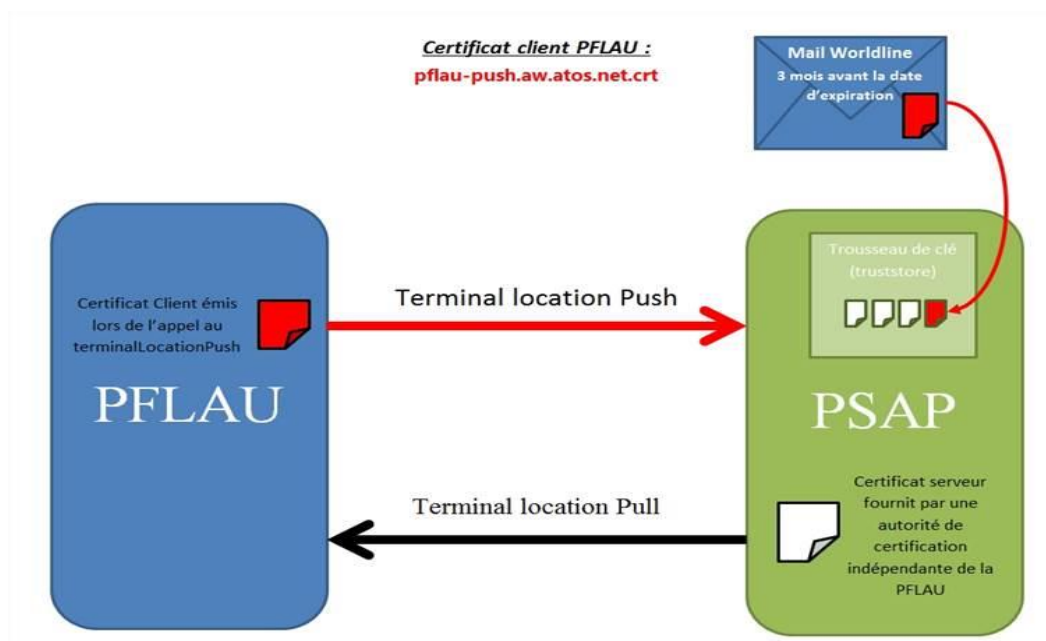
Certificat 2019-2021	
Recevabilité	production
client-push-recevabilite.pflau.fr	client-push.pflau.fr

La demande se fait par mail avec les informations suivantes :

Destinataire :	dl-wl-apnf-pflau@worldline.com
Objet du mail :	[PFLAU] Demande de récupération du certificat advantage push
Corps	<p>Bonjour,</p> <p>Pouvez-vous nous fournir les certificats Advantage de recevabilité et de production pour la validation de réception de vos appels terminal-location-push au contact suivant : nom.prénom@domaine.yyy</p> <p>Cordialement,</p>

Le contact fourni doit être une personne unique (ou une mailing liste très restreinte) pour éviter la diffusion trop large de ce certificat.

Procédure de renouvellement tous les deux ans :



4 Recevabilité fonctionnelle

4.1 Présentation

La **recevabilité fonctionnelle** permet aux **opérateurs** et/ou **PSAP** de **valider** leurs **interfaçages** avec la **PFLAU**.

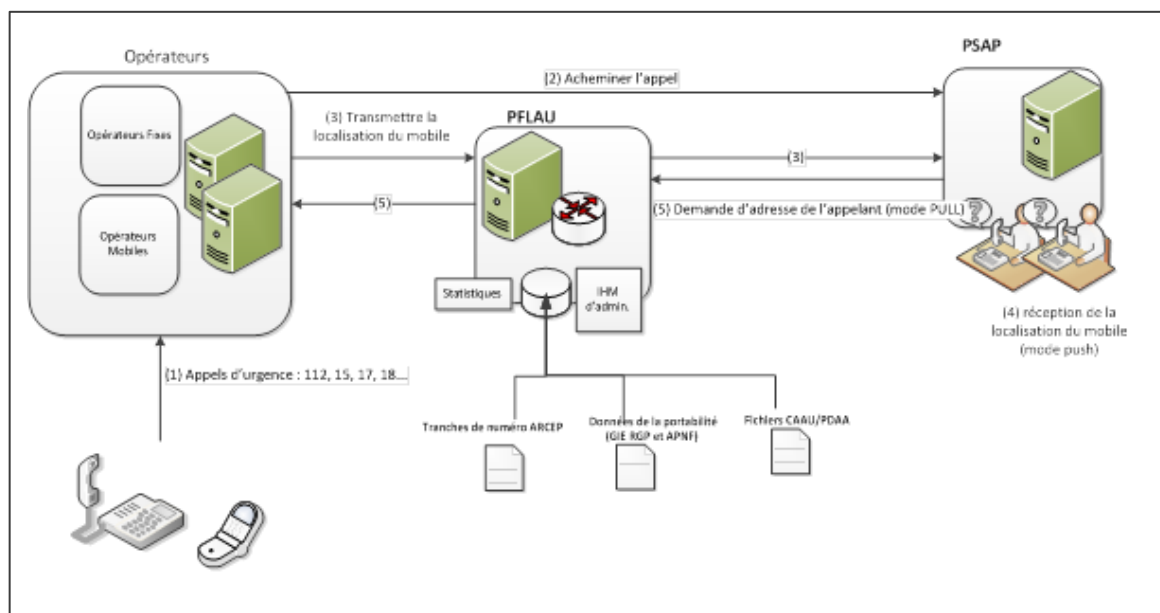
Elle se fait **en autonomie** par chaque acteur, via l'IHM de recevabilité (pour rappel : <https://ihm-recevabilite.pflau.fr/>)

Elle se fait **en mode « one to one »**, sans acheminement des appels vers l'acteur ciblé.

L'ensemble des tests est effectué sur l'environnement de **recevabilité**. Aucun test de performance ne peut être réalisé sur cet environnement.

4.2 Architecture fonctionnelle

4.2.1 Vue d'ensemble



4.2.2 Périmètre à valider

4.2.2.1 Opérateur

L'opérateur doit valider sa conformité pour :

- l'envoi d'une localisation à la PFLAU : *pushLocation*, si c'est un **MNO**
- répondre aux demandes d'information de la PFLAU : *getAddress* et *getaddressSVH*, **pour l'ensemble des opérateurs**

Si c'est un opérateur habilité à répondre aux sollicitations SVH :

- répondre aux demandes de soumission d'une localisation : *getLocationSvh*.
- l'envoi d'une localisation à la PFLAU suite à une demande de localisation : *pushLocationSvh*, Si c'est un opérateur de réseau.

4.2.2.2 PSAP

Le PSAP doit valider sa conformité pour :

- recevoir une localisation à la PFLAU : *terminalLocationPush*
- demander des informations à la PFLAU : *terminalLocationPull*

Si c'est un PSAP habilité à émettre des sollicitations SVH :

- demander des informations à la PFLAU : *terminalLocationPullSVH*
- demander des localisations à la PFLAU : *terminallocalisationpullSVH*
- recevoir une localisation à la PFLAU : *terminalLocationPushSVH*

4.3 Acteurs et Outils

La recevabilité fonctionnelle implique les acteurs suivants :

	Qui ?	Rôle
Pour un Opérateur	Opérateur	- Lancement des tests
	Worldline	- Validation des tests
Pour un PSAP	PSAP	- Lancement des tests
	Intégrateur PSAP	- Assure le support de leurs PSAP
	Worldline	- Validation des tests

Elle se fait au moyen des outils suivants :

	QUI	Rôle
Mode d'emploi recevabilité PFLAU	Opérateur/PSAP	- Description du protocole à suivre par l'opérateur
IHM Web de recevabilité	Opérateur	- Suivi d'avancement de la recevabilité - Lancement des tests : simulation des flux PFLAU=>OP
	PSAP	- Suivi d'avancement de la recevabilité - Lancement des tests : simulation des flux PFLAU=>PSAP
PFLAU de <u>recevabilité</u> Opérateur/Worldline (mode bouchonné)	Opérateur/PSAP	- Envoi/Réception des flux testés
NDI de test	Opérateur	- Les NDI répondants aux différents scénarii sont propre à chaque opérateur. L'opérateur a donc la responsabilité des NDI utilisés pour ses tests de recevabilité (getAddress)
	PSAP	- Mode bouchonné : chaque PSAP peut renseigner un NDI correctement formaté présent dans la liste des NDIs de test (information disponible sur l'IHM)
PSAPPhone de test	Opérateur	- Les appels sont bouchonnés (pas d'acheminement PSAP). Chaque opérateur MNO doit renseigner le PSAPPhone fictif Worldline pour ses tests de recevabilité (pushLocation)

Types de localisation	PSAP	- 1 exemple de données valides par type de localisation (ellipse, polygone, arcBand), sélectionnable via l'IHM de recevabilité (cf. ci-après détail des tests)
-----------------------	------	--

4.4 Protocole

4.4.1 Opérateur

L'**opérateur lance séquentiellement les tests** indiqués sur l'IHM de recevabilité.

Les résultats de ses tests **du jour** sont affichés sur l'IHM sous forme de tableau, selon les logs du serveur PFLAU :

- si le test est **validé** : statut OK, informations relatives aux tests effectués (horodatage, statut ...)
- si le test **échoue** : statut NOK, horodatage, trace d'erreur permettant l'investigation;

Un lien vers les traces soap des tests effectués par l'opérateur est disponible.

Lorsqu'il le juge pertinent, l'opérateur choisit de passer à l'étape suivante. Une vérification automatique est effectuée dans les logs PFLAU pour valider que le **dernier test** lancé par l'opérateur sur cette étape est en **statut OK**. Le cas échéant, l'opérateur ne peut pas passer à l'étape suivante. (Cf. conditions de passages listées à cette étape dans l'IHM)



Après validation d'une étape, le retour arrière n'est pas possible via l'IHM. Si cela est requis, il faut en faire la demande à Worldline qui réalise l'action sous les meilleurs délais en fonction de ses disponibilités.



Durant toute sa recevabilité fonctionnelle, l'opérateur a à sa disposition un **lien d'accès aux traces SOAPS PFLAU correspondantes à ses tests** (téléchargement des logs bruts de l'opérateur uniquement pour la journée courante)

4.4.2 PSAP



Tout PSAP avec un intégrateur ne peut accéder à la consultation des CGUs qu'à partir du moment où son intégrateur et son chef de projet Ministère qui lui est rattaché ont été créés.

Dans le cas d'un PSAP sans intégrateur, l'APNF a en charge la création de l'intégrateur.

Le **PSAP lance séquentiellement les tests** indiqués sur l'IHM de recevabilité.

Le lancement de ces tests fait suite à la validation de la phase de raccordement technique

Chaque test fait l'objet d'une **validation** par **Worldline**, selon les logs du serveur PFLAU de recevabilité :

- si le test est **validé** : activation du **prochain test**
- **sinon**, un message est affiché sur l'IHM pour indiquer au PSAP qu'il **doit de nouveau effectuer le test** (une fois qu'il aura mis en place les correctifs nécessaires sur ses WebServices);



Après validation d'une étape, le retour arrière n'est pas possible via l'IHM. Si cela est requis, il faut en faire la demande à Worldline qui réalise l'action sous les meilleurs délais en fonction de ses disponibilités.



Durant toute sa recevabilité fonctionnelle, le PSAP a à sa disposition un **bouton d'export des logs PFLAU correspondants à ses tests** (téléchargement des logs bruts du PSAP uniquement pour la journée courante)

4.5 Liste des services à valider

Qui	Cadre	service
Opérateur	Classique	PushLocation
		getAddress
		NotifyOpérateur
	SVH	getAddressSvh
		getLocalisationSvh
		pushLocationSvh
PSAP	Classique	TerminalLocationPush
		TerminalLocationPull
	SVH	TerminalLocationPush
		TerminalLocationPull
		TerminalLocalisationPullSvh

4.6 Validation des services opérateur

4.6.1 PushLocation

Cette étape n'existe que pour les opérateurs **MNO**.

Le **premier test** à effectuer par l'**opérateur** est celui d'un **pushLocation**.

Les valeurs du PSAP fictif Worldline à utiliser sont les suivantes :

PsapId FR590WRLN avec le PSAPPhone **+33320607979**

Lancement du test : l'**opérateur** envoie une **localisation** depuis son client WS vers la **PFLAU** qui lui retourne un acquittement OK.



Pour rappel, la **résolution d'adresse du site PFLAU** à adresser doit se faire **dynamiquement (TTL < 30sec)**, via une résolution **DNS** (loadbalancing GSLB) pour l'environnement de production.

<https://push-recevabilite.pflau.fr/pushLocation>

Résultat du test : pas de prise en compte du **psapPhone (bouchon)**, mais **contrôles** et envoi d'un **acquittement OK**

Validation du test sur l'IHM de recevabilité : L'opérateur peut consulter les traces des hits de push reçus par la plateforme (pour le jour courant). Dans le cas où un problème de certificat client opérateur pour le **pushLocation** est détecté, il n'y aura pas de génération de logs dans ce cas bien précis. En effet, comme la plateforme ne peut pas faire confiance à la requête envoyée par l'opérateur, il est plus sécurisé de ne pas analyser le contenu de celle-ci pour remplir les différents champs des logs. L'opérateur aura le retour KO directement via son client.

- Exemple de tests :

Les résultats des tests sont affichés sous la forme suivante (la mise à jour des données affichées dans le tableau s'opère via un bouton « refresh ») :

PushLocation

Confidentiel

Date serveur PFLAU (UTC)	dateTime In (UTC)	Function	duration	idTransaction	psapPhone	Statut	codeErreur	descErreur	lienSoap
2014-08-14 06:34:52.54 6	2014-08-14 T06:34:51 Z	pushLocation	0.068	FR000OPER- 20140814- 06:34:51.6 42- 3367501338 2	+333206079 79	OK			url Fichier Soap
2014-08-14 06:34:53.14 5	2014-08-14 T06:34:53 Z	pushLocation	0.039	FR000OPER- 20140814- 06:34:50.6 42- 3367501338 2	+333206079 79	KO	ERR0001	Format Localisation incorrect	url Fichier Soap
2014-08-14 06:31:33.78 9	2014-08-14 T06:33:24 Z	pushLocation	0.079	FR000OPER- 20140814- 06:33:24.6 65- 3311010981	+333206079 79	OK			url Fichier Soap

Tous les échanges de la journée liés à l'opérateur sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que le dernier test soit « OK ».

le fichier SOAP contient les logs des requêtes suivantes :

- pushLocation_request
- pushLocation_response

Pendant la phase de VABF, les logs sont conservés pendant 7 jours.

En fin de VABF, les logs SOAP présentés sur l'IHM ne sont gardés que 24H.

Une fois cette étape validée, il est impossible pour l'opérateur de lancer de nouveaux tests à partir des champs mis à disposition.

Si un opérateur souhaite revenir sur cette étape, il doit en faire la demande par email à Worldline.

4.6.2 PushLocationSvh

Cette étape n'existe que pour les opérateurs **habilités à recevoir des requêtes SVH**.

Le **test** à effectuer par l'**opérateur** est celui d'un **pushLocationSvh**.

Les valeurs du psap fictif Worldline à utiliser sont les suivantes :


Psapid FR590WRLN avec le PSAPPhone **+33320607979**


Recevabilité de l'opérateur OPER

- 1. CGU
- 2. INFOS VPN
- 3. PISK
- 4. CONFIG VPN
- 5. TEST VPN OPÉRATEUR
- 6. TEST VPN WORLDLINE
- 7. TEST PUSH
- 8. TEST PUSH SVH
- 9. TEST GET ADDRESS
- 10. TEST GET LOCATION SVH
- 11. TEST NOTIFY
- 12. VALIDATION WORLDLINE
- 13. VALIDATION APNF

8. Test du Push Location SVH

[Etape précédente](#)

Veuillez envoyer un push SVH depuis votre plateforme puis actualiser la liste des logs ci-dessous en cliquant sur le bouton  .
Le dernier test effectué doit avoir le statut 'OK' afin de valider l'étape.

Logs de la journée 

Nombre de lignes 10 ▼

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	TransId	PsapPhone	Statut	Err n°	Err description	Lien Soap
Aucune donnée									

Le dernier test doit avoir le statut 'OK' afin de passer à l'étape suivante.

[Valider l'étape](#)

[Retour](#)

Lancement du test : l'**opérateur** envoie une **localisation** depuis son client WS vers la **PFLAU** qui lui retourne un acquittement OK.



Pour rappel, la **résolution d'adresse du site PFLAU** à adresser doit se faire **dynamiquement (TTL < 30sec)**, via une résolution **DNS** (loadbalancing GSLB) pour l'environnement de production.

<https://push-recevabilite.pflau.fr/pushLocation>

Résultat du test : pas de prise en compte du **psapPhone (bouchon)**, mais **contrôles** et envoi d'un **acquittement OK**

Validation du test sur l'IHM de recevabilité : L'opérateur peut consulter les traces des hits de push reçus par la plateforme (pour le jour courant). Dans le cas où un problème de certificat client opérateur pour le **pushLocationSvh** est détecté, il n'y aura pas de génération de logs dans ce cas bien précis. En effet, en cas de certificat non valide, la plateforme ne peut pas faire confiance à la requête envoyée par l'opérateur. Ainsi, par sécurité la requête est rejetée avant tout traitement, y compris un traitement de log. L'opérateur aura le retour KO directement via son client.

- Exemple de tests :

Les résultats des tests sont affichés sous la forme suivante (la mise à jour des données affichées dans le tableau s'opère via un bouton « refresh ») :

PushLocationSvh

Date serveur PFLAU (UTC)	dateTime In (UTC)	Function	duration	idTransaction	psapPhone	Statut	codeErreur	descErreur	lienSoap
2014-08-14 06:34:52.546	2014-08-14 T06:34:51Z	pushLocationSvh	0.068	FR000OPER-20140814-06:34:51.642-33675013382	+33320607979	OK			url Fichier Soap
2014-08-14 06:34:53.145	2014-08-14 T06:34:53Z	pushLocationSvh	0.039	FR000OPER-20140814-06:34:50.642-33675013382	+33320607979	KO	ERR0001	Format Localisation incorrect	url Fichier Soap
2014-08-14 06:34:53.145	2014-08-14 T06:34:53Z	pushLocationSvh	0.039	FR000OPER-20140814-06:34:50.642-33675013382	+33320607979	KO	ERR0000	Erreur XSD : Il manque le bloc SVH	url Fichier Soap
2014-08-14 06:31:33.789	2014-08-14 T06:33:24Z	pushLocationSvh	0.079	FR000OPER-20140814-06:33:24.665-3311010981	+33320607979	OK			url Fichier Soap

Tous les échanges de la journée liés à l'opérateur sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que le dernier test soit « OK ».

le fichier SOAP contient les logs des requêtes suivantes :

- pushLocation_request
- pushLocation_response

Pendant la phase de VABF, les logs sont conservés pendant 7 jours.

En fin de VABF, les logs SOAP présentés sur l'IHM ne sont gardés que 24H.

Une fois cette étape validée, il est impossible pour l'opérateur de lancer de nouveaux tests à partir des champs mis à disposition.

Si un opérateur souhaite revenir sur cette étape, il doit en faire la demande par email à Worldline.

4.6.3 getAddress - getAddressSVH

La validation de la fonctionnalité getAddress et getAddressSVH consiste respectivement en **1 à 3 tests selon l'opérateur**.

4.6.3.1 Informations de l'opérateur

Il s'agit du **cas standard** où l'opérateur est interrogé pour l'un de ses clients finaux.

Ce test est à effectuer par **tous les opérateurs**, en simulant le *getAddress* depuis l'**IHM de recevabilité** qui propose un champ de formulaire libre pour le NDI à passer en paramètre ainsi qu'une possibilité d'éditer l'URL de *getAddress* :

Lancement du test : l'opérateur se lance un appel depuis l'IHM en précisant un NDI de sa base client afin de retourner à la PFLAU ses propres informations.

Résultat du test : l'opérateur retourne à la PFLAU les informations clients du NDI

Validation du test sur l'IHM de recevabilité : L'opérateur peut consulter les traces des appels *getAddress* (pour le jour courant).




Un test *getAddress* et un test *getAddressSVH* doivent être réalisés par tous les opérateurs car tous peuvent être appelés dans un cadre classique ou SVH. L'URL *getAddress* et *getAddressSVH* peuvent être identiques. (Cf. documentation de spécifications PFLAU pour plus de détails)

4.6.3.2 Rebond (selon l'opérateur)

Il s'agit du **cas** où l'opérateur a défini dans sa déclaration le fait que **des rebonds** peuvent intervenir sur certains NDI appartenant à un autre opérateur qu'il connaît.

Ce test est à effectuer par **les opérateurs**, en simulant le *getAddress* depuis l'**IHM de recevabilité** qui propose une case à cocher pour déclarer que l'appel courant est avec rebond possible :

Lancement du test : l'opérateur lance un appel depuis l'IHM qui retourne à la PFLAU le nom d'un autre opérateur qui possède l'adresse (Rebond)

La liste des logs se rafraîchit automatiquement mais vous pouvez forcer l'actualisation en cliquant sur le bouton 
Le dernier test effectué doit avoir le statut 'OK' afin de valider l'étape.

NDI	Numéro	<input type="checkbox"/>	Rebond	Envoyer la requête
NDI SVH	Numéro	<input checked="" type="checkbox"/>	Rebond	Envoyer la requête



L'identification d'un NDI « réel » répondant à ce scénario peut ne pas être aisée.

L'opérateur peut forcer le comportement pour un NDI donné via sa base de tests interne utilisée lors de la recevabilité fonctionnelle.

Résultat du test : l'opérateur en cours de recevabilité retourne à la PFLAU le nom d'un autre opérateur à contacter.

Validation du test sur l'IHM de recevabilité : L'opérateur peut consulter les traces des appels getAddress (pour le jour courant).

4.6.3.3 OPTA (selon l'opérateur)

Il s'agit du **cas spécifique** où un opérateur client souhaite **valider le rôle d'OPTA** d'un autre opérateur avec lequel il est en accord contractuel, c'est-à-dire lorsqu'il peut être amené à renvoyer les informations clientes pour le compte de cet opérateur client.

Ce test est réalisé en simulant le *getAddress* depuis **l'IHM de recevabilité** par **l'opérateur client**.

Lancement du test : **l'opérateur client** lance un appel (saisie de l'un de ces NDI) depuis l'IHM qui transmet la demande vers l'OPTA.

Celui-ci **retourne** à la PFLAU **les infos pour le compte de son opérateur client**



L'identification d'un NDI « réel » répondant à ce scénario peut ne pas être aisée.

L'opérateur peut forcer le comportement pour un NDI donné via sa base de tests interne utilisée lors de la recevabilité fonctionnelle.

Résultat du test : l'OPTA retourne à la PFLAU les informations clientes du NDI de l'opérateur client

Validation du test sur l'IHM de recevabilité : L'opérateur client et l'OPTA peuvent consulter les traces des appels getAddress (pour le jour courant) en retour OK.

Pour les cas de test en échec ou sans retour direct sur l'IHM, l'opérateur client doit valider avec son OPTA que les données retournées coïncident. L'OPTA peut alors consulter les traces des appels getAddress (pour le jour courant) depuis l'IHM afin de transmettre les données à son client.

La **validation de l'étape** devra émaner de l'opérateur client depuis l'IHM avec un dernier test en OK.

Les résultats des tests sont affichés sous la forme suivante :

getAddress

dateTime UTC	dateTime In	Function	Duration	idTransaction	psapPhone	psaplId	Msisdn	statut	codeErreur	descErreur	lienSoap
2014-08-14 06:43:01.548	2014-08-14T06:42:43Z	getAddress	0.073	FR590WR LN20140 8140642	+33320 607979	FR5 90W RLN	+33 601 020 304	OK			url Fichier Soap
2014-08-14 06:35:55.326	2014-08-14T06:35:53Z	getAddress	0.103	FR590WR LN20140 8140635	+33320 607979	FR5 90W RLN	+33 130 042 254	OK			url Fichier Soap
2014-08-14 06:35:55.326	2014-08-14T06:35:53Z	getAddress	0.103	FR590WR LN20140 8140635	+33320 607979	FR5 90W RLN	+33 130 042 254	OK			url Fichier Soap

Tous les échanges de la journée liés à l'opérateur sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que le dernier test soit « OK ».

Le fichier SOAP contient les logs des requêtes suivantes :

- getAddress_request
- getAddress_response
- getAddressSvh_request
- getAddressSvh_response

Pendant la phase de VABF, les logs sont conservés pendant 7 jours.

En fin de VABF, les logs SOAP présentés sur l'IHM ne sont gardés que 24H.

4.6.4 getLocationSvh

Cette étape n'existe que pour les opérateurs habilités à recevoir **des requêtes SVH**.
La validation de la fonctionnalité getLocationSVH consiste en une salve de tests.

Il s'agit du **cas standard** où l'opérateur de réseaux est interrogé pour l'un de ses clients finaux.

Il faut simuler le *getLocationSvh* depuis l'IHM de recevabilité qui propose un champ de formulaire libre pour le NDI à passer en paramètre ainsi qu'une possibilité d'éditer l'URL de getlocalisationSvh :

Recevabilité de l'opérateur OPER

1. CGU
2. INFO SVH
3. PDK
4. CONFIG VPN
5. TEST VPN OPÉRATEUR
6. TEST VPN WORLDLINE
7. TEST PUSH
8. TEST PUSH SVH
9. TEST GET ADDRESS
10. TEST GET LOCATION SVH
11. TEST NOTIFY
12. VALIDATION WORLDLINE
13. VALIDATION APNF

10. Test du Get Location SVH

Étape précédente

Veuillez générer un getLocationSvh depuis notre plateforme en utilisant le formulaire ci-dessous.

Mettre à jour l'URL de getLocationSvh URL getLocationSvh Mettre à jour

La liste des logs se rafraîchit automatiquement mais vous pouvez forcer l'actualisation en cliquant sur le bouton .
Le dernier test effectué doit avoir le statut "OK" afin de valider l'étape.

NDI Numéro Envoyer la requête

Logs de la journée

Nombre de lignes 10

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	Transid	PsapPhone	PsapId	Ndi	Statut	Err n°	Err description	Lien Soap
Aucune donnée											

Le dernier test doit avoir le statut "OK" afin de passer à l'étape suivante.

Valider l'étape

Retour

Lancement du test : l'opérateur se lance un appel depuis l'IHM en précisant un NDI de sa base client afin de retourner à la PFLAU l'acquiescement de la requête.

Résultat du test : l'opérateur retourne à la PFLAU l'acquiescement de la prise en compte de la demande du NDI

Validation du test sur l'IHM de recevabilité : L'opérateur peut consulter les traces des appels getAddress (pour le jour courant).

4.6.5 notifyOperator

Les opérateurs ayant implémenté cette fonctionnalité testent l'appel à la méthode notifyOperator.

Il est réalisé en simulant le **notifyOperator** depuis l'**IHM de recevabilité**. Des données fictives (bouchons) sont envoyées à l'opérateur.

The screenshot shows a web interface titled "Recevabilité de l'opérateur OPER". On the left is a vertical list of steps from 1 to 13. Step 11, "11. TEST NOTIFY", is highlighted with an orange circle. Above the main content area, the title "11. Test du Notify Operator" is displayed in orange. Below the title, there is a green button labeled "Etape précédente". The main content area contains the text: "Veuillez générer un notifyOperator depuis notre plateforme en cliquant sur le bouton ci-dessous. Une fois la requête reçue, vous pouvez valider l'étape." Below this text is a blue button labeled "Envoyer la requête". At the bottom of the interface, there is a blue button labeled "Valider l'étape" and a "Retour" link with a left arrow icon.

La validation de cette étape confirme la recevabilité fonctionnelle de l'opérateur qui devient **éligible à la phase d'activation et de mise en production**.

L'**APNF** et **Worldline** sont **notifiés par mail** de cette fin de recevabilité.

4.7 Validation des services classiques PSAP

4.7.1 terminalLocationPush

Le **premier test** à effectuer par le **PSAP** est celui d'une **réception de localisation de la PFLAU**.

L'appel est à simuler depuis l'**IHM de recevabilité** qui propose une liste déroulante avec les différents types de localisation à tester par le PSAP : **ellipse, polygone ou arcBand**.

Recevabilité du Psap FR990PSAP

1. CGU

2. INFOS SSL

3. CONF SSL

4. TEST PUSH

5. TEST PULL

6. VALIDATION WORLDLINE

7. VALIDATION APNF

4. Test du Terminal location push

Etape précédente

Veuillez générer un push depuis notre plateforme en utilisant le formulaire ci-dessous.

La liste des logs se rafraîchit automatiquement mais vous pouvez forcer l'actualisation en cliquant sur le bouton .

Le dernier test effectué doit avoir le statut 'OK' afin de valider l'étape.

Envoi d'un test Terminal Location Push

Ellipse

Jeux de valeurs

Position

214.69 268.55

Semi major axis

55.66

Semi minor axis

89.64

Orientation

350

Lancer le test

Logs de la journée

Nombre de lignes 10

Date serveur PFLAU (UTC)

Date requête (UTC)

Type

Durée

TransId

PsapPhone

Statut

Err n°

Err description

Lien Soap

Aucune donnée

Retour

Lorsque le PSAP choisit son type de push, l'IHM lui propose 2 solutions :

- Saisir manuellement les valeurs des paramètres associés au type de push sélectionné (l'ensemble des champs est affiché sur l'IHM)
 - Opter pour un test prédéfini via une liste déroulante.
- Dans ce mode, les champs sont automatiquement renseignés mais le PSAP a tout de même la possibilité de les modifier.

Rappel des champs à renseigner pour chaque type de push :

- Ellipse :
 - Champ « pos » constitué d'un couple de doubles (exemple :47.9178089 1.8935533) ,
 - Champ « semiMajorAxis » qui est de type double (exemple : 1805),
 - Champ « semiMinorAxis » qui est de type double (exemple : 1505),
 - Champ « orientation » qui est de type double (exemple : 143).
- Polygon :
 - Champ « posList» constitué d'une liste de couple de doubles (exemple : 48.8360001 2.2920001 ; 48.8360001 2.3020001 ; 48.8460001 2.3020001 ; 48.8260001 2.2920001).
- ArcBand :
 - Champ « pos » constitué d'un couple de doubles (exemple :47.9178089 1.8935533) ,
 - Champ « innerRadius » qui est de type double (exemple : 1805),
 - Champ « outerRadius » qui est de type double (exemple : 1661.55),
 - Champ « startAngle » qui est de type double (exemple : 2215.4),
 - Champ « openingAngle » qui est de type double (exemple : 120).



Au démarrage des tests, la valeur présentée dans le champ « **Votre URL webservice PSAP** » est extraite du **fichier CAAU** précédemment intégré.

S'il le souhaite, le PSAP peut ponctuellement modifier cette valeur pour effectuer des tests en recevabilité.

Elle **ne sera pas répliquée** sur l'environnement de production.

Lancement du test : le PSAP s'envoie une localisation depuis l'IHM qui lui transmet des informations bouchonnées (mode opératoire mis en place en fin de VABF)

Résultat du test : le PSAP reçoit la localisation.

Validation du test sur l'IHM de recevabilité : **Worldline valide le test** sur l'IHM de recevabilité, dès qu'un hit est effectué avec succès **pour chaque type de localisation**, en fonction des **traces** observées dans les **logs serveur PFLAU**. Cette validation permet de passer au test suivant.

Confidentiel

Les résultats des tests sont affichés sous la forme suivante :

dateTime UTC	dateTime In	Function	duration	idTransaction	psapPhone	statut	codeErreur	descErreur	lienSoap
2014-07-25T14:39:17Z	2014-07-25T14:39:17Z	Terminal	0.068	FR000WRLD-20140725-14:39:17.33	+33238221819	OK			url
		-		7-					Fichier
		location		33675013382					Soap
		-push							
2014-07-25T14:39:07Z	2014-07-25T14:39:07Z	Terminal	0.068	FR000WRLD-20140725-14:39:07.33	+33238221819	KO	ERR0001	Format	url
		-		7-				Localisati	Fichier
		location		33675013382				on	Soap
		-push						incorrect	
2014-07-25T14:38:07Z	2014-07-25T14:38:07Z	Terminal	0.068	FR000WRLD-20140725-14:38:07.33	+33238221819	KO	ERR0001	PSAP	url
		-		7-				inconnu	Fichier
		location		33675013382					Soap
		-push							
2014-07-25T14:37:57Z	2014-07-25T14:37:57Z	Terminal	0.068	FR000WRLD-20140725-14:39:37.57	+33238221820	OK			url
		-		7-					Fichier
		location		33675013382					Soap
		-push							

Tous les échanges de la journée liées au PSAP sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que le dernier test soit « OK ».

Le fichier SOAP contient les logs des requêtes suivantes :

- Terminal-Location-push_request (*) *un des 3 bouchons sélectionnés*
- Terminal-Location-push_response

Pendant la phase de VABF, les logs sont conservés pendant 7 jours.

En fin de VABF, les logs SOAP présentés sur l'IHM ne sont gardés que 24H.

Une fois cette étape validée, il est impossible pour le PSAP ou l'intégrateur de lancer de nouveaux tests à partir des champs mis à disposition.

Si un PSAP ou un intégrateur souhaite revenir sur cette étape, il doit en faire la demande par mail à Worldline.

4.7.2 terminalLocationPull

Le **second test** à effectuer par le **PSAP** est celui d'une **demande d'adresse à la PFLAU**.

Recevabilité du Psap FR990PSAP

1. CGU

2. INFOS SSL

3. CONF SSL

4. TEST PUSH

5. TEST PULL

6. VALIDATION WORLDLINE

7. VALIDATION APNF

5. Test du Terminal location pull

Etape précédente

Voici les conditions à respecter pour pouvoir valider cette étape :

- Il existe au moins un test OK et un test KO.
- Le dernier test doit être OK.
- L'id de transaction est unique et respecte le bon format pour chaque test pull. Veuillez consulter notre [FAQ](#).
- La marge de temps entre la date de l'appel du service pull (champ Date requête (UTC)) et la date de la réception effective de la requête (champ Date serveur PFLAU (UTC)) ne dépasse pas 10s pour chaque test.

Le contrôle est fait sur les 5 dernières lignes de tests. Si le nombre de tests ne dépasse pas 5, le contrôle est fait sur toutes les lignes.

Logs de la journée

Nombre de lignes 10

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	Transld	PsapPhone	Statut	Err n°	Err description	Lien Soap
Aucune donnée									

×

Attention, vous ne pouvez pas valider l'étape.

Si dessous la liste des erreurs et les Transld correspondants à chaque test en erreur :

- Le dernier test doit avoir le statut 'OK'
- Le Transld doit avoir des valeurs différentes pour chaque test
- Ces Transld ne respectent pas la bonne syntaxe. Pour plus d'informations à propos du Transld, veuillez consulter la [FAQ](#)
- Un écart de plus de 10s entre
--> **Date requête (UTC)** correspondant à la date que vous envoyez lors de l'appel du service pull
--> et **Date serveur PFLAU (UTC)** correspondant à la date de réception effective de la requête.
Merci de vérifier l'heure que vous envoyez lors de l'appel du service pull.
- Les tests doivent contenir au moins un test OK et un test KO

Valider l'étape

Retour

Lancement du test : le **PSAP** envoie une **demande d'adresse** depuis son client WS vers la PFLAU qui lui retourne des **informations simulées** (bouchonnées).

Pour rappel, la résolution d'adresse du site PFLAU à adresser doit se faire **dynamiquement (TTL < 30sec)**, via une résolution **DNS** (loadbalancing GSLB)

Résultat du test : Pas de prise en compte de la demande : mais **contrôles** et **envoi d'une réponse statique simulée** (bouchonnée) (mode opératoire mis en place en fin de VABF).

Validation du test sur l'IHM de recevabilité : **Worldline valide le test** sur l'IHM de recevabilité, dès qu'un hit est effectué avec succès, en fonction des **traces** observées dans les **logs serveur PFLAU**. Cette validation permet de passer au test suivant.

Mode d'emploi recevabilité PFLAU

© Worldline

En validation APNF | Version V004-02 | 29 October 2020 | Page 55 of 67

Confidentiel

Les résultats des tests sont affichés sous la forme suivante :

dateTime UTC	dateTime In	Function	duration	idTransaction	psapPhone	statut	codeErreur	descErreur	lienSoap
2014-07-25T14:39:27Z	2014-07-25T14:39:27Z	Terminal - location -pull	0.068	FR750SDIS20 14012345678 9012	+33134511 398	OK			
2014-07-25T14:39:07Z	2014-07-25T14:39:07Z	Terminal - location -pull	0.068	FR750SDIS20 14012345678 9012	+33134511 398	OK			
2014-07-25T14:36:57Z	2014-07-25T14:36:57Z	Terminal - location -pull	0.068	FR750SDIS20 14012345678 9012	+33238221 819	NOK	ERR009 3	Adresse IP rejetée	url Fichier Soap
2014-07-25T14:36:47Z	2014-07-25T14:36:47Z	Terminal - location -pull	0.068	FR750SDIS20 14012345678 9012	+33238221 819	NOK	ERR000 9	PSAP non raccordé	url Fichier Soap

Tous les échanges de la journée liés au PSAP sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que :

- Le dernier test soit « OK »
- Toutes les transactions ID des tests soient différents
- Les dates soient en UTC.
- Il existe un test « KO »

Le fichier SOAP contient les logs des requêtes suivantes :

- Terminal-location-pull_request_xml (*) *un des NDI associé à l'opérateur fictif WRLN qui répond en tant qu'OPTA*
- Terminal-location-pull_response

Cette dernière validation confirme **la recevabilité fonctionnelle du PSAP** qui peut être activé et **mis en production**.

L'APNF, Worldline et le Chef de Projet Ministériel du PSAP sont **notifiés par mail** de cette fin de recevabilité.

4.8 Validation des services SVH PSAP



Les horaires HNO sont les mêmes qu'en production et communs à tous les utilisateurs. De ce fait, Worldline ne bascule un opérateur spécifique en horaire HNO à la demande. **En recevabilité** afin de pouvoir tester le contrôle HO/HNO, nous avons défini une période HNO quotidienne de 10h30 à 17h30 (heure de Paris). Donc pour tester les erreurs « horaire non HNO » veuillez lancer ces tests entre 8h30 et 10h30.

4.8.1 terminalLocalisationPullSVH

Le **premier test** à effectuer par le **PSAP** est celui d'une **demande de localisation à la PFLAU**.

- 1. CGU
- 2. INFOS SSL
- 3. DEMANDE LOCALISATION
- 4. TEST PUSH
- 5. TEST PULL
- 6. VALIDATION APNF
- 7. MISE EN PRODUCTION

3. Test de demande localisation

[Etape précédente](#)

Voici les conditions à respecter pour pouvoir valider cette étape :

- Il existe au moins un test OK et un test KO.
- Le dernier test doit être OK.
- L'id de transaction est unique et respecte le bon format pour chaque demande de localisation. Veuillez consulter notre [FAQ](#).
- La marge de temps entre la date de l'appel du service localisation (champ Date requête (UTC)) et la date de la réception effective de la requête (champ Date serveur PFLAU (UTC)) ne dépasse pas 10s pour chaque test.

Le contrôle est fait sur les 5 dernières lignes de tests. Si le nombre de tests ne dépasse pas 5, le contrôle est fait sur toutes les lignes.

Logs de la journée

Nombre de lignes | 10 ▼

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	TransId	PaspPhone	Statut	Err n°	Err description	Lien Soap
Aucune donnée									

✕ Attention, vous ne pouvez pas valider l'étape.

Si dessous la liste des erreurs et les TransId correspondants à chaque test en erreur :

- Le dernier test doit avoir le statut "OK"
- Le TransId doit avoir des valeurs différentes pour chaque test
- Ces TransId ne respectent pas la bonne syntaxe. Pour plus d'informations à propos du TransId, veuillez consulter la [FAQ](#).
- Un écart de plus de 10s entre :
 - Date requête (UTC) correspondant à la date que vous envoyez lors de l'appel du service localisation
 - et Date serveur PFLAU (UTC) correspondant à la date de réception effective de la requête

Merci de vérifier l'heure que vous envoyez lors de l'appel du service localisation.

- Les tests doivent contenir au moins un test OK et un test KO

[Valider l'étape](#)

Lancement du test : le PSAP envoie une demande d'adresse depuis son client WS vers la PFLAU qui lui retourne des informations **simulées** (bouchonnées).



Pour rappel, la résolution d'adresse du site PFLAU à adresser doit se faire **dynamiquement (TTL < 30sec)**, via une résolution **DNS** (loadbalancing GSLB)

Résultat du test : Pas de prise en compte de la demande : mais **contrôles** et **envoi d'une réponse statique simulée** (bouchonnée) (mode opératoire mis en place en fin de VABF).

Validation du test sur l'IHM de recevabilité : **Worldline valide le test** sur l'IHM de recevabilité, dès qu'un hit est effectué avec succès, en fonction des **traces** observées dans les **logs serveur PFLAU**. Cette validation permet de passer au test suivant.

Confidentiel

Les résultats des tests sont affichés sous la forme suivante :

dateTime UTC	dateTime In	Function	duration	idTransaction	psapPhone	statut	codeErreur	descErreur	lienSoap
2014-07-25T14:39:27Z	2014-07-25T14:39:27Z	terminal Localist ionPullS vh	0.068	FR750SDIS20 14012345678 9012	+33634511 398	OK			
2014-07-25T14:39:07Z	2014-07-25T14:39:07Z	terminal Localist ionPullS vh	0.068	FR750SDIS20 14012345678 9012	+32434511 398	NOK	ERR001 8	Opérateur non SVH	
2014-07-25T14:36:48Z	2014-07-25T14:36:48Z	terminal Localist ionPullS vh	0.068	FR750SDIS20 14012345678 9012	+33700000 000	NOK	ERR001 7	Usage abusif du service	url Fichier Soap
2014-07-25T14:36:47Z	2014-07-25T14:36:47Z	terminal Localist ionPullS vh	0.068	FR750SDIS20 14012345678 9012	+33700000 000	OK			
2014-07-25T08:36:57Z	2014-07-25T08:36:57Z	terminal Localist ionPullS vh	0.068	FR750SDIS20 14012345678 9012	+33600000 000	NOK	ERR001 5	Appel hors HNO	url Fichier Soap

Tous les échanges de la journée liés au PSAP sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que :

- Le dernier test soit « OK »
- Toutes les transactions ID des tests soient différents
- Les dates soient en UTC.
- Il existe un tests « KO »

Le fichier SOAP contient les logs des requêtes suivantes :

- TerminalLocalisationPullSvh_request_xml (*) *un des NDI associé à l'opérateur fictif WRLN qui répond en tant qu'OPTA*
- TerminalLocalisationPullSvh_response

4.8.2 TerminalLocationPushSVH

Le **second test** à effectuer par le **PSAP** est celui d'une **réception de localisation de la PFLAU**.

L'appel est à simuler depuis l'**IHM de recevabilité** qui propose une **liste déroulante** avec les différents types de localisation à **tester par le PSAP : ellipse, polygone ou arcBand**.

Pour tous les types de localisation, les champs nécessaires au renseignement du bloc SVH est également personnalisable.

Descriptions	Exemples
Source de la localisation :	CRA, Géolocalisation
Informations complémentaires	Numéro non localisé, Numéro Localisé en Espagne
Message d'erreur fonctionnelle	Pas sur le réseau opérateur
Date / Heure de la localisation fournie (UTC0)	20200313-04:25:38.125
Profondeur d'analyse réalisée (optimum) :	48h
Nature de la réponse	Barycentre, Antenne

1. CGU
2. INFOS SSL
3. DEMANDE LOCALISATION
4. TEST PUSH
5. TEST PULL
6. VALIDATION APNF
7. MISE EN PRODUCTION

Recevabilité SVH du Psap FR990MAWA

4. Test du Terminal location push

[Etape précédente](#)

Veuillez générer un push depuis notre plateforme en utilisant le formulaire ci-dessous.

La liste des logs se rafraichit automatiquement mais vous pouvez forcer l'actualisation en cliquant sur le bouton

Le dernier test effectué doit avoir le statut 'OK' afin de valider l'étape.

Envoi d'un test Terminal Location Push

URL du webservice Psap

http://tqftp01s:8006/mockPushTerminalLocationSoapBinding

Type de localisation

Ellipse

Jeux de valeurs

Position

Indiquez la position

Semi major axis

Indiquez le semi major axis

Semi minor axis

Indiquez le semi minor axis

Orientation

Indiquez l'orientation

Lancer le test

Logs de la journée

Nombre de lignes

10

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	TransId	PsapPhone	Statut	Err n°	Err description	Lien Soap
Aucune donnée									

Le dernier test doit avoir le statut 'OK' afin de passer à l'étape suivante.

Valider l'étape

Lorsque le PSAP choisit son type de push, l'IHM lui propose 2 solutions :

- Saisir manuellement les valeurs des paramètres associés au type de push sélectionné (l'ensemble des champs est affiché sur l'IHM)
- Opter pour un test prédéfini via une liste déroulante.

Dans ce mode, les champs sont automatiquement renseignés mais le PSAP a tout de même la possibilité de les modifier.

Rappel des champs à renseigner pour chaque type de push :

- Ellipse :
 - Champ « pos » constitué d'un couple de doubles (exemple :47.9178089 1.8935533) ,
 - Champ « semiMajorAxis » qui est de type double (exemple : 1805),
 - Champ « semiMinorAxis » qui est de type double (exemple : 1505),
 - Champ « orientation » qui est de type double (exemple : 143).
- Polygon :
 - Champ « posList» constitué d'une liste de couple de doubles (exemple : 48.8360001 2.2920001 ; 48.8360001 2.3020001 ; 48.8460001 2.3020001 ; 48.8260001 2.2920001).
- ArcBand :c
 - Champ « pos » constitué d'un couple de doubles (exemple :47.9178089 1.8935533) ,
 - Champ « innerRadius » qui est de type double (exemple : 1805),
 - Champ « outerRadius » qui est de type double (exemple : 1661.55),
 - Champ « startAngle » qui est de type double (exemple : 2215.4),
 - Champ « openingAngle » qui est de type double (exemple : 120).



Au démarrage des tests, la valeur présentée dans le champ « **Votre URL webservice PSAP** » est **extraite du fichier CAAU** précédemment intégré.

S'il le souhaite, le PSAP peut ponctuellement modifier cette valeur pour effectuer des tests en recevabilité.

Elle **ne sera pas répliquée** sur l'environnement de production.

Lancement du test : le PSAP s'envoie une localisation depuis l'IHM qui lui transmet des **informations simulées** (bouchonnées) (mode opératoire mis en place en fin de VABF)

Résultat du test : le PSAP reçoit la localisation.

Validation du test sur l'IHM de recevabilité : Worldline valide le test sur l'IHM de recevabilité, dès qu'un hit est effectué avec succès **pour chaque type de localisation**, en fonction des **traces** observées dans les logs serveur PFLAU. **Cette validation permet de passer au test suivant.**

Confidentiel

Les résultats des tests sont affichés sous la forme suivante :

dateTime UTC	dateTime In	Function	duration	idTransaction	psapPhone	statut	codeErreur	descErreur	lienSoap
2014-07-25T14:39:17Z	2014-07-25T14:39:17Z	terminal Location PushSvh	0.068	FR000WRLD-20140725-14:39:17.337-33675013382	+33238221819	OK			url Fichier Soap
2014-07-25T14:39:07Z	2014-07-25T14:39:07Z	terminal Location PushSvh	0.068	FR000WRLD-20140725-14:39:07.337-33675013382	+33238221819	KO	ERR0001	Format Localisation incorrect	url Fichier Soap
2014-07-25T14:38:07Z	2014-07-25T14:38:07Z	terminal Location PushSvh	0.068	FR000WRLD-20140725-14:38:07.337-33675013382	+33238221819	KO	ERR0001	PSAP inconnu	url Fichier Soap
2014-07-25T14:37:57Z	2014-07-25T14:37:57Z	terminal Location PushSvh	0.068	FR000WRLD-20140725-14:39:37.577-33675013382	+33238221820	OK			url Fichier Soap

Tous les échanges de la journée liée au PSAP sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que le dernier test soit « OK ».

Le fichier SOAP contient les logs des requêtes suivantes :

- Terminal-Location-push_request (*) *un des 3 bouchons sélectionnés*
- Terminal-Location-push_response

Pendant la phase de VABF, les logs sont conservés pendant 7 jours.

En fin de VABF, les logs SOAP présentés sur l'IHM ne sont gardés que 24H.

Une fois cette étape validée, il est impossible pour le PSAP ou l'intégrateur de lancer de nouveaux tests à partir des champs mis à disposition.

Si un PSAP ou un intégrateur souhaite revenir sur cette étape, il doit en faire la demande par mail à Worldline.

4.8.3 terminalLocationPullSVH

Le **troisième test** à effectuer par le **PSAP** est celui d'une **demande d'adresse à la PFLAU**.

Recevabilité SVH du Psap FR990PSAP

1. CGU

2. INFOS SSL

3. TEST LOCALISATION

4. TEST PUSH

5. TEST PULL

6. VALIDATION APNF

7. MISE EN PRODUCTION

5. Test du Terminal location pull

Etape précédente

Voici les conditions à respecter pour pouvoir valider cette étape :

- Il existe au moins un test OK et un test KO.
- Le dernier test doit être OK.
- L'id de transaction est unique et respecte le bon format pour chaque test pull. Veuillez consulter notre [FAQ](#).
- La marge de temps entre la date de l'appel du service pull (champ Date requête (UTC)) et la date de la réception effective de la requête (champ Date serveur PFLAU (UTC)) ne dépasse pas 10s pour chaque test.

Le contrôle est fait sur les 5 dernières lignes de tests. Si le nombre de tests ne dépasse pas 5, le contrôle est fait sur toutes les lignes.

Logs de la journée

Nombre de lignes | 10

Date serveur PFLAU (UTC)	Date requête (UTC)	Type	Durée	Transld	PsapPhone	Statut	Err n°	Err description	Lien Soap
Aucune donnée									

✗ Attention, vous ne pouvez pas valider l'étape.

Si dessous la liste des erreurs et les Transld correspondants à chaque test en erreur :

- Le dernier test doit avoir le statut 'OK'
- Le Transld doit avoir des valeurs différentes pour chaque test
- Ces Transld ne respectent pas la bonne syntaxe. Pour plus d'informations à propos du Transld, veuillez consulter la [FAQ](#)
- Un écart de plus de 10s entre
--> **Date requête (UTC)** correspondant à la date que vous envoyez lors de l'appel du service pull
--> et **Date serveur PFLAU (UTC)** correspondant à la date de réception effective de la requête.
Merci de vérifier l'heure que vous envoyez lors de l'appel du service pull.
- Les tests doivent contenir au moins un test OK et un test KO

Lancement du test : le PSAP envoie une demande d'adresse depuis son client WS vers la PFLAU qui lui retourne des **informations simulées** (bouchonnées)



Pour rappel, la **résolution d'adresse du site PFLAU** à adresser doit se faire **dynamiquement (TTL < 30sec)**, via une résolution **DNS** (loadbalancing GSLB)

Résultat du test : Pas de prise en compte de la demande : mais **contrôles** et **envoi d'une réponse statique bouchonnée** (mode opératoire mis en place en fin de VABF).

Validation du test sur l'IHM de recevabilité : Worldline valide le test sur l'IHM de recevabilité, dès qu'un hit est effectué avec succès, en fonction des **traces** observées dans les **logs serveur PFLAU**. Cette validation permet de passer au test suivant.

Les résultats des tests sont affichés sous la forme suivante :

dateTime UTC	dateTime In	Function	duration	idTransaction	psapPhone	statut	codeErreur	descErreur	lienSoap
2014-07-25T14:39:27Z	2014-07-25T14:39:27Z	Terminal-location-pull	0.068	FR750SDIS20140123456789012	+33134511398	OK			
2014-07-25T14:39:07Z	2014-07-25T14:39:07Z	Terminal-location-pull	0.068	FR750SDIS20140123456789012	+33134511398	OK			
2014-07-25T14:36:57Z	2014-07-25T14:36:57Z	Terminal-location-pull	0.068	FR750SDIS20140123456789012	+33238221819	NOK	ERR0093	Adresse IP rejeté	url Fichier Soap
2014-07-25T14:36:47Z	2014-07-25T14:36:47Z	Terminal-location-pull	0.068	FR750SDIS20140123456789012	+33238221819	NOK	ERR0009	PSAP non raccordé	url Fichier Soap

Tous les échanges de la journée liés au PSAP sont affichés. Le tableau est trié par ordre « dateTimeUTC » décroissant.

Pour valider l'étape, il faut que :

- Le dernier test soit « OK »
- Toutes les transactions ID des tests soient différents
- Les dates soient en UTC.
- Il existe un tests « KO »

Le fichier SOAP contient les logs des requêtes suivantes :

- Terminal-location-pull_request_xml (*) *un des NDI associé à l'opérateur fictif WRLN qui répond en tant qu'OPTA*
- Terminal-location-pull_response

Cette dernière validation confirme la recevabilité fonctionnelle du PSAP qui peut être activé et **mis en production**.

L'APNF, Worldline et le Chef de Projet Ministériel du PSAP sont **notifiés par mail** de cette fin de recevabilité.

5 Mise En Production et après ?

5.1 Mise en production

Une fois les différents services validés techniquement et fonctionnellement, le PSAP ou l'opérateur peut être **mis en production**.

Cette étape est effectuée par l'**APNF** et **Worldline**.

L'**opérateur** ou le **PSAP** sont alors **complètement intégrés aux flux bout en bout de production et reçoivent une notification par email pour les en informer**. Ils ont également désormais accès à leurs informations sur l'**IHM d'administration avec les mêmes login et password que l'IHM de recevabilité**.

La **mise en service**, ainsi que de le monitoring, est ensuite de la responsabilité de l'opérateur ou du PSAP intégrateur.

5.2 Et après ?

5.2.1 Mise à jour des certificats PFLAU





Tous les deux ans en février le certificat lié aux appels terminal_location_push et getAddress par la PFLAU périment et font l'objet d'un renouvellement.

À ce titre, tous les deux ans en fin d'année PSAP et opérateurs raccordés réceptionnent un email pour la bulle de recevabilité et un email pour la bulle de production.

Le certificat à ajouter dans le truststore y sera fourni au format texte afin de s'assurer que votre client email ne filtre pas les fichiers .CRT en pièce jointe.

Nous recommandons à chaque PSAP et opérateur, suite à leur activation en production sur la PFLAU, la mise en place d'une procédure interne permettant de comprendre rapidement le pourquoi de la réception de cet email, ainsi que l'action qui doit en découler chez vous.

Voici les emails types qu'il est possible de recevoir : (exemple des renouvellements de 2019)

Destinataire	Bulle Recevabilité	Bulle Production
PSAP intégrateur	 PFLAU Renouvellement YYYY	 PFLAU Renouvellement YYYY
Mail du contact Opérateur	 PFLAU Renouvellement YYYY	 PFLAU Renouvellement YYYY

5.2.2 Mise à jour des certificats des services opérateur et/ou PSAP.

Vous avez mis en place des services sur vos serveurs qui sont appelés par la PFLAU. Ces services sont exposés avec un certificat serveur pour assurer la connexion en https.

Pour Les PSAP vous avez également un certificat que vous joignez à vos appels au service de la PFLAU pour signer vos appels.

Dans ces cas, c'est à vous d'assurer leurs renouvellements. Et la PFLAU ne procédera pas à une alerte de péremption de ceux-ci.

Nous vous invitons à prévoir, dès la fin de mise en production de la PFLAU, une procédure interne permettant de rappeler la fin de validité de vos certificats avec une procédure explicite pour comprendre rapidement le pourquoi de cette notification et quelle action est à réaliser.

PS : Par expérience, la réception de mail de renouvellement de certificat sur un service qui tourne depuis plusieurs années sans modification est anxiogène pour l'intervenant qui reçoit le mail.

NB : L'envoi de mail à l'APNF ou à Worldline, ne vous sera d'aucune aide sur ce point de renouvellement.

Point d'attention à avoir pour ce renouvellement :

- Le CN doit être en cohérence avec le DNS exposé par votre service.
- Vous devez conserver la même autorité de certification et valider que la chaîne de certificat et la même (CA Root et CA intermédiaire).

Si la chaîne de certification change, il est *nécessaire de prévenir l'équipe PFLAU* en avance de phase pour que nous mettions à jour le truststore de notre côté. le *délai de prévenance est de 1 mois au minimum*.

- Pour les PSAP, le CN du certificat joint aux appels fait vers la PFLAU doit **impérativement** rester inchangé. À défaut vos appels seraient refusés par la PFLAU.

Si vous êtes contraint de procéder à un changement de ce CN, il sera **impératif de prévenir la PFLAU** pour signaler ce phénomène et demander d'ajouter provisoirement l'autorisation du nouveau CN pour le PSAP visé. le *délai de prévenance est de 1 mois au minimum*.

Vous êtes autonome pour faire la modification de vos certificats, toutefois, si le jour de votre modification en production, vous constatez un défaut.

Il sera de votre responsabilité de procéder à un rollback pour rétablir le bon fonctionnement de votre service. Vous pourrez alors nous contacter pour procéder à la réalisation d'une nouvelle recevabilité de votre service impacté depuis l'IHM de recevabilité. Cela implique que vous disposiez d'une plateforme de qualification fonctionnelle, ou à minima d'une URL spécifique aux tests pour ne pas impacter votre service de production. Là encore un délai de prévenance d'un mois est requis pour la réservation des ressources humaines nécessaires pour vous assister.

C'est pourquoi l'anticipation des renouvellements de mots de passe est très importante de votre côté.

5.2.3 Migration de vos services exposés à la PFLAU.

Dans la vie d'un projet, les migrations et/ou modifications de services sont courantes.

Vous disposez de l'IHM d'administration, pour changer en autonomie l'URL à appeler pour vos services exposés.

Nous vous recommandons de procéder avant votre migration à une nouvelle recevabilité spécifique de ce service via l'IHM de recevabilité de la PFLAU.

La bulle de recevabilité est dé-corrélée de la bulle de production. Donc vous pouvez exécuter une recevabilité de votre futur service tout en ayant votre ancien service fonctionnel sur la bulle de production. Cela nécessite que l'URL d'appel de votre ancien et futur service soit différente.

Pour ce faire il faudra demander à l'équipe PFLAU de vous rebasculer en étape de recevabilité sur le service impacté.

Les conditions tarifaires pour la réalisation de cette recevabilité seront étudiées lors d'un KickOff à organiser entre l'intervenant, l'APNF et Worldline, pour définir :

- Le planning de réalisation de la(des) action(s)
Il faut en effet s'assurer de la disponibilité des ressources humaines côté Worldline en cas de besoin d'assistance. le délai de prévenance est de **1 mois au minimum**.
- Le niveau d'autonomie dans les actions :
 - Autonomie totale : Il s'agit d'une migration facile, et aucune assistance particulière de la part de Worldline n'est nécessaire. Par défaut on prévoit 1HJ pour les contrôles pré et post migration vue de la PFLAU.
 - Autonomie Partielle : l'intervenant estime qu'il existe un doute raisonnable sur la maîtrise de la migration. Un forfait de 3HJ renouvelable d'assistance sera convenu avec l'intervenant, et une facture post payée sera émise par Worldline en cas de dépassement de ce forfait.

NB : Dans le cas où vous feriez le choix de procéder à la migration en totale autonomie, puis modifier l'URL directement depuis l'IHM d'administration sans avoir réalisé de recevabilité.

Si votre migration ne se passe pas comme prévu, il sera de votre responsabilité de :

- procéder à un rollback de votre service
- contacter l'APNF et l'équipe PFLAU pour planifier une recevabilité en bonne et due forme.

5.2.4 Je constate une baisse de trafic entrant sur mes service

La météo sur l'IHM d'administration est là pour vous donner un état de santé de la plateforme.

Une baisse de trafic qui aurait pour origine un défaut et/ou une maintenance de la part d'un intervenant de la PFLAU ou un incident identifié du service PFLAU vous y sera remontée sur la journée.

(Cf. documentation IHM pour plus de détail)

5.2.5 Je suis un opérateur et j'ai une maintenance de mon service à réaliser qui le rendra indisponible.

En tant qu'opérateur vous disposez sur votre page de détail de l'IHM d'administration, d'une interface vous permettant de déclarer une maintenance en cours sur l'un de vos services.

WebService impacté	getAddress
Début Maintenance	
Fin Maintenance	
Message Maintenance	

L'intérêt est triple :

- Éviter de lever des alertes sur la PFLAU
- Prévenir les utilisateurs de la PFLAU, dans la Météo de l'IHM d'administration, avec un affichage anonymisées, qu'un opérateur est en maintenance.
- En cas de déclaration de maintenance, un code spécifique est instantanément retourné au PSAP. Cela permet ainsi d'éviter au PSAP d'attendre 18 secondes un retour en timeout à sa requête initiale, évitant ainsi une dégradation de toute la PFLAU.