PFLAU
Guide du futur opérateur

association de la portabilité des numéros fixes

Association des **P**lateformes de **N**ormalisation des **F**lux inter-opérateurs

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

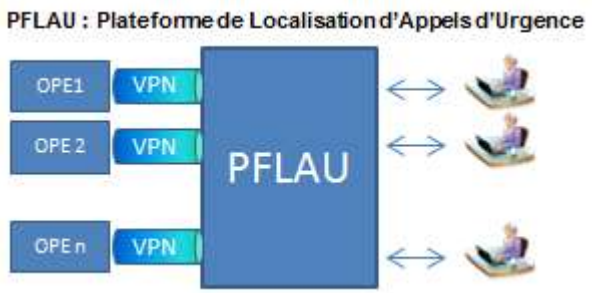
Introduction

Contexte

Pour répondre efficacement à l'article **D98-8** du code des postes et des communications électroniques, les opérateurs ont mis en place une plateforme centralisée mutualisant les échanges entre eux et les centres de réception des appels d'urgences afin de fournir les données relatives à la localisation de l'appelant.

Principe de fonctionnement

Pour répondre à cette exigence, **les opérateurs mettent en place une plateforme mutualisée pour septembre 2015** interconnectée avec les SI de portabilité (fixe et mobile), les opérateurs et les plateformes d'appels des services d'urgences (PSAP)



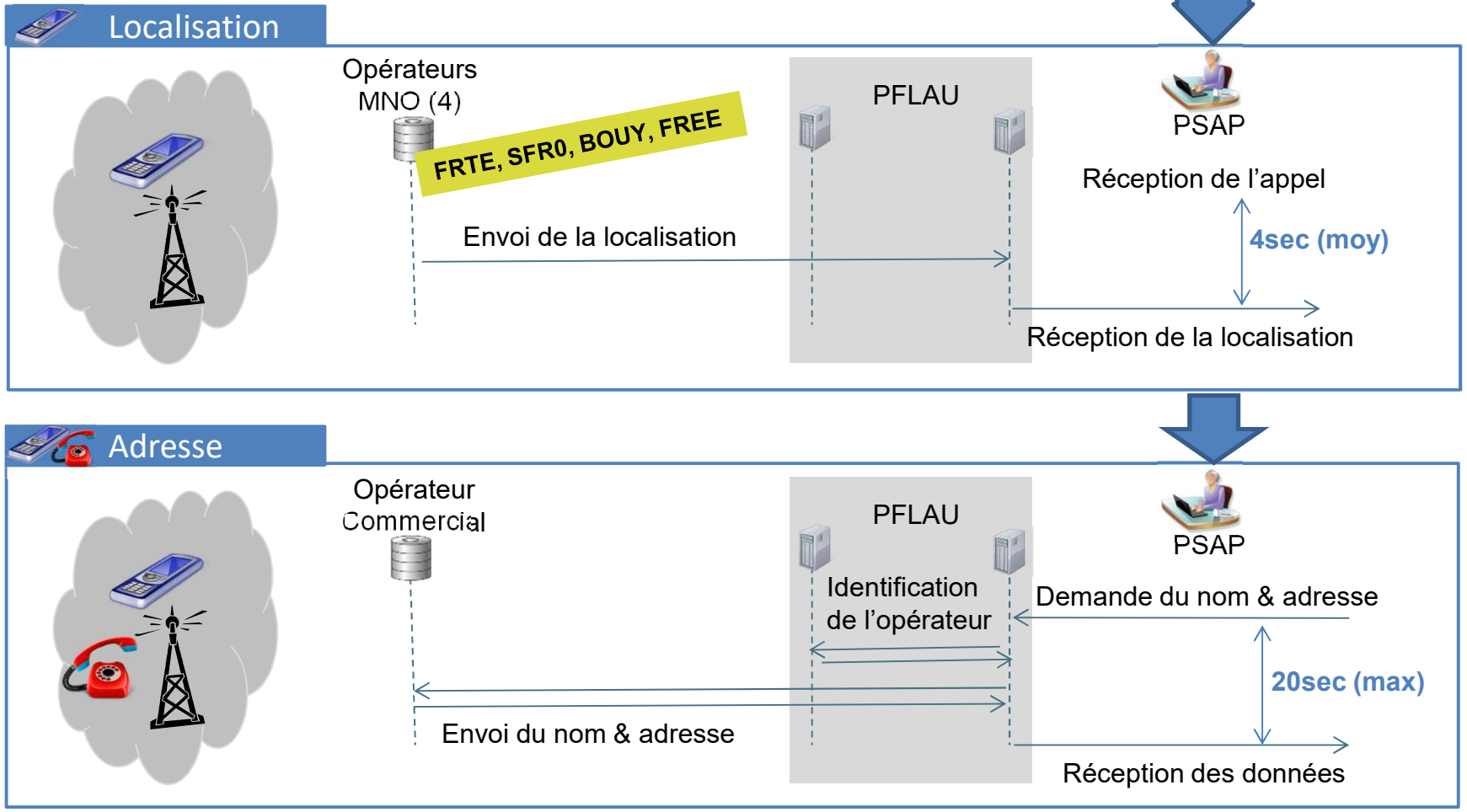
Objectifs du guide

Ce support a pour objectif de **présenter la solution PFLAU** et de guider les opérateurs :

- dans la détermination de leur(s) rôle(s) vis-à-vis de la solution,
- dans le processus de raccordement,
- dans l'utilisation de l'outil de recevabilité

Principe de fonctionnement de la PFLAU (2/3)

Les appels sont acheminés aux PSAP sans transiter par la PFLAU

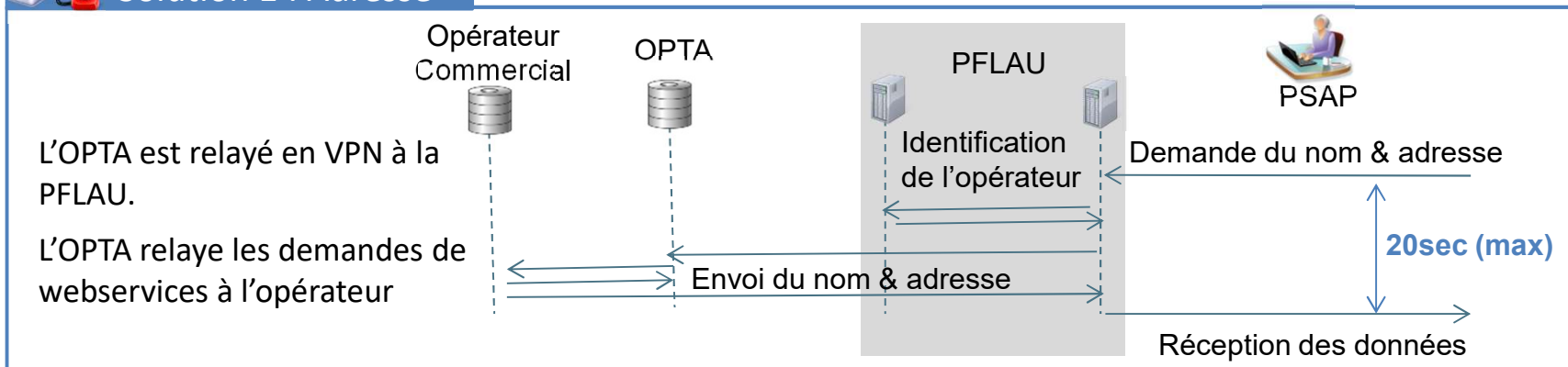


Principe de fonctionnement avec un OPTA (3/3)

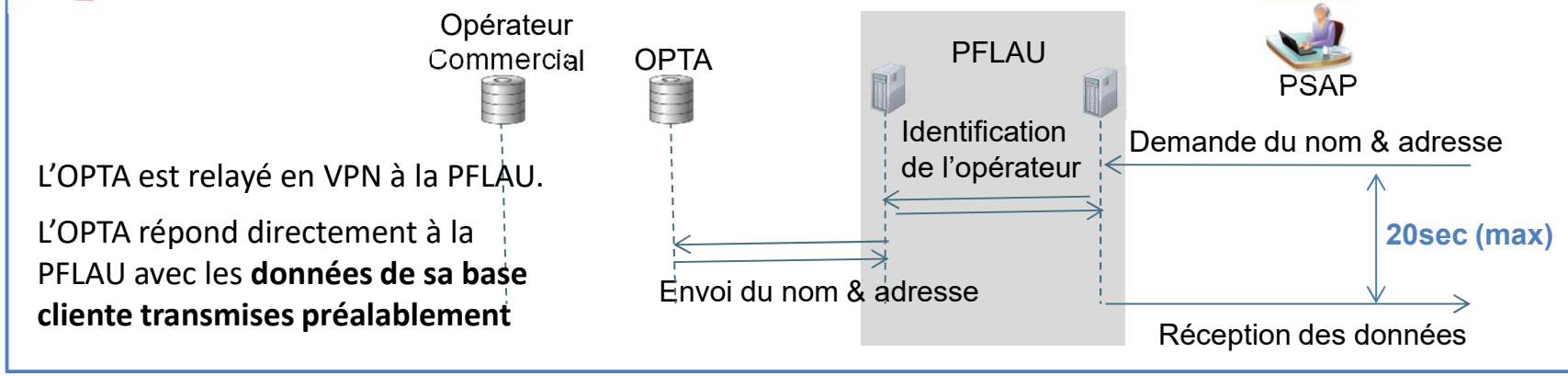
Un OPTA peut proposer une des deux solutions suivantes à son client opérateur :

- Solution 1 : relaye de webservices
- Solution 2 : réponse directe en hébergeant la base cliente de l'opérateur

Solution 1 : Adresse



Solution 2 : Adresse



Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Les acteurs

Acteur	Communication	Rôle
Opérateurs	IHM, WS	Répondre aux demandes d'adresse et envoyer la localisation pour les MNO.
Autorités d'Etat	IHM	Ajuster les seuils « Alerte » et « Warning » pour un PSAP pendant une crise
PSAP	IHM, WS	Envoyer des demandes d'adresse et recevoir les localisations des appels mobiles.
GIE/EGP	FTP	Envoyer les portabilités des numéros mobiles
APNF	FTP	Envoyer les portabilités des numéros fixes
Préfectures	ENVOL (Linshare)	Envoyer les plans d'acheminement préfectoraux des appels d'urgence (fichiers PDAA et CAAU)
Chefs de Projet Ministères	IHM	Suivre l'activité des recevabilités PSAP

La PFLAU est une plateforme reliant les opérateurs et les centres d'urgence (PSAP).

Pour assurer sa fonction d'aiguillage, elle doit disposer en interne des tables de portabilité.

Ordre du jour

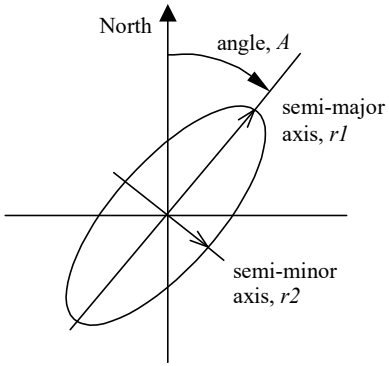
- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Push : Localisation pour les 4 MNO (*)

(*) FRTE, SFR, BYTEL, FREE

Latitude / longitude basées sur la norme WGS84 – 2D (⇔ EPSG::4326)

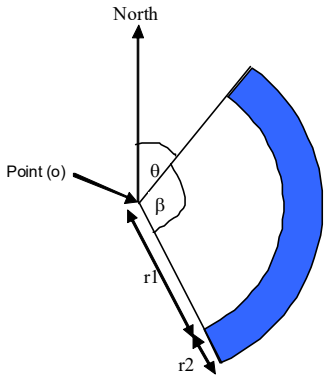
Ellipsoid



Centre = barycentre de la cellule
=> orientation=0, semiMajorAxis=r, SemiMinorAxis=r

```
<gs:Ellipsoid  srsName="urn:ogc:def:crs:EPSG::4326"">
<gml:pos>48.884 2.245</gml:pos>
<gs:semiMajorAxis uom="urn:ogc:def:uom:EPSG::9001">
                    7.7156
</gs:semiMajorAxis>
<gs:semiMinorAxis uom="urn:ogc:def:uom:EPSG::9001">
                    3.31
</gs:semiMinorAxis>
<gs:orientation uom="urn:ogc:def:uom:EPSG::9102">
                    142
</gs:orientation>
</gs:Ellipsoid>
```

ArcBand



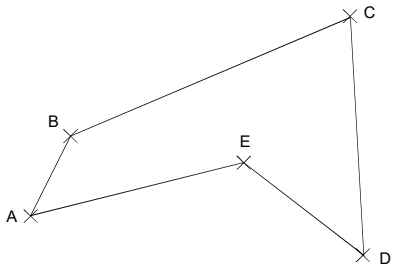
Centre = le pylône

```
<gs:ArcBand srsName="urn:ogc:def:crs:EPSG:: 4326">

<gml:pos>48.884 2.245</gml:pos>

<gs:innerRadius uom="urn:ogc:def:uom:EPSG::9001">
                    1661.55
</gs:innerRadius>
<gs:outerRadius uom="urn:ogc:def:uom:EPSG::9001">
                    2215.4
</gs:outerRadius>
<gs:startAngle uom="urn:ogc:def:uom:EPSG::9102">
                    266
</gs:startAngle>
<gs:openingAngle uom="urn:ogc:def:uom:EPSG::9102">
                    120
</gs:openingAngle>
</gs:ArcBand>
```

Polygone




```
<gml:Polygon
srsName="urn:ogc:def:crs:EPSG::4326"
  xmlns:gml="http://www.opengis.net/gml">
<gml:exterior>
      <gml:LinearRing>
        <gml:posList>
          48.887 2.245
          48.884 2.245
          48.884 2.243
          48.887 2.243
        </gml:posList>
      </gml:LinearRing>
</gml:exterior>
</gml:Polygon>
```

Pull : Données de l'appelant

Nom & Adresse pour les opérateurs commerciaux

```
<m:GetAddressResponse>

<m:PhoneCall>
   <dc:date>2014-03-13T06:23:36Z</dc:date>
   <m:id>FR950SDIS201400013412</m:id>
   <m:psapPhone>+33134355930</m:psapPhone>
   <m:psapId>FR950SDIS</m:psapId>
   <a:NDI>+33130108203</a:NDI>
</m:PhoneCall>

<m:Operator>
   <m:operatorIn>SFR0</m:operatorIn>
   <m:operatorOut>SFR0</m:operatorOut>
   <m:operatorToContact/>
</m:Operator>

<a:UAA>
   <a:TN>NDI</a:TN>
   <a:TA>FACT</a:TA> <!-- Facturation -->
    <a:N10>SFR0</a:N10> <!– Code Opérateur ARCEP -->
   <a:U1a>Linagora</a:U1a>
   <a:U1b>Spécialiste de l'opensource</a:U1b>
   <a:U8>65351865027231</a:U8> <!– SIRET -->
   <a:L4>72 rue Roque de Fillol</a:A7>
   <a:A7> 92299</a:A7>
   <a:A7bis>92062</a:A7bis>  <!– INSEE -->
   <a:A10> Puteaux </a:A10>
   <a:AL>172 rue Roque de Fillol, 92299 Puteaux</a:AL>
</a:UAA>

</m:GetAddressResponse>
```

Heure d' appel du webservice par le PSAP (GMT)

Basée sur la décision ARCEP 06-0639 - annuairiste

Les erreurs techniques seront traitées avec une réponse SOAPFAULT (code retour, code erreur, message erreur, message libre opérateur)

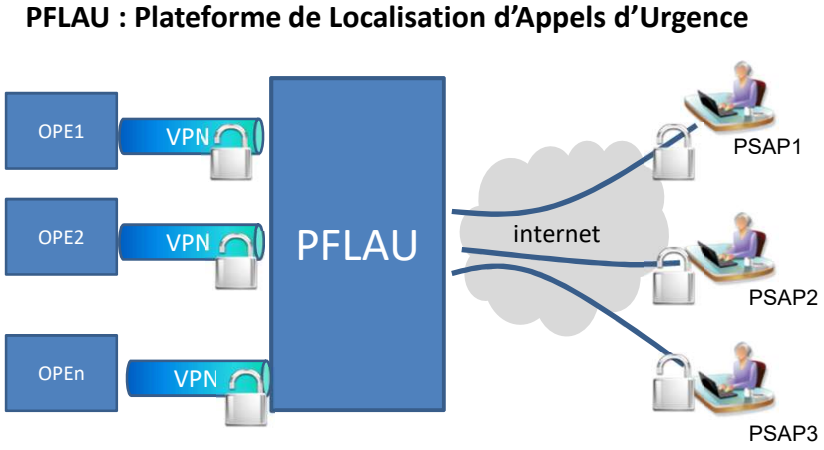
Les erreurs fonctionnelles seront traitées dans le bloc Status de la réponse standard SOAP.

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

L'architecture (1/3)

1) Une plateforme centralisée



Plateforme d'aiguillage sécurisée et hautement disponible

2) Deux webservices

push

Les 4 opérateurs MNO envoient la localisation (lat/long) de l'appelant au

Echanges cryptés via le VPN

pull

Le PSAP demande à la PFLAU l'adresse d'un numéro reçu lors de l'appel d'urgence.

Echanges cryptées Certificat publique

Authentification cryptées :

- Simple cryptage pour le push (VPN)
- Double cryptage pour le pull (VPN + Certificat serveur)

L'architecture (2/3)

DNS ATOS (GSLB : PROD & QUALIF)			Usage	Accès
DNS - SCL	ns3.atos.net	**160.92.121.6**	.	Internet
DNS - VDM	ns4.atos.net	**193.56.46.248**	.	Internet
URI : QUALIF			**Usage**	**Accès**
Webservice getAddress	Uri Pull de l'opérateur	**160.92.118.70**	Demande de getAddress en QUALIF	VPN
IHM	http://qlf-pflau-ihm.aw.atos.net/authent		IHM	VPN & Internet
URI : PROD			**Usage**	**Accès**
Webservice getAddress	Uri Pull de l'opérateur	**160.92.118.65 et 160.92.118.97**	Demande de getAddress en PROD	VPN
IHM	http://pflau-ihm.aw.atos.net/		IHM	VPN & Internet

(*) Attention : il faut faire une résolution DNS pour connaitre l'IP (Site A ou Site B)

L'architecture : SSL (3/3)

- La résolution de l'uri sera fait en se connectant au DNS Atos (cf slide précédent)
- Pour un pull, le PSAP doit présenter son certificat client

Comment puis-je vérifier les informations de mon .JKS ?
Il suffit de lancer depuis votre serveur la commande :*keytool -list -v -keystore ksSignSortant.jks*
Vérifier que l'entry type est positionné à « **PrivateKeyEntry** » et non « **trustedCertEntry** ».

Exemple de code Java pour lier mon certificat Client à ma requête pull :
Voici un estrait du code Worldline qui reste à adapter en fonction de votre propre code.

```
KeyStore ks = KeyStore.getInstance("JKS");
…
ks.setEntry(jksCertifAlias, ks.getEntry(jksCertifAlias, ppEntryKeyPwd), ppJKS);

KeyManagerFactory kmf = KeyManagerFactory.getInstance(KeyManagerFactory.getDefaultAlgorithm());
kmf.init(ks, password);
messageSender.setKeyManagers(kmf.getKeyManagers());
wsTemplate.setMessageSender(messageSender);
```

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

SLA

Fonction	Communication	SLA
WS getAddress	WS	18 sec maximum après la demande.
WS pushLocation	WS	4sec après avoir reçu l'envoi WS de l'opérateur.
Performance (pic)	WS	100 requêtes/sec (push et pull) au maximum au niveau national
Performance (moy)	WS	1 à 2 requêtes/sec (push et pull) au maximum au niveau national

Opérateur commercial

FRTE, SFRO, BOUY, FREE

Les SLA ne sont applicables uniquement que sur l'environnement de PROD.

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Conditions financières

	Type	Qui facture ?	Description
Raccordement	**Solution 1 :** raccordement VPN entre l'opérateur et la PFLAU (OPE <-> PFLAU)		
	CAPEX (VPN)	Worldline	1 950 €/opérateur
	OPEX (VPN)	Worldline	1 920 €/an/opérateur
	Solution 2 : raccordement via un intermédiaire appelé OPTA (OPE <-> OPTA <-> PFLAU)		
	CAPEX (lien OPTA)	OPTA	Voir les tarifs des OPTA
	OPEX(lien OPTA)	OPTA	Voir les tarifs des OPTA
Usage	OPEX (Usage)	APNF	Quelques centimes d'euros par appel

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Comment adhérer à la solution ? (1/3)

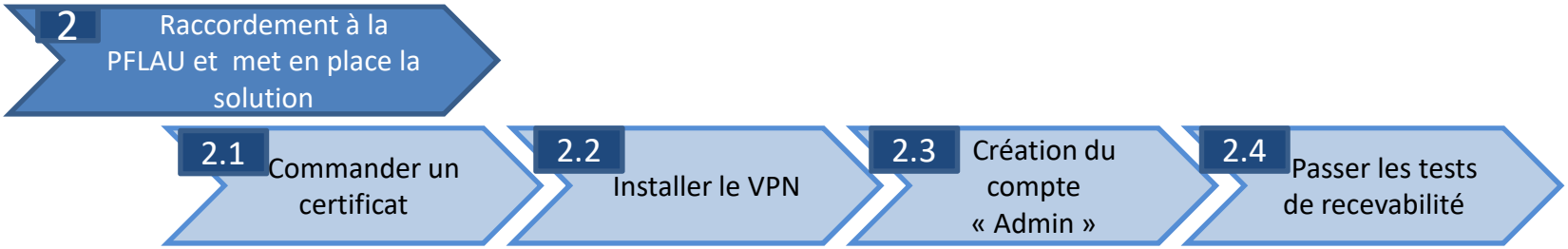
Etape 1 (acteur : Opérateur)
L'opérateur adhère à la PFLAU et accepte le règlement interne précisant les usages liés aux données personnelles..

Etape 2 (acteur : Opérateur)
L'opérateur met en place la nouvelle fonctionnalité de la solution logicielle et les interfaces nécessaires au raccordement à la PFLAU.

Etape 3 (acteur : Opérateur)
L'opérateur teste le webservice « getAddress » en mode bouchonné sur l'environnement de QUALIF.

Etape 4 (acteur : APNF)
L'APNF active le service PFLAU pour l'opérateur une fois les tests passés avec succès.

Comment adhérer à la solution ? (2/3)



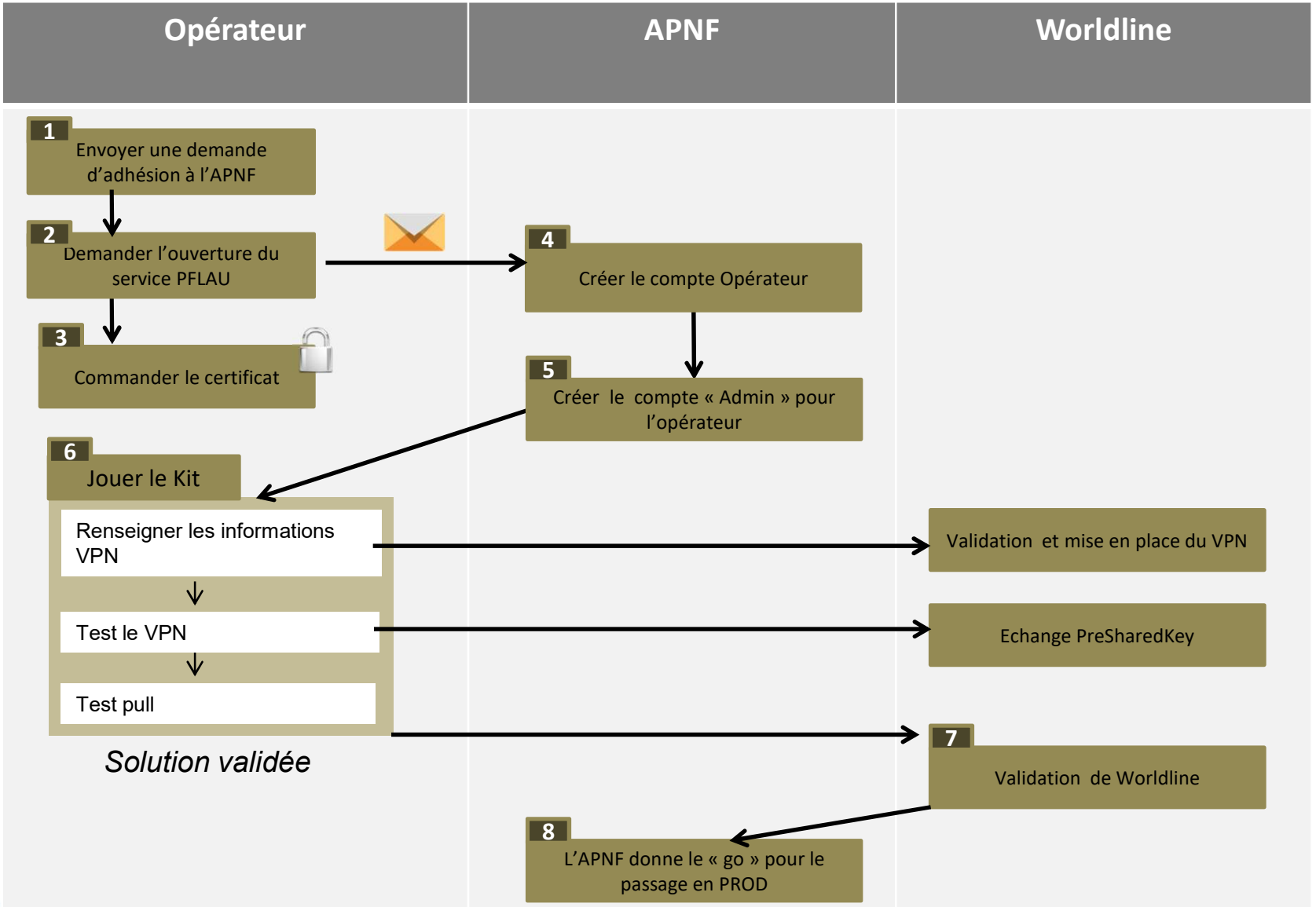
Tâche 2.1 (acteur : Opérateur)
L'opérateur commande un certificat serveur en SHA256 à une des trois autorités suivantes : Entrust, OpenTrust et Verisign/Symantec.

Tâche 2.2 (acteur : Opérateur/Wordline)
L'opérateur installe le VPN après avoir envoyé les informations de connexion et reçu la clé partagée (PSK PreshareKey) de Worldline. La phase finale de l'installation se fera lors d'une conférence téléphonique.

Tâche 2.3 (acteur : APNF)
L'APNF crée le « PSAP Admin » à la réception de l'email. Le « PSAP Admin » reçoit automatiquement un email précisant son « mot de passe ».

Tâche 2.4 (acteur : opérateur)
L'utilisateur « opérateur » procède aux tests du webservice « getAddress »

Comment adhérer à la solution ? (3/3)



Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Certificat : Générer un CSR

Balise	Certificat QUALIF Serveur	Certificat PROD Serveur
C	FR	FR
ST	« OPERATEUR Z »	« OPERATEUR Z »
L	VANNES	VANNES
O	« OPERATEUR Z » SI	« OPERATEUR Z » SI
OU	Serveur	Client
CN	pflau.qual.operateur-Z.fr	pflau.qual.operateur-Z.fr

openssl genrsa -aes256 -out **<cle_privee>**.key 2048

AVEC passphrase protégeant la clé privée :

openssl req -newkey rsa:2048 -keyout **<cle_privee>**.key -out **<fichier>**.csr -subj '/CN=[cf. tabkleau]/OU=[cf. tabkleau],O=[cf. tabkleau]/C=FR'

SANS passphrase protégeant la clé privée :

openssl req -newkey rsa:2048 -keyout **<cle_privee>**.key -out requete.csr -nodes -subj '/CN=[cf. tabkleau]/OU=[cf. tabkleau],O=[cf. tabkleau]/C=FR'

Comment installer un certificat ?

Comment puis-je vérifier les informations de mon .JKS ?
Il suffit de lancer depuis votre serveur la commande :*keytool -list -v -keystore ksSignSortant.jks*
Vérifier que l'entry type est positionné à « **PrivateKeyEntry** » et non « **trustedCertEntry** ».

Exemple de code Java pour lier mon certificat Client à ma requête pull ?
Voici un extrait du code Worldline qui reste à adapter en fonction de votre propre code.

```
KeyStore ks = KeyStore.getInstance("JKS");
…
ks.setEntry(jksCertifAlias, ks.getEntry(jksCertifAlias, ppEntryKeyPwd), ppJKS);

KeyManagerFactory kmf = KeyManagerFactory.getInstance(KeyManagerFactory.getDefaultAlgorithm());
kmf.init(ks, password);
messageSender.setKeyManagers(kmf.getKeyManagers());
wsTemplate.setMessageSender(messageSender);
```

Exemple de code Java pour lier mon certificat Client à ma requête pull ?
Voici un extrait du code Worldline qui reste à adapter en fonction de votre propre code.

```
KeyStore ks = KeyStore.getInstance("JKS");
…
ks.setEntry(jksCertifAlias, ks.getEntry(jksCertifAlias, ppEntryKeyPwd), ppJKS);

KeyManagerFactory kmf = KeyManagerFactory.getInstance(KeyManagerFactory.getDefaultAlgorithm());
kmf.init(ks, password);
messageSender.setKeyManagers(kmf.getKeyMan
```

Ordre du jour

- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Comment valider ma solution ?

Se connecter https://qlf-pflau-ihm.aw.atos.net/web/authent
à l'IHM avec son **compte « Admin » PSAP** et dérouler les 10 étapes suivantes :

Phase	Nb d'actions	Description
1	1	Cocher la case pour indiquer que les « mécanismes de sécurité protégeant les données personnelles » ont été lu
2 3 4	1 + 0 + 0	**Configuration VPN :** Infos VPN + PSK + Config VPN
5 6	1 + 1	**Test VPN :** Opérateur + Worldline
7	0	Test push
8	2	**Tests pull**
9 10	0	Validation Worldline et APNF
Total	**6**	**Actions à réaliser**

Comment valider ma solution ?

Infos VPN

1 | 2,3,4 | 5,6 | 7 | 8 | 9,10

	Champ	Exemple
contact projet (MOA)	Nom	DUPONT François
	Téléphone	+331xxxxxxxx (tel du chef de projet)
	Fax	
	Email	francois.dupont@operateur.com
Contact Technique	Nom	BOULANGER Hugues
	Tel	+331xxxxxxxx
	Fax	
	Email	hugues.boulanger@operateur.com
Paramètres VPN	VPN en mode PSK en SHA256 Cf. « Fiche d'interconnexion VPN-SHA2_Worldline.pdf » (*) Pour l'opérateur utilisant un OPTA, il doit seulement préciser son OPTA (les paramètres VPN sont cachés)	

Comment valider ma solution ?

Test VPN

Validation par Worldline avec l'opérateur lors d'une **conférence téléphonique**

Comment valider ma solution ?

Test push

Hors-Scope
(déjà réalisé par les 4 MNO)

Comment valider ma solution ?

Test pull complet (11/11)

1 | 2,3,4 | 5,6 | 7 | 8 | 9,10

NDI	Description	Message
+33200000002	NDI inconnu	Err0004 – Réponse Standard avec un bloc Status

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Body>
<SOAP-ENV:Fault>
   <faultcode>SOAP-ENV:Server</faultcode>
   <faultstring>ERR0004</faultstring>
   <detail>
      <UnprocessableMessageFault>
         <detailMsg>NDI Inconnu</detailMsg>
      </UnprocessableMessageFault>
   </detail>
</SOAP-ENV:Fault> </SOAP-ENV:Body> </SOAP-ENV:Envelope>
```

Il faut finir les tests « pull » avec un test « OK »
=> Lancer un dernier test avec le **+33232831633**

Comment valider ma solution ?

Test pull

Input – « Kit recevabilité »	Output cartographique

NDI : +33232831633 Go
 	
L'opérateur sélectionne un numéro de son choix (présent dans base de QUALIF pour un test nominal) :
 	
Exemple :
Boutique Bytel (76) : 02 32 83 16 33
	
	
	`<a:UAA>`
	`<a:N10>WRLN</a:N10>`
	`<a:U1a>Club Bouygues Telecom</a:U1a>`
	`<a:U1b>BOUYGUES TELECOM ROUEN RD</a:U1b>`
	`<a:U8b>397480930</a:U8b>`
	`<a:L4>89 RUE DU GROS HORLOGE</a:A7>`
	`<a:A7> 76000</a:A7>`
	`<a:A10>ROUEN</a:A10>`
	`</a:UAA>`

Comment valider ma solution ?

Validation

1 2,3,4 5,6 7 8 9,10

Les étapes 9 et 10 sont réalisées par Worldline et l'APNF

Ordre du jour

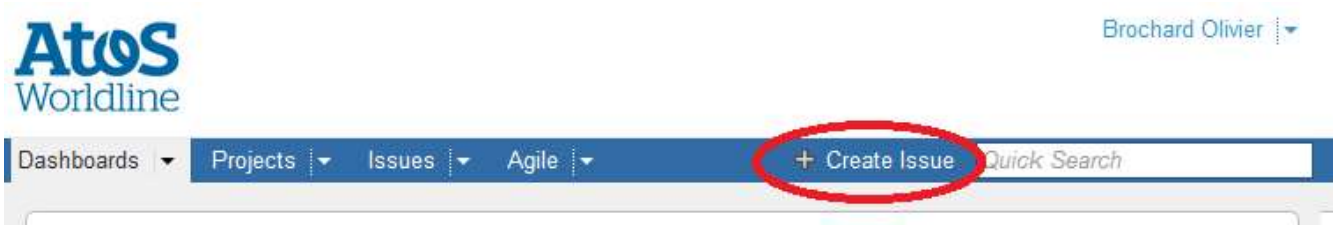
- Introduction
- Les acteurs
- Le processus de localisation
- L'architecture
- Les SLA
- Conditions financières
- Comment utiliser le service ?
- Comment commander un certificat ?
- Comment valider ma solution ?
- Comment déclarer une anomalie ?

Comment déclarer une anomalie?

1) Ouvrir l'IHM « JIRA »

https://jira.itsm.atosworldline.com/jira/secure/Dashboard.jspa

2) Cliquer sur « Create Issue »



Priorité	Description
Critique ou Bloquant	Une anomalie critique empêche le déroulement correct de la VABF.
Majeur	Une anomalie majeure est un écart avec les spécifications sur des fonctionnalités essentielles du service.
Mineur ou Trivial	Une anomalie mineure représente tout autre écart avec les spécifications du lot. Une documentation incorrecte peut également faire l'objet d'une anomalie, au maximum majeure.