Connexion à la PFLAU

Statut :	Finalisé
Editeur :	JEREMIE BIZART
Date d’export :	2024-10-25 15:14:57
Classification :	Confidentiel

Sommaire

1 Évolutions successives

Version	Date	Description	Auteur(s)
01	21/10/2024	Création du document	J. Bizart

2 Introduction

2.1 Objet du document

Ce document sert de référence pour l'interconnexion des parties prenantes du projet aux différents services mis en place sur la PFLAU.

2.2 Responsabilités liées au document

Le chef de projet Worldline est responsable de la rédaction du Dossier de Spécifications ; L'APNF est responsable de sa validation.

2.3 Abréviations

APNF	**A**ssociation pour les **P**lateformes de **N**ormalisation des **F**lux inter-opérateurs
CAAU	**C**entre d'**A**ccueil des **A**ppels d'**U**rgence
CRA	**C**ompte **R**endu d'**A**ppel
GIE-EGP	**G**roupement d'**I**ntérêt **E**conomique **E**ntité de la **G**estion de la **P**ortabilité
HNO	**H**oraire **N**on **O**uvré
IHM	**I**nterface **H**omme **M**achine
OCE	**O**pérateur de **C**ommunication **É**lectronique
OPTA	**Op**érateur **T**echnique d'**A**limentation
PDAA	**P**lan **D**épartementale d'**A**cheminement des **A**ppels
PFLAU	**P**late**F**orme mutualisée de **L**ocalisation des **A**ppels d'**U**rgence
PSAP	**P**ublic **S**afety **A**nswering **P**oint
SVH	**S**auvegarde de la **V**ie **H**umaine
WL	**W**orld**L**ine
WS	**W**eb**S**ervice(s)

2.4 Document de référence

	Nom du document	Version	Description
1	DSP-APNF-PFLAU-E-DSF-001-34 Dossier de Conception PFLAU.pdf	34	Document décrivant toutes les règles métier du projet PFLAU.
2	Package WSDL PFLAU V7.zip	7	Package de WSDL et XSD pour construire le squelette des services PFLAU sur lesquels il faut ensuite appliquer les règles métier du Dossier de Conception PFLAU. Ce dossier contient un fichier Readme.pdf d'une page qui explique le contenu de ce dossier Zip.

3 Service PUSH opérateur

3.1 Introduction

L'opérateur initie le FLUX PUSH pour envoyer une localisation sur la PFLAU.
Deux facteurs peuvent déclencher l'envoi d'une requête PUSH :

- L'émission par l'opérateur d'un appel voix mobile à destination d'un centre de secours
- La réception par l'opérateur d'une demande SVH d'envoi de localisation.

Sur ce flux PUSH, les services PushLocation et PushLocationSVH sont accessibles sur la PFLAU via Internet.
La PFLAU applique deux contrôles :

1. Le contrôle des IP exposées par l'opérateur
2. Le contrôle du certificat joint à la requête PushLocation de l'opérateur (contrôle mTLS).

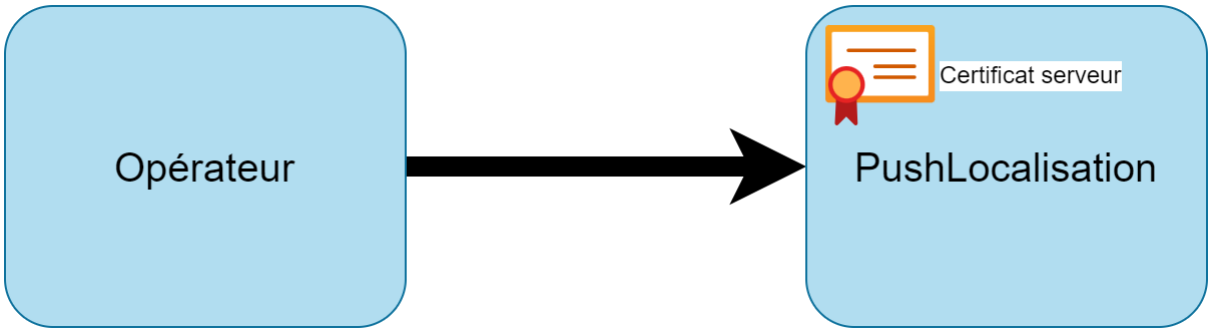
Pour envoyer sa requête d'envoi de localisation, l'opérateur doit appliquer la résolution DNS de l'URL du service pour atteindre les serveurs maintenus opérationnels par Worldline.
Pour plus de détails, veuillez-vous reporter au document de spécification fonctionnelle référencé dans la section "Documents de référence".

3.2 Les URL

Destinations	URL
Service Push de recevabilité	https://push-recevabilite.pflau.fr/pushLocation
Service PUSH de production	https://push.pflau.fr/pushLocation

3.3 Les Certificats

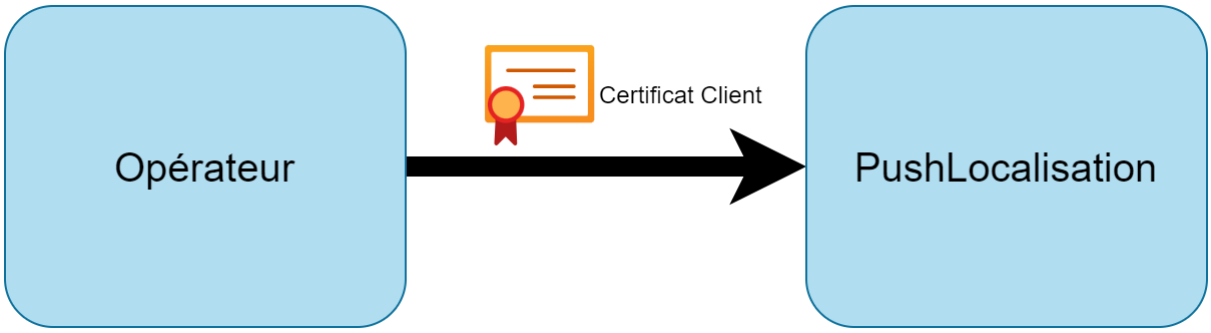
3.3.1 Certificats serveur exposé par la PFLAU



NB
Ce n'est pas un paramètre à modifier sur l'IHM de recevabilité ou l'IHM d'administration de la PFLAU.
S'il y a des actions à mener, elles ont lieu quelque part sur les outils internes des opérateurs dont Worldline n'a aucune connaissance.

Les certificats serveurs des services sont émis par des autorités publiques de confiance.
La confiance de ces certificats peut donc reposer sur le magasin de confiance partagé à l'échelle du système.
Les certificats serveurs ne sont plus fournis afin de ne pas effectuer la confiance sur les certificats.
Cette pratique sera difficile à maintenir car la durée de vie de certains certificats pourrait tendre prochainement à se réduire.

3.3.2 Les certificats Client joint aux appels des opérateurs :



Worldline commande, pour les opérateurs MNO (qui génèrent du PUSH sur la PFLAU), les certificats clients à joindre aux requêtes PushLocation et PushLocationSVH.
Pour qu'un opérateur s'identifie auprès de PFLAU, il doit générer une paire de clés (privée/publique).
L'opérateur conserve secrètement sa clé privée et communique sa clé publique à PFLAU au moyen d'un CSR.
PFLAU retourne le certificat commandé sur la base du CSR.
L'opérateur utilise sa clé privée et le certificat pour s'identifier lors de ses requêtes vers PFLAU PUSH.
Pour la génération du CSR, nous avons besoin :

- Du bon CN : client-push-***<code arcep de l'opérateur en minuscule>***-recevabilite.pflau.fr
  Par exemple pour l'opérateur avec le code ARCEP OPER, sont cn est client-push-*oper*-recevabilite.pflau.fr
- Du RSA 2048 ou ECC P256
- Pas besoin de SAN
- Le CSR doit avoir pour but la commande d'un certificat Client.

X509v3 Extended Key Usage:
TLS Web Client Authentication

Nous avons besoin d'un CSR pour le certificat client de recevabilité et d'un autre pour la production.
L'autorité de certification que nous utilisons est Sectigo.

Environnement	Certificat
Recevabilité	client-push-***<code arcep de l'opérateur en minuscule>***-recevabilite.pflau.fr
Production	client-push-***<code arcep de l'opérateur en minuscule>***.pflau.fr
Racine	Sectigo RSA Organization Validation Secure Server CA

3.4 Algorithme de chiffrement, Sécurisation https sur le flux PUSH

Aujourd'hui, la PFLAU ne peut être appelée en TLS 1.3 sur la plateforme Legacy ; seul le TLS 1.2 est valide.
Voici la liste des ciphers supportés :

- ECDHE RSA AES256 GCM SHA384
- DHE RSA AES256 GCM SHA384
- ECDHE RSA AES128 GCM SHA256
- DHE RSA AES128 GCM SHA256
- ECDHE RSA AES256 SHA384
- DHE RSA AES256 SHA256
- ECDHE RSA AES128 SHA256
- DHE RSA AES128 SHA256

3.5 Renouvellement des certificats

Les certificats renouvelés ne peuvent avoir une durée de validité supérieur à 13 mois.
Worldline ne peut commander les nouveaux certificats qu'un mois avant leurs fins de validité.
La période pendant laquelle les opérateurs doivent inclure les nouveaux certificats à leurs truststore est donc limité à une période de 2 à 3 semaines.
Si ce n'est déjà fait, vous pouvez donc noter dès aujourd'hui dans votre agenda ou autres outils et avec reconduction annuelle, le planning suivant :

Quand	Quoi	Qui
De mi-juin à mi-juillet :	**Le Rappel** Worldline rappelle les dates de fin de validité des certificats et qu'une action de mise à jour de truststore est attendue de votre part. *L'opérateur peut fournir à Worldline les CSR des certificats client PUSH.*	**WL** Opérateur
De mi-juillet à mi-aout :	**L'annonce de l'agenda** Worldline communique aux opérateurs le calendrier de mise à jour des certificats. ***L'opérateur doit fournir à Worldline les CSR des certificats client PUSH.***	**WL** **Opérateur**
Premier jour ouvrée de septembre :	***Remise des certificats*** Worldline fournit les certificats fournis par Sectigo et les ajouts à son truststore	***WL***
À la date annoncée :	**Mise à jour du certificat** L'opérateur bascule sur l'utilisation du nouveau certificat pour le service PUSH	**Opérateur**
Après la date annoncée :	**Mise au propre du truststore WL** Worldline supprime l'ancien certificat Client de l'opérateur de son truststore.	**WL**

4 Service PULL opérateur

4.1 Introduction

Les centres de secours (PSAP) initient le FLUX PULL pour envoyer une demande d'adresse ou de localisation sur la PFLAU.
Trois facteurs peuvent déclencher l'envoi d'une requête PULL :

- L'émission par un centre de secours d'une demande d'adresse suite à la réception d'un appel voix fixe ou mobile
- L'émission par la police nationale ou la gendarmerie d'une demande d'adresse dans le cadre d'un usage défini par SVH
- L'émission par la police nationale ou la gendarmerie d'une demande d'envoi de localisation dans le cadre d'un usage défini par SVH

Sur ce flux PULL, les services getAddress, GetAddressSVH et GetLocationSVH sont accessibles chez les opérateurs via Internet.
Lors de l'appel au service de l'opérateur, la PFLAU :

1. Procède à une résolution DNS pour envoyer la requête au serveur actif de l'opérateur.
2. Contrôle le certificat serveur exposé par le service de l'opérateur.
    a. Le certificat fait partie d'une autorité de certification autorisée par la PFLAU.
    b. La date de validité du certificat est en cours.
    c. L'id du certificat n'est pas présent dans la CRL de l'autorité de certification.
    d. Le certificat comporte un attribut CN ou SAN conforme à l'entrée DNS utilisée pour contacter l'opérateur.
    Ainsi, l'utilisation d'un certificat WildCard n'est pas refusée par la PFLAU. Cependant, il faut configurer le CN pour qu'il corresponde au DNS.
    De même, l'exposition d'une URL contenant une IP, comme "https://127.0.0.1/servicePULL", impliquerait d'avoir un certificat dont le CN expose "127.0.0.1".
3. Joindre un certificat client dans la requête au service de l'opérateur.

Pour réceptionner la requête, l'opérateur :

- Peut contrôler l'IP exposée par la PFLAU lors de l'appel.
- Passe l'étape d'authentification :
  L'authentification se base sur la présentation d'un certificat dont on a confiance et une preuve de détention de la clé privée : le serveur envoie un challenge que le client signe avec la clé privée, vérifiable par le serveur à partir du certificat client présenté.
- Passe l'étape de l'autorisation :
  L'autorisation se base sur les attributs du certificat client présenté. CN avec une valeur correspondant à une entrée DNS.
  Nous déconseillons fortement le contrôle spécifique de champs tels que l'Organization (champs O:) du certificat, qui chez Worldline peut varier d'un certificat à un autre.
  Dans l'histoire de la PFLAU, ce champ a pu être "Atos Worldline", "Atos", "Worldline FR", "Worldline" et cette liste n'est pas exhaustive.

Pour plus de détails, veuillez-vous reporter au document de spécification fonctionnelle référencé dans la section "Documents de référence".

4.2 Les URL

Les opérateurs mettent à jour leurs URL PULL depuis les IHM de recevabilité et d'administration dans la fiche de détail de leur opérateur.

Bulle	URL
Recevabilité	https://ihm-recevabilite.pflau.fr
Production	https://ihm-administration.pflau.fr

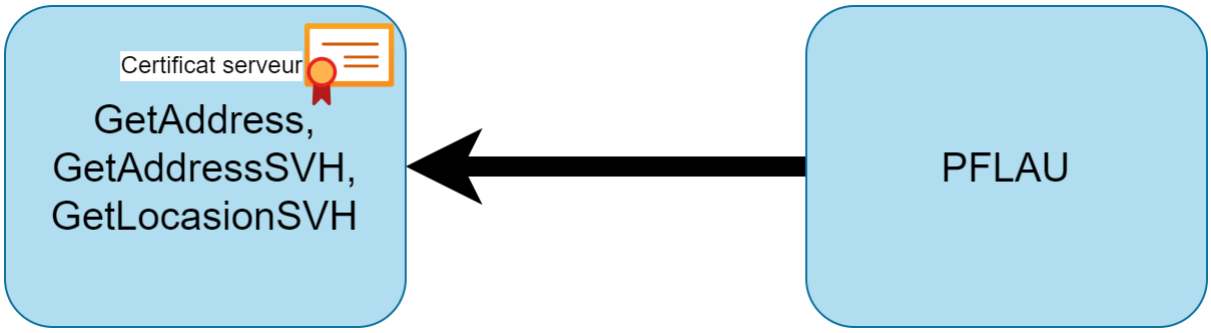
4.3 Les adresse IP présentées par la PFLAU :

Depuis la bulle de recevabilité, nous nous présentons avec l'IP : 160.92.143.41
Depuis la bulle de production, nous nous présentons avec les IP : 160.92.143.40 et 160.92.56.129

NB
Veuillez noter qu'entre janvier et mars 2025, la PFLAU migrera vers une nouvelle plateforme et nous exposerons de nouvelles plages d'IP en bulle de recevabilité, puis en production.
Elles vous seront communiquées à l'avance.

4.4 Les Certificats

4.4.1 Certificats serveur exposé par l'opérateur



NB
Ce certificat n'est pas géré par la PFLAU. Aucun contrôle de renouvellement futur de ce certificat n'est appliqué par la PFLAU et il ne fait donc l'objet d'aucune alerte dans ce cas.
Ce certificat est de la responsabilité de l'opérateur. C'est à l'opérateur d'en assumer le renouvellement avec des procédures qui lui sont internes.

Les certificats Client joint aux appels de la PFLAU :

En raison du grand nombre d'opérateurs raccordés à la PFLAU, ce certificat est commun à tous les appels PULL de tous les opérateurs.
De plus, c'est le même certificat client qui est présenté, quel que soit le service PULL ciblé (GetAddress, GetAddressSVH ou GetLocationSVH).
Ainsi, c'est Worldline qui gère et commande ce certificat.
Nos certificats utilisent les attributs suivants :

- CN : client-pull-recevabilite.pflau.fr ou client-pull.pflau.fr
- PK : RSA - 2048
- SAN : dNSName=client-pull-recevabilite.pflau.fr ou dNSName=client-pull.pflau.fr

L'autorité de certification que nous utilisons est Sectigo.

CN	Certificat
client-pull-recevabilite.pflau.fr	-----BEGIN CERTIFICATE----- MIIG7TCCBdWgAwIBAgIRAPjKr8aMIeJbMKfs/f2tEZcwDQYJKoZIhvcNAQELBQAw gZUxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAO BgNVBAcTB1NhbGZvcmQxGDAWBgNVBAoTD1NlY3RpZ2gTGltaXRlZDE9MDsGA1UE AxM0U2VjdGlnby9SU0EgT3JnYW5penF0aW9uIFZhbGlkYXRpb24gU2VjdCJlIFNl cnZlciBDQTAeFw0yNDA5MDYwMDAwMDBaFw0yNTEwMDYyMzU5NTlaMGUxCzAJBgNV BAYTAkZSMRYwFAYDVQQIEw1JbGUtZGUtRnJhbmNlMRIwEAYDVQQKEwlXb3JsZGxp bmUxKjAoBgNVBAMTIWNsaWVudC1wdWxsLXJlY2V2YWJpbGl0ZS5wZmxhdS5mcjCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALwwXsZmmB5f/Zih08cgwTLc MxQLjXiAqgeuqNCv9VwhKSskH06X54/vRIA+KqLSAq2bW3fs+wAELlLKvTMg2uxy cqDQBBtBsDbmv3mSGOwNRJjMzRvDPx/m8ghy2tRURBxW5HS81L55tlkzwvYzw+gU QbFwCYtr+3r2ptAxnyLbNE+wEi+uUVI15RJ8y5BI3qaiHCDn4JpEHKwsQUaYkdnU vGmvgjjHwzvRpThLSwOgZvKVJfLNSJ3ulytXheY7NVGz6FsA4+UUBHoUYsl5r1/h I0XESm1O9LJxlnGKpgpso8+/1oJm19vUEiEtK8GWNMDLfu2LT5rHsbiIBfKtLbMC AwEAAaOCA2UwggNhMB8GA1UdIwQYMBaAFBfZiiUnZ/kxwklD2TA2RIxsqU/rMB0G A1UdDgQWBBR6uP/FhStykb6iwihtnY251YWYDAOBgNVHQ8BAf8EBAMCBaAwDAYD VR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwSgYDVR0g BEMwQTA1BgwrBgEEAbIxAQIBAwQwJTAjBggrBgEFBQcCARYXaHR0cHM6Ly9zZWN0 aWdvLmNvbS9DUFMwCAYGZ4EMAQICMFoGA1UdHwRTMFEwT6BNoEuGSWh0dHA6Ly9j cmwuc2VjdGlnby5jb20vU2VjdGlnb1JTQU9yZ2FuaXphdGlvbIZhbGlkYXRpb25T ZWN1cmVTZXJ2ZXJDQS5jcmwwgYoGCCsGAQUFBwEBBH4wfDBVBggrBgEFBQcwAoZJ aHR0cDovL2NydC5zZWN0aWdvLmNvbS9TZWN0aWdvU1NBT3JnYW5penF0aW9uVmFs aWRhdGlvblNlY3VyZVNlcnZlckNBLmNydDAjBggrBgEFBQcwAYYXaHR0cDovL29j c3Auc2VjdGlnby5jb20wggF9BgorBgEEAdZ5AgQCBIIBbQSCAWk8Zw8JAN3cyjSV 1+EWBeeVMvrHn/g9HFDf2wA6FBJ2CiysuBqqAAABkcgZ+wYAAAQDAEcwRQIgbqkg ww50n1o76QM6UqOiUKKFP+hi9uqO6jyjQOTiD68CIQCHrfajT5DlDBmfG1ZcA0hT +IrP4OB1yCZNknFvDWtKMAB2AA3h8jAr0w3BQGISCepVlvxHdHyx1+kw7w5CHrR+ Tqo0AAABkcgZ+s0AAAQDAEcwRQIhAIjQmMcjBNCWf5OkNjLBzCDZHtSMfPry3iOp I4nZ0SxfAiBWGI0pU1qIIP0VPUH4+X/wyvWkCq6NLpMqUL4pO4gStAB1ABLxTjS9 U3JMhAYZw48/ehP457Vih4icbTAFhOv1hiY6AAABkcgZ+poAAAQDAEYwRAIgXx1X AEZM0z93pWbWxzH+FnAq611ARKjMkcYsG0fozuICIGMJfo8xjj/Kcn+F2gRRwAQk 95CzF3x1smJqrrh6JvdjMCwGA1UdEQQiMCOCIWNsaWVudC1wdWxsLXJlY2V2YWJp bG10ZS5wZmxhdS5mcjANBgkqhkiG9w0BAQsFAAOCAQEAM50OS/oCmnTKC9c7Cpjq Q2c1C8Dn3Tx1JsWaZMQHbgtvbIs1IvZMMklvKMB2HZ6Bngvo2Lh7QiiPPCuXbk4y LiEl8to+IWBCI10mJovjti4jKw1OAAxP1t1j0SjPagCSDSSdDqgWt1hXsKTvNMH6 JBGOEbBOyiSRqrdOA6yDVMGHeNpBGf5tiZQJrX9LOrKqaruVUBlNG+84Z8jEAn25 kfO2rZUGUB42L0L/MTiCFPtRMcKw8lQBDpDyk/UIUy9wn2hnujBZ20T5VSsRmEoq sgojwIk7J6WisniS27/If74Ikz0yu1p+9x1T7h9ZACWOc1lUvx+N6CjOx+w8+bI4 FA== -----END CERTIFICATE-----
client-pull.pflau.fr	-----BEGIN CERTIFICATE----- MIIG0jCCBbqgAwIBAgIQc5Fmvsh8Wuv4AK5dFm0gQDANBgkqhkiG9w0BAQsFADCB lTELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G A1UEBxMHU2FsZm9yZDEYMBYGA1UEChMPU2VjdGlnbyBMaW1pdGVkMT0wOwYDVQQD EzRTZWN0aWdvIFJTQSBPcmdhbml6YXRpb24gVmFsaWRhdGlvbiBTZWN1cmUgU2Vy dmVyIENBMB4XDTI0MDkwNjAwMDAwMFoXDTI1MTAwNjIzNTk1OVowWDELMAkGA1UE BhMCR1IxFjAUBgNVBAgTDUlsZS1kZS1GcmFuY2UxEjAQBgNVBAoTCVdvcmxkbGlu ZTEdMBsGA1UEAxMUY2xpZW50LXB1bGwucGZsYXUuZnIwggEiMA0GCSqGSIb3DQEB AQUAA4IBDwAwggEKAoIBAQCkO/FAfgTzAYClb9QXOETUotLjfVjFlcepkLvkHYpk LY1+/GWF4mqsB6oDr49I0wpXEy3qFnUqjFiZ21WHrSBhn/obzBy15cVZfEuxObmY NaxYeLM6P3ai4btVlNdGLDAOwRiMiuhVP9tW1i/1LCnqDRDQ1Z7W0Tzj62PCTQoy eTJItBZGIvQXkmrI4rajpqxkABFghFxKIBye1zBFx91aFh4c7/7h6AUwWr2+1GiO HcvGD/ClgQ930Ix8LFoPAel4mwjGeAJlFkY3DttD8+gvhVaN8+IKyNQtOc19KZN H4a3YIzaUIGViKosGmuSDUbtzbMw7VfpkBOVKzEPximbAgMBAAGjggNYMIIDVDAf BgNVHSMEGDAWgBQX2dYlJ2f5McJJQ9kwNkSMbKlP6ZadBgNVHQ4EFgQUeNYNS0re HW7gFCAglpWNa49gdzswDgYDVR0PAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYD VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMEoGA1UdIARDMEEwNQYMKwYBBAGy MQECAQMEMCUwIwYIKwYBBQUHAgEWF2h0dHBzOi8vc2VjdGlnby5jb20vQ1BTMAgG BmeBDAECAjBaBgNVHR8EUzBRME+gTaBLhklodHRwOi8vY3JsLnNlY3RpZ28uY29t L1NlY3RpZ29SU0FPcmdhbml6YXRpb25WYWxpZGF0aW9uU2VjdXJlU2VydmVyQ0Eu Y3JsMIGKBggrBgEFBQcBAQR+MHwwVQYIKwYBBQUHMAKGSWh0dHA6Ly9jcnQuc2Vj dGlnby5jb20vU2VjdGlnb1JTQU9yZ2FuaXphdGlvbIZhbGlkYXRpb25TZWN1cmVT ZXJ2ZXJDQS5jcmwwIwYIKwYBBQUHMAGGF2h0dHA6Ly9vY3NwLnNlY3RpZ28uY29t MIIBfQYKKwYBBAHWeQIEAgSCAW0EggFpAWcAdQDd3Mo0ldfhFgXnlTL6xS/4PRxQ 39sAOhQSdgosrLvIKgAAAZHIFzxkAAAEAwBGMEQCIBOcvDbH4yn09bGmvesQVBwW M/9AF8qUY8AKMuacuom/AiBECyL53e2Xv1TfqKiP2057j5EaQw2GGDXRdXI6/vz0 LAB2AA3h8jAr0w3BQGISCepVLvxHdHyx1+kw7w5CHrR+Tqo0AAABkcgXPAoAAAQD AEcwRQIgWubBzhfwN0E9GO7AWmTTXgIJstFxjvzz4qTENy5vgMCIQCwlHq3bVOw LxwbCZo7TY9X9BiHgIE0Ote+zMSrvwLfOwB2ABLxTjS9U3JMhAYZw48/ehP457Vi h4icbTAFhOv1hiY6AAABkcgXO/4AAAQDAEcwRQIgfVY/c26AxfFKZaWZ7dXzy6kj NWInqpkU8aaYd9UzDLoCIQC4YycgkcO0m2WSRNI+Mz6FQ/ZsF1AXtt5r10jcYoEH VzAfBgNVHREEGDAWghRjbGllbnQtcHVsbC5wZmxhdS5mcjANBgkqhkiG9w0BAQsF AAOCAQEAJ7fQQphx5aiG0OHrkOE78ub5eC1vvHpvV1TXE/xIP9hBOWA7zY2c9ydM aAjGuOPFCCuZAnK9NtWsaQ/o9lsu8XNYPcGL6B47/7okLmDUjESLeCeijtDRGmsQ phCeHoKGl2j5H89avSjYeNs8D3KMR0AKPAjP1ZscrF+Y0NT01+ws5KedrotwMzZ0 jR/SPWJL/5O9/QAw12uP9RAcbuAUBuKiNsuy1+V6U2P0krOV0EulPnXytFSvztqr idlv59mzc3kCovpWO6h4GLs/zSK7sKP2pPqn+IuIzteuPOtvVXhjZwo8yHqVqGvN 1V4ivkyyWRtPkkrFP5U0+Fobb4uu2Q== -----END CERTIFICATE-----
Sectigo RSA Organization Validation Secure Server CA	-----BEGIN CERTIFICATE----- MIIGGTCCBAGgAwIBAgIQE31TnKp8MamkM3AZaIR6jTANBgkqhkiG9w0BAQwFADCB iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCks1dy0KZXJzZXkxFDASBgNVBAcTC0pl cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFU1RSVVNUIE51dHdvcmsxLjAsBgNV BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTgx MTAyMDAwMDAwWhcNMzAxMjMxMjM1OTU5WjCBlTELMAkGA1UEBhMCR0IxGzAZBgNV BAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEYMBYGA1UE ChMPU2VjdGlnbyBMaW1pdGVkMT0wOwYDVQQDEzRTZWN0aWdvIFJTQSBPcmdhbml6 YXRpb24gVmFsaWRhdGlvbiBTZWN1cmUgU2VydmVyIENBMIIBIjANBgkqhkiG9w0B AQEFAAOCAQ8AMIIBCgKCAQEAnJMCRkVKUkiS/FeN+S3qU76zLNXYqKXsW2kDwB0Q 9lkz3v4HSKjojHpnSvH1jcM3ZtAykffFnQRgxLVK4oOLp64m1F06XvjRFnG7ir1x on3Izq3g7lBSoDpFUd54k2xiYPHkVpy3O/c8Vdjf1XoxfDV/E1Fw4Sy+BKzL+k/h fGVqwECn2Xyl Y4QZ4ffK76q06Fha2Znj2t+OErK43DOyNtoUHZZYQkBuCyKFHFEi rsTIBkVtkuZntxkj5Ng2a4XQf8dS48+wdQHgibSov4o2TqPgbOuEQc6l1Qgie5dQ YkUeCaXMn2xXcEAG2yDoG9bzk4unMp63RBUJ16/9fAEc2wIDAQABo4IBbjCCAWow HwYDVR0jBBgwFoAUU3m/WqorSs9UgOHYm8Cd8rIDZsswHQYDVR0OBBYEFBfZ1iUn Z/kxwklD2TA2RIxsqU/rMA4GA1UdDwEB/wQEAwIBhjASBgNVHRMBAf8ECDAGAQH/ AgEAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAbBgNVHSAEFDASMAYG BFUdIAAwCAYGZ4EMAQICMFAGA1UdHwRJMEcwRaBDoEGGP2h0dHA6Ly9jcmwudXN1 cnRydXN0LmNvbS9VU0VSVHJ1c3RSU0FDZXJ0awZpY2F0aW9uQXV0aG9yaXR5LmNy bDB2BggrBgEFBQcBAQRqMGgwPwYIKwYBBQUHMAKGM2h0dHA6Ly9jcnQudXN1cnRy dXN0LmNvbS9VU0VSVHJ1c3RSU0FBZGRUcnVzdENBLmNydDAlBggrBgEFBQcwAYYZ aHR0cDovL29jc3AudXN1cnRydXN0LmNvbTANBgkqhkiG9w0BAQwFAAOCAgEATHNA lsnD5m5bwOO69Bfhrgkfyb/LDCUW8nNTs3Yat6tIBtbNAHwgRUNFbBZaGxNh10m6 pAKkrOjOzi3JKnSj3N6uq9BoNviRrzwB93fVC8+Xq+uH5xWo+jBaYXEgscBDxLmP bYox6xU2JPti1Qucj+1mveZhUZeTh2HvbC1bP6mESkGYTQxMD0g3NR0N6Fg9N3 OSBGltqnxloWJ4Wyz04PToxcvr44APhL+XJ71PJ616IphdAEutNCLFGIUi7RPSRn R+xVzBv0yjTqJsHe3cQhifa6ezIejpZehEU4z4CqN2mLY8d0FUiRnG3wTqN3yhsc SPr5z0noX0+FCuKPkBurcEya67emP7SsXaRfz+bYipaQ908mgWB2XQ8kd5GzKjGf FlqyXYwcKapInI5v03hAcNt37N3j0VcFcC3mSZiIBYRiBXBWdoY5TtMibx3+bfEO s2LEPMvAhblHHrhYB2lAyuBbuMf1a+HNJav5fyakywxnB2sJCNwQs2uRHYiihc 6k/+JLcYCpsM0MF8XPtpvcyiTcaQvKZN8rG61ppnW5YCUtCC+cQKXA0o4D/I+pWV idWkvklsQLI+qGu41SWyxP7x09fn1txDAXYw+zuLXfdKiXyaNb78yvBXAfCNP6CH MntHWpdLgtJmwsQt6j8k9Kf5qLnjatkYYaA7jBU= -----END CERTIFICATE-----

4.5 Algorithme de chiffrement, Sécurisation https sur le flux PULL

Actuellement les opérateurs exposent un service https en tls1.2 et certain en tls1.3.
La PFLAU accepte à ce jour d'émettre des requêtes vers les 2 versions du protocole
WL recommande l'utilisation des ciphers suivants :

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV
- TLS_RSA_WITH_NULL_SHA256
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_NULL_SHA
- SSL_RSA_WITH_NULL_SHA

4.6 Renouvellement des certificats Clients

Les certificats renouvelés ne peuvent avoir une durée de validité supérieure à 13 mois.
Worldline ne peut commander les nouveaux certificats qu'un mois avant leur fin de validité.
La période pendant laquelle les opérateurs doivent inclure les nouveaux certificats dans leur truststore est donc limitée à 2 à 3 semaines.
Si ce n'est déjà fait, vous pouvez noter dès aujourd'hui dans votre agenda ou autres outils, avec reconduction annuelle, le planning suivant :

Quand	Quoi	Qui
De mi-juin à mi-juillet :	**Le Rappel** Worldline rappelle les dates de fin de validité des certificats et qu'une action de mise à jour de truststore est attendue de votre part.	**WL**
De mi-juillet à mi-aout :	**L'annonce de l'agenda** Worldline communique aux opérateurs le calendrier de mise à jour des certificats. Une période de recouvrement permet à l'opérateur d'autoriser simultanément l'ancien et le futur certificat client.	**WL**
Dans les premiers jours ouvrés de septembre :	***Remise des certificats*** Worldline fournit les certificats émis par Sectigo.	***WL***
Sur la période de recouvrement annoncé :	**Mise à jour du certificat** L'opérateur ajoute le nouveau certificat client à son truststore.	**Opérateur**
À la date annoncé	**Bascule de certificat Client** Worldline utilise le nouveau certificat client.	**WL**
Après la date annoncée :	**Mise au propre du truststore opérateur** L'opérateur peut supprimer l'ancien certificat client de la PFLAU de son truststore.	**Opérateur**

Voici un exemple de cadencement de renouvellement :

À ce jour, la PFLAU n'est pas équipée pour tenir à jour un annuaire des équipes techniques de toutes les parties prenantes de la PFLAU, d'autant plus que ces contacts peuvent changer d'une année sur l'autre.
Ainsi, pour garantir une procédure reproductible chaque année, Worldline se base sur les contacts renseignés sur la PFLAU.
Ainsi, les communications annuelles mentionnées ci-dessus sont adressées aux comptes Opérateur Manager, qui ont la responsabilité de remonter les informations à leur(s) équipe(s) en charge d'effectuer les actions nécessaires.
De même, il est de la responsabilité de l'Opérateur Manager, en cas de changement d'activité, de s'assurer qu'il a pris les dispositions nécessaires en contactant l'APNF pour demander une réattribution de son compte à son remplaçant.