



# Guide Web Services IGC-Santé

# Guide d'utilisation Web Service Plateforme IGC-Santé « ANS »

Version 1.1.0 du 06/10/2021

Historique du document			
Version	Date	Auteur	Commentaires
1.0.0	12/02/2016	ASIP Santé	Première version publiée
1.0.1	02/06/2016	ASIP Santé	Prise en compte des remarques du support
1.1.0	06/10/2021	ANS	Changement de nom ANS

# Sommaire

Sommaire .....	3
1 Références.....	5
2 Résumé.....	7
2.1 Objet du document .....	7
2.2 Présentation de l'interface Web Service.....	7
2.3 Présentation de l'outil de test Web Service (SoapUI) .....	8
3 Glossaire .....	11
4 Avertissements .....	13
5 Démarrage.....	14
5.1 Pré requis.....	14
5.2 Installation de la carte.....	16
6 Les produits délivrés par la plateforme IGC-Santé.....	18
6.1 Présentation des produits .....	18
6.2 Cas particulier de l'adresse email protégée .....	19
7 Habilitations .....	20
8 Configurations .....	23
8.1 Fichier XSD.....	23
8.2 Fichier WSDL.....	26
9 Authentification.....	29
10 Signature .....	31
11 Création d'une CSR.....	34
11.1 Etape 1 : génération de la clé privée .....	35
11.2 Etape 2 : création de la CSR.....	35
12 Gestion des Certificats Logiciels de test.....	38
13 Demande de création de certificat.....	39
13.1 Demande de Lot de certificat .....	39
13.2 Réponse de la demande de lot de certificats.....	45
13.2.1 Exemples de cas passant .....	46
13.2.2 Exemple de cas non passant.....	47
13.3 Notifications en lien avec la demande de certificat .....	50
13.4 Cas non passants au niveau des contrôles métiers.....	52
14 Retrait d'un certificat .....	55
14.1 Demande de retrait d'un certificat.....	55
14.2 Transmission du certificat .....	59
14.3 Notifications en lien avec le retrait de certificat .....	61
14.4 Cas non passants .....	62
15 Révocation de certificat.....	66
15.1 Demande de révocation d'un certificat.....	66
15.2 Réponse de la demande .....	71
15.3 Notifications en lien avec la révocation .....	73
15.4 Cas non passants .....	75

16	Renouvellement de certificat .....	77
16.1	Demande de renouvellement de certificat .....	77
16.2	Réponse de la demande de renouvellement .....	83
16.3	Notifications en lien avec le renouvellement.....	85
16.4	Cas non passants .....	87
17	Suivi de l'activité.....	90
17.1	Demande de suivi .....	91
17.2	Réponse de la demande de suivi.....	95
17.3	Cas non passants .....	103
18	Tableaux des erreurs Web Service .....	108
19	Tableaux des erreurs métiers transverses .....	113
20	Annexe – Titre Annexe .....	122
21	Annexe – Table des figures.....	123
22	Annexe – Liste des tableaux .....	126
23	Notes .....	127

# 1 Références

Documents de référence				
N°	Version	Date	Auteur	Document
[1]	1.0.0	28/01/2016	ASIP Santé	Guide d'utilisation IHM ASIP_IGC-Sante_Guide-IHM_160128_v1.0.0
[2]	1.0.0	28/01/2016	ASIP Santé	Guide Web Service Annexe 1 ASIP_IGC-Sante_Guide-WebService-Annexe1_160128_v1.0.0
[3]	1.0.0	28/01/2016	ASIP Santé	Guide Web Service Support ASIP_IGC-Sante_Guide-WebService-Support_160128_v1.0.0

Tableau 1 : Documents de référence

## 2 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

Nom	Site Web	Lien avec la Cryptolib CPS
Apple	<a href="http://www.apple.com">www.apple.com</a>	Mac OS X
Google	<a href="http://www.google.com">www.google.com</a>	Google Chrome
Microsoft	<a href="http://www.microsoft.com">www.microsoft.com</a>	Windows, CSP, Internet Explorer, C#, .NET, TSE
Mozilla	<a href="http://www.mozilla.org">www.mozilla.org</a>	Mozilla Firefox
Oracle	<a href="http://www.oracle.com">www.oracle.com</a>	Java, SunMSCAPI

Tableau 2 : Entreprises citées

## 3 Résumé

### 3.1 Objet du document

Ce document a pour but de décrire l'interface Web Service hébergée par la plateforme de gestion des certificats pour l'ANS.

### 3.2 Présentation de l'interface Web Service

Le canal Web Service (WS) permet à un acteur personne physique d'interagir indirectement avec la plateforme IGC-Santé via une application utilisatrice ou un serveur.

L'acteur signe les actions demandées à la plateforme IGC-Santé, ce qui permet de s'assurer de l'identité de l'acteur ayant demandé l'action.

Les appels Web Services sont sans état. Ils font toujours l'objet d'une réponse en retour.

Dans le cas où le processus du canal Web Service a rencontré une erreur, l'erreur est retournée dans la réponse Web Service. Les opérations disponibles avec le canal Web Service sont listées ci-dessous :

- Demande de création de certificat
- Retrait de certificat
- Révocation d'un certificat
- Renouvellement d'un certificat
- Suivi de l'activité

#### **Urls d'accès au Web Service :**

<https://pfc-auth.eservices.esante.gouv.fr/ws-srv>

- Pour les serveurs appelant les Web Services avec un certificat serveur

<https://pfc-auth.eservices.esante.gouv.fr/ws-apt>

- Pour les applications permettant à une personne de faire la requête et d'insérer sa carte pour signer avec son certificat de signature personnel

### 3.3 Présentation de l'outil de test Web Service (Soap UI)

Afin d'illustrer les différents Web Services, l'outil Soap UI est présenté dans ce document en tant que **démonstrateur**. Il est utilisé uniquement pour fournir les exemples du document.

Une présentation rapide de l'outil permet de comprendre les copies d'écran utilisées pour effectuer les tests.

**Vue d'ensemble de l'outil :**

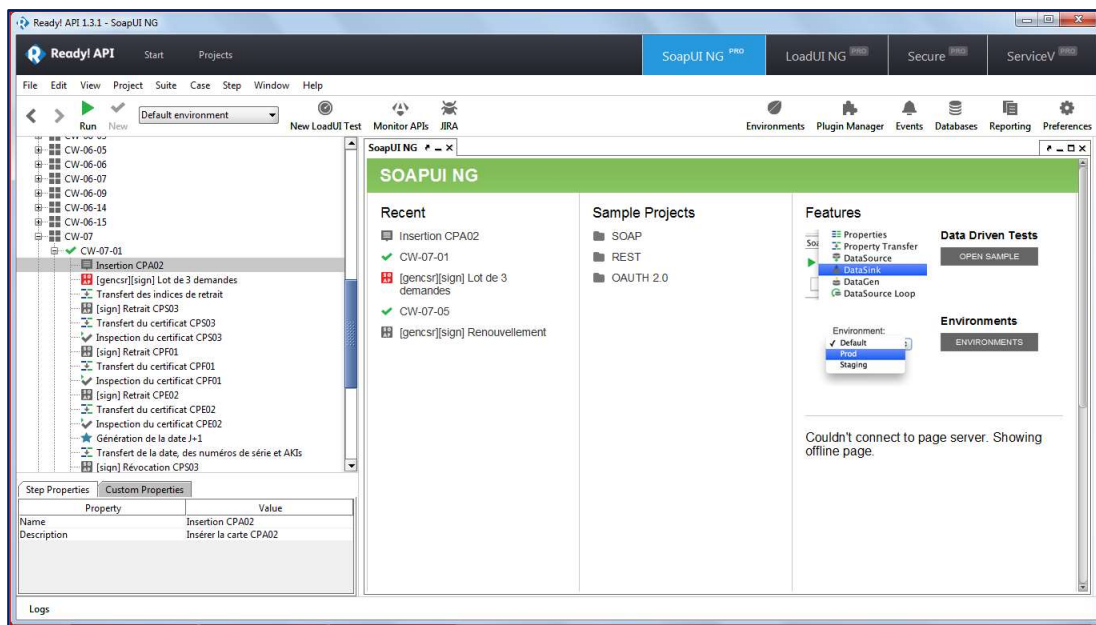


Figure 1 : Présentation Soap UI

Le fichier XML correspondant à la demande est généré :



Figure 2 : Présentation Soap UI - XML généré



On récupère ensuite le fichier XML de réponse :



Figure 3 : Présentation Soap UI - Réponse de la demande

L'ensemble du processus permet ainsi de tester les web services.

A noter que chaque demande au Webservice doit contenir une **signature** générée à partir de la carte utilisée. Cette signature permet de connaître l'identité du demandeur : le demandeur est le signataire de la demande.

Cette signature est générée automatiquement par l'outil Soap UI :

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header><SOAP-SEC:Signature SOAP-ENV:actox="some-URI" SOAP-ENV:mustUnderstand="1"
xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315#WithComments" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xm1enc-morereferenc-sha256" />
<ds:Reference URI="#Body"><ds:Transform><ds:Transform Algorithm="
http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
</ds:Transform><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xm1enc-sha256" />
<ds:DigestValue>JCC1BC88jInBJ9M47btiXukyzf8yJGV8rKnBUD9H6U=</ds:DigestValue></ds:Reference>
</ds:SignedInfo><ds:SignatureValue>DeTC2fjUbrU0ggK+9a7R31K8315Exj2PYf+C5Na8OrSYfB/qbe0FR6y/L8OVV13gayB4B9YhpcV
N0tCEB05H0+knaVauVfZeTk71192dL91EMr+XBG1mGcBU1bUAIms7mbint8/aVPL4+ENtQaNs7a
JJa3TPxvX1cWkTeY+htC63FdcoU8coVja9mc6Xno2mjnJCjmetOtWeGK13RFtSyRqReuceWdCV
mGHyPpuKLA1D6eazf8e+H36L4+9T2URkS4xIhCegDE9FXgYOHJekOh+TBNJo51qqCVARqWGHTRU
1UPQ9b/oy3MwujG6SHdi9MB5hmSday3M/451JA==
</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509SubjectName>
CN=00B9804408 + OID.2.5.4.4=MANIPCH0440 + OID.2.5.4.42=PATRICK,
OU=Manipulateur ERM, O=TEST, C=FR</ds:X509SubjectName><ds:X509Certificate>
MIIFoCCBgUgAwIBAgIDWgQMAOCQsGSIb3DQEBBQUMFEwCzAJBgNVBAYTAkESMQ0wCwYDVQQK
EwURVRVRBdRwCQYDVQQLZXJURVRVUIFBS0ZFU1NJT050RDmaFjAUBgNVBAUFDVRFU1QyQ0c0BU1NF
LTVZvhoBtUvM47AxdEAMdAdXh0f8MjAm4IjI5MjE1OTU5MjBm4QvCQYDVQGEWJGUjENBGA1UE
CMBEVTYVVKX2B0cGAIUEc0QWwuaXB1bGF0ZXVvIEVSTTE3MDEGA1UEAAdG90EB0CGy9uHQ0GAS
BgNVBAUC01BThk1Q09yWHDQMA4GA1UEKjQREUEFUUK1DSzCCASIVDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALFKM41XV31vrCgW+kjCjrEtp/1TK/WCVz8ua/czv5YGok9DTAPF4130uJ3M010
z6/0VgvrLc6BQm7Lj4+QmBnaAddcXCk+on2gFALNaSia7ly9KhfQ40M/REYTWaGkAku4+/Tg0p
EEcb6t/f4nD11kYtCJAdcc07higl1nuPgaBBOBjD3Gah/nV1IE9Vvftva0VgtoRY8Rt3TgI0u
A0xCe8fuv1KLc6115jcaJRE0DA2ugAE8QD+UydhAyFD1D8ErbdfVuE1GDc8VC6U/g2rkjgP8ab6
G0w3yPaRp95CjVmo00f8GR8e f21oPyaUk362WQZyah2cXmuUCAwEAACAmhggJNBBGALUd
IwQYBAAFYVU00013+IbC3kqaQgrFBSS9LqB0CA1U4dQqMBST1B57yMgJidTG5jdRCQy+pn5
RTACBqV7RQ8BAf8EAMCBAwAvrIVR01BAncCgYIKoZIh80QBAQwQwKvIVR0QEBQvIoAPMjAxNTAx
MDEwMDEAMDFagQ8yMDEwMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAM
VR0TBAIwADCBvqYVVR0fB1G2MIgMdugCaA3hjVodSHR018vVWsu0fVpmUuE21vLh8wcy5eci9j
cmvvdCVzdc9URVUIEBAQVVR0fB1G2MIgMdugCaA3hjVodSHR018vVWsu0fVpmUuE21vLh8wcy5eci9j
ZnIVY249d0VadCBjbc2UtdMxvvdT10EXN0I8Byb2Z1c3Npb25uZWwba10EXN0LGM9ZnI/Y2Vy
dGlnaW9ndGVyZXZvY2F0aW9ubGlzdDtiak5hcnkwQVVR0uSHIwC09yga0SobGRhcDovL2Fu
bnVhaXJ1L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2
bnVhaXJ1L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2
ba10EXN0LGM9ZnI/ZGVadGVyZXZvY2F0aW9ubGlzdDtiak5hcnkwQVVR0uSHIwC09yga0SobGRhcDovL2Fu
bnVhaXJ1L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2L2l2
NDCCCGQ8egFRAQIDBBQFTFTvdJjUwMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAMDEAM
CCQ8egFRAQIDBBQAMdVYIKoF6AUCBAgcEAwIBVjANBgkqhkiG9w0BAQUFAAOCARAJtV44xK
D6n+IN/0NMI6j3c383CYahKwDy/n/ghbyMnqeh/5Yec0VJUCg3rXu4TCfAg3h9lp36ka46w
yCk+3iemTC+9ebQ3TmmFoSINv6lyT59Kc4xYcljuttKFRvgA2uj96EJZemKfetJX41/o+DdEzem
X44EP5UQ0vT+ckR1qi3K2NaVQryQ00AutRDBtkLFDwaXoiaxdnlsQ17Chmaehci+KcC+TavWbpL
u02K0n3Zed/4qIyVh48b5hETcp+LKA0Hy47a+Gu0wSQA7axT+KaInbckTbY1E80kNnyePaC3FX0p
79M57IwGede300SpRVYF5yn+18In2rwm=</ds:X509Certificate></ds:X509Data>
</ds:KeyInfo></ds:Signature></SOAP-SEC:Signature></SOAP-ENV:Header>
<SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
<vs:requeteRenouvellementCertificat xmlns:vs="http://www.nfcou.in.com/NS/">
<AKI>c049a9149982cedd16148490c63bcb1fd8791fd</AKI>
<numeroSerie>49aa3433d672424ef6265d6b2f873ff8</numeroSerie>
<mailDemandeur>cps11@yopmail.com</mailDemandeur>
<mailPersonneAInformer>pics11@yopmail.com</mailPersonneAInformer>
<CSP>-----BEGIN CERTIFICATE REQUEST-----
MIICQCCASCAQwADCCASIVDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAlI0
VR3pQjXJCNDe+2VQ/z812/7yFmXQQ0tsQ00avx4CCD3o7FwVf88yppTiqVUQ858
tu98+86eFC1/tK0xokDE2aov1a+GcN2Prr7V4mCQ9Gh6DCml1vRFM13C2vns

```

→ Signature du fichier XML

Figure 4 : Présentation Soap UI - Exemple de signature

## 4 Glossaire

Abréviation	Signification
ANS	Agence du numérique en santé
CDA	Carte de Directeur de structure Autorisée
CDE	Carte de Directeur d'Établissement
CL	Certificat Logiciel
CN	Common Name
CPA	Carte de Personnel Autorisé
CPE	Carte de Personnel d'Établissement
CPF	Carte de Professionnel de santé en Formation
CPS	Carte de Professionnel de Santé
CPx	Famille de cartes à puce émises par l'ANS comprenant CDA, CDE, CPA, CPE, CPF et CPS
CRL	Liste des certificats révoqués
CSR	Certificate Signing Request (requête de signature de certificat)
FQDN	Fully Qualified Domain Name
IGC	Infrastructure de Gestion de Clés, PKI en anglais ou Infrastructure à Clés Publiques i.e. ICP
LDAP	Lightweight Directory Access Protocol
ORG	Offre pour les produits rattachés à une structure
PA	Personnel Autorisé
PC	Politique de certification
PE	Personnel d'établissement
PFCNG	Plateforme de fourniture de certificats de nouvelle génération
PFCNG-MG	Module de gestion de la plateforme de fourniture de certificats nouvelle génération

Abréviation	Signification
PFCNG-IGC	Module IGC de la plateforme de fourniture de certificats nouvelle génération
PIN	Personal Identification Number (numéro personnel d'identification)
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure (IGC)
PRO	Offre pour les produits de portée « structure » liés à une personne physique
PS	Offre pour les produits de portée « personnel » liés à une personne physique
SERV	Offre pour les produits rattachés à un serveur pour une structure
SI	Système d'Information
SSL	Secure Sockets Layer
URL	Uniform Resource Locator

Tableau 3 : Glossaire

## 5 Avertissements

### **Sur le nécessaire strict respect des procédures décrites dans le présent document**

L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent document.

Toutes les procédures qui y sont décrites ont été préalablement testées par l'ANS. Le non-respect de ces procédures est susceptible d'engendrer des dysfonctionnements dans l'environnement de travail de l'utilisateur.

En cas de dysfonctionnement, quel qu'il soit, l'ANS prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent document.

### **Sur les liens externes**

Le présent document contient des liens vers des sites Internet.

Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ANS et l'ANS n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ANS quant à leur contenu.

L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.

### **Sur les copies d'écran et les lignes de commande**

Les lignes de commandes données ci-après le sont à titre indicatif. Elles documentent des cas « passants » qui peuvent différer d'un système à l'autre.

Les copies d'écran présentées dans ce document sont données à titre illustratif.

Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.

### **Citations**

L'ANS est contrainte de citer le nom de certaines entreprises recensées au « Tableau 2 : Entreprises citées » afin d'apporter toute l'aide nécessaire aux utilisateurs.

Les entreprises citées peuvent prendre contact avec l'ANS à l'adresse email

[monserviclient.certificats@asipsante.fr](mailto:monserviclient.certificats@asipsante.fr) pour toute demande en lien avec la citation les concernant.

Les entreprises non citées dans ce document et ayant une activité en lien avec ce document peuvent également se faire connaître auprès de l'ANS en la contactant à la même adresse.

### **Contact**

Toute question en rapport avec le contenu du présent document doit être adressée à l'adresse suivante : [monserviclient.certificats@asipsante.fr](mailto:monserviclient.certificats@asipsante.fr)

Tableau 4 : Avertissements

## 6 Démarrage

### 6.1 Pré requis

Avant de pouvoir utiliser l'interface de gestion des certificats, les prérequis suivants sont à vérifier :

- **La carte CPx :**

**Pour pouvoir utiliser l'interface, l'utilisateur doit posséder une carte CPx.**

La carte CPx est une carte d'identité professionnelle électronique. Elle contient les données d'identification de son porteur (identité, profession, spécialité) mais aussi ses situations d'exercice (Cabinet ou établissement). Cette carte permet à son titulaire d'attester de son identité et de ses qualifications professionnelles. Elle est protégée par un code confidentiel propre à son porteur.

Il existe différents types de cartes suivant la profession exercée et le niveau de responsabilité du porteur :

- carte CPS : Carte de Professionnel de Santé
- Carte CPE : Carte de Personnel d'Etablissement
- Carte CPA : Carte de Personnel Autorisé
- Carte CDA : Carte de Directeur de structure Autorisé
- Carte CDE : Carte de Directeur d'Etablissement
- Carte CPF : Carte de Professionnel en Formation.

- **Cryptolib CPS**

Afin de pouvoir lire les droits figurant sur la carte du porteur, une Cryptolib CPS est requise sur le poste utilisateur.

Le lecteur de carte apparait généralement en bas à droite sur la barre de tâche du poste utilisateur :



: Pas de carte porteur dans le lecteur



: Carte porteur insérée dans le lecteur

**Vérifier la version de votre Cryptolib CPS :**

**Version minimale supportée :**

- **5.0.13 (Version Windows)**
- **5.0.8 (Version Mac OS X)**

**Les versions recommandées sont accessibles sur les URLS suivantes :**

- <http://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-windows>  
**(Version Windows)**
- <https://esante.gouv.fr/services/espace-cps/telechargements-libres/cryptolib-cps-mac-os-x>  
**(Version MAC)**

Pour cela, effectuer un clic droit sur la CryptoLibs un pop-up s'affiche :

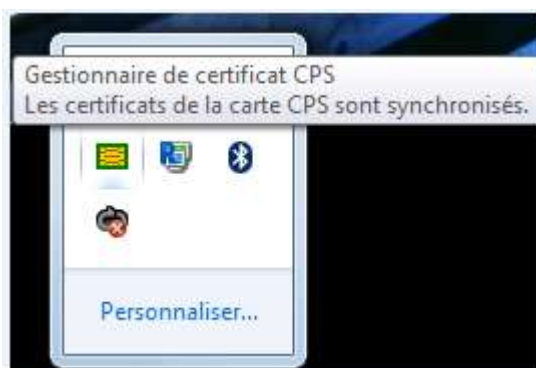


Figure 5 - Barre des tâches, lancement de la console CCM

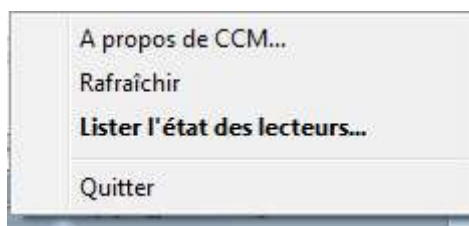


Figure 6 - Menu de la console CCM

A partir de là, pour lire la version de la Cryptolib CPS installée sur le poste, sélectionner « A propos de CCM » un pop-up récapitulant la version de la Cryptolib CPS s'affiche :

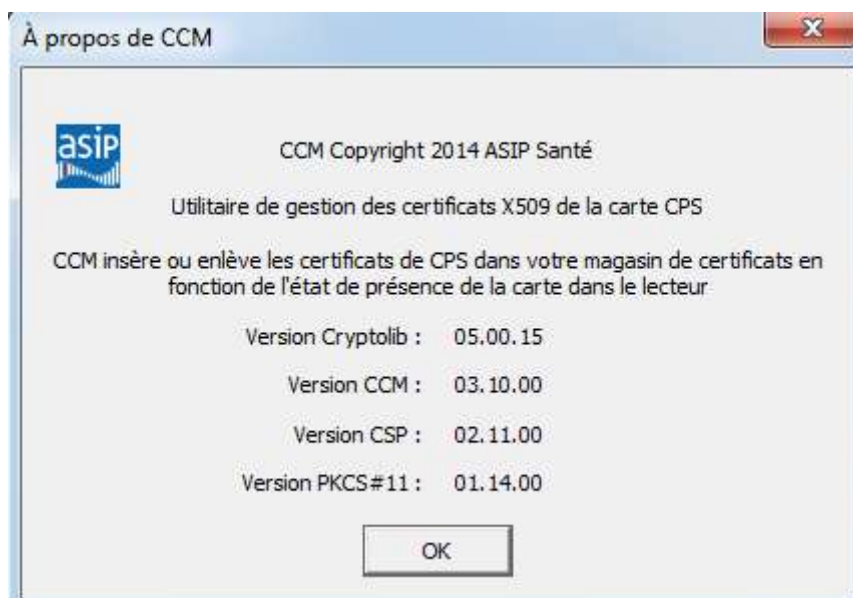


Figure 7 - Fenêtre "A Propos CCM"

## 6.2 Installation de la carte

L'accès à l'ensemble des modules de l'application n'est possible qu'à l'aide d'une carte CPx. Voici les étapes à dérouler pour vérifier l'installation des prérequis nécessaires pour l'utilisation de la carte.

- **Installation correcte de la carte**

Cette partie est principalement destinée aux nouveaux utilisateurs.



Figure 8 : carte CPx à installer

- **Vérification de la synchronisation des certificats et visualisation des données**

Le gestionnaire de certificats CPS permet la lecture et la synchronisation des données de la carte. Pour vérifier que la synchronisation est bien effective, il faut ouvrir le gestionnaire de certificats CPS.

Le gestionnaire de certificats CPS peut se trouver sur la barre des tâches.

La mention « **Les certificats de la carte CPx sont synchronisés** » doit apparaître.



Figure 9 : Gestionnaire de certificat CPS

Si ce message n'apparaît pas, ouvrir le gestionnaire et cliquer sur « **Activer la surveillance des lecteurs** » :



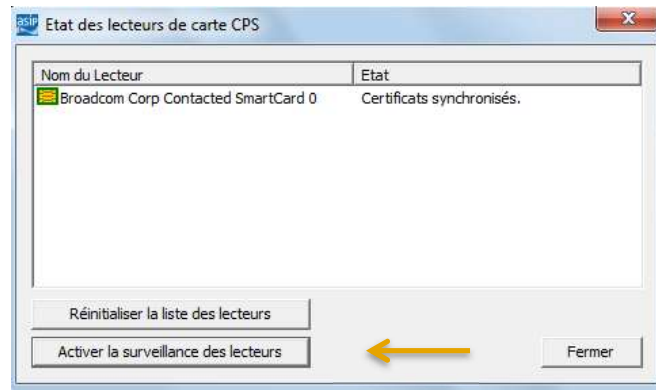


Figure 10 : Gestionnaire de certificat CPS - Etat des lecteurs

## 7 Les produits délivrés par la plateforme IGC-Santé

### 7.1 Présentation des produits

Les certificats émis par l'IGC-Santé sont regroupés autour de quatre offres appelées : PS, PRO, ORG et SERV :

- Offre **PS** : certificats logiciels garantissant l'identité d'un professionnel de santé sous sa propre responsabilité (appelés PS)
- Offre **PRO** certificats logiciels liés à une personne physique garantissant l'identité d'une personne physique (PS, PF, PE ou PA) sous la responsabilité d'une Structure
- Offre **ORG** : certificats logiciels rattachés à une Structure et garantissant l'identité d'une application associée à la Structure
- Offre **SERV** : certificats logiciels rattachés à un serveur pour une Structure et garantissant l'identité d'un serveur associés à la Structure.

Certificats logiciel de l'IGC-Santé	Usage cryptographique	Offre
<b>ORG_AUTH_CLI</b>	Il permet aux applications associées à une structure de s'authentifier vis-à-vis d'un tiers, un serveur ou une application	<b>ORG</b>
<b>ORG_SIGN</b> (cachet)	Il permet la signature électronique d'objets (de documents, courriers électroniques..) par une application sous la responsabilité d'une structure	<b>ORG</b>
<b>ORG_CONF</b>	Il permet à un utilisateur de chiffrer des données à destination de cette structure, qui est la seule à pouvoir déchiffrer les données qui lui sont destinées	<b>ORG</b>
<b>SERV_SSL_SERV</b>	Il permet à un serveur web appartenant à une structure de s'authentifier vis-à-vis d'un tiers, un module client ou une personne physique, voire en tant que client à un autre serveur distant	<b>SERV</b>
<b>SERV_SIGN</b> (cachet)	Il permet la signature électronique d'objets par un serveur associé à une structure	<b>SERV</b>
<b>SERV_S/MIME</b>	Il permet à un serveur de signer des objets et de déchiffrer les données qui lui sont destinées, sous la responsabilité de la structure concernée	<b>SERV</b>
<b>SERV_CONF</b>	Il permet à un utilisateur de chiffrer des données à destination d'un serveur (sous la responsabilité de la structure concernée) qui est le seul à pouvoir déchiffrer les données qui lui sont destinées	<b>SERV</b>
<b>PS_AUTH</b>	Il permet à un professionnel de santé de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).	<b>PS</b>
<b>PS_SIGN</b>	Il permet à un professionnel de santé de signer des objets (documents électroniques,..)	<b>PS</b>
<b>PS_CONF</b>	Il permet à un utilisateur de chiffrer des données à destination du professionnel de santé porteur de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées.	<b>PS</b>
<b>PRO_AUTH</b>	Il permet à un professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de s'authentifier vis-à-vis d'un tiers (serveur, application ou autre personne physique).	<b>PRO</b>

Certificats logiciel de l'IGC-Santé	Usage cryptographique	Certificats logiciel de l'IGC-Santé
<b>PRO_SIGN</b>	Il permet à professionnel de santé (PS), à un personnel d'établissement (PE) ou à un personnel autorisé (PA) dans le cadre d'une structure identifiée, de signer des objets (documents électroniques,...).	<b>PRO</b>
<b>PRO_CONF</b>	Il permet à un utilisateur de chiffrer des données à destination du porteur de ce certificat de confidentialité, qui est le seul à pouvoir déchiffrer les données qui lui sont destinées.	<b>PRO</b>

## 7.2 Cas particulier de l'adresse email protégée

Pour certains certificats logiciels (PRO\_CONF, PRO\_SIGN, PS\_CONF, PS\_SIGN, SERV\_CONF, SERV\_SIGN, SERV\_S/MIME, il est nécessaire de renseigner lors de la demande une adresse de messagerie. Cette adresse de messagerie est inscrite dans le certificat et appelée « adresse email protégée ».

Des contrôles spécifiques sont effectués lors de la demande de certificat logiciel afin de s'assurer qu'une adresse email protégée n'est utilisée que par un et un seul porteur de certificats en cours de validité. Ce contrôle est effectué sur l'ensemble des certificats émis au titre de toutes les offres (PS, PRO et SERV).

## 8 Habilitations

Chaque utilisateur (personne disposant d'une carte CPx) possède des habilitations qui lui sont propres. Ces habilitations déterminent les droits applicatifs de l'utilisateur sur l'interface de gestion des certificats.

Les habilitations sont nécessaires pour pouvoir utiliser l'application.

Chaque utilisateur est identifié par des informations présentes dans la carte CPx qu'il utilise pour s'authentifier vis-à-vis de la PPFNG. Toute personne qui dispose d'une carte CPx possède des habilitations pour utiliser des services de la plateforme IGC-Santé.

On distingue deux types d'habilitations :

- **Les habilitations directement déduites** du type de personne (*habilitations implicites*)

Il existe différents types de personne :

- PS : Professionnel de santé
- PF : Professionnel en formation
- PA : Personnels autorisés
- PE : Personnels d'établissement de santé.

- **Les habilitations nominatives** : elles sont liées à une demande explicite (*habilitations explicites*).

**Pour pouvoir accéder aux services de l'application pour les offres PRO, SERV et ORG, il est indispensable qu'une demande d'habilitation de l'acteur ait été faite au préalable. La procédure pour l'habilitation d'un acteur est décrite dans l'Espace CPS du portail de l'ANS (<http://esante.gouv.fr>).**

Les habilitations permettent de définir des rôles sur l'application en fonction du périmètre et du type d'offre :

Rôle	Type d'Offre	Périmètre	Habilitation
<b>Administrateur technique</b>	ORG	Structures référencées lors de la demande d'habilitation de l'administrateur technique	Explicite
<b>Administrateur technique</b>	SERV	Structures et Domaine référencés lors de la demande d'habilitation de l'administrateur technique	Explicite
<b>Administrateur technique</b>	PRO	Structures et Domaine référencés lors de la demande d'habilitation de l'administrateur technique	Explicite
<b>Porteur CL</b>	PS		Implicite
<b>Porteur CL</b>	PRO		
<b>Porteur CL</b>	PRO	Structure de rattachement	Implicite
<b>Demandeur (PS ou PF) à titre personnel</b>	PS		Implicite

Tableau 5 : Habilitations Rôle/Périmètre

Les rôles déterminent les actions possibles sur l'interface :

	Demander	Renouveler	Retirer	Annuler	Révoquer	Suivre
<b>Porteur CL</b>					√	√
<b>Demandeur PS à titre personnel</b>	√	√	√	√	√	√
<b>Demandeur PF à titre personnel</b>	√	√	√	√	√	√
<b>Administrateur technique</b>	√	√	√	√	√	√

Tableau 6 : Actions autorisées en fonction du rôle

Les types d'offre déterminent les usages possibles :

Nom	PS	PRO	ORG	SERV
<b>AUTH</b>	√	√		
<b>AUTH_CLI</b>			√	
<b>SIGN</b>	√	√	√	√
<b>S/MIME</b>				√
<b>SSL_SERV</b>				√
<b>CONF</b>	√	√	√	√

Tableau 7 : Type d'offre / Usage

### **Périmètre des habilitations explicites**

Chaque habilitation explicite contient une référence à une Structure. Plusieurs habilitations explicites peuvent être déclarées pour un même utilisateur : un utilisateur peut donc être habilité pour un ensemble de Structures.

Une habilitation explicite pour l'offre **PRO** référence une Structure et contient des précisions sur les domaines utilisables lors d'une demande de certificat :

- L'habilitation autorise uniquement la commande de certificat pour le nom de domaine précisé dans l'habilitation (l'habilitation déclarée débute par les caractères « \*@ »).
- L'habilitation permet la commande de certificat pour le nom de domaine précisé dans l'habilitation, ainsi que pour tout sous domaine du domaine précisé dans l'habilitation (l'habilitation déclarée débute par le caractère « \* »).
- L'habilitation autorise uniquement la commande de certificat pour un sous-domaine du nom de domaine précisé dans l'habilitation (l'habilitation déclarée débute par le caractère « \*. »).

Une habilitation explicite pour l'offre **ORG** référence une Structure.

Une habilitation explicite pour l'offre **SERV** référence une Structure et contient des précisions sur les domaines ou noms de serveur utilisables lors d'une demande de certificat. De plus cette habilitation explicite donne également accès à l'offre **ORG** pour la Structure concernée par l'habilitation.

Pour l'offre **SERV** et l'usage **SSL serveur**, une habilitation explicite contient les précisions suivantes :

- L'habilitation autorise uniquement la commande de certificat pour le FQDN précisé dans l'habilitation (l'habilitation déclarée ne débute pas par le caractère « \* »).
- L'habilitation autorise uniquement la commande de certificat pour un FQDN constitué d'un nom de serveur suivi du nom de domaine précisé dans l'habilitation (l'habilitation déclarée débute par le caractère « \* »).

Pour l'offre SERV hors usage SSL serveur, une habilitation explicite contient les précisions suivantes :

- L'habilitation autorise uniquement la commande de certificat pour le nom de domaine précisé dans l'habilitation (l'habilitation déclarée ne débute pas par le caractère « \* »).
- L'habilitation permet la commande de certificat pour tout sous domaine du domaine précisé dans l'habilitation (l'habilitation déclarée débute par le caractère « \* »).

## **Les habilitations sont portées par le signataire des différentes demandes**

## 9 Configurations

### 9.1 Fichier XSD

Ce fichier permet de dire quelles sont les balises autorisées, ou et combien de fois elles peuvent apparaître et ce qu'elles contiennent (nombres, caractères, expression régulières...).

On utilise ce type de fichier pour vérifier qu'un xml est bien conforme à la structure préalablement fixée.

*(Voir Fichier XSD en Annexe 1)*

#### Exemple d'un fichier de paramétrage XSD

Pour chaque élément décrit dans le fichier, on retrouve le champ « name » qui correspond à la balise qui sera utilisée dans le fichier XML :

```
<xsd:element maxOccurs="1" minOccurs="1" name="usage" ←
    type="tns:usageEnum">
    <xsd:annotation>
        <xsd:documentation>
```

Usage de l'offre du produit demandé.  
 o L'offre PS comprend les usages Authentification (AUTH), Signature (SIGN), S/MIME (CONF)  
 o L'offre PRO comprend les usages Authentification (AUTH), Signature (SIGN), S/MIME (CONF)  
 o L'offre ORG comprend les usages Authentification Client (AUTH\_CLI), Signature Cachet (SIGN), Chiffrement (CONF)  
 o L'offre SERV comprend les usages Authentification Serveur (SSL\_SERV), Signature cachet (SIGN), Signature + Chiffrement (S/MIME), Chiffrement (CONF)

```
        </xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:element name="idNatStruct" maxOccurs="1"
minOccurs="0"
    type="tns:nationalId">
    <xsd:annotation>
        <xsd:documentation>
```

Identifiant National de Structure pour les demandes d'offre PRO, ORG et SERV

```
        </xsd:documentation>
    </xsd:annotation>
```

```

</xsd:element>

<xsd:element name="idNatBeneficiaire" maxOccurs="1"
  minOccurs="0" type="tns:nationalId">
  <xsd:annotation>
    <xsd:documentation>

```

Identifiant National du Bénéficiaire  
pour les demandes d'offre PRO

```

    </xsd:documentation>
  </xsd:annotation>
</xsd:element>

<xsd:element name="idNatTiers" maxOccurs="1"
  minOccurs="0"
  type="tns:nationalId">
  <xsd:annotation>
    <xsd:documentation>

```

Identifiant National du Tiers pour le cas  
ou le  
demandeur qui a signé la demande est AdminASIP et  
agit pour un tiers

```

    </xsd:documentation>
  </xsd:annotation>
</xsd:element>

```

Les champs « maxOccurs » et « minOccurs » :

- Si minOccurs égal à 1 ou >, l'élément est obligatoire. (Exemple : typeDemande)
- Si minOccurs égal 0, l'élément est facultatif. (Exemple : idNatTiers)

```

<xsd:element name="typeDemande" type="tns:requestTypeEnum"
  minOccurs="1" maxOccurs="1">
  <xsd:annotation>
    <xsd:documentation>
      Indique si
      il s'agit d'une requête de suivi : des
      demandes de
      certificats, des demandes de
      révocation ou des produits
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>

<xsd:element name="idNatTiers" maxOccurs="1" minOccurs="0"
  type="tns:nationalId">
  <xsd:annotation>
    <xsd:documentation>
      Identifiant National du Tiers pour le

```



cas ou le

AdminASIP et                   demandeur qui a signé la demande est  
  agit pour un tiers

```
                                          </xsd:documentation>
                                          </xsd:annotation>
                                          </xsd:element>
```

## 9.2 Fichier WSDL

WSDL signifie *Web Service Description Language* et doit être fourni par le fournisseur du Service Web.

Le fichier WSDL est en langage XML, il permet de décrire l'utilisation complète du service. Il permettra à de nombreux programmes ou langages de programmation de découvrir automatiquement un service et de gérer les modalités d'échanges SOAP (définition abstraite des services, port d'échange, protocole d'échange, encodage, ainsi que (URL) du service).

Urls d'accès Wsdl :

<https://pfc-auth.eservices.esante.gouv.fr/ws-srv/?wsdl>

<https://pfc-auth.eservices.esante.gouv.fr/ws-apt/?wsdl>

*(Voir Fichier WSDL en Annexe 1)*

**Partie extraite du fichier de paramétrage WSDL :**

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions name="WS" targetNamespace="http://www.pfcng.in.com/WS/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:tns="http://www.pfcng.in.com/WS/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  <wsdl:documentation>
    Service: WS
    Version: 1.0
    Owner: Imprimerie Nationale
  </wsdl:documentation>
  <wsdl:types>
    <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://www.pfcng.in.com/WS/xsd">
      <xsd:import namespace="http://www.pfcng.in.com/WS/"
        schemaLocation="pfcng-ws.xsd" />
    </xsd:schema>
  </wsdl:types>

  <wsdl:message name="requeteDemandeCertificats">
```

```

        <wsdl:documentation>Requete de demande de
certificats</wsdl:documentation>
        <wsdl:part name="parameters"
element="tns:requeteDemandeCertificats"></wsdl:part>
    </wsdl:message>

    <wsdl:message name="reponseDemandeCertificats">
        <wsdl:documentation>Reponse a la requete de demande de
certificats
        </wsdl:documentation>
        <wsdl:part name="parameters"
element="tns:reponseDemandeCertificats"></wsdl:part>
    </wsdl:message>

    <wsdl:portType name="WS">
        <wsdl:operation name="demanderCertificats">
            <wsdl:documentation>Interface de demande de certificats
            </wsdl:documentation>
            <wsdl:input
message="tns:requeteDemandeCertificats"></wsdl:input>
            <wsdl:output
message="tns:reponseDemandeCertificats"></wsdl:output>
        </wsdl:operation>
    </wsdl:portType>

    <wsdl:binding name="WSSOAP" type="tns:WS">
        <soap:binding style="document"
            transport="http://schemas.xmlsoap.org/soap/http" />

        <wsdl:operation name="demanderCertificats">
            <wsdl:documentation>Interface de demande de certificats
            </wsdl:documentation>
            <soap:operation soapAction="demanderCertificats" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
        </wsdl:operation>
    </wsdl:binding>

```

```
<wsdl:service name="WS">  
  <wsdl:port name="WSSOAP" binding="tns:WSSOAP">  
    <soap:address location="www.pfcng.in.com" />  
  </wsdl:port>  
</wsdl:service>  
</wsdl:definitions>
```

## 10Authentification

Il existe 2 mécanismes d'authentification :

1. URL permettant de retirer des certificats serveurs

<https://pfc.eservices.esante.gouv.fr/cxf/ws-srv>

L'accès au Web Service est sécurisé par une authentification mutuelle serveur/serveur.

Le certificat serveur SSL de la plateforme IGC-Santé est fourni par l'ASIP.

Le certificat serveur SSL de l'application serveur est fourni par l'ASIP. Le DN du certificat autorisé est chargé dans une liste blanche vérifiée par la plateforme IGC-Santé après vérification de la validité du certificat.

Seuls les certificats SSL serveurs issus des ACIs suivantes sont acceptés :

- AC IGC-SANTE ELEMENTAIRE ORGANISATIONS
- TEST AC IGC-SANTE ELEMENTAIRE ORGANISATIONS

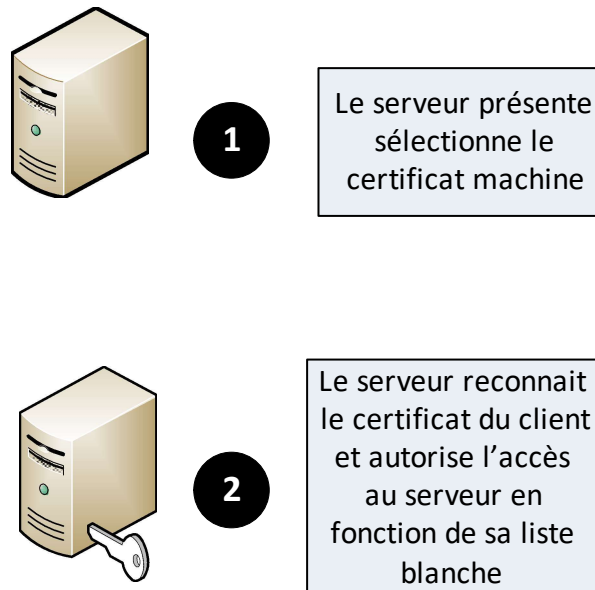


Figure 11 - Schéma authentification serveur

2. URL permettant de retirer des certificats clients

<https://pfc.eservices.esante.gouv.fr/ws-apt>

L'accès au Web Service est sécurisé par une authentification mutuelle client/serveur par carte CPx.

Seuls les porteurs de carte CPx avec un certificat d'authentification issu des ACIs suivantes sont acceptés :

- AC IGC-SANTE ELEMENTAIRE PERSONNES
- AC IGC-SANTE STANDARD PERSONNES
- AC IGC-SANTE FORT PERSONNES
- TEST AC IGC-SANTE ELEMENTAIRE PERSONNES
- TEST AC IGC-SANTE STANDARD PERSONNES
- TEST AC IGC-SANTE FORT PERSONNES

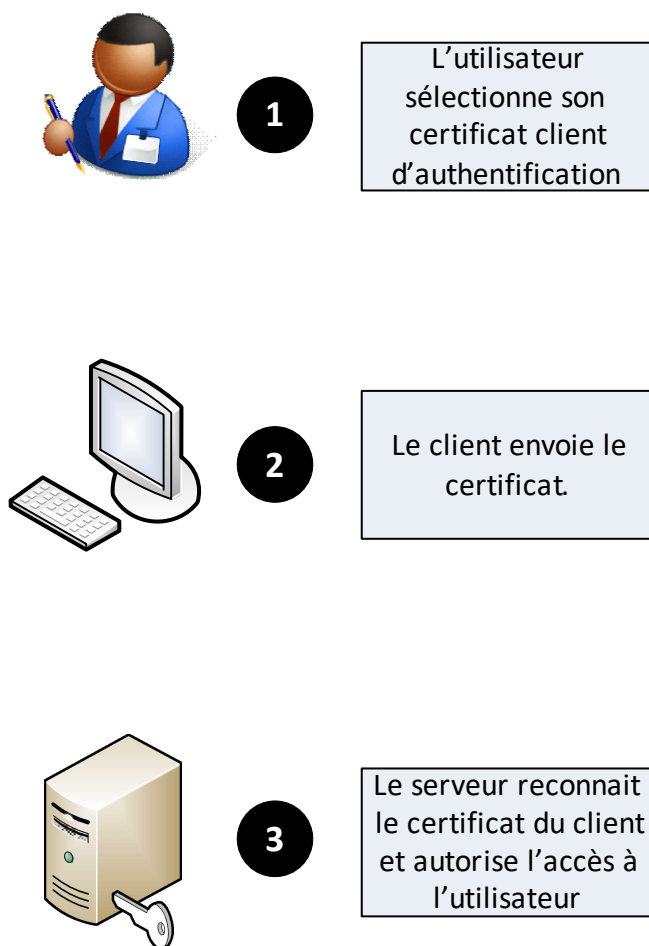


Figure 12 - Schéma d'authentification client

# 11 Signature

Quelle que soit l'opération invoquée via le canal Web-Service, tous les messages doivent être signés par l'acteur ayant les habilitations nécessaires. *(Voir exemple de signature en Annexe 1)*

## Certificats de signature :

Seuls les porteurs de carte CPx avec un certificat de signature issu des ACIs suivantes sont acceptés :

- AC IGC-SANTE ELEMENTAIRE PERSONNES
- AC IGC-SANTE STANDARD PERSONNES
- AC IGC-SANTE FORT PERSONNES
- TEST AC IGC-SANTE ELEMENTAIRE PERSONNES
- TEST AC IGC-SANTE STANDARD PERSONNES
- TEST AC IGC-SANTE FORT PERSONNES

## Format :

Comme le démontre les exemples qui accompagne ce guide, la signature est insérée dans la requête Web Service selon le standard **SOAP DSIG** basé sur **XML DSIG**.

## Exemple d'une signature type :

```

<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
    <ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference URI="#Body">
      <ds:Transforms>
        <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </ds:Transforms>
      <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
    <ds:DigestValue>iMbIV+80L8Uv6F6PFtqsaGazyiPa7jNVr+G+wZ8MF5g=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>

  <ds:SignatureValue>rpW5IJUAbE8TvA4IPh8EcGsEv6rSHVfr967iL4DEf2Cw0fsUKdswP+BF/IG/
LqdwWsDrUo951FK
nLftXDsaq+vbLG+IgOZ1nimbkzp1Jd7F0Rx12vzlKz3rjsD8mi30f5EaZJKGsCkfxZEJJRFHkBtE
5QyiyGasndaUgBXABt0Rvb9BGJpr9b-fv12ozKNoFM407tBONVr7BxIs1gned2f5VZ+YcSFqFIj9f
Lr1RFwgn0BeB0Am93RwKhb/GsExz3oGDTvGIOj14P/qGGf/6/pVXTY87X+IpeHLC5Kr0LTzirT2g
wdlLu0z7tuLZMKMbQWQ6UXtNF1rPwiNcyqmjyQ==</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>

```

```
<ds:X509SubjectName>CN=500000000028969/CPAT0002 +
OID.2.5.4.4=AGENT0000028960002 + OID.2.5.4.42=DENISE, OU=300000000028969,
L=Paris (75), O=TEST, C=FR</ds:X509SubjectName>
```

```
<ds:X509Certificate>MIIFrzCCBJegAwIBAgIDW6iqMA0GCSqGSIb3DQEBBQUAME0xCzAJBgNVBAYT
TakZSMQ0wCwYDVQK
EwRURVNUMRcwFYDVQQLew5URVNUIFNuu1VDVFSRTEWMBQGA1UEAxMNVEVTVCBDEFTU0UtMzAe
Fw0xNTAxMDEwMDAwMDFAwF0yMDAyMjkyMTU5NTlaMIGYMQswCQYDVQQGEwJGUjENMAsGA1UEChME
VEVTVDEtMBEgA1UEBxQKUGFyaXMgKDC1KTEYMBYGA1UECzMpMzAwMDAwMDAwMDI4OTY5MUswHwYD
VQDExg1MDAwMDAwMDAwMjg5NjkwQ1BBVDAwMDIwGQYDVQQEFBJBR0VOVDAwMDAwMjg5NjAwMDIw
DQYDVQQqFAZERU5JU0UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZebJfWTCUkcVH
NNqCA47qTM3E1G1CSjM5XJTVqg5BzBcEZhgr0/nofpK72Nbiyzv+KHYADrGg1bQ7+YXvFLVb8u2
JlZ6JetfRZR2UF+yCfqJ6YpZpFroo0PaW9lC9Buo6jDNiWhJKcajqNbzWfATlMPkPq8eJ6WU15
YkApYvn47uCn9FtLD9/VmyuMJFhI0EJEJGgur6PY19ZTYXtLeuGuBq1SQ8c+Edf7GgBIOwWuVnK6d
Ru4IS84DW4E9LM30310+01g0W/VZj3UsjMHGKPKzBItPgYig0YrSbqIh7wWvRnm14Lmwx20y7Cf
Oi/gZ8ccgqlyUr/ZzFsRaZqDAGMBAAGjggJKMIIICrjAFBgNVHSMEGDAWgBRuchVnSRaJ5fDd0hHU
cB/sa1XbajAdBgnVH04EFgQU87bhpz5lKmwAAGWkt07rs1D7H18wDgYDVR0PAQH/BAQDAgBAMBGM
A1UdJQMMAAoGCCsGAQUFBWEMEMCsGA1UdEAQkMCKADzIwMTUwMTAxMDAwMDAxwoEPMjAyMDAxMzEy
MzU5NTlaMBkGA1UdIAQSMBAwDgYMKoF6AUCDBWkCAGIBMAkGA1UdEwQCMAAwgboGA1UdHwSBsjCB
rZA7oDmgN4Y1aHR0cDovL2FubnVhaXJlLmdpcC1jcHMuznIvY3JzL3Rlc3QvVEVTVCBDEFTU0Ut
My5jcmmwckBuoGyGamxkYXA6Ly9hbm51YWlyZS5naXAAtY3BzLmZyL2NuPXRlc3QgY2xhc3NlLTM5
b3U9dGVzdCBzdHJ1Y3R1cmUsbz10ZXN0LGM9ZnI/Y2VydGlmawNhdGVyZXZvY2F0aW9ubGlzdDti
aW5hcnkwdQYDVR0uBG4wbDBqoGigZoZkbGRhcDovL2FubnVhaXJlLmdpcC1jcHMuznIvY249dGVz
dCBjbGFzc2U0MyxvdT10ZXN0IHN0cnVjdHVyZSxvPXRlc3QsYz1mcj9kZw0YXJlLmd9jYXRpb25s
aXN0O2JpbmFyeTARBGlghkgBhvhCAQEEBAMCBSAwIwYIKoF6AUCBAGMEFxmVODAYNTAwMDAwMS8y
NTAwMzAzNTkyMA8GCCqBegFHAQIFBAMEAYAwDwYIKoF6AUCBAGIEAwIBAzANBggqhkkiG9w0BAQUF
AAOCAQEAMuUwRls0Z04ZxjGg7D02I4tBrKvW/vkaTsT6HvNvMvJImDMUPVy3BxJPmvHrpjx1qo+I
GgCYvxX03JD0v5NCP7C8oX5efLbCTpr2+pA3t2T764m02xCc0Au5yBcdamaHJkhB2AevujjgpJ2m
lbjjPW2S8YceRHDarSY46lCAi2tYf1VB3Cv4oJM0q0+tX5C20lKfIMjpPpIyPJSJbYX9TKnvhajG
/dhYZHwduKY67pGLb1oE3/B2567q0LH63Kr2WRF/3hC90RPFYoiWA3zzB1n753gKGeXWZvnI2KA5
azYwM23LURon+LceG2i6v0hdevrKVk0meV5xWTjYZYilgA==</ds:X509Certificate>
```

```
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
```

La signature électronique va faire appel à deux familles d’algorithmes, afin de pouvoir garantir l’authenticité et l’intégrité d’un titre porteur.

- L’algorithme utilisés et RSA,
- La fonction de hachages et SHA.

• **Contenu de la signature :**

Information	Valeur
Signature	La signature au format XMLDSIG
Certificat utilisé	Le certificat complet utilisé pour signer le message

**Tableau 8 : Contenu de la signature**

La signature électronique est formée de trois composantes :

- Le document porteur de la signature,
- La signature elle-même,
- Le certificat électronique authentifiant le signataire.



La signature électronique garantit :

- Authentification,
- Confidentialité,
- Intégrité des données,
- Non-répudiation.

Optionnellement la signature peut comprendre d'autres éléments.

L'exemple ci-dessous permet de visualiser la structure complète d'une signature dans l'enveloppe SOAP (Les éléments suffixés par ? et + sont optionnels).

```
<ds:Signature ID?>
  <!-- Elements XMLDSig -->
  <ds:SignedInfo>
    <ds:CanonicalizationMethod/>
    <ds:SignatureMethod/>
    (<ds:Reference URI? >
      (<ds:Transforms>) ?
      <ds:DigestMethod>
      <ds:DigestValue>
    </ds:Reference>)+
  </ds:SignedInfo>
  <ds:SignatureValue>
    (<ds:KeyInfo>) ?
  </ds:Signature>
```

Le composant de signature de l'outil client web service utilisé doit compléter les informations suivantes dans la capsule du message :

- Méthode de canonisation (ds : CanonicalizationMethod)
- Méthode de signature (ds : SignatureMethod) : rsa\_sha256
- La référence de signature (ds : Reference) : #Body  
=> calcul du hash du body dans la balise <SOAP-ENV:Body>
- Algorithme de transformation (ds : Transforms) : signature enveloppée
- Méthode de calcul du condensat (ds : DigestMethod) : sha256
- => Chiffrement de la signature du hash contenu dans la balise <ds:SignatureValue> à partir de la clé publique du certificat .
- Infos clé publique du client (ds : KeyInfo) :
  - X509Data
    - <X509SubjectName>
    - <X509Certificate>

Le composant de signature de l'outil client web service utilisé doit réaliser les vérifications suivantes :

- Vérification que le certificat contient l'usage de signature (keyusage=nonRepudiation)
- Validation du certificat et de sa chaîne de certification (période de validité et CRL). Les ACI acceptées sont les suivantes : CPS2Ter avec les Classe-1 (PS), Classe-2 (PE/PA directeur), Classe-3 (PE/PA).

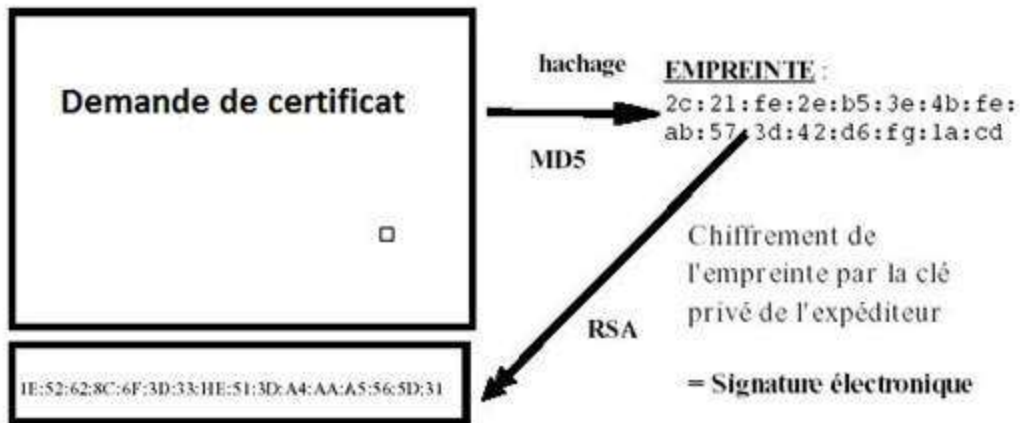


Figure 13 : Process Signature

## 12 Création d'une CSR

Ce paragraphe les étapes pour la création d'une CSR qui contient les informations strictement nécessaires pour un traitement par la plateforme IGC-Santé.

L'utilisation de l'outil OpenSSL en ligne de commandes est retenue et les copies d'écran présentées correspondent à une utilisation en environnement Windows.

La création de la CSR repose sur l'enchaînement de deux étapes

- Etape 1 : génération d'une nouvelle clé privée,
- Etape 2 : création de la CSR en utilisant la clé privée obtenue à l'étape 1.

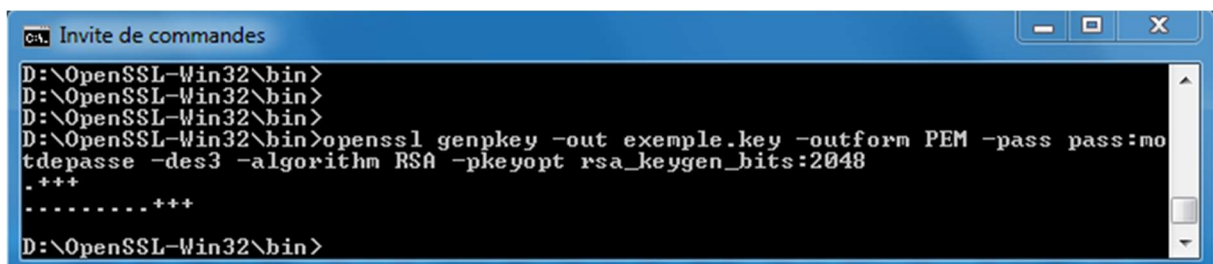
## 12.1 Etape 1 : génération de la clé privée

La commande est la suivante :

```
openssl genpkey -out exemple.key -outform PEM -pass pass:motdepasse -des3 -algorithm  
RSA -pkeyopt rsa_keygen_bits:2048
```

Génération de la clé privée	
%OPENSSL_HOME%\openssl.exe genpkey	<a href="https://www.openssl.org/docs/apps/genpkey.html">https://www.openssl.org/docs/apps/genpkey.html</a>
	Génération de clé rsa
-out "exemple.key"	Fichier de sortie
-outform PEM	Format du fichier de sortie
-pass "pass :motdepasse"	Mot le passe qui protège l'accès à la clé privée
-des3	Algorithme utilisé pour chiffrer le fichier qui contient la clé privée
-passout "pass :motdepasse"	Mot le passe qui protège l'accès à la clé privée
-algorithm RSA	Algorithme utilisé pour produire la clé
-pkeyopt rsa_keygen_bits:2048	Caractéristique de la clé : longueur de la clé 2048 bits

Tableau 9 : OpenSSL : Génération d'une clé privée



```

C:\OpenSSL-Win32\bin>
D:\OpenSSL-Win32\bin>
D:\OpenSSL-Win32\bin>
D:\OpenSSL-Win32\bin>openssl genpkey -out exemple.key -outform PEM -pass pass:motdepasse -des3 -algorithm RSA -pkeyopt rsa_keygen_bits:2048
.+++
.....+++
D:\OpenSSL-Win32\bin>

```

Figure 14 : Génération d'une clé privée

Le fichier *exemple.key* contient la nouvelle clé privée.

## 12.2 Etape 2 : création de la CSR

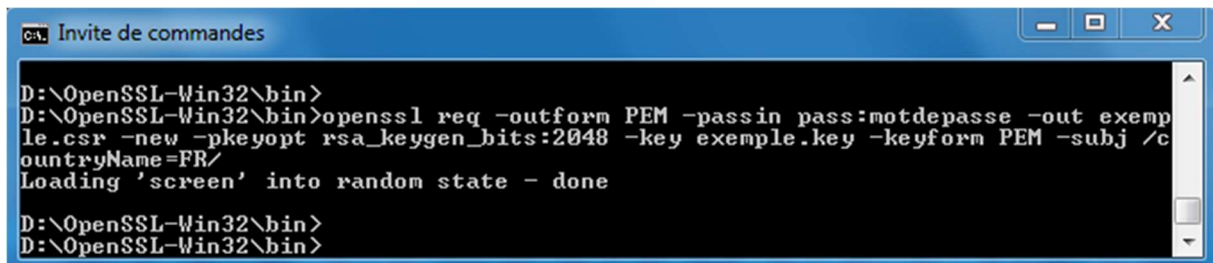
La commande est la suivante :

```
openssl req -outform PEM -passin pass:motdepasse -out exemple.csr -new -pkeyopt  
rsa_keygen_bits:2048 -key exemple.key -keyform PEM -subj /commonName=Demande/
```

Création de la CSR	
%OPENSSL_HOME%\openssl.exe req	<a href="https://www.openssl.org/docs/apps/req.html">https://www.openssl.org/docs/apps/req.html</a>
-outform "PEM"	Création de la CSR
-passin "pass:foo"	Format du fichier de sortie
-out "exemple.csr"	Mot de passe pour accéder à la clé privée
-new	Fichier de sortie
-pkeyopt rsa_keygen_bits:2048	Demande de création de la CSR
-key exemple.key	Algorithme utilisé pour produire la clé publique
-keyform PEM	Fichier qui contient la clé privée
-subj /countryName=FR/	Format de la clé privée
	Paramètre du DN (non utilisé pour la production du certificat mais il faut une information pour construire la CSR)

Tableau 10 : OpenSSL : Construction d'une CSR pour l'IGC-Santé

Le fichier *exemple.csr* contient la CSR.



```

C:\> Invite de commandes
D:\OpenSSL-Win32\bin>
D:\OpenSSL-Win32\bin>openssl req -outform PEM -passin pass:motdepasse -out exemple.csr -new -pkeyopt rsa_keygen_bits:2048 -key exemple.key -keyform PEM -subj /countryName=FR/
Loading 'screen' into random state - done
D:\OpenSSL-Win32\bin>
D:\OpenSSL-Win32\bin>
  
```

Figure 15 : Exemple de génération d'une CSR

La création de la CSR est terminée.

Les fichiers contenant la CSR et la clé privée sont présents dans le répertoire utilisé pour les lancer les commandes.

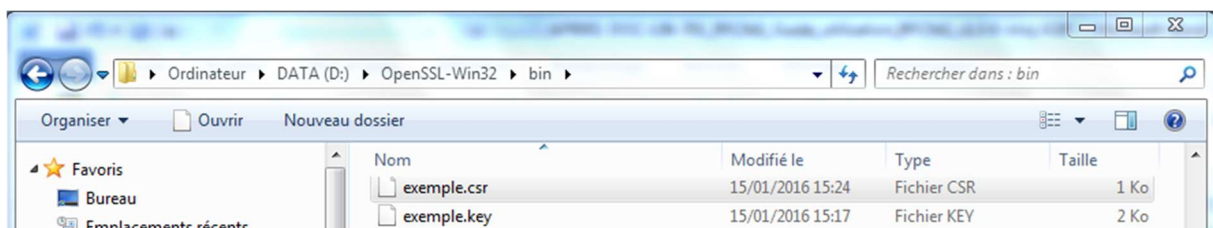


Figure 16 : OpenSSL - CSR et Clé générées

A titre d'illustration voici le contenu d'une CSR en page suivante

## Certificate Request:

## Data:

Version: 0 (0x0)

Subject: CN=demande

## Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

## Modulus:

```
00:b0:f5:7b:10:38:da:d9:ae:17:30:92:cc:67:e5:
72:b9:15:75:68:87:85:b4:c8:69:d6:74:9b:79:2d:
41:4c:60:15:39:8f:28:f5:35:9a:79:06:67:cd:0b:
f1:b4:d7:4d:33:58:11:de:af:38:e2:4f:ec:3f:74:
40:69:4a:38:78:69:3e:76:be:8d:2a:37:77:01:19:
51:45:5d:8b:6d:01:2d:3e:b8:cb:26:1f:f6:45:6c:
cb:22:e6:e1:22:e3:57:7c:cf:d2:fa:b1:6b:82:65:
27:da:b8:9c:de:4a:3e:e3:e1:98:44:3d:76:32:a5:
eb:ff:9f:44:db:4e:ad:11:c6:2f:c9:7c:4f:88:35:
a2:51:3b:77:58:f4:27:4e:99:bb:94:51:d5:75:04:
a5:b5:c5:17:85:9b:a5:4f:20:28:62:ae:aa:da:8d:
70:20:2b:2a:23:96:6c:43:f2:32:5d:ef:44:36:53:
95:a1:50:e1:0c:10:8f:39:3c:37:a5:a6:27:dc:50:
cf:72:dd:12:28:66:01:e1:81:bc:6c:66:f0:e8:83:
fd:b8:0b:ac:20:e0:74:e2:44:9c:57:59:0f:a7:09:
cc:37:ed:b0:8f:23:67:99:36:8d:be:4b:16:e9:b8:
e1:64:13:36:f7:26:e4:c6:e8:0a:d9:ab:63:a6:6c:
46:b1
```

Exponent: 65537 (0x10001)

## Attributes:

a0:00

## Signature Algorithm: sha256WithRSAEncryption

```
62:8e:bb:ff:df:ee:d8:da:20:f7:47:82:73:50:58:99:98:7b:
d3:9d:00:bf:31:7a:6a:2c:67:e4:97:ab:a3:23:4a:d7:51:56:
30:ca:fa:09:8a:82:27:03:45:52:d8:3d:8a:bb:0c:dd:15:30:
2b:7e:1e:cb:b1:ba:27:f2:d2:5b:1d:b3:c4:c6:9c:4c:b5:08:
ac:58:e6:f8:84:fe:c6:02:0d:14:f5:38:83:0d:b2:a3:f5:96:
b4:6b:57:40:10:44:4c:c4:96:f9:d8:8f:3d:65:41:20:eb:26:
cd:7d:17:3b:b8:32:9a:35:b7:0d:b4:89:51:e0:ba:90:42:fc:
de:dd:1e:f7:1b:df:cb:46:d9:9b:18:c0:a3:01:52:10:22:10:
ac:b5:f5:49:dc:d5:8a:20:8f:d0:84:57:61:37:dc:e7:e6:0b:
db:79:4f:7e:eb:d1:5d:ed:78:7d:96:b0:d0:40:52:a7:25:0b:
4a:42:94:00:b9:ad:c0:c9:19:db:c8:b0:2d:1b:b2:f9:3b:18:
fa:25:98:0a:77:5e:65:c7:2e:18:e9:f3:a9:b9:d3:1f:9d:87:
c2:79:00:db:ee:02:8b:43:f1:f0:72:0b:e7:39:0f:16:b1:7f:
ec:2a:d8:c7:85:01:e6:da:2b:06:62:17:80:c1:07:60:78:55:
07:cd:71:c2
```

-----BEGIN CERTIFICATE REQUEST-----

```
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHZGVtYW5kZTCCASlwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALD1exA42tmuFzCSzGflcrkVdWiHhbtIadZ0m3ktQUxg
FTmPKPU1mnkGZ80L8bTXXTTNYEd6vOOJP7D90QGKOHhpPna+jSo3dweZUUVdi20B
LT64yyYf9kVssyLm4SLjV3zP0vqxa4JlJ9q4nN5KPUPhmEQ9djKl6/+fRnOrRHG
L8l8T4g1oIE7d1j0J06Zu5RR1XUEpbXFF4WbpU8gKGKuqtqNcCarKiOWbEPyMI3v
RDZTlAFQ4QwQjzk8N6WmJ9xQz3LdEihmAeGBvGxm8Oid/bgLrCDgdOJEnFdZD6cj
zDftsI8jZ5k2jb5LFum44WQTNvcm5MboCtmrY6ZsRrECAwEAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQBijrv/3+7Y2iD3R4JzUfiZmHvTnQC/MXpqLGfkl6ujl0rXUVYw
yyvoJiolnA0VS2D2KuwzdFTArfh7Lsbon8tJbHbPExpMtQisWO4hP7GAg0U9TiD
DbKj9Za0a1dAEERMxJb52I89ZUEg6ybNfRc7uDkaNbcNtlIR4LqQQvze3R73G9/L
RtmbGMCjAVIQLhCstfVJ3NWkII/QhFdhN9zn5gvbeU9+69Fd7Xh9lRdQQFKnJQtK
```

```
QpQAua3AyRnbyLAtG7L5Oxj6JZgKd15lxy4Y6fOpudMfnYfCeQDb7gKLQ/Hwcvn  
OQ8WsX/sKtjHhQHm2isGYheAwQdgeFUHzXHC  
-----END CERTIFICATE REQUEST-----
```

Figure 17 : OpenSSL - Exemple de CSR

L'opération est terminée, cette CSR peut être chargée pour finaliser la demande d'un Certificat Logiciel.

Le fichier contenant la clé privée doit être placée sur un support sécurisé.

## 13 Gestion des Certificats Logiciels de test

La plateforme IGC-Santé permet de délivrer des certificats logiciels de production ou de test. Les principes de fonctionnement sont les suivants :

- Les certificats logiciels de tests sont identiques aux certificats de production. : toutes les offres et tous les usages présentés sont disponibles. Les Certificats Logiciels sont simplement émis par des AC de test.
- L'accès aux services de la plateforme IGC-Santé pour gérer des Certificats Logiciels de tests impose de disposer d'une carte CPx de test. Une carte CPx de test permet de gérer uniquement des Certificats Logiciels de test et réciproquement une carte CPx de production permet de gérer uniquement des Certificats logiciels de Production.
- Pour gérer des certificats logiciels de test, l'utilisateur doit au préalable avoir été habilité. Les habilitations pour la gestion des Certificats Logiciels de test sont distinctes de celles utilisées pour la gestion de Certificats logiciels de production, mais les principes utilisés sont identiques à ceux décrits dans le paragraphe « 8 - Habilitations».
- Le fonctionnement des services de la plateforme IGC-Santé est identique pour les Certificats Logiciels de production ou de test.

## 14 Demande de création de certificat

Le système externe appelant le Web Service de la plateforme IGC-Santé envoie un lot d'une ou plusieurs demandes de certificat par le canal Web-Services.

Lors de la demande de création de certificat par Web Service, la CSR doit être fournie par le demandeur.

Un lot de demandes est limité à 20 demandes.

Selon l'offre, la demande peut s'appliquer sur une structure, un bénéficiaire ou sur les deux.

- Offre PS : certificats logiciels de portée « personnel » liés à une personne physique
- Offre PRO : certificats logiciels de portée « structure » liés à une personne physique
- Offre ORG : certificats logiciels rattachés à une Structure
- Offre SERV : certificats logiciels rattachés à un serveur pour une Structure.

### 14.1 Demande de Lot de certificat

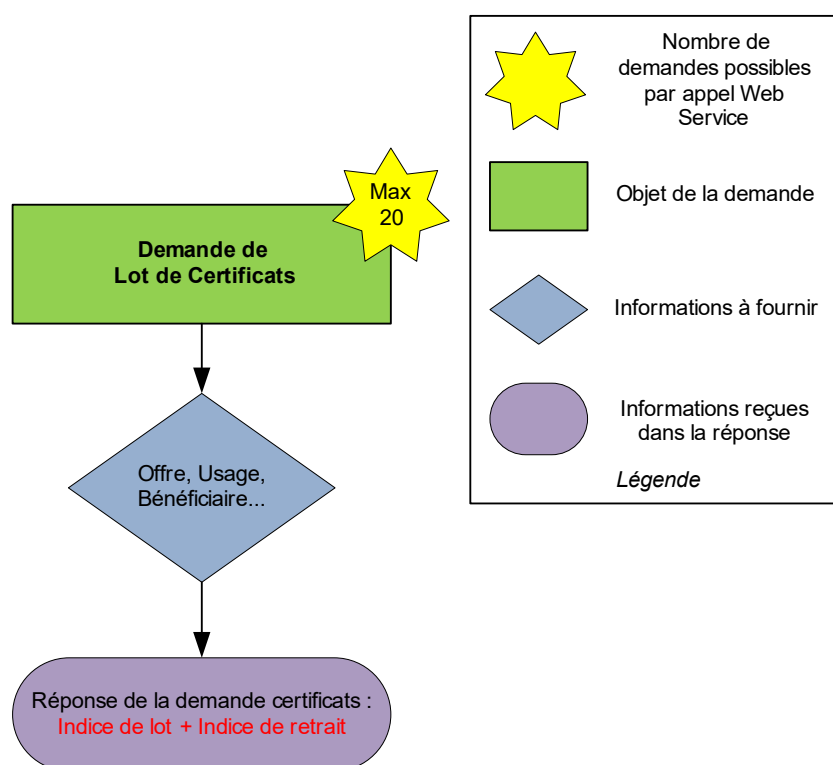


Figure 18 - Schéma de lot de certificats

Un lot inclut une ou plusieurs demandes de certificats dans un message unique signé par l'acteur.

Si le lot contient plus de 20 demandes, le message sera rejeté par le Web-Service qui renverra une erreur.

Les paramètres d'entrée sont saisis pour la demande de certificat (*Pour plus de détails, voir le tableau des paramètres en entrée*) :

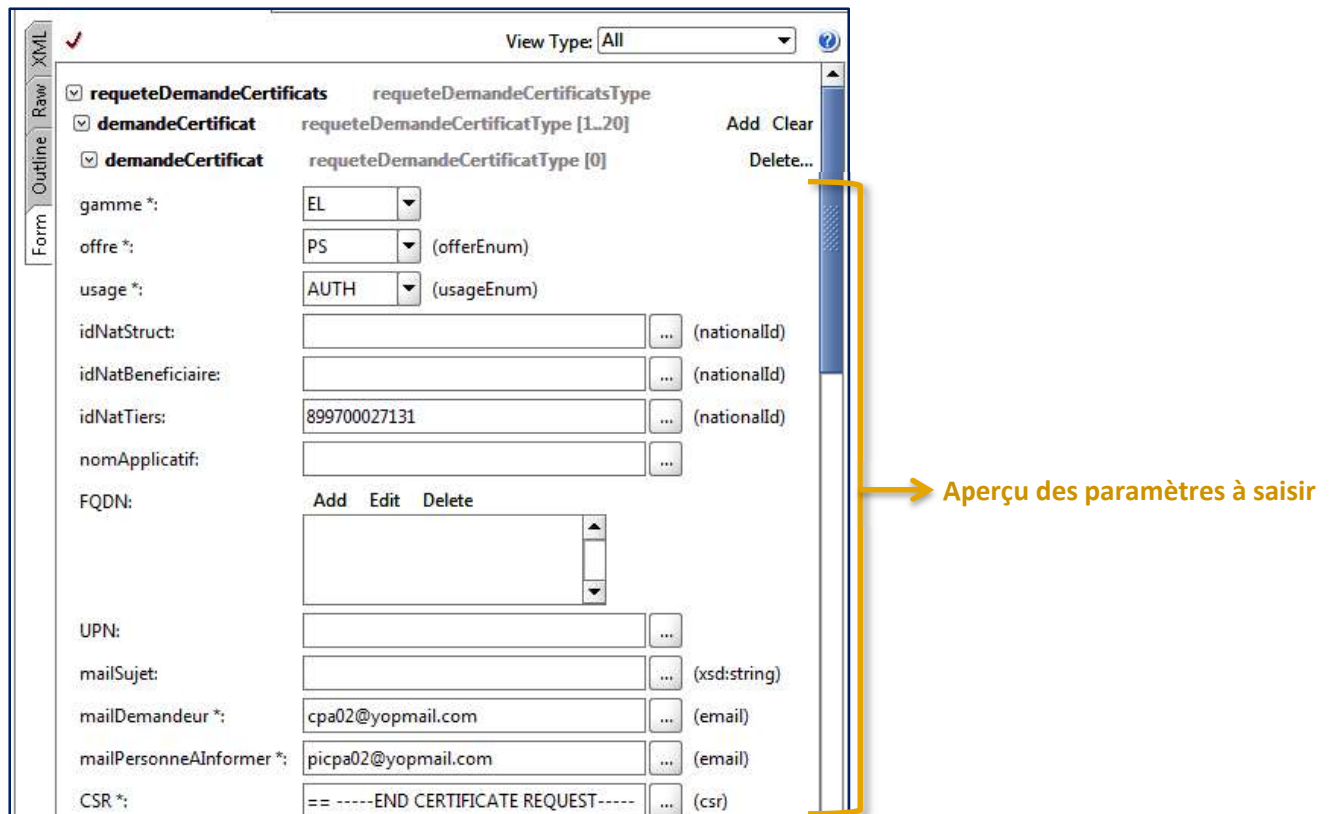


Figure 19 : Demande de lot de certificat - Exemple SOAP UI

- ➔ Offre : Type d'offre à saisir
  - ➔ Usage : choisir l'usage du certificat
  - ➔ IdNatStruct : Identifiant national de la structure
  - ➔ IdNatBeneficiaire : Identifiant national du bénéficiaire
  - ➔ CSR (cf paragraphe 12)
  - ➔ MailDemandeur : concerne la personne qui fait la demande. Ce champ est obligatoire. Il permet de recevoir les notifications par email des actions réalisées ou à réaliser (confirmation de la demande, mise à disposition du certificat...)
  - ➔ MailPersonneAInformer : élément obligatoire à renseigner. Il permet de recevoir les notifications par email à titre informatif des actions réalisées. (confirmation de la demande, l'information de la mise à disposition du certificat auprès de l'acteur...)
- ...

**Aperçu de la demande de certificat sous format XML :**

*(Voir exemple de fichier XML en Annexe 1)*



```

<ds:SignatureValue>rpw5IUAbE8TvA4Iph8EcGsEv6rSHVfr967iL4Def2Cw0fsUKdswP+BF/IG, Lqdw0wsDrUo951FK
nLftXDSaq+vbLG+IqOZ1nimbkzplJd7F0Rxl2vzlkz3rjsD8mi30f5EaZJKGsCkFXZEJjRfHkBE
5QyiyGasndaUgEXABt0Rvb9BGJpr9bFv12ozKNoFM407tBONvr7BxIsIqned2f5VZ+YcSFqFLj9f
Lr1RFwgn0BeBOAm93RwKhb/GsExz3oGDTvGIOj14P/qGGf/6/pVXTY87X+IpeH1C5Kr0LTzirT2g
wdLlu0z7tuLZMRmbQWQ6UXtNF1rPwiNcyqmjyQ==</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509SubjectName>CN=50000000028969/CPAT0002 + OID.2.5.4.4=AGENT0000028960002 + OID.2.5.4.42=DENISE,
    <ds:X509Certificate>MIIFRzCCBjEgAwIBAgIDW6iQMA0GCSqGSIb3DQEBAQUAAwIqNBAYTAKzSMQ0wCwYDVOQQK
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</SOAP-SEC:Signature>
</SOAP-ENV:Header>
<SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
  <ws:requeteDemandeCertificats xmlns:ws="http://www.pfong.in.com/WS/">
    <demandeCertificat>
      <gamme>EL</gamme>
      <offre>PS</offre>
      <usage>AUTH</usage>
      <idNatTiers>899700027131</idNatTiers>
      <mailDemandeur>cpa02@yopmail.com</mailDemandeur>
      <mailPersonneAInformer>picpa02@yopmail.com</mailPersonneAInformer>
      <CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKQ
+kIU9Jxc6QuNs5uEb9n1KD2nLjvushfmeLAZPH3V7edN6KdqEMzNRlpopcWHRgAY
iSEivmYQtdcPvwuV0kF1I34vLVNKKDT6XZVgy0YD7h9lixckGrPQw7XWytchjrey
1bkdj0grDhFOiGf+Lm4Xc06LON5EUEV0gmQ7v7B4fZbo7BhiMgy+Po68n9xCAP5X
KuiqECg/QkV5pITBhqLmVmNmF11M10VRHEItQMX/25tT8BkREY/j1FUh+1LXzDcd
Tkjt+rXXqWJQFE0TrBOZ12ob/9GMA2EumubO3rJfK3Xo9x3beOG7bJsE4JptJ0v
YFFIVDy4i55KFxpATTkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAAuOpZI7fm5J+q
xryQj3VjM1C51QsXmZSedIRoAF6rslIvcK7ooqoQ7eIibbJt8GNSF9Y+p3EYX8Dg
AQz8FL2SnPFTiV+i8D2+kjkqLrkGrQd4v9PERDTnwc6triggDLyLTlgQRQzJ8khE
ivSLEPztKwJQ0qD/pG3eZe6J9REvbaavYR04hd30CBAC5ceJvRpa0jHrxIeHp4u
xFSp712GIo1ShSmBoUEgy8hhGOXEjqlkAWdl0L1WSXuIprDE810syamchmP5L+p
2zVNdUQj2Mi aMRQsCxfrOp58SAjFT8OQ2iqhZ2EViGgaHc/UBSgXpITN0169Dfh
XtG5epPnjQ==
-----END CERTIFICATE REQUEST-----</CSR>
    </demandeCertificat>
  </ws:requeteDemandeCertificats>
</SOAP-ENV:Body>
</SOAP-ENV:Header>
</SOAP-ENV:Header>

```

Aperçu de la Signature du fichier XML

Corps du fichier XML

Figure 20 : Demande de lot de certificat - Exemple de requête

On retrouve les informations saisies dans le corps du XML généré :

```

<demandeCertificat>
  <gamme>EL</gamme>
  <offre>PS</offre>
  <usage>AUTH</usage>
  <idNatTiers>899700027131</idNatTiers>
  <mailDemandeur>cpa02@yopmail.com</mailDemandeur>
  <mailPersonneAInformer>picpa02@yopmail.com</mailPersonneAInformer>

```

Figure 21 : Demande de lot de certificat - Requête - Détail

Egalement la CSR envoyée :

```

<CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKQ
+kIU9Jxc6QuNs5uEb9n1KD2nLjvushfmeLAZPH3V7edN6KdqEMzNRlpopcWHRgAY
iSEivmYQtdcPvwuV0kF1I34vLVNKKDT6XZVgy0YD7h9lixckGrPQw7XWytchjrey
1bkdj0grDhFOiGf+Lm4Xc06LON5EUEV0gmQ7v7B4fZbo7BhiMgy+Po68n9xCAP5X
KuiqECg/QkV5pITBhqLmVmNmF11M10VRHEItQMX/25tT8BkREY/j1FUh+1LXzDcd
Tkjt+rXXqWJQFE0TrBOZ12ob/9GMA2EumubO3rJfK3Xo9x3beOG7bJsE4JptJ0v
YFFIVDy4i55KFxpATTkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAAuOpZI7fm5J+q
xryQj3VjM1C51QsXmZSedIRoAF6rslIvcK7ooqoQ7eIibbJt8GNSF9Y+p3EYX8Dg
AQz8FL2SnPFTiV+i8D2+kjkqLrkGrQd4v9PERDTnwc6triggDLyLTlgQRQzJ8khE
ivSLEPztKwJQ0qD/pG3eZe6J9REvbaavYR04hd30CBAC5ceJvRpa0jHrxIeHp4u
xFSp712GIo1ShSmBoUEgy8hhGOXEjqlkAWdl0L1WSXuIprDE810syamchmP5L+p
2zVNdUQj2Mi aMRQsCxfrOp58SAjFT8OQ2iqhZ2EViGgaHc/UBSgXpITN0169Dfh
XtG5epPnjQ==
-----END CERTIFICATE REQUEST-----</CSR>

```

Figure 22 : Demande de lot de certificat - Requête - CSR

Description du message de la requête de Demande de lot de certificat dans le fichier WSDL :

```
<wsdl:message name="requeteDemandeCertificats">
  <wsdl:documentation>Requete de demande de
certificats</wsdl:documentation>
  <wsdl:part name="parameters"
element="tns:requeteDemandeCertificats"></wsdl:part>
</wsdl:message>
```

### **Description de l'opération de la Demande de certificat dans le fichier WSDL :**

```
<wsdl:operation name="demanderCertificats">
  <wsdl:documentation>Interface de demande de certificats
</wsdl:documentation>
  <wsdl:input
message="tns:requeteDemandeCertificats"></wsdl:input>
  <wsdl:output
message="tns:reponseDemandeCertificats"></wsdl:output>
</wsdl:operation>
```

```
<wsdl:operation name="demanderCertificats">
  <wsdl:documentation>Interface de demande de certificats
</wsdl:documentation>
  <soap:operation soapAction="demanderCertificats" />
  <wsdl:input>
    <soap:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal" />
  </wsdl:output>
</wsdl:operation>
```

Chaque demande de certificat du lot est contenue dans une balise (20 demandes maximum) :  
**<demandeCertificat>** :

#### **Extrait du fichier XSD :**

```
<xsd:complexType name="requeteDemandeCertificatsType">
  <xsd:sequence>
    <xsd:element name="demandeCertificat"
type="tns:requeteDemandeCertificatType"
minOccurs="1" maxOccurs="20"></xsd:element>
  </xsd:sequence>
</xsd:complexType>
```

Voici les paramètres d'entrée de la requête de Demande de certificat :

Donnée	Balise XML (Voir fichier XSD)	Objet métier	Type de contrôle	Contrôle du paramètre
<b>idNat_Tiers</b>	<b>&lt;idNatTiers&gt;</b>	Demande de certificat logiciel Acteur -	Présence	Facultatif
			Type	Chaîne de caractères (64 caractères)
<b>offre</b>	<b>&lt;offre&gt;</b>	Demande de certificat logiciel - Offre	Valeurs possibles	« PS », « PRO », « SERV », « ORG »
			Présence	Obligatoire
			Type	Chaîne de caractères (maximum 4 caractères)
<b>gamme</b>	<b>&lt;gamme&gt;</b>	-	Valeurs possibles	« EL »
			Présence	Obligatoire
			Type	Chaîne de caractères (maximum 2 caractères)
<b>idNat_struct</b>	<b>&lt;idNatStruct&gt;</b>	Demande de certificat logiciel Structure -	Présence	Obligatoire pour les offres PRO, ORG et SERV Interdit pour l'offre PS
			Type	Chaîne de caractères (maximum 64 caractères)
<b>idNat_beneficiaire</b>	<b>&lt;idNatBeneficiaire&gt;</b>	Demande de certificat logiciel Bénéficiaire -	Présence	Obligatoire pour l'offre PRO Interdit pour les offres PS, SERV et ORG
			Type	Chaîne de caractères (maximum 64 caractères)
<b>usage</b>	<b>&lt;usage&gt;</b>	Produit Usage -	Valeurs possibles	Les valeurs possibles dépendent de l'offre <ul style="list-style-type: none"> <li>• PS : « AUTH », « SIGN », « CONF »</li> <li>• PRO : « AUTH », « SIGN », « CONF »</li> <li>• ORG : « AUTH_CLI », « SIGN », « CONF »</li> <li>• SERV : « SSL_SERV », « SIGN », « S/MIME », « CONF »</li> </ul>
			Présence	Obligatoire
			Type	Chaîne de caractères (maximum 8 caractères)
<b>nomApplicatif</b>	<b>&lt;nomApplicatif&gt;</b>	Produit Service -	Présence	Obligatoire pour les offres ORG et SERV (sauf usage SSL_SERV) Interdit pour les autres offres / usages
			Type	Chaîne de caractères (maximum 63 caractères)
			Format	Noms de domaine conformes à la RFC1035

Donnée	Balise XML (Voir fichier XSD)	Objet métier	Type de contrôle	Contrôle du paramètre
<b>FQDN</b>	<b>&lt;FQDN&gt;</b>	Produit - Domaines	Présence	Obligatoire pour l'offre SERV et l'usage SSL_SERV (peut être renseigné jusqu'à 5 fois) Interdit pour les autres offres et usages
			Type	Chaîne de caractères (maximum 63 caractères)
			Format	Compatible avec la RFC1035
<b>UPN</b>	<b>&lt;UPN&gt;</b>	Produit - UPN	Présence	Facultatif pour les offres PS et PRO uniquement pour l'usage AUTH Interdit pour les autres offres / usages
			Type	Chaîne de caractères (maximum 150 caractères)
			Format	Adresse email compatible avec la RFC5322
<b>mailSujet</b>	<b>&lt;mailSujet&gt;</b>	Produit - Email Sujet	Présence	Obligatoire pour l'offre SERV : usages SIGN, S/MIME et CONF Facultatif pour les offres PS et PRO : usages SIGN et CONF Interdit pour les autres offres / usages
			Type	Adresse email
			Format	Compatible avec la RFC5322
<b>mailInformeur</b>	<b>&lt;mailPersonnelInformeur&gt;</b>	Demande de certificat logiciel - Email Notification	Présence	Obligatoire
			Type	Adresse email
			Format	Compatible avec la RFC5322
<b>CSR</b>	<b>&lt;CSR&gt;</b>	Produit - CSR	Présence	Obligatoire
			Type	Chaîne de caractères (maximum 1536 caractères)
			Format	Base 64 Compatible avec la RFC2986 associée à PKCS10
<b>mailDemandeur</b>	<b>&lt;mailDemandeur&gt;</b>	Demande de certificat logiciel - Email Acteur	Présence	Obligatoire
			Type	Adresse email
			Format	Compatible avec la RFC5322

**Tableau 11 : Paramètres d'entrée de la Demande de certificat**

## 14.2 Réponse de la demande de lot de certificats

Le système envoie en réponse Web-Service l'accusé de réception du lot.

La réponse de la demande contient une première partie sur le Lot de la demande (Indice de lot, Statut du lot et Message d'erreur éventuel).

Ensuite, pour chaque demande, une réponse est apportée dans la balise **<demande>**. (Indice de retrait, message d'erreur ...)

Extrait du fichier XSD :

```
<xsd:element name="demande" type="tns:reponseDemandeCertificat"
             minOccurs="0" maxOccurs="20">
</xsd:element>
```

Voici les paramètres de la réponse de la demande :

Web service		Balise XML (Voir fichier XSD)	Entrée	
Paramètre lié au lot de demandes	Paramètre lié à chaque demande <demande>		Objet Métier	Donnée ou valeur
<b>indiceLot</b>		<b>&lt; indiceLot&gt;</b>	-	Indice de lot 1 seule occurrence
<b>statutLot</b>		<b>&lt; statutLot&gt;</b>	-	« OK » ou un code d'erreur
<b>message</b>		<b>&lt; message&gt;</b>	-	« » si le lot est correct Sinon le message d'erreur associé
	<b>indiceDemande</b>	<b>&lt; indiceDemande&gt;</b>	Demande de Certificat Logiciel	Numéro 20 occurrences maximum
	<b>statutDemande</b>	<b>&lt; statutDemande&gt;</b>	-	« OK » si la demande est validée, le code d'erreur sinon
	<b>message</b>	<b>&lt; message&gt;</b>	-	« » si la demande est validée ou le message associé au code d'erreur sinon
	<b>indiceRetrait</b>	<b>&lt; indiceRetrait&gt;</b>	Produit	Indice de retrait Web Service Autant d'occurrences que pour indiceDemande

Tableau 12 : Paramètres de la réponse de certificat

**Description du message de la réponse de Demande de lot de certificat dans le fichier WSDL :**

```
<wsdl:message name="reponseDemandeCertificats">
  <wsdl:documentation>Reponse a la requete de demande de
    certificats
  </wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:reponseDemandeCertificats"></wsdl:part>
</wsdl:message>
```

Plusieurs cas sont possibles dans la réponse :

- Si tous les paramètres sont vérifiés avec succès, pour chaque demande de certificat logiciel :  
Le lot et les demandes sont au **<statut> OK** (*voir exemple ci-dessus*) : La balise **<message>** est vide pour le lot et pour les demandes. Toutes les demandes sont traitées.
- La Demande de certificat logiciel passe à l'état « **Demande validée** »
- Le Produit passe à l'état « **Produit à retirer** »

Si une erreur survient à cette étape (vérification syntaxique du lot), pour toutes les demandes :

- Le lot complet est rejeté : Le **<statut>** contient le code erreur et le **<message>** contient le libellé de l'erreur. Le traitement s'arrête et les demandes ne sont pas traitées.
- Chaque Demande de certificat logiciel passe à l'état « **Demande non traitée** »
- Chaque Produit passe à l'état « **Produit annulé** »

### 14.2.1 Exemples de cas passant

**Aperçu de la réponse d'un cas passant d'une demande de lots de certificats sous format XML :**

*(Voir exemple de fichier XML en Annexe 1)*

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseDemandeCertificats>
      <indiceLot>1445339982457</indiceLot>
      <statutLot>OK</statutLot>
      <message/>
      <demande>
        <indiceDemande>759</indiceDemande>
        <statutDemande>OK</statutDemande>
        <message/>
        <indiceRetrait>759</indiceRetrait>
      </demande>
      <demande>
        <indiceDemande>760</indiceDemande>
        <statutDemande>OK</statutDemande>
        <message/>
        <indiceRetrait>760</indiceRetrait>
      </demande>
      <demande>
        <indiceDemande>761</indiceDemande>
        <statutDemande>OK</statutDemande>
        <message/>
        <indiceRetrait>761</indiceRetrait>
      </demande>
    </ns3:reponseDemandeCertificats>
  </ns2:Body>
</ns2:Envelope>
```

Figure 23 : Demande de lot de certificat – Exemple de Réponse

On retrouve dans le corps du fichier **les informations sur le lot** de la demande :

```
<ns3:reponseDemandeCertificats>
  <indiceLot>1445339982457</indiceLot>
  <statutLot>OK</statutLot>
  <message/>
```

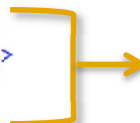


Figure 24 : Demande de lot de certificat – Réponse – Statut du Lot

Egalement, pour chaque demande, on retrouve **les informations de la demande** :

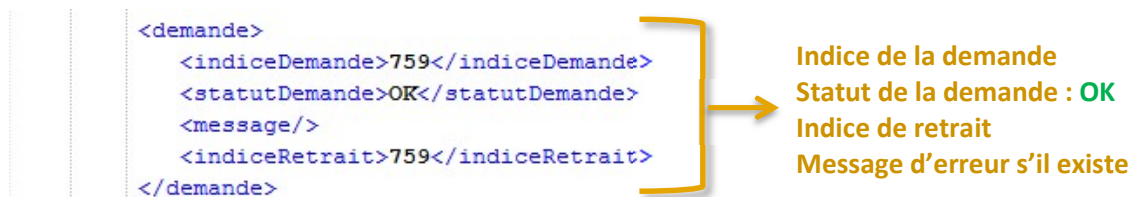


Figure 25 : Demande de lot de certificat - Réponse – Statut de la Demande

## 14.2.2 Exemple de cas non passant

Aperçu de la réponse d'un cas non passant d'une demande de lots de certificats sous format XML :

```

<ns3:reponseDemandeCertificats>
  <indiceLot/>
  <statutLot>WSMG-00000023</statutLot>
  <message>Le lot ne peut pas contenir plus de 20 demandes. Veuillez
renouveler votre demande.</message>
</ns3:reponseDemandeCertificats>

```

- Le lot est au **<statut>** KO : certaines demandes n'ont pas été traitées. (Le **<statut>** de la demande contient le code erreur. Le **<message>** de la demande contient le libellé de l'erreur). Les demandes au **<statut>** OK ont été traitées.

Le **<message>** du lot reprend le libellé d'erreur de la demande en erreur.

```

<indiceLot>1447682134768</indiceLot>
  <statutLot>KO</statutLot>
  <message>Pour les offres PRO, ORG et SERV, « idNat_Struct » est
obligatoire.</message>
  <demande>
    <statutDemande>WSMG-00000032</statutDemande>
    <message>Pour les offres PRO, ORG et SERV, « idNat_Struct » est
obligatoire.</message>
  </demande>
  <demande>
    <indiceDemande>59</indiceDemande>
    <statutDemande>OK</statutDemande>
    <message></message>
    <indiceRetrait>59</indiceRetrait>
  </demande>
  <demande>
    <indiceDemande>60</indiceDemande>
    <statutDemande>OK</statutDemande>
    <message></message>
    <indiceRetrait>60</indiceRetrait>
  </demande>
  <demande>
    <indiceDemande>61</indiceDemande>
    <statutDemande>OK</statutDemande>
    <message></message>
    <indiceRetrait>61</indiceRetrait>
  </demande>

```

```
<demande>  
  <indiceDemande>63</indiceDemande>  
  <statutDemande>OK</statutDemande>  
  <message></message>  
  <indiceRetrait>63</indiceRetrait>  
</demande>
```



Ces informations peuvent être consultées :

- En envoyant une demande de suivi (Voir partie « 14. Suivi de l'activité ») : Champ **<etat>**
- Sur l'interface IHM Menu « **Suivi des demandes de produits** » et « **Suivi des certificats** » Onglet « **Historique** ». (Voir Guide d'utilisation IHM Ref [1])

Exemple de Suivi de Certificats :

Numéro ↕	Numéro produit ↕	Canal ↕	Date ↕	Code action ↕	Etat produit ↕	Type acteur ↕	Acteur ↕
2	2	WS	17/12/2015 14:24	ACT_DCL_001	Demandé	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)
6	2	WS	17/12/2015 14:24	ACT_DCL_005	À retirer	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)

Figure 26 : Exemple de Suivi de certificats - Demande

## 14.3 Notifications en lien avec la demande de certificat

Quand l'utilisateur effectue une demande de certificat par Web Service, il reçoit ensuite des notifications par email. (Ainsi que la personne à informer)

Pour chaque demande, une notification de validation de la demande est envoyée.

- **Notification de Validation de la demande (PS, PRO, CONF, SIGN)** : Envoyée à la personne dont l'email a été renseigné dans le champ <mailDemandeur>.

Cette notification est envoyée lorsque la demande est validée et conforme.

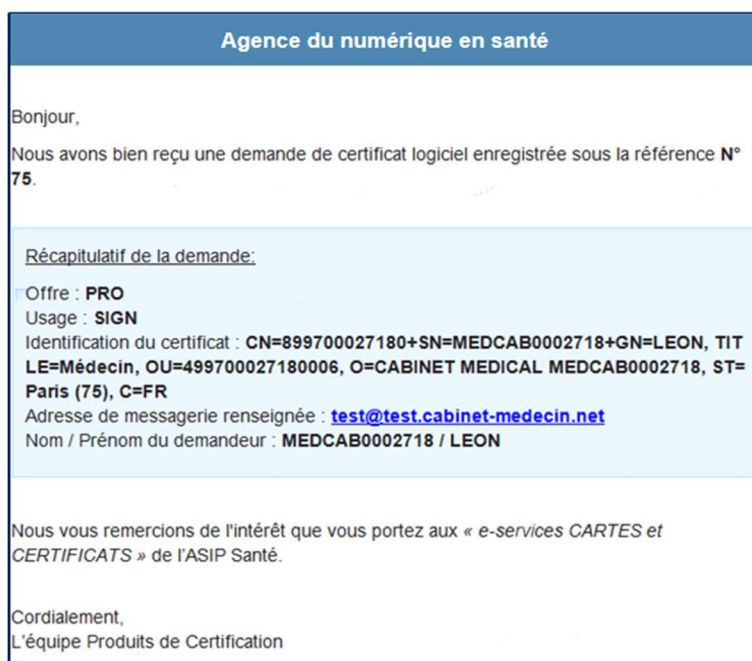
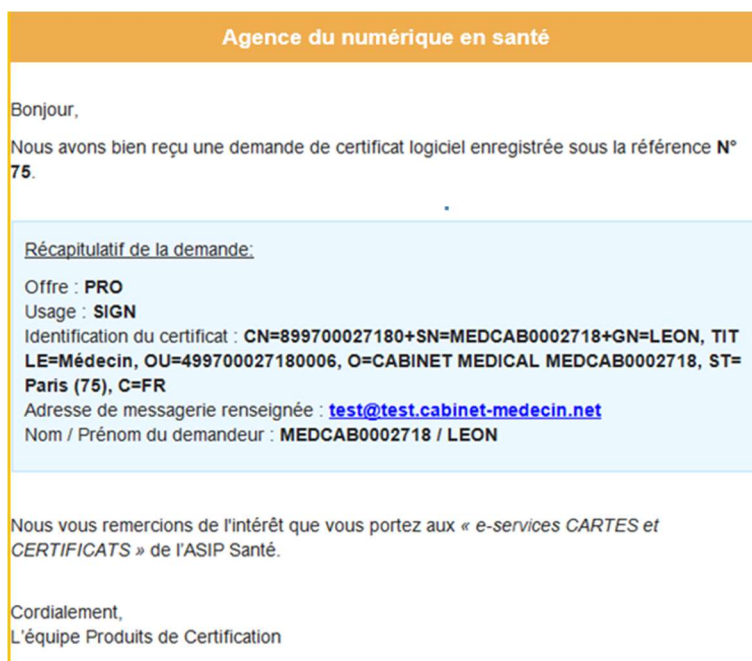


Figure 27 : Notification de la demande de certificat - Acteur

**Objet de l'email** : « **Agence du numérique en santé - Produits de Certification >>> Confirmation de la demande <N° de demande interne plateforme IGC-Santé >** »

- **Notification de Validation de la demande (PS, PRO, CONF, SIGN)** : Envoyée à la personne dont l'email a été renseigné dans le champ **<mailPersonneAInformer>**.



**Figure 28 : Notification de la demande de certificat - Personne à informer**

**Objet de l'email** : « [POUR INFORMATION] Agence du numérique en santé - Produits de Certification >>> Confirmation de la demande **<N° de demande interne plateforme IGC-Santé>** ».

## 14.4 Cas non passants au niveau des contrôles métiers

Les contrôles métiers sont réalisés au niveau de chaque demande indépendamment du lot.

- **Exemple 1 :**

L'utilisateur effectue une demande de certificat pour une structure sur laquelle il n'a pas d'habilitation.

→ La demande de certificat ne doit pas aboutir.

Voici un aperçu du XML généré (*la signature a été tronquée pour plus de visibilité sur le document*) :

```

<ds:SignatureValue>IEEE6FYBNFNyQpe47qGByv9581WF+eVKLYlhwc5B/yiYN2Fhs7Xr1CaTjGJrOKP/EZefZu8nk1tV
UHK0pJMX7MPcj1ncjEwFeNbBpbY6eT+eTTgMy1vbfBJ9aj2jfqWQuKMB3tLx7ej8oHmLq1EC1c8
szA++6i jCLsVj9nQysFowpquCM06VG1703sqhjTrkh3UOI6a+XMEuTbR6IYvzmietuKqJ7YiT1O
I3LJP3Jj/a8WpKMiNG90AvtlqSwrenMwuD3q+g99S3eLR3j3vjHcqBf4b5AJE9LHg0TB3CFVM8oC
nbSkwgQ/mhS7JkmnMa5B60eLZZkIcDbpdIE4Q==</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509SubjectName>CN=899700027131 + OID.2.5.4.4=PHARMACH0002713 + OID.2.5.4.42=CAROLE, OU=Pharmacien, O=TEST,
    <ds:X509Certificate>MIIFtTCCBJ2gAwIBAgIDW6ewMA0GCSqGSIb3DQEBBQUAMFExCzAJBgNVBAYTAkZSMQ0wCwYDVQQK
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</SOAP-SEC:Signature>
</SOAP-ENV:Header>
<SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
  <ws:requeteDemandeCertificat xmlns:ws="http://www.pfongq.in.com/WS/">
    <demandeCertificat>
      <gamme>EL</gamme>
      <offre>PRO</offre>
      <usage>CONF</usage>
      <idNatStruct>499700027180006</idNatStruct>
      <idNatBeneficiaire>899700027131</idNatBeneficiaire>
      <mailDemandeur>cps03@yopmail.com</mailDemandeur>
      <mailPersonneAInformer>pics03@yopmail.com</mailPersonneAInformer>
      <CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAJ9F
XMx+/y+OwmPMj+xsBorzNQt3IJgN2p38GE+bdGwKvn7D13ZF7j8sctXDMI2uZPN
mh7GkvlfjxMPhoNAOf7Yt2torB21ola7Q9snjdNkanAKURULr6ZZnDmX1lvj+A6r
PYTf2ReeiMdoGh8LfeJ2GVB9YD03BpDLVKWj+r6pwB72Ebn0nqg3vmwhCmEgkU2
pQM5tG41ekRfR0t9TN5Ku3ntIoscGw4vUnS2088CBVI8vGeXuVZNYBs4tRpD1IUI
rme/BpwaHPoEvLPHY75FIDJGcu89mKAKBDZQJpAWCVwLzHxusRUEsDsqaF5+Hpv
I211+EsqquLacoX5DzUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEATgh6uABHmj+L
rtQFuOr9dwZQPpigs70Yvj1vCs1WvyNX95o1kh2EqKUN2Wjy1391YftJLwvaVuz
ekGdwIziBsp0Qwv6DEcyTKeaw8oxxi0J2bTYje8Z15b0ujH1PVfH808Rd0vFF/D
4ZQLSHL3z14ziE/HBrMIebbxBJHgF3tVMSNW/w1K02wgP3V2eSrlDyy8ve7rNAC8
Ue457Sti4pSIRwTf0eyXvt00Lsau/VnSi035AfixYzYmrM7V+99DeUfoWRdspdIM
p2n2o4R3atd57CLB9xnIiOrfag2Qn2FwISY1K/GsvfTrm4UF1PjA9qw5hu9w6jDw
BihTTU/i6w==
-----END CERTIFICATE REQUEST-----</CSR>
  </demandeCertificat>
</ws:requeteDemandeCertificat>
</SOAP-ENV:Body>
</SOAP-ENV:Document>

```

Figure 29 : Demande de lot de certificat - Cas non passant 1 - Requête

L'utilisateur n'a pas d'habilitation sur la structure 499700027180006.

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcnr.in.com/WS/">
  <ns2:Body>
    <ns3:reponseDemandeCertificats>
      <indiceLot>1445520238081</indiceLot>
      <statutLot>KO</statutLot>
      <message>Echec lors de la validation de demande de certificat : L'acteur n'est pas habilité sur le périmètre de la structure.</message>
      <demande>
        <indiceDemande>834</indiceDemande>
        <statutDemande>WSMG-00000010</statutDemande>
        <message>Echec lors de la validation de demande de certificat : L'acteur n'est pas habilité sur le périmètre de la structure.</message>
        <indiceRetrait>834</indiceRetrait>
      </demande>
    </ns3:reponseDemandeCertificats>
  </ns2:Body>
</ns2:Envelope>
```

Figure 30 : Demande de lot de certificat - Cas non passant 1 - Réponse

Détail de l'erreur :

Le lot est **KO** :

```
<indiceLot>1445520238081</indiceLot>
<statutLot>KO</statutLot>
<message>Echec lors de la validation de demande de certificat : L'acteur n'est pas habilité sur le périmètre de la structure.</message>
```

Figure 31 : Demande de lot de certificat - Cas non passant 1 - Réponse - Statut du lot

La demande contient le code erreur :

```
<demande>
  <indiceDemande>834</indiceDemande>
  <statutDemande>WSMG-00000010</statutDemande>
  <message>Echec lors de la validation de demande de certificat : L'acteur n'est pas habilité sur le périmètre de la structure.</message>
  <indiceRetrait>834</indiceRetrait>
</demande>
```

Figure 32 : Demande de lot de certificat - Cas non passant 1 - Statut de la demande

Le statut contient le code de l'erreur : **WSMG-00000010**.

Le message contient le message d'erreur : **Echec lors de la validation de demande de certificat : L'acteur n'est pas habilité sur le périmètre de la structure.**

• **Exemple 2 :**

L'utilisateur effectue une demande de certificat (Lot de 3 demandes).

L'adresse email sur la demande n°1 n'est pas correctement renseignée.

→ La demande ne doit pas aboutir car l'adresse email du demandeur doit être correctement renseignée.

Voici l'extrait du XML :

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header><SOAP-SEC:Signature SOAP-ENV:actor="some-URI
wAJGafUvvtvjEMmwP6AA5kaCJAqPzOSKqt1Co/L8zI9GgHFea08fLfiPGYuHDHvd1cmjtrlySpVYZ
754Sb0qK7RHmwgmS0w66W1YLX2r6+DYBpgS2BGJZDnt+w0tX1LbrtYHT3fRf793c18tKKV2v0cc
dA9xGQrRynCV5HoGmDE2BWJjiQQ6f1PJWZMVLwa/dX6kWtV+pQBgCDyrJtSCss66xob+kRRRhmV
I12zucNewBIN6y/Uvndm7cPTjEdtt95uc61MGg==</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509SubjectName>CN=50000000028969/CPAT0002 + OID.
</demandeCertificat>
  <gamme>EL</gamme>
  <offre>PS</offre>
  <usage>AUTH</usage>
  <mailDemandeur>cpa02@yopmail</mailDemandeur>
  <mailPersonneAInformer>piopa02@yopmail.com</mailPersonneAInformer>
  <CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJkk
AoPhsXUAqUrWcUjnPPjepyUAJYeRpYtg2g/wcdgt5nitRH0tCWkamgUDo7dgAEwk
eG4iYDmTG2OJREgaqnR2wX7/+wep61Qhmc16HpeAnAPHeAPRYu2TdGvvOBf/FtGZ
VJUkxJ9m/ZmkYH0uz3XpUQUyfd8v9xH4G0jCU2M62udr1M3DBken08RU+56eSQU
5g9EMftiuuOHKpYsDj3WyswQ/jS2ooxey3e02Gi8GwKohenWYOIH90xJoeukEI6W
2rcMDjXaifPfmqRMiDWIwQkwehk/OKFL6PH8IRcMw7If0bWP83bCgClpEymXoiKK
t65u35FFjDk26T21qzkCAwEAATANBgkqhkiG9w0BAQsFAAOCQAQEAgl1J2QX2xRYM
pCxoXBkMwArIMWXU2RMH5iRkhLhFP2MwJpnr14NI8BKIhd6rqs/YXzHquj8LO9mj
Bc444p7AGe1DIICbWr7x19jz08o/KDCt1V13YwbZnp5xoUNZok5YyaZHPgJ030Bh
F3G1sw7dQ6CUjp4u8OC2Ue1nMzPzvkt0yaJrJeZUKoR1rrc/souFj09R+1120xg
p24qLrEKtyzkNhykg089Yy1ZCwx1B2xyYBF11C2pTua/CjsfBQFIztaTdJkN4j
gdwbZ1YfV1WSaJmAgGxxkTGqB1Woch050tLN9LnmDpPY0a4iP4zCsTK+y4NUlkgr
PoCqyFAtbg==
-----END CERTIFICATE REQUEST-----
```

Figure 33 : Demande de lot de certificat - Cas non passant 2 - Requête

L'adresse email du demandeur n'est pas correcte : il manque la fin de l'adresse « .com »

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfong.in.com/WS/">
  <ns2:Body>
    <ns3:responseDemandeCertificats>
      <indiceLot>1445527604541</indiceLot>
      <statutLot>WSMG-00000005</statutLot>
      <message>Contenu de la demande non valide : mailDemandeur. Veuillez vérifier que les paramètres en entrée sont corrects et renouveler votre demande.</message>
    </ns3:responseDemandeCertificats>
  </ns2:Body>
</ns2:Envelope>
```

Figure 34 : Demande de lot de certificat - Cas non passant 2 - Réponse

Détail de l'erreur :

```
<indiceLot>1445527604541</indiceLot>
<statutLot>WSMG-00000005</statutLot>
<message>Contenu de la demande non valide : mailDemandeur. Veuillez vérifier que les paramètres en entrée sont corrects et renouveler votre demande.</message>
```

Figure 35 : Demande de lot de certificat - Cas non passant 2 - Réponse - Statut du lot

Le lot est **KO** : le lot complet est rejeté car la vérification syntaxique du fichier est en erreur.

Le statut contient le code de l'erreur : **WSMG-00000010**.

Le message contient le message d'erreur : **Contenu de la demande non valide : MailDemandeur. Veuillez vérifier que les paramètres en entrée sont corrects et renouveler votre demande.**

## 15 Retrait d'un certificat

Le système externe appelant le Web Service de la plateforme IGC-Santé demande le retrait du certificat avec l'indice de retrait Web Service qui lui a été communiqué en retour de la demande de certificat.

Le WS ne permet de demander le retrait d'un certificat que si la demande de création de ce certificat a été faite par ce même canal WS. Une demande de retrait ne concerne qu'un seul certificat.

Seul le demandeur initial (le signataire de la demande) peut effectuer le retrait

### 15.1 Demande de retrait d'un certificat

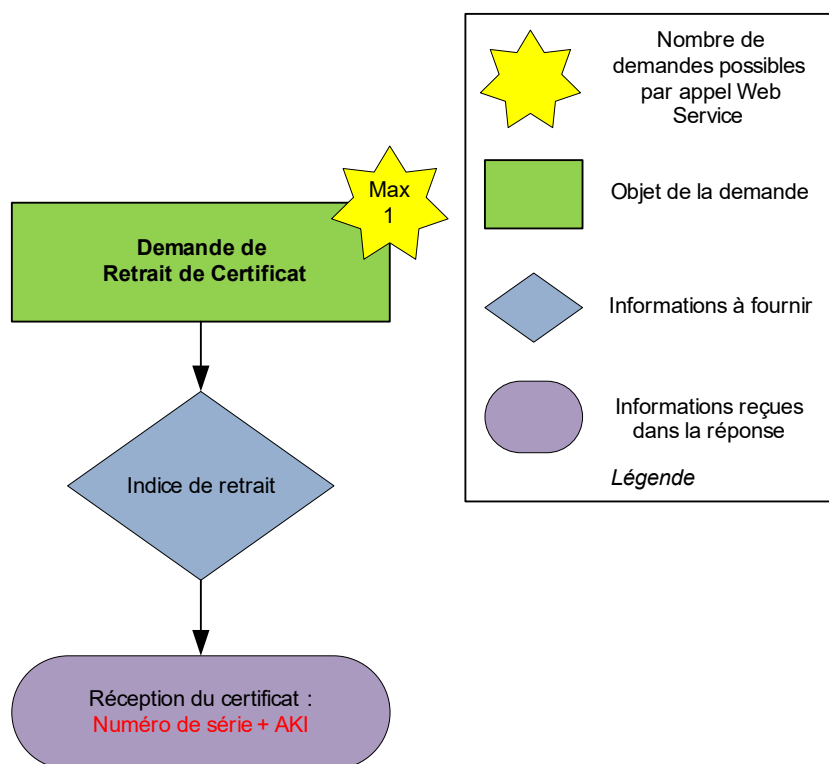
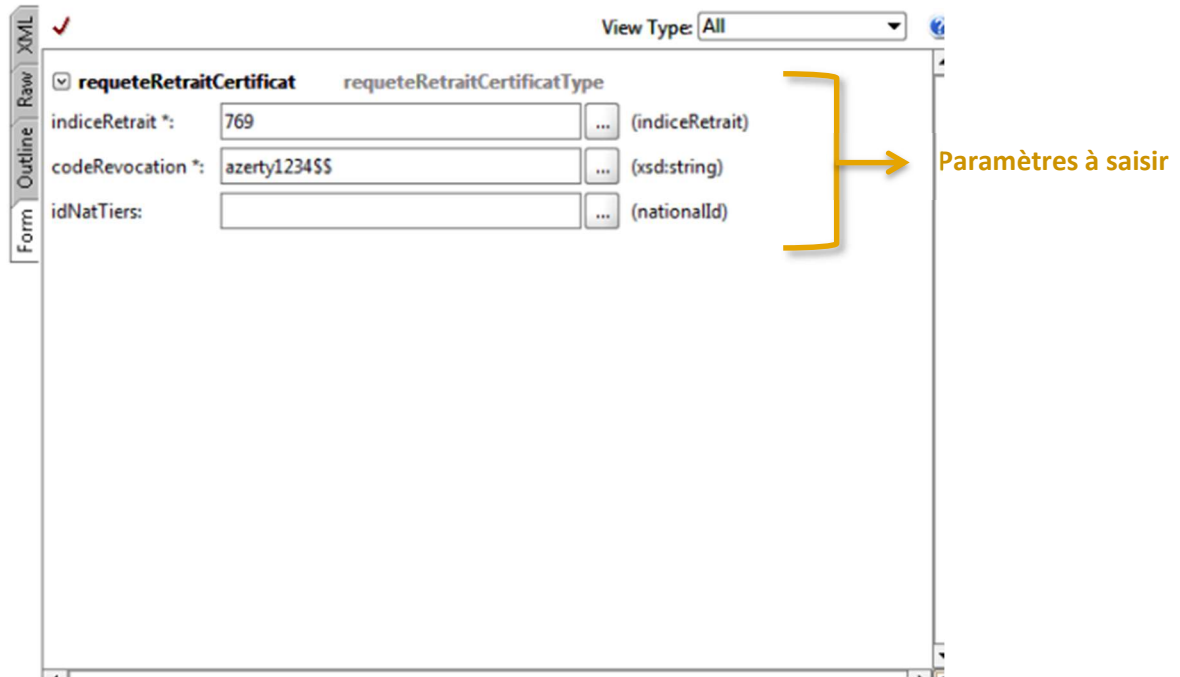


Figure 36 - Demande de retrait d'un certificat

Le système externe appelant envoie un appel Web Service de retrait de certificat avec l'indice de retrait client Web Service qui lui a été communiqué dans l'accusé de réception de la demande de certificat.

Les paramètres d'entrée suivants sont saisis pour la demande de retrait :



View Type: All

**requeteRetraitCertificat**    requeteRetraitCertificatType

indiceRetrait *:	<input type="text" value="769"/>	...	(indiceRetrait)
codeRevocation *:	<input type="text" value="azerty1234\$\$"/>	...	(xsd:string)
idNatTiers:	<input type="text"/>	...	(nationalId)

Paramètres à saisir

Figure 37 : Retrait d'un certificat - Exemple SOAP UI

- ➔ L'indice de Retrait a préalablement été récupéré dans la réponse de demande de certificat.
- ➔ Un code de révocation doit être également envoyé (Permet une révocation future)



**Aperçu de la demande de retrait de certificat sous format XML :**

(Voir exemple de fichier XML en Annexe 1)

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header><SOAP-SEC:Signature SOAP-ENV:actor="some-URI" SOAP-ENV:mustUnderstand="1"
    xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#withComments"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#Body"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
      <ds:DigestValue>heQK0yy9VQu+nS+8JwYx9rY209ZugjNUIQ7wZ6F72yk=</ds:DigestValue></ds:Reference></ds:SignedInfo>
    <ds:SignatureValue>CuqSjYxrS0i14KdVk/erJzv0iBMWTHtN795hZH+tPyjFwy2bdDghtmmSI4me47baLtxi8x8A9y9AH
      qlQWbtXv1fr/Q89650fjbA6aYU1/QXahWgY1eJm6x/29VrdAzI4nG+CLP+1ySXPiFw5Y2AaekY5K
      onl1njscFLa66Uv5HgD2AYGARJt.FAiCny1VBvCf+i4qk8XRpbP34JrqrZtPj2ILMeQWzaPd0NFnd4
      z13fmJL/DwW5qHa/pnDcdS5+jpHkqpXwL+ZuCdpyN7yPh0nFWOR24ZgJ391NsZm2o6y0WflaAAC
      ESE6FWWAY4/UgNhaktQRJQNBQpaw1eoIQ8KvPA=</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:X509SubjectName>CN=00B9804408 + OID.
      EwRURVNUMRswGQYDVQLExJURVNUIFBSTOZFU1NJTO5ORUwxFjAUBGNVBAAMTDVRFU1QgQ0xBU1NF
      LTEwHhcnMTUwMTAxMDAwMDAxWhcNMjAwMjI5MjE1OTU5WjBwMQswCQYDVQGEwJGUjENMAsGA1UE
      CHMEVEVTVDEZMBoGA1UECmVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90
      BgNVBAUQODI1OTU5WjBwMQswCQYDVQGEwJGUjENMAsGA1UECmVudG90ZG90ZGVzLWVudG90ZG90
      ADCCAQoCggEBALFkWAH1XV3lwrCgw+kjCjErp/1TK/WCVzHua/cZvSYGok9DTAPP41A0uJSMW10
      z6/0Vqwr.Lc6BQWn7tJ4rQt5nADdtcXCs+on2gFAiNaSia7lyKhfQ40W/REYTWkGUKAxu4+/FgMp
      EEcb6t/f4nd11EoYtCJAudco7hig1qInuPGaDBoZbjD3Gsh/nVLIz9Vvftvz0Vgt0RY8Rt3TqI0u
      AXcZ8fuv1KLCs6115jcsJrzODA2ugAZ8QDrUYdhAyFD1DHZrbdKvuELGoc8VC6U/g2rkJgPHz6
      G0Gw3yPaRp95CjVxuo00fHGRBs f21oPyzwDk362WQZyah2cXmuUCAwEAACAOCAMfwggjFMB8GA1Ud
      IwQYMBAFHYQNU00i3+MbgC3kqQgrPBS9LqMB0GA1UdDgQWBbTiH57yoWgjiDtG5jdHCOgy+pn9
      RTAObgNVHQ8BAf8EBAMCBsAwEwYDVR01BAAwCgYIKwYBBQUHAwQwKwYDVR0QBCQwIoAPMjAxNTAx
      MDEwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
      VR0TBAIwADCCBvgYDVFR0BFIg2MIgzMDugOaa3hjVodHRwOi8vYV5udWVpcmUuZ21lLnNwcy5mci9j
      cmwrdGVzdC9URVNUIEENMQVNTRS0xLmNybDBoOHKgcIZubGRhcDovL2FubnVhaXJlLmdpcC1jcmMn
      ZnIvY249dGVzdCBjbGFzZ2U5MjE1OTU5WjBwMQswCQYDVQGEwJGUjENMAsGA1UECmVudG90ZG90
      dG1maWVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90
      bnVhaXJlLmdpcC1jcmMnZnIvY249dGVzdCBjbGFzZ2U5MjE1OTU5WjBwMQswCQYDVQGEwJGUjENM
      bz10ZXN0LGM9ZnIvZG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90ZG90ZGVzLWVudG90ZG90ZGVz
      MCMGCGCgBegFHAQIDBBcTFTgWmjUwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
      CCqBegFHAQICBAMCAQAwDwYIKoF6AUoBAgCEAwIBYjANBgkqhkiG9w0BAQUFAAOCAQEAtvI4ixK
      D6n+iN/0FMZi6Jjcc383CYahKYWoY/n/ghbyNknqeh/6YE00VJUCg3rXu4TGCfAg3h9lp36ka46w
      yCk+3iemTQ+9ebxQ3TmnFosINw6LyT59Kx4xYc1jwtkFRvrgA2uj96EJZwmKfstJX41/o+DdEZem
      Xd4ZP5Q0vT+oKR1qi3K2NsYGrYqKxAutRDBTKlFOxaXoisxdnimQ170hmmaehci+KkC+TmvWbPL
      uU2KHn3EmD/MqIyVH48h5ETcp+LKA8Hy47s+GuOwSQA7axT+KmInbkTbYlZ8MbXnyePaC3FX8p
      -79M97IGmde300SpHYVf5yn+i8ln2rw=</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature></SOAP-SEC:Signature>
    </SOAP-ENV:Header><SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
      <ws:requeteRetraitCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
        <indiceRetrait>769</indiceRetrait>
        <codeRevocation>azerty1234$$</codeRevocation>
      </ws:requeteRetraitCertificat></SOAP-ENV:Body></SOAP-ENV:Envelope>
  
```



Figure 38 : Retrait de certificat - Exemple de requête

On retrouve les informations saisies dans le corps du XML généré :

```

<ws:requeteRetraitCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
  <indiceRetrait>765</indiceRetrait>
  <codeRevocation>azerty1234$$</codeRevocation>
</ws:requeteRetraitCertificat></SOAP-ENV:Body></SOAP-ENV:Envelope>

```

Indice de retrait

Code de révocation

**Description du message de la requête de Retrait de certificat dans le fichier WSDL :**

```

<wsdl:message name="requeteRetraitCertificat">
  <wsdl:documentation>Requete de demande de
  retrait</wsdl:documentation>
  <wsdl:part name="parameters"
  element="tns:requeteRetraitCertificat"></wsdl:part>
</wsdl:message>

```

**Description de l'opération de Retrait de certificat dans le fichier WSDL :**

```
<wsdl:operation name="retirerCertificat">
  <wsdl:documentation>Interface de demande de retrait
</wsdl:documentation>
  <wsdl:input
    message="tns:requeteRetraitCertificat"></wsdl:input>
  <wsdl:output
    message="tns:reponseRetraitCertificat"></wsdl:output>
</wsdl:operation>
```

```
<wsdl:operation name="retirerCertificat">
  <wsdl:documentation>Interface de demande de retrait
</wsdl:documentation>
  <soap:operation soapAction="retirerCertificat" />
  <wsdl:input>
    <soap:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal" />
  </wsdl:output>
</wsdl:operation>
```

Voici les paramètres d'entrée de la requête de Retrait de certificat :

Donnée	Balise XML (Voir fichier XSD)	Objet métier	Type de contrôle	Contrôle du paramètre
<b>idNat_Tiers</b>	<b>&lt; idNatTiers&gt;</b>	Demande de certificat logiciel - Acteur	Présence	Facultatif
			Type	Chaîne de caractères (64 caractères)
<b>indiceRetrait</b>	<b>&lt; indiceRetrait&gt;</b>	Produit - Indice de retrait Web Service	Présence	Obligatoire
			Type	Chaîne de caractères (20 caractères)
<b>codeRevocation</b>	<b>&lt; codeRevocation&gt;</b>	Produit - Code revocation	Présence	Obligatoire
			Type	Chaîne de caractères (64 caractères)

Tableau 13 : Paramètres d'entrée du retrait de certificat

## 15.2 Transmission du certificat

La plateforme IGC-Santé transmet le certificat au système externe dans la réponse Web-Service qui est décrite dans le tableau suivant :

Réponse Web Service	Balise XML (Voir fichier XSD)	Renseigné à partir de	
Paramètre		Objet Métier	Donnée ou valeur
statut	< statut>	-	« OK » ou code d'erreur
message	< message>	-	« » si la demande est validée ou le message associé au code d'erreur sinon
certificat	< certificat>	Produit - Certificat	Certificat encodé au format PEM base64

Tableau 14 : Paramètres de transmission du certificat

### Description du message de la réponse de Retrait de certificat dans le fichier WSDL :

```
<wsdl:message name="reponseRetraitCertificat">
  <wsdl:documentation>Reponse a la requete de demande de retrait
</wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:reponseRetraitCertificat"></wsdl:part>
</wsdl:message>
```

La Demande de certificat logiciel passe de l'état « Demande transmise » à l'état « **Demande close** ». Le Produit passe de l'état « Produit retiré » à l'état « **Produit actif** ».

Ces informations peuvent être consultées :

- En envoyant une demande de suivi (Voir partie « Suivi de l'activité ») : Champ **<etat>**
- Sur l'interface IHM Menu « **Suivi des demandes de produits** » et « **Suivi des certificats** » Onglet « **Historique** ». (Voir Guide d'utilisation IHM Ref [1])

### Exemple de Suivi des demandes de Certificats :

Numéro	Numero demande	Canal	Date	Code action	Etat demande	Type acteur	Acteur
1	1	WS	17/12/2015 14:24	ACT_DCL_001	Enregistrée	Mandataire	ADJOINTPHARM RPPS PASCALINE (89970002
5	1	WS	17/12/2015 14:24	ACT_DCL_005	Validée	Mandataire	ADJOINTPHARM RPPS PASCALINE (89970002
9	1	SYSTEM	17/12/2015 14:25	ACT_JGC_003	Transmise	PFCNG-MG	
10	1	WS	17/12/2015 14:25	ACT_RET_003	Close	Mandataire	ADJOINTPHARM RPPS PASCALINE (89970002

Figure 39 : Exemple Suivi des demandes de Certificats - Transmission

### Exemple de Suivi de Certificats :

Numéro	Numero produit	Canal	Date	Code action	Etat produit	Type acteur	Acteur
1	1	WS	17/12/2015 14:24	ACT_DCL_001	Demandé	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)
5	1	WS	17/12/2015 14:24	ACT_DCL_005	À retirer	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)
9	1	WS	17/12/2015 14:25	ACT_RET_006	Retiré	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)
10	1	WS	17/12/2015 14:25	ACT_RET_003	Actif	Mandataire	ADJOINTPHARM RPPS PASCALINE (899700027230)

Figure 40 : Exemple Suivi des Certificats - Transmission

### Aperçu de la transmission de certificat sous format XML :



## 15.3 Notifications en lien avec le retrait de certificat

Une fois le certificat retiré, les notifications suivantes sont envoyées :

- **Notification du retrait d'un certificat** : Envoyée à la personne dont l'email a été renseigné dans le champ <mailDemandeur>.



Figure 44 : Notification de retrait de certificat - Acteur

Objet de l'email : « Agence du numérique en santé - Produits de Certification >>> Confirmation du retrait du certificat <Nom AC émettrice> / <N° de série du certificat> »

- **Notification du retrait d'un certificat** : Envoyée à la personne dont l'email a été renseigné dans le champ <mailPersonneAInformer>.



Figure 45 : Notification du retrait de certificat - Personne à informer

Objet de l'email : « [POUR INFORMATION] Agence du numérique en santé - Produits de Certification >>> Confirmation du retrait du certificat <Nom AC émettrice> / <N° de série du certificat> »

## 15.4 Cas non passants

- **Exemple 1 :**

L'utilisateur qui effectue le retrait de certificat n'est pas celui qui a effectué la demande.

En effet, l'acteur doit être le même entre la demande et le retrait du certificat → La demande de retrait ne doit pas aboutir.

Voici le XML généré :

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header><SOAP-ENV:Header><X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#"><SignatureValue><KeyInfo><X509Data><X509Certificate><X509Certificate></X509Certificate></X509Data></SignatureValue></X509Certificate></Header><SOAP-ENV:Body><requeteRetraitCertificat xmlns="http://schemas.xmlsoap.org/soap/envelope/"><indiceRetrait>811</indiceRetrait><codeRevocation>Azerty1234$$</codeRevocation></requeteRetraitCertificat></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Figure 46 : Retrait de certificat - Cas non passant 1 - Requête

La signature du XML contient l'identité de l'utilisateur qui fait la demande de retrait. Lors de la vérification de la demande de retrait, la plateforme IGC-Santé vérifie que l'identité de l'utilisateur est la même que pour la demande de certificat : si ce n'est pas le cas, la demande de retrait est en erreur.

Voici la réponse :

```

<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRetraitCertificat>
      <statut>WSMG-00000030</statut>
      <message>Vous n'êtes pas l'acteur de la demande de certificat logiciel. Votre demande est refusée.</message>
    </ns3:reponseRetraitCertificat>
  </ns2:Body>
</ns2:Envelope>
  
```

Figure 47 : Retrait de certificat - Cas non passant 1 - Réponse

Détail de l'erreur :

```

<statut>WSMG-00000030</statut>
<message>Vous n'êtes pas l'acteur de la demande de certificat logiciel. Votre demande est refusée.</message>
  
```

Figure 48 : Retrait de certificat - Cas non passant 1 - Statut de la réponse

Le statut contient le code de l'erreur : **WSMG-00000030**.

Le message contient le message d'erreur : **Vous n'êtes pas l'acteur de la demande de certificat logiciel. Votre demande est refusée.**

- Exemple 2 :

L'indice de retrait saisi pour le retrait du certificat est erroné et inconnu. La demande de retrait ne doit pas aboutir.

Voici le XML généré :

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:
  3nP4oRVzpiixYm58+I10TOP5u6hdT7OJar03tL3wtcWJB77OV8gI/US7AFxTSrFR426V9wXNxeB4
  AkJR1SRJIMekpQAN4oYwZm3js25Kg1H+pLRZHMxXCZKGdtEcJWZ+ZOFroxDe44DBStJQ6UOL/NDAJ
  RzgdW0i2KsxbpLbzaA3i1kyHrIpOkRYNuaamQqU33/gcqnno7SJ0t3ST2HC/qmJoPD2b0Stfzszg
  w1hMHG7WAe8MDFyR1nm0C+O75Ue9JrvIHJ8rlw==</ds:SignatureValue><ds:KeyInfo><ds:X509Data><d
  EwRURVNUMRcwfQYDvQQLEw5URVNU1FNUU1VDVFVSRTEWMBQGA1UEAxMNVEVTVCBDETEFTU0UtMjAe
  Fw0xNTAxMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
  VEVTVDDETMBEGA1UEBxQKUGFyaXMgKDC1KTEYMBYGA1UECzMpMzAwMDAwMDAwMDAwMDAwMDAwMDAw
  VQQDEXg1MDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
  ODAAwMDEwDgYDVOQQqFADSEFSTEVMTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7o
  fmwBVy25dW4gFOaQCJFTi+93+H/5Z2Yxd1QQ/ygEORN1qKd592wUQyPjj11bkZjFtLME/NGT7Jbk
  FhobgfBBGZi1jjnKYhW694KThwT5B7oy/1vYrmJ8Qv7oF2NMkpNUhKxwalBOP/doK9idetpKL9sF
  ElgT/ybjode0GvQ9JDW2QPT+6LcuCHQi jrQ9GKGU9CNH40OgL5cfkbwI+3Wssmio3t1bs2EwHMG2
  v4DxmDsZkRGPzUTkuAJXQcR1Iydp8LOYORMumJzzUza71YBmorOgLEE4Gp04qdC4qQKQzb6HivIO
  3+Q5Ct1074DZDYW5sybwe5rLk3oD0yZr4QIDAQABo4ICSjCCAkywHwYDVR0jBBgwFoAURHISicJy
  d5vbCjuPSjKuTiyvwHYwHQYDVR0OBBYEFPT9jqif33IOKXHZKY0Z1y jI1bZ8MA4GA1UdDwEB/wQE
  AwIGwDATBgNVHSUEDDAKBggrBgEFBQcDBDARBgNVHRAEJDAIga8yMDE1MDEwMTAwMDAwMDAwMDAw
  MjAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMD
  HR8EgbIwga8wO6A5oDeGNWh0dHA6Ly9hbm51YWlyZS5naXA6Y3BzLmZyL2Nybc90ZXN0L1RFU1Qg
  Q0xBU1NFRTIuY3JsmHCgbqBshmpsZGFwOi8vYW5udWFpcMUuZ21wLWwncy5mci9jbj10ZXN0IGNs
  YXNzZS0yLG91PXRlc3Qgc3RydwN0dXJ1LG89dGVzdCcxjPWZyP2N1cnRpZm1jYXRlcmlzL2V2b2NhZGlV
  bmhpc3Q7YmluYXJ5J5MHUGA1UdLgRuMGwwaGBooGaGZGxkYXA6Ly9hbm51YWlyZS5naXA6Y3BzLmZy
  L2NuPXRlc3QgY2xhc3N1LTI1sb3U9dGVzdCBzdHJ1Y3R1cmUscz10ZXN0LGM9ZnI/ZGVsdGFyZXZv
  Y2F0aW9ubGlzdDtiaW5hcnkwEQYJYIZIAYb4QgEBBBAQDAgUGMCMGCCqBgFAAQAIDBBcTFTTgmMjUw
  MDAwMDEwMjUwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
  hvCNAQEFBQADggEBAFWaq+frk5Dcie76vQFQ4qLr6VhdD1u828M77Q1+tT4erqkP4gydHMD13Sg
  m0wxFeS+xPwOzJqWYCLXuYgHr3oTckLroE66+XX2uQHMuQsT51HUSgGacrIeIid4ysGz19ZGWfYA
  Nego25OyE6kejyocqTRqLrK1OCJEW6ys9Ecgf8LgaO7NM2qQadFYUqNgFnbDrc23bx1PPg3Lm+F
  wUBFJYXb4C15sI7Xjsur3blcHcfbYta5cdHXja0UbuU4AGJ3MHRbHGEqb8QaNLwOz0OY6XmsD+Wgr
  G3keFXdtSfKKVDeJp+fcXzV3Ale7xmBVspjOewJwwQoMadFyUbwB8Qw==</ds:X509Certificate></ds:X509D
  <indiceRetrait>1749</indiceRetrait>
  <codeRevocation>Azerty1234$$</codeRevocation>
</ws:requeteRetraitCertificat></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Figure 49 : Retrait de certificat - Cas non passant 2 - Requête



L'indice de retrait 1749 n'existe pas.

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRetraitCertificat>
      <statut>WSMG-00000027</statut>
      <message>Indice de retrait inconnu. Veuillez renouveler votre demande.</message>
    </ns3:reponseRetraitCertificat>
  </ns2:Body>
</ns2:Envelope>
```

Figure 50 : Retrait de certificat - Cas non passant 2 - Réponse

Message d'erreur : Indice de retrait inconnu. Veuillez renouveler votre demande.

Le statut contient le code de l'erreur : **WSMG-00000027**.

Le message contient le message d'erreur : **Indice de retrait inconnu. Veuillez renouveler votre demande.**

## 16 Révocation de certificat

Le WS PFNCG-MG permet de demander la révocation de n'importe quel certificat logiciel quelle que soit l'interface utilisée lors de la demande de création. Une demande de révocation ne concerne **qu'un seul certificat**.

### 16.1 Demande de révocation d'un certificat

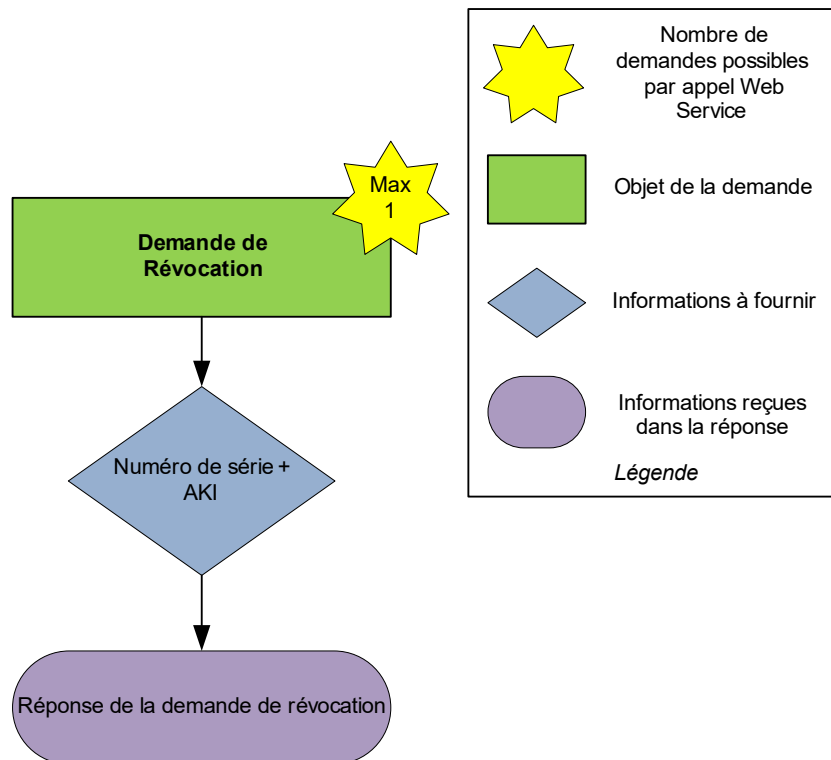
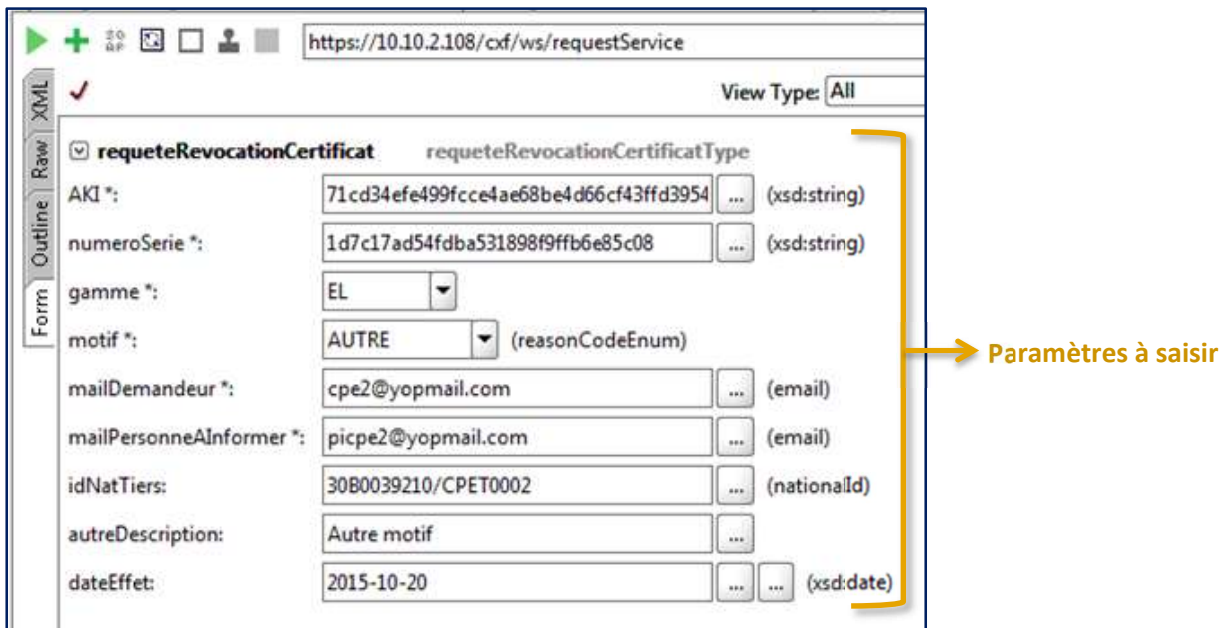


Figure 51 - Demande de révocation d'un certificat

Le système externe appelant envoie un appel Web Service de demande de révocation à la plateforme IGC-Santé.

Les paramètres d'entrée suivants sont saisis pour la demande de révocation :



Paramètre	Valeur saisie	Type
AKI *	71cd34efe499fccc4ae68be4d66cf43ffd3954	(xsd:string)
numeroSerie *	1d7c17ad54fdb531898f9ffb6e85c08	(xsd:string)
gamme *	EL	
motif *	AUTRE	(reasonCodeEnum)
mailDemandeur *	cpe2@yopmail.com	(email)
mailPersonneAInformer *	picpe2@yopmail.com	(email)
idNatTiers	30B0039210/CPET0002	(nationalId)
autreDescription	Autre motif	
dateEffet	2015-10-20	(xsd:date)

Figure 52 : Révocation de certificat - Exemple SOAP UI

- ➔ Il est possible de choisir la date d'effet de la révocation dans le champ dateEffet
- ➔ Un motif de révocation est également demandé dans le champ motif.
  
- ➔ MailDemandeur : concerne la personne qui fait la demande. Ce champ est obligatoire. Il permet de recevoir les notifications par email des actions réalisées ou à réaliser (confirmation de la demande, mise à disposition du certificat...)
- ➔ MailPersonneAInformer : élément obligatoire à renseigner. Il permet de recevoir les notifications par email à titre informatif des actions réalisées. (confirmation de la demande, l'information de la mise à disposition du certificat auprès de l'acteur...)
- ...

**Aperçu de la demande de révocation de certificat sous format XML :**

*(Voir exemple de fichier XML en Annexe 1)*

```

<ds:SignatureValue>IRHwgeK11eLBTBtDQQ7NSNQzXGSN4SWIgbCrA70HwNfwCdtbSpGA+BfY0s9u5P+8oLYfe5IjXPa
spnPI7NE2o+BhS//vFRi+RTbgQD3piEQE1cgW/xWoMiUEi541IqOP2Cb8Pw7OrkLHR2iWio8jz0y
1bdiGF7CknzxwD+wboU/V9FrzU0mMAFHdFY9rqWbKF4dwhx1m3Bx/1nVVLyNipHLOY34peGqIHm
vmB16lvxIPdRSWlvrBF07cqlEiJyHxGQ6E80uikTtwr1esn3BXNpwGJ89w6wiGwNHe5cc5c1vDT
Aiv+cjeHQ8ldcZTdNk5HJ3j20epQR55An2BzZg==</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509SubjectName>CN=50000000028969/CPAT0002 + OID.2.5.4.4=AGENT0000028960002 + OID.2.5.4.42=DENISE,
    <ds:X509Certificate>MIIFrzCCBJegAwIBAgIDW6iqMAOGCSqGSIB3DQEBBQUAME0xCzAJBgNVBAYTAkZSMQJwCwYDVQQK
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</SOAP-SEC:Signature>
</SOAP-ENV:Header>
<SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
  <ws:requeteRevocationCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
    <AKI>71cd34efe499f0ce4ae68be4d66cf43ffd3954b8</AKI>
    <numeroSerie>1d7c17ad54fdb5310566c1889b63506</numeroSerie>
    <gamme>EL</gamme>
    <motif>AUTRE</motif>
    <mailDemandeur>cpe2@yopmail.com</mailDemandeur>
    <mailPersonneAInformer>picpe2@yopmail.com</mailPersonneAInformer>
    <idNatTiers>30B0039210/CPET0002</idNatTiers>
    <autreDescription>Autre motif</autreDescription>
    <dateEffet>2015-10-21</dateEffet>
  </ws:requeteRevocationCertificat>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Figure 53 : Révocation de certificat - Exemple de requête

On retrouve les informations saisies dans le **corps du XML** généré :

```

<ws:requeteRevocationCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
  <AKI>71cd34efe499f0ce4ae68be4d66cf43ffd3954b8</AKI>
  <numeroSerie>1d7c17ad54fdb5310566c1889b63506</numeroSerie>
  <gamme>EL</gamme>
  <motif>AUTRE</motif>
  <mailDemandeur>cpe2@yopmail.com</mailDemandeur>
  <mailPersonneAInformer>picpe2@yopmail.com</mailPersonneAInformer>
  <idNatTiers>30B0039210/CPET0002</idNatTiers>
  <autreDescription>Autre motif</autreDescription>
  <dateEffet>2015-10-21</dateEffet>
</ws:requeteRevocationCertificat>

```

Figure 54 : Révocation de certificat - Requête - Détails

**Description du message de la requête de Révocation de certificat dans le fichier WSDL :**

```
<wsdl:message name="requeteRevocationCertificat">
  <wsdl:documentation>Requete de demande de revocation
</wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:requeteRevocationCertificat"></wsdl:part>
</wsdl:message>
```

**Description de l'opération de Révocation de certificat dans le fichier WSDL :**

```
<wsdl:operation name="revoquerCertificat">
  <wsdl:documentation>Interface de demande de revocation
</wsdl:documentation>
  <wsdl:input
    message="tns:requeteRevocationCertificat"></wsdl:input>
  <wsdl:output
    message="tns:reponseRevocationCertificat"></wsdl:output>
</wsdl:operation>
```

```
<wsdl:operation name="revoquerCertificat">
  <wsdl:documentation>Interface de demande de revocation
</wsdl:documentation>
  <soap:operation soapAction="revoquerCertificat" />
  <wsdl:input>
    <soap:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal" />
  </wsdl:output>
</wsdl:operation>
```

Voici les paramètres d'entrée de la requête de Révocation de certificat :

Donnée	Balise XML (Voir fichier XSD)	Objet métier	Type de contrôle	Contrôle du paramètre
idNat_Tiers	< idNatTiers>	Demande de révocation - Acteur	Présence	Facultatif
			Type	Chaîne de caractères (maximum 64 caractères)
AKI	< AKI>	Produit - AKI	Présence	Obligatoire
			Type	Chaîne de caractères (maximum xx caractères)
Numéro de série	< numeroSerie>	Produit - Numéro de série	Présence	Obligatoire
			Type	Chaîne de caractères (maximum xx caractères)
gamme	< gamme>	-	Valeurs possibles	« EL »
			Présence	Obligatoire
			Type	Chaîne de caractères (maximum 2 caractères)
motifcode	< motif>	Demande de révocation - Motif	Valeurs possibles	« VOL », « PERTE », « FIN_DACTIVITE », « AUTRE »
			Présence	Obligatoire
			Type	Chaîne de caractères (maximum 14 caractères)
autredesc	< autreDescription>	Demande de révocation - Motif autre	Présence	Obligatoire si le motif de révocation est « AUTRE » Interdit pour les motifs de révocation »VOL », « PERTE » et « FIN_DACTIVITE »
			Type	Chaîne de caractères (maximum 150 caractères)
dateEffet	< dateEffet>	Demande de révocation - Date révocation	Présence	Facultatif
			Type	Date
			Format	YYYY-MM-DD
mailDemandeur	< mailDemandeur>	Demande de révocation - Email Acteur	Présence	Obligatoire
			Type	Chaîne de caractères (maximum 150 caractères)
			Format	Compatible avec la RFC5322
mailInformer	< mailPersonneA Informer>	Demande de révocation - Email Notification	Présence	Obligatoire
			Type	Chaîne de caractères (maximum 150 caractères)
			Format	Compatible avec la RFC5322

Tableau 15 : Paramètres d'entrée de la requête de révocation

## 16.2 Réponse de la demande

La plateforme IGC-Santé envoie par réponse au Web-Service l'accusé de réception de la demande :

Réponse Web Service	Balise XML (Voir fichier XSD)	Renseigné à partir de	
		Objet Métier	Donnée ou valeur
<b>statut</b>	<b>&lt; statut&gt;</b>	-	« OK » ou code d'erreur
<b>message</b>	<b>&lt; message&gt;</b>	-	« » si la demande est acceptée ou le message associé au code d'erreur sinon

Tableau 16 : Paramètres de réponse de révocation

### Description du message de la réponse de Révocation de certificat dans le fichier WSDL :

```
<wsdl:message name="reponseRevocationCertificat">
  <wsdl:documentation>Reponse a la requete de demande de
  revocation
  </wsdl:documentation>
  <wsdl:part name="parameters"
  element="tns:reponseRevocationCertificat"></wsdl:part>
</wsdl:message>
```

### Aperçu de la réponse de la demande de révocation sous format XML :

*(Voir exemple de fichier XML en Annexe 1)*

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRevocationCertificat>
      <statut>OK</statut>
      <message/>
    </ns3:reponseRevocationCertificat>
  </ns2:Body>
</ns2:Envelope>
```

Figure 55 : Révocation de certificat - Exemple de réponse

On retrouve dans le corps du fichier le **statut** de la réponse : **OK**

```
<ns2:Body>
  <ns3:reponseRevocationCertificat>
    <statut>OK</statut>
    <message/>
  </ns3:reponseRevocationCertificat>
</ns2:Body>
</ns2:Envelope>
```

Figure 56 : Révocation de certificat - Réponse - Statut de la réponse

Le Produit passe de l'état « Produit actif » à l'état « **Produit révoqué** ».

Ces informations peuvent être consultées :

- En envoyant une demande de suivi (Voir partie « Suivi de l'activité ») : Champ **<etat>**
- Sur l'interface IHM Menu « **Suivi des demandes de révocation** » et « **Suivi des certificats** » Onglet « **Historique** ». (Voir Guide d'utilisation IHM Ref [1])



## 16.3 Notifications en lien avec la révocation

Lorsque le certificat est révoqué, des notifications sont envoyées afin d'informer des actions effectuées.

- **Notification de la révocation d'un certificat** : Envoyée à la personne dont l'email a été renseigné dans le champ `<mailDemandeur>`.



Figure 57 : Notification de la révocation de certificat - Acteur

Objet de l'email : « **Agence du numérique en santé - Produits de Certification >>> Confirmation de la révocation du certificat <Nom AC émettrice> / <N° de série du certificat> »**

- **Notification de la révocation d'un certificat** : Envoyée à la personne dont l'email a été renseigné dans le champ `<mailPersonneAInformer>`.



Figure 58 : Notification de la révocation de certificat - Personne à informer

Objet de l'email : « [POUR INFORMATION ]Agence du numérique en santé - Produits de Certification >>> Confirmation de la révocation du certificat *<Nom AC émettrice>* / *<N° de série du certificat>* »

## 16.4 Cas non passants

- **Exemple 1 :**

La demande de révocation est envoyée avec un numéro de série erroné. → La demande de révocation ne peut pas aboutir.

Voici le XML généré (*la signature a été tronquée pour plus de visibilité dans le document*) :

```

<ds:SignatureValue>PHwA5fS1BK50Wdlg3g1999t4upP2tIfJJ94ymPE2g8PrXBnfc0102vHBLCKLYz6/+h0qrujGL8ua
CEPF68DQPmpoDqDwyb15141+5L1+XegANNeCeTspr2d4021TP2eAk5GVEq837CihzppfmJ+qSFUv
kAKqIWcGF3LJ9rZUwgnSHdehefqKvV9+w8K2cUhVcFmxRYCE1FjfhQH717yf4S94+4Vua0S0w42
620TwW16uKzNCi6S/T/DR3DadJzsPcNWgvzdLZS2wbrokaQt0ZxtndvMVbbrCkfxo6wXa2EQJxJ
lzi49hAzZe4/+Uh4GbVQ1vyVTGH/Ija3eVRQfQ=
```

```

</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509SubjectName>CN=00B9804408 + OID.2.5.4.4=MANIPCH0440 + OID.2.5.4.42=PATRICK, OU=Manipulateur ERM,
    <ds:X509Certificate>MIIFozCCBIugAwIBAglDw6gQMA0GCSqGSIb3DQEBBQUAMFExCzAJBgNVBAYTAKZSMQ0wCwYDVQQK
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</SOAP-SEC:Signature>
</SOAP-ENV:Header>
<SOAP-ENV:Body SOAP-SEC:id="Body" xmlns:SOAP-SEC="http://schemas.xmlsoap.org/soap/security/2000-12">
  <ws:requeteRevocationCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
    <AKI>c049a9149982cedd16148490c63bcb1fdf8791fd</AKI>
    <numeroSerie>1234567890</numeroSerie>
    <gamme>EL</gamme>
    <motif>VOL</motif>
    <mailDemandeur>cps11@yopmail.com</mailDemandeur>
    <mailPersonneAInformer>picps11@yopmail.com</mailPersonneAInformer>
  </ws:requeteRevocationCertificat>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Figure 59 : Révocation de certificat - Cas non passant 1 - Requête

Le numéro de série 1234567890 n'existe pas.

Voici la réponse :

```

<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRevocationCertificat>
      <statut>WSMG-00000008</statut>
      <message>Erreur lors la recherche de certificat. Veuillez vérifier et renouveler votre demande.</message>
    </ns3:reponseRevocationCertificat>
  </ns2:Body>
</ns2:Envelope>

```

Figure 60 : Révocation de certificat - Cas non passant 1 - Réponse

Le statut contient le code de l'erreur : **WSMG-00000008**.

Le message contient le message d'erreur : **Echec lors de la recherche de certificat. Veuillez vérifier et renouveler votre demande.**

- **Exemple 2 :**

L'utilisateur fait une demande de révocation d'un certificat qui n'est pas encore actif : un certificat non retiré. → La demande de révocation ne doit pas aboutir.

Voici le XML généré (*la signature a été tronquée pour plus de visibilité dans le document*) :

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Header><SOAP-SEC:Signature SOAP-ENV:actor="some-URI"
<ds:SignatureValue>XU/emzJucGQ+aICxsud9YRraypAX/7kf9WjXHWKRSJmT74ojK601VHxdaIipwnLVa5h0dGFu930y
9VRdi6RCmVnXlmuOpdHEMi4CSQhz9HTjTGedovr6p14DEwbNWQX7CSQh5r3oVIJMpLMggqD1KFO/
XgMQjv2CjChEhbTnVLA5+uhV/xTLWdJs/yqwAbH3RQnSy9s21+iJSmMjTgQLG1dEA/Ywt45WzRtQ
/cTZTtueJocMyoXpEKKfr7WeSJ7zb2H1/mzi+3/OSQLnmVjgtZopAQH64XPLmXGCj0Kqa40IeZiHu
mqqJ8tMk1XhFfqNK+PPfpf9s4BQGYBQ8ndsQ==</ds:SignatureValue><ds:KeyInfo>
<ds:X509Data><ds:X509SubjectName>CN=950B000409 + OID.2.5.4.4=REMPLEXETUSAGE0040 + OID.2.5.4.42=MARYSE, OU=Sage-femme en formation, O=TEST,
</ws:requeteRevocationCertificat xmlns:ws="http://www.pfcng.in.com/WS/">
  <AKI>c049a9149982cedd16148490c63bcb1fd8791fd</AKI>
  <numeroSerie>49aa3433d672424e8c27f28af4c4dde6</numeroSerie>
  <gamme>EL</gamme>
  <motif>AUTRE</motif>
  <mailDemandeur>cpe2@yopmail.com</mailDemandeur>
  <mailPersonneAInformer>picpe2@yopmail.com</mailPersonneAInformer>
  <idNatTiers>950B000409</idNatTiers>
  <autreDescription>Autre motif</autreDescription>
  <dateEffet>2015-10-22</dateEffet>
</ws:requeteRevocationCertificat></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Figure 61 : Révocation de la demande - Cas non passant 2 - Requête

Le certificat correspondant n'est pas encore actif.

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRevocationCertificat>
      <statut>WSMG-00000012</statut>
      <message>Échec lors de l'enregistrement de la demande de révocation : Le produit n'est pas dans l'état "Produit actif" ou dans l'état "Produit retiré"
      Veuillez vérifier et renouveler votre demande.</message>
    </ns3:reponseRevocationCertificat>
  </ns2:Body>
</ns2:Envelope>
```

Figure 62 : Révocation de certificat - Cas non passant 2 - Réponse

Le statut contient le code de l'erreur : **WSMG-00000012**.

Le message contient le message d'erreur : **Echec lors de l'enregistrement de la demande de révocation : le produit n'est pas dans l'état « Produit actif » ou dans l'état « Produit retiré ». Veuillez vérifier et renouveler votre demande.**

## 17Renouvellement de certificat

### 17.1 Demande de renouvellement de certificat

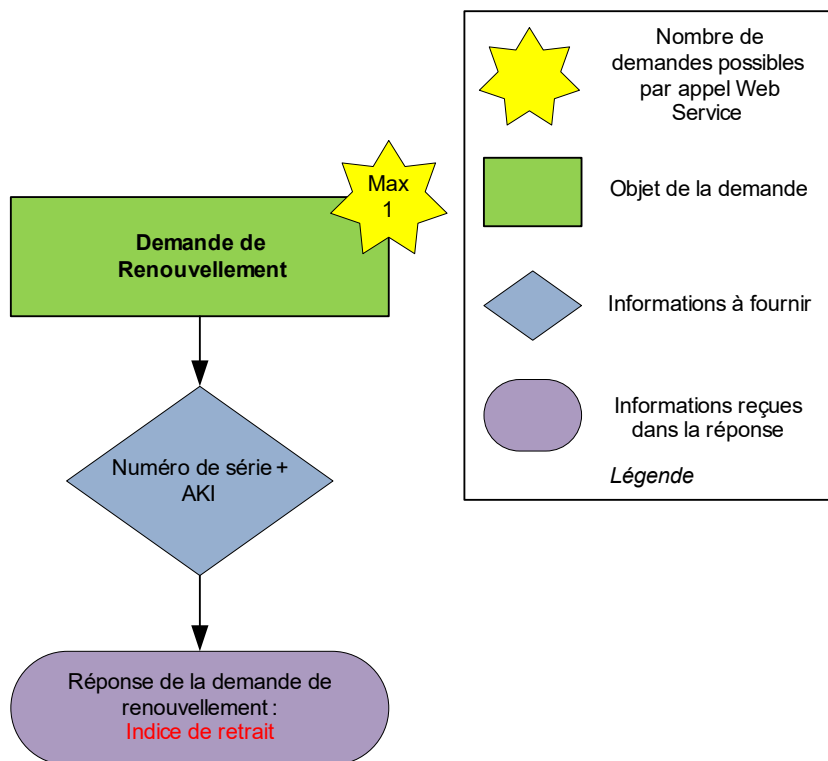
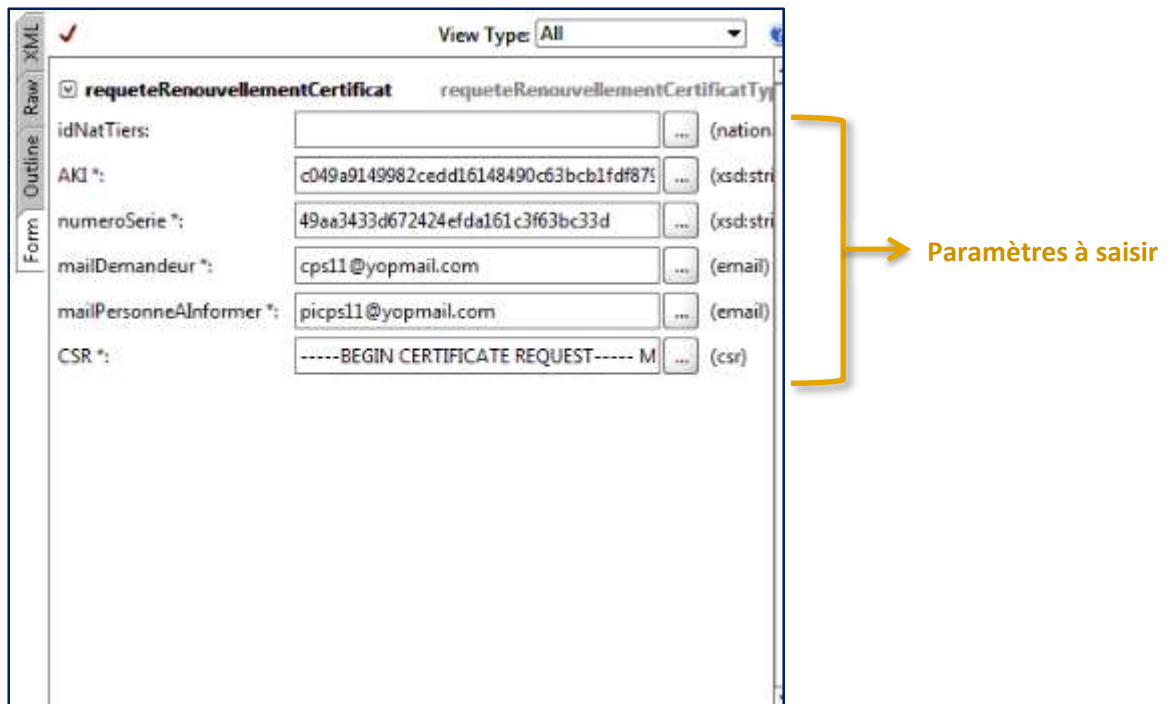


Figure 63 - Demande de renouvellement d'un certificat

Le système externe appelant envoie une demande de renouvellement pour **un seul certificat** par le canal Web-Services. La demande de renouvellement comporte la référence unique de l'ancien certificat (**couple AKI et numéro de série**), ainsi qu'une nouvelle CSR.

Les paramètres d'entrée suivants sont saisis pour la demande de renouvellement :



View Type: All

requeteRenouvellementCertificat    requeteRenouvellementCertificatTyp

idNatTiers:	<input type="text"/>	...	(nation
AKI *:	c049a9149982cedd16148490c63bcb1fd875	...	(xsd:stri
numeroSerie *:	49aa3433d672424efda161c3f63bc33d	...	(xsd:stri
mailDemandeur *:	cps11@yopmail.com	...	(email)
mailPersonneAInformer *:	picps11@yopmail.com	...	(email)
CSR *:	-----BEGIN CERTIFICATE REQUEST----- M	...	(csr)

Paramètres à saisir

Figure 64 : Renouvellement de certificat - Exemple SOAP UI

- ➔ IdNatTiers : Ce champ non obligatoire permet d'identifier un tiers avec son identifiant national
- ➔ Aki : Identificateur de la clé du certificat à renouveler
- ➔ NumeroSerie : Numéro de série de la clé du certificat à renouveler
- ➔ MailDemandeur : Adresse email de la personne qui demande le renouvellement
- ➔ MailPersonneAInformer : Adresse email de la personne à informer.
- ➔ CSR : nouvelle CSR

**Qu'est-ce qu'une CSR :**

*La CSR contient des informations d'identifications du demandeur et la clé publique choisie par le demandeur. La clé privée correspondante n'est pas incluse dans le CSR, mais est utilisée pour signer numériquement la demande.*

*Le CSR peut être accompagné d'autres informations d'identification ou des preuves d'information requises par l'autorité de certification.*

La CSR est au **format PKCS#12**. Ce format permet de stocker clés privées et certificats dans un seul fichier chiffré.

Les informations présentes dans la CSR sont :

- Sujet constitué de :
  - Common Name (CN=)
  - Organisation (O=)
  - Pays (C=)
- Clé publique
- Signature de la CSR par la clé privée
  - Algorithme : sha256WithRSAEncryption
  - Valeur

Aperçu de la demande de renouvellement de certificat sous format XML :

(Voir exemple de fichier XML en Annexe 1)



Figure 65 : Renouvellement de certificat - Exemple de requête

On retrouve les informations saisies dans le corps du XML généré :



Figure 66 : Renouvellement de certificat - Réponse - Détails



```

<CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJzA
u+4KYQOTbEuaqJk6LRJGtrYnb0Iq62WMQxhYdcNy2gYgdqF8KikEfy/IsMXGVYIX
BjC8tmXRWLNz2S1zY2vPjmqPOYuiFb0QvtmlWduF0QQhe/tYT2IH8xS77fhsMQCB
MobMdHLMOhCkjd8QvMK0Itk+L4ZNWeYbZ2O5bV+OU1VWuZ3B6cXiolyoaVtmc0bU
bzIidXZrfsGLXHWB3GZSbNHUNy0kmhNoHsbTIv8BBHRLRLPHnrBO/0w/qpw11fB9
kSp1j1YXRQRufXPWC92JdK07gcxTcGP2quyJC4JX6dn7+JJN3Vn3WrFc00JJmO+9
aTsRwRAuIx7RTVeaGgUCAwEAATANBgkqhkiG9w0BAQsFAADCAQEAYejIc4WMC4Pd
BnoOXVdvQuxnQmJlorKARYMIXkLHB+EpPj07ZRSuWP7z13OT41rJnjoUqF+ZKbJj
u3z7QQY4QPq7i7s9uHoldYAZsFjj8HDF/h+ezo5MbaTRLpJ5wM4u4hAdIjEy1uEu
GVuPQGlk6RxxqOz+qbKuyxZKReRZsf+dLc/WOm/Z4b2CWREzbjpy1LJAmRc0LIy1
LXD+AE68q3rRj3lqJeHAS1OZbhEJCAMOF5o2U9/P/faj7jf/3kLY6SzM9sb+vdBq
T7fEhACj11WPrSTT8aGUT+3oxdV4zFsLxnVhyrxJUTkWarN1HhjugDBNGp5dtPLJ
4dwx5yAS+g==
-----END CERTIFICATE REQUEST-----
</CSR>

```



Figure 67 : Renouvellement de certificat - Réponse - CSR

### Description du message de la requête de Renouvellement de certificat dans le fichier WSDL :

```

<wsdl:message name="requeteRenouvellementCertificat">
  <wsdl:documentation>Requete de demande de renouvellement
  </wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:requeteRenouvellementCertificat"></wsdl:part>
</wsdl:message>

```

### Description de l'opération de Renouvellement de certificat dans le fichier WSDL :

```

<wsdl:operation name="renouvelerCertificat">
  <wsdl:documentation>Interface de demande de
  renouvellement
  </wsdl:documentation>
  <wsdl:input
    message="tns:requeteRenouvellementCertificat"></wsdl:input>
  <wsdl:output
    message="tns:reponseRenouvellementCertificat"></wsdl:output>
</wsdl:operation>

```

```

<wsdl:operation name="renouvelerCertificat">
  <wsdl:documentation>Interface de demande de
  renouvellement
  </wsdl:documentation>
  <soap:operation soapAction="renouvelerCertificat" />
  <wsdl:input>
    <soap:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal" />
  </wsdl:output>
</wsdl:operation>

```

Voici les paramètres d'entrée de la requête de Renouvellement de certificat :

Donnée	Balise XML (Voir fichier XSD)	Objet métier	Type de contrôle	Contrôle du paramètre
idNat_Tiers	< idNatTiers>	Demande de certificat logiciel - Acteur	Présence	Facultatif
			Type	Chaîne de caractères (64 caractères)
AKI	< AKI>		Présence	Obligatoire
			Type	Chaîne de caractères (maximum xx caractères)
Numéro de série	<numeroSerie >		Présence	Obligatoire
			Type	Chaîne de caractères (maximum xx caractères)
mailInformer	< mailPersonne AInformer>	Demande de certificat logiciel - Email Notification	Présence	Obligatoire
			Type	Adresse email
			Format	Compatible avec la RFC5322
CSR	< CSR>	Produit - CSR	Présence	Obligatoire
			Type	Chaîne de caractères (maximum 768 caractères)
			Format	Base 64 Voir la RFC2986 associée à PKCS10
mailDemandeur	< mailDemandeur >	Demande de certificat logiciel - Email Acteur	Présence	Obligatoire
			Type	Adresse email
			Format	Compatible avec la RFC5322

**Tableau 17 : Paramètres d'entrée de la requête de renouvellement de certificat**

Les autres informations présentes sur une demande de création de certificat (offre, gamme, IdNat de la structure, IdNat du bénéficiaire, nom d'applicatif, FQDN, usage, UPN, mailSujet) seront récupérées à partir du certificat à renouveler.

## 17.2 Réponse de la demande de renouvellement

La réponse Web Service est décrite dans le tableau suivant :

Réponse Web Service	Balise XML (Voir fichier XSD)	Renseigné à partir de	
		Objet Métier	Donnée ou valeur
<b>indiceRetrait</b>	<b>&lt; indiceRetrait&gt;</b>	Produit	Indice de retrait Web Service
<b>statut</b>	<b>&lt; statut&gt;</b>	-	« OK » si la demande est validée, le code d'erreur sinon
<b>message</b>	<b>&lt; message&gt;</b>	-	« » si la demande est acceptée ou le message associé au code d'erreur sinon

Tableau 18 : Paramètres de réponse de renouvellement de certificat

### Description du message de la réponse de Renouvellement de certificat dans le fichier WSDL :

```
<wsdl:message name="reponseRenouvellementCertificat">
  <wsdl:documentation>Reponse a la requete de demande de
  renouvellement
  </wsdl:documentation>
  <wsdl:part name="parameters"
  element="tns:reponseRenouvellementCertificat"></wsdl:part>
</wsdl:message>
```

### Aperçu de la réponse pour le renouvellement de certificat sous format XML :

*(Voir exemple de fichier XML en Annexe 1)*

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
]
  <ns2:Body>
]
  <ns3:reponseRenouvellementCertificat>
    <statut>OK</statut>
    <message/>
    <indiceRetrait>819</indiceRetrait>
  </ns3:reponseRenouvellementCertificat>
</ns2:Body>
</ns2:Envelope>
```

Figure 68 : Renouvellement de certificat - Exemple de réponse

On retrouve dans le corps du fichier le **statut** de la réponse : **OK**

```
<statut>OK</statut>
```

Figure 69 : Renouvellement de certificat - Réponse - Détail du statut

Et l'**indice de retrait** (obligatoire pour le retrait du certificat) :

```
<indiceRetrait>819</indiceRetrait>
```

Figure 70 : Renouvellement de certificat - Réponse - Indice de retrait

Si tous les paramètres sont vérifiés avec succès, pour chaque renouvellement de certificat logiciel :

- La Demande de certificat logiciel reste à l'état « **Demande validée** »
- Le Produit reste à l'état « **Produit à retirer** »

Si une erreur survient à cette étape, pour toutes les demandes :

- La Demande de certificat logiciel passe de l'état « Demande validée » à l'état « **Demande non traitée** »
- Le Produit passe de l'état « Produit à retirer » à l'état « **Produit annulé** »

*Ces informations peuvent être consultées :*

- *En envoyant une demande de suivi (Voir partie « Suivi de l'activité ») : Champ <etat>*
- *Sur l'interface IHM Menu « **Suivi des demandes de produits** » et « **Suivi des certificats** » Onglet « **Historique** ». (Voir Guide d'utilisation IHM Ref [1])*

## 17.3 Notifications en lien avec le renouvellement

Quand l'utilisateur effectue un renouvellement de certificat par Web Service, il reçoit ensuite des notifications par email. (Ainsi que la personne à informer)

- **Notification de Validation de la demande (PS, PRO, CONF, SIGN)** : Envoyée à la personne dont l'email a été renseigné dans le champ **<mailDemandeur>**.

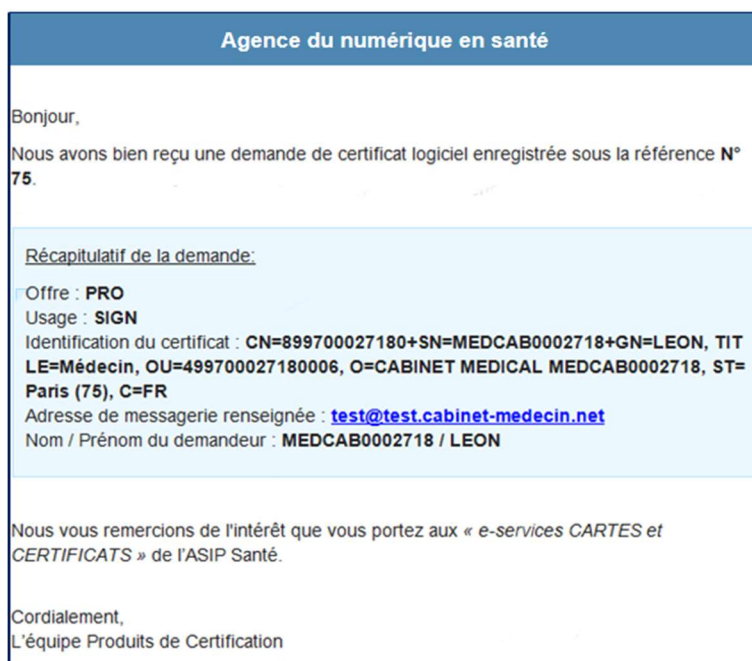


Figure 71 : Notification de validation de la demande - Acteur

**Objet de l'email** : « **Agence du numérique en santé - Produits de Certification** >>> Confirmation de la demande **<N° de demande interne plateforme IGC-Santé >** »

- **Notification de Validation de la demande (PS, PRO, CONF, SIGN)** : Envoyée à la personne dont l'email a été renseigné dans le champ **<mailPersonneAInformer>**.

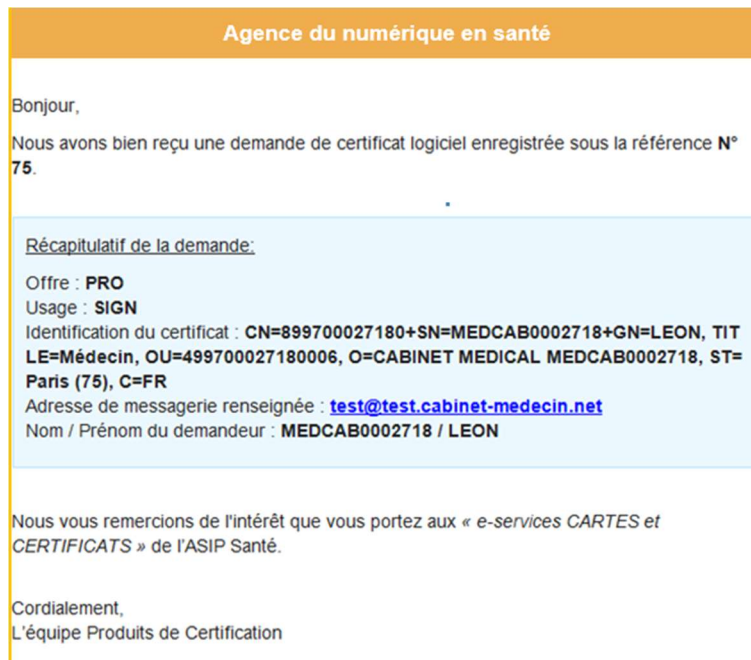


Figure 72 : Notification de la validation de la demande - Personne à informer

Objet de l'email : « [POUR INFORMATION] Agence du numérique en santé - Produits de Certification >>> Confirmation de la demande <N° de demande interne plateforme IGC-Santé > ».

## 17.4 Cas non passants

- **Exemple 1 :**

La demande de renouvellement est correcte mais l'utilisateur envoie une CSR déjà utilisée pour un autre certificat.

→ La demande de renouvellement ne doit pas aboutir.

Voici le XML généré :

```
<AKI>c049a9149982cedd16148490c63bcb1fd8791fd</AKI>
<numeroSerie>49aa3433d672424e9704d5aa2e954397</numeroSerie>
<mailDemandeur>cps11@yopmail.com</mailDemandeur>
<mailPersonneAInformer>picps11@yopmail.com</mailPersonneAInformer>
<CSR>-----BEGIN CERTIFICATE REQUEST-----
MIICQzCCASsCAQAwADCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMVi
N6OXp55vep1yBn69cSLLnXTaCOFD1/cqBrSgta5dJ/s+61eNMDCHBycXYMPvKq5R
wFwpi41Lm1qui70zKHEofsPY1suYnZGW9J69e/gR8vUVXliJOL3ROiePd2iC/j4w
npw4z5uLkIVWhXx2/L/4buckpPykU5J4pbXkvuu81ftMez+KvRzKyFVAcXMhoIOC
c21kEmcpSrfLd2sCNPtKiE81zozDRq+0jIKT7QsQWxu+b3mu/03eXlu21LD37/i
bWBXEePpgEOYnloGzazzW28hRdjLS1yWFyKURzFvoRPv1T+j15xJ12CnbSVMrKx7
2NIdZgpb1GH1RP3nAzMCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAsLBeQdnym1
VuUZwaiazTRPGt4X8IuuwA3R+E1p7if7SWXKVXnnjKUxiR3ZtfVej68/CXhUAQ3B
Bg7FdNxEGhdsFwMiZvs2Beh9W3ketYUdPPEUrnszKTPV0vLEXnY7U+SMgcC66CR
RZNte/8VsIxYUD4Z6qU5nLouYxTvi68yXhh1ycSesBrJJxvNHccoNlfBbUXbaqyZ
FNT1pZ0Qe5pjiN3ugDQd9T9mnY45huyW/DpBW++WwcAKQSn0EFixBnU/OyR150On
sF8zmfRACoEo1G/mRY6hh6wq6MFb+BykHbKdFSBb3Sg+UYS7WrJvwzg47loYeRx5
wag6uwk47Q==
-----END CERTIFICATE REQUEST-----
```

Figure 73 : Renouvellement de certificat - Cas non passant 1 - Requête

Le fichier ne comporte aucune erreur. La CSR est correcte mais a déjà fait l'objet d'une demande de certificat.

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRenouvellementCertificat>
      <statut>WSMG-00000009</statut>
      <message>Échec lors de la validation de CSR : La clé publique pour cette CSR a déjà été présentée
      pour une autre demande (783, PATRICK MANIPCH0440, PATRICK MANIPCH0440, 21/10/2015). Veuillez essayer
      de nouveau avec un autre fichier CSR.</message>
    </ns3:reponseRenouvellementCertificat>
  </ns2:Body>
</ns2:Envelope>
```

Figure 74 : Renouvellement de certificat - Cas non passant 1 - Réponse

Détail du message d'erreur :

```
<message>Échec lors de la validation de CSR : La clé publique pour cette CSR a déjà été présentée pour une autre demande (783, PATRICK MANIPCH0440, PATRICK MANIPCH0440, 21/10/2015). Veuillez essayer de nouveau avec un autre fichier CSR.</message>
```

Figure 75 : Renouvellement de certificat - Cas non passant 1 - Réponse - Message d'erreur

Le statut contient le code de l'erreur : **WSMG-0000009**.

Le message contient le message d'erreur : **Echec lors de la validation de CSR : La clé publique pour cette CSR a déjà été présentée pour une autre demande (783, PATRICK MANIPCH0440, PATRICK MANIPCH0440, 21/10/2015). Veuillez essayer de nouveau avec un autre fichier CSR.**

Le message d'erreur indique la demande qui utilise déjà la CSR envoyée : Demande 783 de Patrick Manipch0440.



- **Exemple 2 :**

Le numéro de série du certificat à renouveler est erroné et ne correspond pas à un certificat existant.

→ La demande ne doit pas aboutir.

Le XML contient toujours la signature en première partie ainsi que la CSR. La partie suivante du fichier XML est importante :

```

<AKI>c049a9149982cedd16148490c63bcb1fdf8791fd</AKI>
<numeroSerie>%%</numeroSerie>
<mailDemandeur>cps11@yopmail.com</mailDemandeur>
<mailPersonneAInformer>picps11@yopmail.com</mailPersonneAInformer>
    
```

Figure 76 : Renouvellement de certificat - Cas non passant 2 - Requête

On voit bien que le numéro de série est faux.

Voici la réponse :

```

<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseRenouvellementCertificat>
      <statut>WSMG-00000008</statut>
      <message>Erreur lors la recherche de certificat. Veuillez vérifier et renouveler votre demande.</message>
    </ns3:reponseRenouvellementCertificat>
  </ns2:Body>
</ns2:Envelope>
    
```

Figure 77 : Renouvellement de certificat - Cas passant 2 - Réponse

Détail du message d'erreur :

```

<message>Erreur lors la recherche de certificat. Veuillez vérifier
et renouveler votre demande.</message>
    
```

Figure 78 : Renouvellement de certificat - Réponse - Message d'erreur

Le statut contient le code de l'erreur : **WSMG-00000008**.

Le message contient le message d'erreur : **Erreur lors de la recherche de certificat. Veuillez vérifier et renouveler votre demande.**

## 18 Suivi de l'activité

Le système externe appelant le Web Service de la plateforme IGC-Santé peut effectuer une demande de suivi pour :

- Le suivi des demandes de certificat logiciel
- Le suivi des produits
- Le suivi des demandes de révocation

La variable N\_max indique le nombre de résultats maximum qui peut être retourné par Web Service pour la fonctionnalité de suivi. N\_Max est valorisé à 500 résultats.

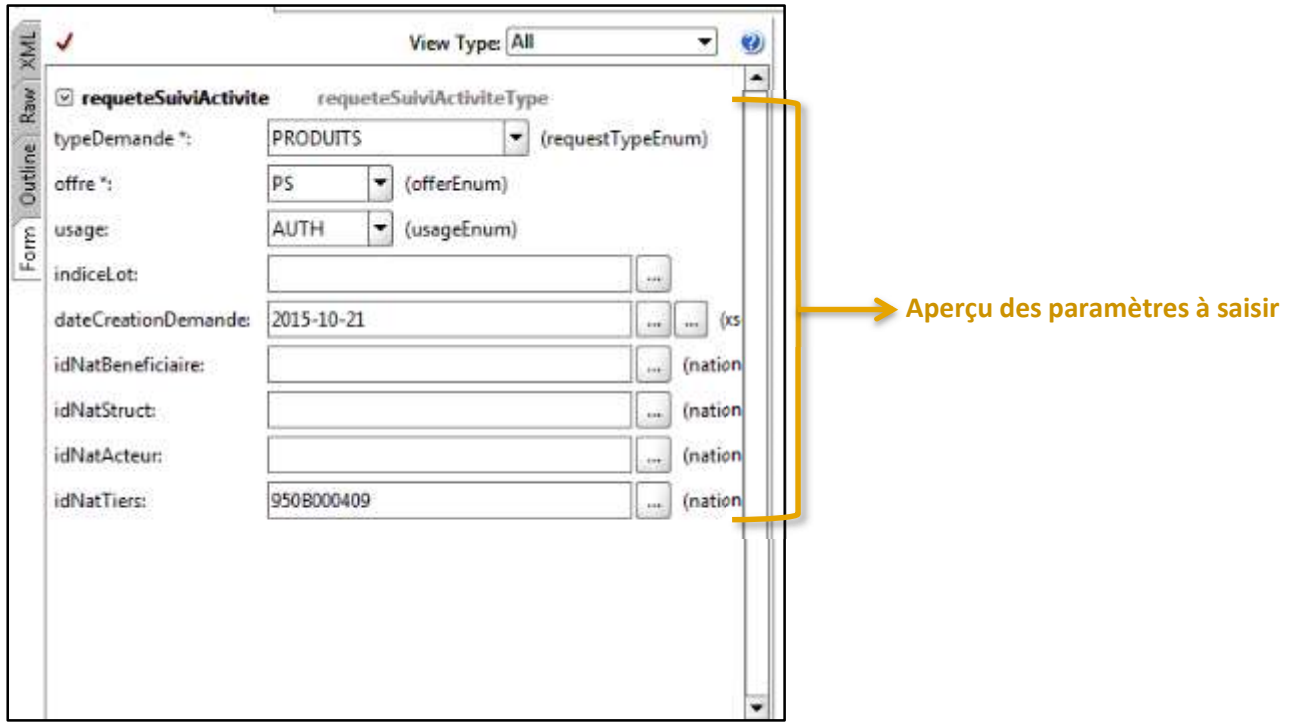
**L'utilisateur est donc limité à 500 réponses par demande de suivi d'activité.**

Pour pouvoir faire des demandes de suivis d'activité, il faut avoir les habilitations nécessaires : les demandeurs PS, les Mandataires et le support peuvent effectuer un suivi d'activité.

- Le suivi des demandes est possible par l'acteur de la demande et par le demandeur PS pour ses propres demandes.
- Pour suivre les certificats et les révocations, les habilitations sur le périmètre sont nécessaires.
- Il est possible également de faire le suivi pour les administrateurs ASIP en mode « Agir pour un tiers ».

## 18.1 Demande de suivi

Le système externe appelant envoie un appel Web Service de suivi à la plateforme IGC-Santé. Les paramètres d'entrée suivants sont saisis pour la demande de renouvellement :



The screenshot shows the SOAP UI configuration for a 'requeteSuiviActivite' request. The 'Form' view is selected, and the 'requestTypeEnum' is set to 'requeteSuiviActiviteType'. The parameters are as follows:

Field	Value	Type
typeDemande *	PRODUITS	(requestTypeEnum)
offre *	PS	(offerEnum)
usage:	AUTH	(usageEnum)
indiceLot:		
dateCreationDemande:	2015-10-21	(xs:dateTime)
idNatBeneficiaire:		(nationalIdentifier)
idNatStruct:		(nationalIdentifier)
idNatActeur:		(nationalIdentifier)
idNatTiers:	950B000409	(nationalIdentifier)

Figure 79 : Suivi de l'activité - Exemple SOAP UI

- ➔ Type de demande : ce champ est obligatoire (PRODUIT, CERTIFICAT, REVOCATION)
- ➔ Offre champ obligatoire: « PS », « PRO », « SERV », « ORG »
- ➔ Usage : Les valeurs possibles dépendent de l'offre
- ➔ IndiceLot : L'indice de lot correspond à celui de la création de la demande WS initiale.
- ➔ Date de création de la demande : Celle-ci correspond à la date du jour de la demande.
- ➔ IdNatBeneficiaire : Identifiant national du bénéficiaire.
- ➔ idNatStruct : Identifiant national de la structure.
- ➔ idNatActeur : Identifiant national de l'acteur (Personne qui effectue la demande).
- ➔ idNatTiers : Identifiant national du tiers

**Aperçu de la demande de suivi de produit sous format XML :**

*(Voir exemple de fichier XML en Annexe 1)*

```

<SOAP-ENV:Header><SOAP-SEC:Signature SOAP-ENV:actor="some-URI" SOAP-ENV:mustI
VPxkTh5o28YNujMEIj3V1UATfD8z3a5sd/M1Ytodj3bJy6S3R+wMkFCymREZQQrQxLcRo4nsDZk+
pK8fWAhs+i8OL2qioMsZcDq64CxFSAS8SdaBX7ii9q4g4JJrjW9iAkMaehIybrJC1/Grq66E1omo
UjR2f2zun1grnpIuwngUPAwOYSS9YrN2gAw8qkbfCfSGLD1osKo5xZtEg13h41fcRvWo8FK360e
E3zjPWakSV3VXopjb7L3e6L4b0ORGGAWnsLpSw==</ds:SignatureValue><ds:KeyInfo><ds:
EwRURVNUMrcwFQYDVOQLEw5URVNUIFNUU1VDVFSRTEWMBQGA1UEAxdNVEVTVCBDFEFTU0U0tMzAe
Fw0xNTAxdDEwMDAwMDFaFw0yMDAyMjkYMTU5NT1aMIGYMQswCQYDVOQGEwJGUjENMAaGA1UEChME
VEVTVDETMDEGA1UEBxQKUGFyaXMgKDC1KTEYMBYGA1UECzMPMzAwMDAwMDAwMDI4OTY5MUawHwYD
VQQDEXg1MDAwMDAwMDAwMjg5NjkvQ1BBVDAwMDIwGQYDVOQEFBjBR0VOVDwMDAwMjg5NjAwMDIw
DQYDVOQEFBAZERU5JU0UwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDZebJfWTCUkcvH
NNqCA47qTM3E1G1CSjM5XJTVqg5BzBcEZhg4ro/nofpk72Nbiyzv+KHYADrGg1bQ7+YXvfLVb8u2
Jlz6JetfRZR2UF+yCfqJ6YpZpFroo0PaW9lC9Buo6jDNieWhJKcajqNbzufATLMPkPq8eJ6WU15
YkApYvn47uCn9FtLD9/VmyuMJFhI0JEJGgur6PY19ZTYXtLeuGuBq1SQ8c+Edf7GgBIOWWuVnK6d
Ru4IS84DW4E9LM3o310+O1gOW/VZj3UsjMHCKPkZbItPgYigOyRabqIh7wEVRnm14LmwX20y7Cf
Oi/gZ8ccgqlyUr/ZzFzRaZqDagMBAAGjggKMIICRjAFBgNVHSMEDAwgBRuchVnSRaJ5fDd0hHU
cB/sa1XbajAdBgNVHQ4EFgQU87bhpz51KmwAAGWkto7rs1D7H18wDgYDVR0PAQH/BAQDAgBAMBG
A1UdJQcMAoGCCaGAQUFBwMEMCsGA1UdEAMCKADzIwMTUwMTAxdDEwMDAwMDAwMDAwMDAwMDAwMDAw
MzU5NT1aMDEGA1UdIAQSMBAwDgYMKoF6AUcDBwKCAgIBMAkGA1UdEwQCMAAwgbogaGA1UdHwSbsjCB
rzA7oDmgN4Y1aHR0cDovL2FubnVhaXJlLmdpcC1jcHMuznIvY3JsL3Rlc3QvVEVTVCBDFEFTU0U0t
My5jcmVwckBuoGyGamxkYXA6Ly9hbm51YWlyZS5naXA6Y3BzLmZyL2NuPXRlc3QgY2xhc3N1LlTMs
b3U9dGVzdCBzdHJ1Y3R1cmUsbz10ZXN0LGM9ZnI/Y2VydG1maWNhdGVyZXZvY2F0aW9ubGlzdDti
aw5hcnkwdQYDVR0uBG4wbDBqGigZozkGRhcDovL2FubnVhaXJlLmdpcC1jcHMuznIvY249dGVz
dCBjbGFzc2U0tMyxvdT10ZXN0IHNOcnVjdHVyZSxvPXRlc3QsYz1mcj9kZWx0YXJlZm9jYXRpb25s
aXNOO2JpbmFyeTARBglghkgBhvhCAQEEBAMCBSAwIwYIKoF6AUcBAGMEFxdMVDAYNTAwMDAwMS8y
NTAwMzAzNTkyMA8GCCqBEGFHAQIFBAMEAYAwDwYIKoF6AUcBAGIEAwIBAZANBgkqhkiG9w0BAQUF
AAOCAQEAMuUwR1sOZO4ZxjGg7D02I4tBrKvW/vkaTsT6HvNvMvJImDMUPVy3BxJpMvHrpjx1qo+I
GgCYvxX03JD0v5NCP7C8oX5efLbCTpr2+pA3t2T764mO2xCc0Au5yBcdamaHJkhB2AevujjgpJ2m
1bjjPW2S8YceRHDarSY461CAi2tYf1VB3Cv4oJM0qO+tX5C2O1KfIMjppIyPJSJbYX9TknvhajG
/dhYZHwduKY67pGLb1oE3/B2567qOLH63Kr2WRF/3hC9ORPFYoiWA3zzB1n753gKGeXWZvnI2KA5
azYwM23LURon+LceG2i6v0hdevrKVk0meV5xWTjYZYilgA==</ds:X509Certificate></ds:X50
<typeDemande>PRODUITS</typeDemande>
<offre>PS</offre>
<usage>AUTH</usage>
<dateCreationDemande>2015-10-21</dateCreationDemande>
<idNatTiers>950B000409</idNatTiers>
</ws:requeteSuiviActivite></SOAP-ENV:Body></SOAP-ENV:Envelope>

```

Figure 80 : Suivi de l'activité - Exemple de requête

On retrouve les informations saisies dans le corps du XML généré :

```

<typeDemande>PRODUITS</typeDemande>
<offre>PS</offre>
<usage>AUTH</usage>
<dateCreationDemande>2015-10-21</dateCreationDemande>
<idNatTiers>950B000409</idNatTiers>
</ws:requeteSuiviActivite></SOAP-ENV:Body></SOAP-ENV:Envelope>

```

Figure 81 : Suivi de l'activité - Requête - Détails

**Description du message de la requête de Suivi de l'activité dans le fichier WSDL :**

```
<wsdl:message name="requeteSuiviActivite">
  <wsdl:documentation>Requete de demande de
    suivi</wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:requeteSuiviActivite"></wsdl:part>
</wsdl:message>
```

**Description de l'opération du Suivi de l'activité dans le fichier WSDL :**

```
<wsdl:operation name="suivreActivite">
  <wsdl:documentation>Interface de demande de suivi
</wsdl:documentation>
  <wsdl:input
    message="tns:requeteSuiviActivite"></wsdl:input>
  <wsdl:output
    message="tns:reponseSuiviActivite"></wsdl:output>
</wsdl:operation>
</wsdl:portType>
```

```
<wsdl:operation name="suivreActivite">
  <wsdl:documentation>Interface de demande de suivi
</wsdl:documentation>
  <soap:operation soapAction="suivreActivite" />
  <wsdl:input>
    <soap:body use="literal" />
  </wsdl:input>
  <wsdl:output>
    <soap:body use="literal" />
  </wsdl:output>
</wsdl:operation>
```

Voici les paramètres d'entrée de la requête de Suivi de l'activité :

Donnée	Balise XML (Voir fichier XSD)	Type de contrôle	Contrôle du paramètre
idNatPS_Tiers	< idNatTiers>	Présence	Facultatif
		Type	Chaîne de caractères (64 caractères)
indiceLot	< indiceLot>	Présence	Facultatif si le paramètre « typeDemande » est valorisé à « DEMANDES_CERTIFICAT » Interdit si le paramètre « typeDemande » est valorisé à « PRODUITS » ou « DEMANDES_REVOCATION »
		Type	Chaîne de caractères (150 caractères)
typeDemande	< typeDemande>	Valeurs possibles	« DEMANDES_CERTIFICAT » pour le suivi des demandes de certificat logiciel, « PRODUITS » pour le suivi des produits, « DEMANDES_REVOCATION » pour le suivi des demandes de révocation
		Présence	Obligatoire

Donnée	Balise XML (Voir fichier XSD)	Type de contrôle	Contrôle du paramètre
		Type	Chaîne de caractères (20 caractères)
<b>offre</b>	<b>&lt; offre&gt;</b>	Valeurs possibles	« PS », « PRO », « SERV », « ORG »
		Présence	Obligatoire
		Type	Chaîne de caractères (maximum 4 caractères)
<b>usage</b>	<b>&lt; usage&gt;</b>	Valeurs possibles	Les valeurs possibles dépendent de l'offre : <ul style="list-style-type: none"> <li>• PS : « AUTH », « SIGN », « CONF »</li> <li>• PRO : « AUTH », « SIGN », « CONF »</li> <li>• ORG : « AUTH_CLI », « SIGN », « CONF »</li> <li>• SERV : « SSL_SERV », « SIGN », « S/MIME », « CONF »</li> </ul>
		Présence	Facultatif
		Type	Chaîne de caractères (maximum 8 caractères)
<b>dateCreationDemande</b>	<b>&lt; dateCreationDemande&gt;</b>	Valeurs possibles	Si le paramètre « typeDemande » est valorisé à « DEMANDES_CERTIFICAT », le paramètre « dateCreationDemande » correspond à l'attribut Demande de certificat logiciel - Date création.  Si le paramètre « typeDemande » est valorisé à « PRODUITS », le paramètre « dateCreationDemande » correspond à l'attribut Demande de certificat logiciel - Date création des demandes associées aux produits recherchés.  Si le paramètre « typeDemande » est valorisé à « DEMANDES_REVOCATION », le paramètre « dateCreationDemande » correspond à l'attribut Demande de révocation - Date création.
		Présence	Facultatif
		Type	Date
		Format	YYYY-MM-DD
<b>idNat_PS_beneficiaire</b>	<b>&lt; idNatBeneficiaire&gt;</b>	Présence	Facultatif si le paramètre « offre » est valorisé à « PRO » Facultatif si « offre » valorisée à PS.  Interdit si le paramètre « offre » est valorisé à, « SERV » ou « ORG »
		Type	Chaîne de caractères (maximum 64 caractères)
<b>idNat_struct</b>	<b>&lt; idNatStruct&gt;</b>	Présence	Obligatoire si le paramètre « offre » est valorisé à « PRO », « SERV » ou « ORG »  Interdit si le paramètre « offre » est valorisé à « PS »
		Type	Chaîne de caractères (maximum 64 caractères)
<b>idNatPS_acteur</b>	<b>&lt; idNatActeur &gt;</b>	Présence	facultatif
		Type	Chaîne de caractères (64 caractères)

**Tableau 19 : Paramètres d'entrée du suivi d'activité**

## 18.2 Réponse de la demande de suivi

Après vérification de la signature et des habilitations, les règles suivantes sont appliquées lors de la recherche des informations de suivi :

- Les paramètres facultatifs non renseignés ne sont pas pris en compte dans la recherche.
- Inversement, tout paramètre renseigné est un filtre de la recherche. Celle-ci est composée par une série de filtres en mode « ET » logique.
- Si la requête renvoie un nombre de réponses supérieur à N\_max, les N\_max réponses sont envoyées dans le message, précédées de l'information suivante : « MESSAGE : La recherche donne un trop grand nombre de résultats. La réponse n'est pas exhaustive et se limite à N\_max réponses. Veuillez restreindre la recherche. »  
**N\_Max est valorisé à 500 résultats.**

La plateforme IGC-Santé envoie par réponse Web-Service l'accusé de réception de la demande avec les informations demandées.

**Si l'utilisateur n'est pas habilité pour la demande, la réponse est en erreur.**

Le statut de la réponse est détaillé comme ci-dessous :

Réponse Web Service	Balise XML (Voir fichier XSD)	Renseigné à partir de	
		Objet Métier	Donnée ou valeur
<b>statut</b>	<b>&lt; statut&gt;</b>	-	« OK » ou code d'erreur
<b>message</b>	<b>&lt; avertissement &gt;</b>	-	<p>Si le paramètre statut est valorisé à « OK », ce champ contient le contenu de la réponse au format XML :</p> <ul style="list-style-type: none"> <li>• Chaque ligne est insérée dans la balise &lt;resultat&gt; avec un nombre maximum N_Max de réponses</li> <li>• Si le champ est multi-valué (par exemple FQDN), la balise du champ est répétée plusieurs fois</li> </ul> <p>Sinon le message associé au code d'erreur est inséré dans une balise &lt;erreur&gt; à l'intérieur du paramètre « message »</p>

Tableau 20 : Paramètres du statut de la réponse du suivi d'activité

On retrouve chaque résultat de la demande de suivi dans la balise **<resultat>**.

Extrait du fichier XSD :

```
<xsd:element name="resultat" type="tns:resultatType"
              minOccurs="0" maxOccurs="500">
</xsd:element>
```

Voici le contenu du paramètre « Résultat » de la réponse du suivi de l'activité.

Extrait du fichier XSD :

```
<xsd:complexType name="resultatType">
  <xsd:choice>
    <xsd:sequence>
      <xsd:element name="erreur" type="xsd:string"
        minOccurs="1"
        maxOccurs="1" />
    </xsd:sequence>
    <xsd:sequence>
      <xsd:element name="numero" type="xsd:string"
        minOccurs="0"
        maxOccurs="1">
        <xsd:annotation>
          <xsd:documentation>
            Numéro de l'objet métier (demande
            de certificat ou demande révocation
            ou produit)
          </xsd:documentation>
        </xsd:annotation>
      </xsd:element>
    </xsd:sequence>
  </xsd:choice>
</complexType>
```

[...]

Balise XML dans le contenu du message	Objet Métier	Donnée ou valeur	Règle	Suivi des demandes de certificat	Suivi des produits	Suivi des demandes de révocation
<b>&lt;numero&gt;</b>	Demande de certificat logiciel	Numéro		X		
	Demande de révocation	Numéro				X
	Produit	Numéro			X	
<b>&lt;canal&gt;</b>	Demande de certificat logiciel	Canal		X	X	
	Demande de révocation					X
<b>&lt;creationDate&gt;</b>	Demande de certificat logiciel	Date création		X		
	Demande de révocation					X
<b>&lt;dateDebutValidite&gt;</b>	Produit	Début validité			X	



Balise XML dans le contenu du message	Objet Métier	Donnée ou valeur	Règle	Suivi des demandes de certificat	Suivi des produits	Suivi des demandes de révocation
<b>&lt;dateFinValidite&gt;</b>	Produit	Fin validité	Si le produit ne fait pas l'objet d'une demande de révocation en cours  Et Si le produit a été retiré : <ul style="list-style-type: none"> <li>donnée renseignée avec la date de fin de validité sur le produit</li> </ul> Sinon vide		<b>X</b>	
<b>&lt;offre&gt;</b>	Demande de certificat logiciel	Offre		<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;usage&gt;</b>	Produit	Usage		<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;idNatStructure&gt;</b>	Demande de certificat logiciel	Structure	Si l'offre est PRO, SERV ou ORG	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;raisonSociale&gt;</b>	Produit	Raison sociale	Si l'offre est PRO, SERV ou ORG	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;idNatAdministrateur&gt;</b>	Demande de certificat logiciel	Administrateur ASIP		<b>X</b>	<b>X</b>	
	Demande de révocation					<b>X</b>
<b>&lt;nomAdministrateur&gt;</b>	Demande de certificat logiciel	Nom administrateur		<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;prenomAdministrateur&gt;</b>	Demande de certificat logiciel	Prénom administrateur		<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;idNatBeneficiaire&gt;</b>	Demande de certificat logiciel	Bénéficiaire	Si l'offre est PS ou PRO	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;nomBeneficiaire&gt;</b>	Produit	Nom bénéficiaire	Si l'offre est PS ou PRO	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;prenomBeneficiaire&gt;</b>	Produit	Prénom bénéficiaire	Si l'offre est PS ou PRO	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;idNatActeur&gt;</b>	Demande de certificat logiciel	Acteur		<b>X</b>	<b>X</b>	
	Demande de révocation					<b>X</b>

Balise XML dans le contenu du message	Objet Métier	Donnée ou valeur	Règle	Suivi des demandes de certificat	Suivi des produits	Suivi des demandes de révocation
<nomActeur>	Demande de certificat logiciel	Nom acteur		X	X	X
<prenomActeur>	Demande de certificat logiciel	Prénom acteur		X	X	X
<etat>	Demande de certificat logiciel	État		X		
	Demande de révocation					X
	Produit				X	
<emailActeur>	Demande de certificat logiciel	Email Acteur		X		
	Demande de révocation					X
<emailNotification>	Demande de certificat logiciel	Email Notification	Recherché à partir de la demande de révocation en cours, ou de la demande de certificat logiciel correspondant au produit	X		
	Demande de révocation					X
<dateExpiration>	-	-	<p>Si le produit ne fait pas l'objet d'une demande de révocation en cours Et</p> <ul style="list-style-type: none"> <li>Si le produit n'a pas été retiré : la date d'expiration de la demande de certificat est calculée (date de validation de la demande + délai de retrait avant annulation)</li> </ul> <p>Sinon :</p> <ul style="list-style-type: none"> <li>vide</li> </ul>	X		

Balise XML dans le contenu du message	Objet Métier	Donnée ou valeur	Règle	Suivi des demandes de certificat	Suivi des produits	Suivi des demandes de révocation
<b>&lt;dateRevocation&gt;</b>	Demande de révocation	Date révocation	Si le produit fait l'objet d'une demande de révocation en cours : <ul style="list-style-type: none"> <li>donnée renseignée avec la date de révocation du produit sur la demande révocation</li> </ul> Sinon : <ul style="list-style-type: none"> <li>vide</li> </ul>			<b>X</b>
<b>&lt;motifRevocation&gt;</b>	Demande de révocation	Motif				<b>X</b>
<b>&lt;motifAutre&gt;</b>	Demande de révocation	Motif autre				<b>X</b>
<b>&lt;numeroSerie&gt;</b>	Produit	Numéro de série	Vide si le produit est dans un des états suivants : « Produit demandé », « Produit à retirer », « Produit annulé ».  Toujours présent sinon (sauf si la demande de certificat a expiré). Il constitue, avec l'autorité, l'identification unique du produit	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;dnAutorite&gt;</b>	Produit	Autorité	Vide si le produit est dans un des états suivants : « Produit demandé », « Produit à retirer », « Produit annulé ».  Toujours présent sinon (sauf si la demande de certificat a expiré). Il constitue, avec le numéro de série, l'identification unique du produit	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;dnSujet&gt;</b>	Produit	Sujet		<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;domaines&gt;</b>	Produit	Domaines	Si multivalué, chaque valeur est séparée par le caractère « espace »	<b>X</b>	<b>X</b>	<b>X</b>
<b>&lt;nomApplicatif&gt;</b>	Produit	Service		<b>X</b>	<b>X</b>	<b>X</b>

Balise XML dans le contenu du message	Objet Métier	Donnée ou valeur	Règle	Suivi des demandes de certificat	Suivi des produits	Suivi des demandes de révocation
<eMailSujet>	Produit	Email Sujet	<p>Recherché à partir du produit de la demande de révocation en cours, ou de la demande de certificat logiciel correspondant au produit</p> <p>Toujours présent l'offre SERV et les usages SIGN, S/MIME et CONF</p> <p>Facultatif pour les offres PS et PRO et les usages SIGN et CONF</p> <p>Vide pour les autres offres / usages</p>	X	X	X

Tableau 21 : Paramètres de la réponse du suivi d'activité

**Description du message de la réponse de Suivi de l'activité dans le fichier WSDL :**

```

<wsdl:message name="reponseSuiviActivite">
  <wsdl:documentation>Reponse a la requete de demande de suivi
</wsdl:documentation>
  <wsdl:part name="parameters"
    element="tns:reponseSuiviActivite"></wsdl:part>
</wsdl:message>

```

**Aperçu de la réponse de suivi de produits sous format XML :**
*(Voir exemple de fichier XML en Annexe 1)*

```

<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseSuiviActivite>
      <statut>OK</statut>
      <avertissement>MESSAGE : La recherche donne un trop grand nombre de résultats.
      La réponse n'est pas exhaustive et se limite à 500 réponses. Veuillez restreindre la recherche.</avertissement>
      <resultat>
        <numero>11</numero>
        <canal>WS</canal>
        <dateCreation>2015-12-16</dateCreation>
        <idNatStruct>10B0039137</idNatStruct>
        <raisonSociale>PHARMACIE DE LA GARE ROUTIERE03913</raisonSociale>
        <idNatActeur>899700027230</idNatActeur>
        <nomActeur>ADJOINTPHARM RPPS</nomActeur>
        <prenomActeur>PASCALINE</prenomActeur>
        <etat>Terminée</etat>
        <mailActeur>cps04@yopmail.com</mailActeur>
        <mailNotification>pics04@yopmail.com</mailNotification>
        <numeroSerie>1d7c17ad54fdba53abba04ee7502106c</numeroSerie>
        <dnAutorite>CN=TEST AC IGC-SANTE ELEMENTAIRE, OU=POUR INTEGRATION SEULEMENT, OU=IGC-SANTE TEST, OU=0002 187512751, O=ASIP-SANTE, C=FR</dnAutorite>
        <dnSujet>CN=Service.HAB04.2.fr, OU=10B0039137, O=PHARMACIE DE LA GARE ROUTIERE03913, ST=Paris (75), C=FR</dnSujet>
        <nomApplicatif>Service.HAB04.2.fr</nomApplicatif>
      </resultat>
      <resultat>
        <numero>13</numero>
        <canal>WS</canal>
        <dateCreation>2015-12-16</dateCreation>
        <idNatStruct>10B0039137</idNatStruct>
        <raisonSociale>PHARMACIE DE LA GARE ROUTIERE03913</raisonSociale>
        <idNatActeur>899700027230</idNatActeur>
        <nomActeur>ADJOINTPHARM RPPS</nomActeur>
        <prenomActeur>PASCALINE</prenomActeur>
        <etat>Terminée</etat>
        <mailActeur>cps04@yopmail.com</mailActeur>
        <mailNotification>pics04@yopmail.com</mailNotification>
        <numeroSerie>1d7c17ad54fdba53f2cbbf27d4ed6389</numeroSerie>
        <dnAutorite>CN=TEST AC IGC-SANTE ELEMENTAIRE, OU=POUR INTEGRATION SEULEMENT, OU=IGC-SANTE TEST, OU=0002 187512751, O=ASIP-SANTE, C=FR</dnAutorite>
        <dnSujet>CN=test.pharmacie.com, OU=10B0039137, O=PHARMACIE DE LA GARE ROUTIERE03913, ST=Paris (75), C=FR</dnSujet>
        <domaines>test.pharmacie.com</domaines>
      </resultat>
    </resultat>
  </ns3:reponseSuiviActivite>
</ns2:Body>
</ns2:Envelope>

```

**Figure 82 : Suivi de l'activité - Exemple de réponse**

On retrouve dans le corps du fichier le **statut** de la réponse : **OK**

Un avertissement est donné : la recherche comporte plus de 500 résultats.

Le fichier étant limité à 500 réponses, tous les résultats n'ont pas pu être envoyés.

```

-
<ns3:reponseSuiviActivite>
  <statut>OK</statut>
  <avertissement>MESSAGE : La recherche donne un trop grand nombre de résultats.
  La réponse n'est pas exhaustive et se limite à 20 réponses. Veuillez restreindre la recherche.</avertissement>

```

**Figure 83 : Suivi de l'activité - Réponse - Statut de la réponse**

On retrouve dans le corps du fichier XML l'ensemble des informations correspondant à la recherche de suivi de produit.

Les réponses sont envoyées à la suite dans la balise <Résultat>.

Voici une réponse :

```
<resultat>
  <numero>54</numero>
  <canal>WS</canal>
  <dateDebutValidite>2015-10-06</dateDebutValidite>
  <dateFinValidite>2018-10-06</dateFinValidite>
  <offre>PS</offre>
  <usage>AUTH</usage>
  <idNatAdministrateur>500000000028969/CPAT0002</idNatAdministrateur>
  <nomAdministrateur>AGENT0000028960002</nomAdministrateur>
  <prenomAdministrateur>DENISE</prenomAdministrateur>
  <idNatBeneficiaire>950B000409</idNatBeneficiaire>
  <nomBeneficiaire>REMPLEXETUSAGE0040</nomBeneficiaire>
  <prenomBeneficiaire>MARYSE</prenomBeneficiaire>
  <idNatActeur>950B000409</idNatActeur>
  <nomActeur>REMPLEXETUSAGE0040</nomActeur>
  <prenomActeur>MARYSE</prenomActeur>
  <etat>Révoqué</etat>
  <numeroSerie>49aa3433d672424e0e1e49e63c3b603b</numeroSerie>
  <dnAutorite>CN=TEST AC IGC-SANTE ELEMENTAIRE PERSONNES,
  OU=POUR INTEGRATION SEULEMENT, OU=IGC-SANTE TEST, OU=0002 187512751, O=ASIP-SANTE, C=FR</dnAutorite>
  <dnSujet>CN=950B000409, SURNAME=REMPLEXETUSAGE0040, GIVENNAME=MARYSE, T=Sage-femme
  en formation, C=FR</dnSujet>
</resultat>
```

Figure 84 : Suivi de l'activité - Réponse - Détails du résultat

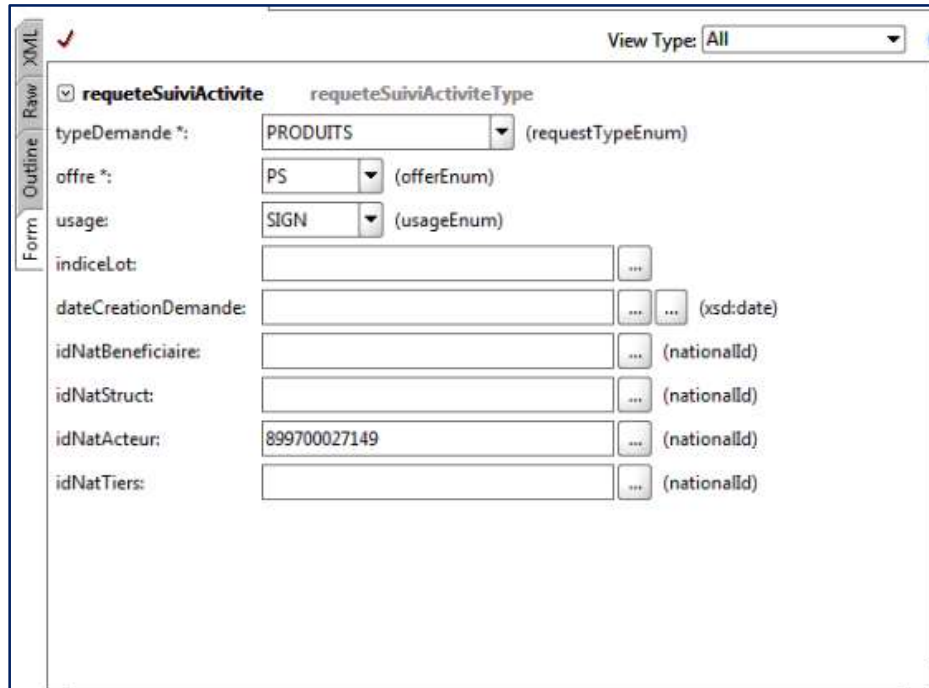
Si l'utilisateur n'est pas habilité pour la demande de suivi, un message d'erreur est retourné :

## 18.3 Cas non passants

- **Exemple 1 :**

L'utilisateur utilise sa carte pour faire la demande mais il saisit l'identifiant national d'une autre personne dans le champ Acteur.

→ La demande de suivi ne doit pas aboutir.



The screenshot shows a web service interface for the 'requeteSuiviActivite' operation. The interface includes a 'View Type' dropdown set to 'All' and a sidebar with 'Form', 'Outline', 'Raw', and 'XML' tabs. The main area displays the following fields and values:

Field	Value	Type
typeDemande *	PRODUITS	(requestTypeEnum)
offre *	PS	(offerEnum)
usage:	SIGN	(usageEnum)
indiceLot:		
dateCreationDemande:		(xsd:date)
idNatBeneficiaire:		(nationalId)
idNatStruct:		(nationalId)
idNatActeur:	899700027149	(nationalId)
idNatTiers:		(nationalId)

Figure 85 : Suivi de l'activité - Cas non passant 1

Voici le XML généré :

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
fr5UcVvKytkl0tuCzKj4agN8HGzmv3UtqWNMKNYOpUYOg8aqE1aho+deZNCtcUJPKxC7iVonxKt9
NRqK/0F6eKQ0hHRLBNiTpawZwg+yUSL9dFqzTS/BCqm925WiSMWK8MZvruD3OFOXhNuoYTuxrIGQ
DI3bA4W5bUPAhPgyhji6R2S6h7XcaiPG1g+BSjvclxDkNVennQ58oNPCuApPRT3Eu0XeQoiGrOjQ
3L7aofHBJSVa0f70uGicpDs+Bu6rIR5qhHvbXQ==</ds:SignatureValue><ds:KeyInfo><ds:
EwRURVNUMRcwFQYDVQQLEw5URVNUIFNUU1VDVfVSRTewMBQGA1UEAxMNVEVTVCBDEFTU0UtmZAE
Fw0xNTAxMDEwMDAwMDFAFw0yMDAyMjkyMTU5NTlaMIGNMQswCQYDVQGEwJGUjenMASGA1UEChME
VEVTVDEtMBEgA1UEBxQKUGFyaXMGKDc1KTETMBEgA1UECzMkMTBcMDAzoTlxMDFFMBoGA1UEAxMT
MzBCMDAzoTlxMCM9DUEVUMDAwMzAZBgNVBAQUEKFTU01TVC1DUzAzOTIxMDAwMzAMBGNVBCoUBU1B
UklFMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXe2yoHX7Xc7oUrn/ampE3p9CuObd
+ahaGpCg2rIQgQwX1PUI+/VfzH8fjoPHCB89wyu2oi7w5HPUBcXm9cPYH3srQBcL1yquo3JFGnGZ
g267zhWeRmKw8g3cbVVMVfbmav36wNcKzoaFq8w0jvMLQoOWeojOqsfLxj2S7NAu2eKqUz7idrfG
32IDYcmqVdG5c0hHvZRRiLbfsM6hMOXb6/UGyiqgukGXLOPFG+hzL71n5nCGb9H1MaqIhb8Hv7x
Yt052au41uhE12xUTPPJ4ooC7eemF7SjHzW/QpLEzAJQAAoV5/b153RQ7ApvmEJE82F2rrrQ3nP
OPu9jldHawIDAQBo4ICSjCCAkYwHwYDVR0jBBgwFoAUBnIVZ0kWieXw3dIR1Haf7GtV22owHQYD
VR0OBBYEFgWDT9BkGEU6LTJJamnLogqXOMfWMA4GA1UdDwEB/wQEAwIGwDATBgNVHSEDDAKBggr
BgEFBQcDBDARBgNVHRAEJDAigA8yMDE1MDEwMTAwMDAwMVqBDzIwMjAwMTMxMjM1OTU5WjAZBgNV
HSAEEjAQM4GDCqBEGFHAwCJAgiCATAJBgNVHRMBAjAAMIIG6BgNVHR8EgbIwga8wO6A5oDeGNWh0
dHA6Ly9hbM51YWlyZS5naXAtY3BzLmZyL2NyY2N0L1RFU1QgQ0xBU1NFLTmuY3JSMHCgBqBs
hmpsZGFwOi8vYW5udWFpcmuUuZ21wLWNwcy5mci9jbj10ZjZ0IGNsYXNzZS0zLG91PXRlc3Qgc3Ry
dWN0dXJlLlG89dGVzdCcxjPWZyP2N1cnRzZmljYXRlcmlmV2b2NhdG1vbmxc3Q7YmluYXJ5MjU5MjU5
LgRuMGwwaqBooGaGZGxkYXA6Ly9hbM51YWlyZS5naXAtY3BzLmZyL2NuPXRlc3QgY2xhc3NlLlTMs
b3U9dGVzdCBzdHJ1Y3R1cmUsbz10ZjZ0LGM9ZnI/ZGVsdGFyZXZvY2F0aW9ubGlzdDtiaW5hcnkw
EQYJYIZIAyb4QgEBBAQDAgUgMCMGCCqBEGFHAQIDBBcTFTgWmjUwMDAwMDEvMjUwMDMwMzU2NDAP
BggqqgXoBRwECBQQDBAGAMA8GCCqBEGFHAQICBAMCAQIwDQYJKoZIhvcNAQEFBQADggEBAEaIgtfL
GD9U5u/Kn5Evx8C7Cwu3Zw81Hy0CNDPARoJJBpIqUfukKAjlj0WcW3Mza/iTipVV4UKCEtAfz8p
m0WAoNB8Lrh4t8gVLQmp5D29AAC0kF67/EQSMgVScjTK557YIhXguT1qFAEcMmJiARmG2RkXjvuhy
15vwwIadLozms6fved1S5dVC4I11PfvIntGyLYJWkP0AfzwnKDUfiszL1YPTgjl/xXutgmH4zJ1
b7v60IfkpgQuGU37DdsQkICs7LXYZufye412SI+WysxSWfUSguBNW2+efY3ufom11QQAGQaNgqyh2
s940KMki+00W5Si/nW8eTs/SpSU0edo=</ds:X509Certificate></ds:X509Data></ds:KeyI
<typeDemande>PRODUITS</typeDemande>
<offre>PS</offre>
<usage>SIGN</usage>
<idNatActeur>899700027149</idNatActeur>
</ws:requeteSuiviActivite></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Figure 86 : Suivi de l'activité - Cas non passant 1 - Requête

Voici la réponse :

```
<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfcng.in.com/WS/">
<ns2:Body>
<ns3:reponseSuiviActivite>
<statut>WSMG-00000043</statut>
<resultat>
<erreur>Erreur lors de la vérification de la validité de la demande de suivi :
Le bénéficiaire n'est pas habilité pour l'offre demandée.</erreur>
</resultat>
</ns3:reponseSuiviActivite>
</ns2:Body>
```

Figure 87 : Suivi de l'activité - Cas non passant 1 - Réponse



## Détail de l'erreur

Le statut contient le code de l'erreur : **WSMG-0000043**.

Le message contient le message d'erreur : **Erreur lors de la vérification de la validité de la demande de suivi : Le bénéficiaire n'est pas habilité pour l'offre demandée.**



Voici la réponse :

```

<ns2:Envelope xmlns:ns2="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns3="http://www.pfeng.in.com/WS/">
  <ns2:Body>
    <ns3:reponseSuiviActivite>
      <statut>WSMG-00000005</statut>
      <resultat>
        <erreur>Contenu de la demande non valide. Veuillez vérifier que les paramètres en entrée
          sont corrects et renouveler votre demande.</erreur>
      </resultat>
    </ns3:reponseSuiviActivite>
  </ns2:Body>
</ns2:Envelope>

```

Figure 89 : Suivi de l'activité - Cas non passant 2 - Réponse

Détail de l'erreur :

Le statut contient le code de l'erreur : **WSMG-00000005**.

Le message contient le message d'erreur : **Contenu de la demande non valide. Veuillez vérifier que les paramètres en entrée sont corrects et renouveler votre demande.**

## 19 Tableaux des erreurs Web Service

Le tableau ci-dessous présente les erreurs remontées par le composant Web-Service (avec les actions associées) à l'application consommatrice du Web Service.

Code	Intitulé	Action	Demande (lot)	Demande (unitaire)	Retrait	Révocation	Renouvellement	Suivi
WSMG-0000002	Signature invalide. Veuillez renouveler votre demande.	<p>Si un des composants de la signature n'est pas valide, soit :</p> <ul style="list-style-type: none"> <li>Signature - La signature au format XMLDSIG</li> <li>Certificat utilisé - Le certificat complet utilisé pour signer le message</li> <li>Police de signature - URL de la police de signature utilisée</li> <li>Date/heure de la signature - Date et heure de la signature (selon le signataire)</li> </ul> <p>Le traitement s'arrête.</p> <p>L'erreur est tracée et renvoyée dans la réponse.</p>	X		X	X	X	X
WSMG-0000005	<p>Contenu de la demande non valide : &lt;complément d'information facultatif&gt;. Veuillez vérifier que les paramètres en entrée sont corrects et renouveler votre demande.</p> <p>Avec &lt;complément d'information facultatif&gt; pouvant être :</p> <p>WSMG-00000032</p> <p>WSMG-00000033</p> <p>WSMG-00000034</p> <p>WSMG-00000035</p> <p>WSMG-00000036</p> <p>WSMG-00000037</p>	<p>Une erreur est rencontrée lors de la vérification des paramètres en entrée.</p> <p>Le traitement s'arrête.</p> <p>L'erreur est tracée et renvoyée dans la réponse.</p>	X	X	X	X	X	X
WSMG-0000007	Erreur lors la recherche de demande. Veuillez vérifier et renouveler votre demande.	<p>Aucune demande correspond aux critères n'est trouvée.</p> <p>Le traitement s'arrête.</p>						X

Code	Intitulé	Action	Demande (lot)	Demande (unitaire)	Retrait	Révocation	Renouvellement	Suivi
		L'erreur est tracée et renvoyée dans la réponse.						
WSMG-0000008	Erreur lors la recherche de certificat. Veuillez vérifier et renouveler votre demande.	Aucune demande correspondant aux critères n'est trouvée.  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.				<b>X</b>		<b>X</b>
WSMG-0000009	Échec lors de la validation de CSR : <raison de l'échec de la validation de la CSR>  Veuillez essayer de nouveau avec un autre fichier CSR.	RMT_ERR_001		<b>X</b>			<b>X</b>	
WSMG-0000010	Échec lors de la validation de demande de certificat. La demande n'est pas valide pour la raison suivante <raison>. Veuillez vérifier et renouveler votre demande.	RMT_ERR_002		<b>X</b>			<b>X</b>	
WSMG-0000011	Échec lors de la validation de demande de retrait : <raison>. Veuillez vérifier et renouveler votre demande.	RMT_ERR_005			<b>X</b>			
WSMG-0000012	Échec lors de l'enregistrement de la demande de révocation : <raison de l'échec de l'enregistrement>. Veuillez vérifier et renouveler votre demande.	RMT_ERR_011				<b>X</b>		
WSMG-0000015	Web-Service PFCNG-IGC inaccessible au retrait technique du certificat. Veuillez renouveler votre demande de retrait ultérieurement.	RMT_ERR_006			<b>X</b>			
WSMG-0000016	Web-Service PFCNG-IGC renvoie une erreur au retrait technique du certificat. Veuillez effectuer une nouvelle demande de certificat.	RMT_ERR_007			<b>X</b>			
WSMG-0000017	Web-Service PFCNG-IGC renvoie une erreur à l'enregistrement de la demande. Veuillez vérifier et renouveler votre demande de certificat.	RMT_ERR_004			<b>X</b>			

Code	Intitulé	Action	Demande (lot)	Demande (unitaire)	Retrait	Révocation	Renouvellement	Suivi
WSMG-0000018	Web-Service PFCNG-IGC inaccessible à l'enregistrement de la demande de certificat. Veuillez renouveler votre demande de retrait ultérieurement.	RMT_ERR_003			<b>X</b>			
WSMG-0000023	Le lot ne peut pas contenir plus de 20 demandes. Veuillez renouveler votre demande.	Si le lot contient (strictement) plus de 20 demandes  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.	<b>X</b>					
WSMG-0000024	La taille du message ne peut pas dépasser 10 méga-octets. Veuillez renouveler votre demande.	Si la taille du message dépasse 10 méga-octets  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.	<b>X</b>					
WSMG-0000027	Indice de retrait inconnu. Veuillez renouveler votre demande.	Si l'indice de retrait n'est pas trouvé  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.			<b>X</b>			
WSMG-0000030	Vous n'êtes pas l'acteur de la demande de certificat logiciel. Votre demande est refusée.	Si l'acteur de la demande de retrait n'est pas celui de la demande certificat logiciel associée au produit  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.			<b>X</b>			
WSMG-0000031	La demande de certificat logiciel n'a pas été faite par le canal WS. Veuillez effectuer votre demande de retrait par le même canal.	Si le canal de la demande certificat logiciel associée au produit n'est pas « WS »  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.			<b>X</b>			

Code	Intitulé	Action	Demande (lot)	Demande (unitaire)	Retrait	Révocation	Renouvellement	Suivi
WSMG-0000032	Pour les offres PRO, ORG et SERV, « idNat_Struct » est obligatoire	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.	<b>X</b>					
WSMG-0000033	Pour l'offre PRO, « idNat_bénéficiaire » est obligatoire	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.	<b>X</b>					
WSMG-0000034	Si usage SSL_SERV : présence d'au moins une balise « FQDN », « mailSujet » est interdit	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.	<b>X</b>					
WSMG-0000035	Si offre SERV » hors usage SSL_SERV ou offre ORG : « nomApplicatif » est obligatoire	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.	<b>X</b>					
WSMG-0000036	<ul style="list-style-type: none"> <li>Si offre PS usage SIGN ou CONF, ou offre PRO usage SIGN ou CONF, ou offre ORG, ou offre SERV : « UPN » est interdit</li> </ul>	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.	<b>X</b>					
WSMG-0000037	<ul style="list-style-type: none"> <li>Si offre SERV usages SIGN, S/MIME et CONF : « mailSujet » est obligatoire</li> <li>Si offre ORG : « mailSujet » est interdit</li> </ul>	L'erreur est tracée, la demande associée n'est pas traitée, si la demande fait partie d'un lot de plusieurs demandes, les autres demandes sont traitées.		<b>X</b>				
WSMG-0000038	Si une erreur survient au cours de la transmission de l'acquittement du Web Service, une erreur est loguée.	Le processus se termine, rien n'est envoyé à l'utilisateur à cause d'une coupure de la communication entre la PFCNG-MG et l'utilisateur.		<b>X</b>			<b>X</b>	
WSMG-0000042	Plus de 5 FQDN sont fournis dans le SAN. Veuillez vérifier et renouveler votre demande.	Si le SAN contient (strictement) plus de 5 FQDN  Le traitement s'arrête.  L'erreur est tracée et renvoyée dans la réponse.	<b>X</b>					
WSMG-0000043	Erreur lors de la vérification de la validité de la demande de suivi : <raison>	RMT_ERR_016						<b>X</b>

Code	Intitulé	Action	Demande (lot)	Demande (unitaire)	Retrait	Révocation	Renouvellement	Suivi
WSMG-0000044	<p>Échec lors de la complétion de la demande de certificat. La demande est en échec pour la raison suivante &lt;raison&gt;. Veuillez vérifier et renouveler votre demande.</p> <p>Avec les valeurs possibles de la variable &lt;raison&gt; étant un sous-ensemble des raisons présentes dans RMT_ERR_002.</p>			<b>X</b>			<b>X</b>	

**Tableau 22 : Erreurs Web Service**



## 20 Tableaux des erreurs métiers transverses

NB. Ce chapitre décrit les erreurs transverses qui sont anticipées et la façon dont elle sont gérées par l'application. Ces erreurs sont encapsulées dans les erreurs web services dans le paramètre <raison>.

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_001	<p>Échec lors de la validation de CSR : &lt;raison de l'échec de la validation de la CSR&gt;</p> <p>Avec la variable &lt;raison de l'échec de la validation de la CSR&gt; qui peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• La signature de la CSR est incorrecte.</li> <li>• La clé publique pour cette CSR a déjà été présentée pour une autre demande (&lt;numéro demande&gt;, &lt;acteur&gt;, &lt;bénéficiaire ou structure&gt;, &lt;date&gt;).</li> </ul>	<p>La CSR n'est pas conforme (PKCS#10) ou sa signature est invalide</p> <p>Le rejet de la CSR entraîne le rejet de la demande (excepté pour le canal IHM).</p> <p>La demande passe de l'état de l'état « Demande enregistrée » à l'état « Demande rejetée »</p> <p>Le produit passe de l'état « Produit demandé » à l'état « Produit annulé ».</p> <p>Le rejet est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché (ERR_IHM_007) et l'utilisateur est invité à recommencer l'envoi de la CSR.</p> <p>Dans le cas du canal Web Service, une erreur Web Service est remontée (WSMG-00000009) et un e-mail de notification est envoyé (NMG-005).</p> <p>L'utilisateur doit faire une nouvelle demande.</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_002	<p>Échec lors de la validation de demande de certificat : &lt;raison de l'échec de la validation&gt;</p> <p>Avec la variable &lt;raison de l'échec de la validation&gt; qui peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• &lt;Erreur_Habilitation&gt;</li> <li>• L'acteur n'existe pas dans l'annuaire</li> <li>• Le bénéficiaire n'existe pas dans l'annuaire</li> <li>• La structure n'existe pas dans l'annuaire</li> <li>• Le type de produit n'est pas ouvert à la commande.</li> <li>• L'adresse de messagerie protégée est déjà renseignée pour un autre produit &lt;numéro produit&gt; en cours de validité et contenant un autre DN (certificat de personne physique) ou un autre idNatStruct (certificat d'organisation).</li> <li>• Les paramètres de la demande et du produit ne sont pas cohérents avec les données contenues dans le référentiel identité : &lt;donnée demande ou produit&gt; incohérente avec &lt;donnée référentiel identité&gt;.</li> <li>• Les contraintes sur les caractéristiques de la demande ou du produit ne sont pas respectées : &lt;attribut métier&gt; &lt;contrainte non respectée&gt;.</li> </ul>	<p>La demande n'est pas valide car elle ne répond pas à tous les critères.</p> <p>Le non respect des règles métier entraîne le rejet de la demande (excepté pour le canal IHM).</p> <p>La demande passe de l'état « Demande enregistrée » à l'état « Demande rejetée ».</p> <p>Le produit passe de l'état « Produit demandé » à l'état « Produit annulé ».</p> <p>Le rejet est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché (ERR_IHM_063).</p> <p>Dans le cas du canal Web-Service, une erreur Web-Service est remontée (WSMG-00000010).</p> <p>Dans le cas du canal Web Service Mail, une erreur Web-Service est remontée (WSMMG-00000006).</p> <p>Pour les canaux Web Service et Web Service mail, un e-mail de notification est envoyé (NMG-005).</p> <p>L'utilisateur doit faire une nouvelle demande.</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_003	Web-Service PFCNG-IGC inaccessible à l'enregistrement technique de la demande de certificat	<p>Le Web-Service PFCNG-IGC n'est pas disponible ou ne répond pas avant le délai paramétré.</p> <p>Pour les canaux IHM et Web-Service Mail, l'enregistrement de la demande dans la PFCNG-IGC est réalisé de façon asynchrone par le système PFCNG-MG.</p> <p>Pour les canaux IHM et Web Service Mail :</p> <p>Dans ce cas plusieurs tentatives sont réalisées. Ces tentatives sont décrites dans le document [P2_SIS_IGC] au § II.3. Configuration du connecteur. Chaque tentative est enregistrée en traçabilité. Un e-mail de notification est envoyé pour avertir que la demande est mise en attente (NMG-013).</p> <p>Si les tentatives n'ont pas abouti, la demande de certificat échoue : elle passe à l'état « Demande non traitée » et le produit passe à l'état « Produit annulé ». L'échec est enregistré en traçabilité. L'utilisateur doit faire une nouvelle demande de certificat.</p> <p>Dans le cas du canal Web-Service, l'enregistrement de la demande dans la PFCNG-IGC est réalisé au sein du processus de retrait.</p> <p>En cas d'échec, la demande de retrait est annulée et l'utilisateur doit faire une nouvelle demande de retrait.</p> <p>La demande de certificat est conservée à l'état « Demande validée » et le produit à l'état « Produit à retirer ». L'échec est enregistré en traçabilité. Une erreur Web-Service est remontée (WSMG-00000018).</p> <p>Pour les trois canaux, un e-mail de notification est envoyé (NMG-005).</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_004	<p>Web-Service PFCNG-IGC renvoie une erreur à l'enregistrement technique de la demande</p>	<p>La demande de certificat a été validée par le système PFCNG-MG mais elle est rejetée par le système PFCNG-IGC. La demande ne pourra pas être traitée.</p> <p>La demande passe à l'état « Demande non traitée » et le produit passe à l'état « Produit annulé »</p> <p>L'erreur est enregistrée en traçabilité.</p> <p>Dans le cas du canal Web-Service, une erreur est remontée (WSMG-0000017).</p> <p>Dans le cas du canal Web Service Mail, une erreur est remontée (WSMMG-0000013).</p> <p>Pour les trois canaux, un e-mail de notification est envoyé (NMG-005).</p> <p>L'utilisateur doit faire une nouvelle demande de certificat.</p>
RMT_ERR_005	<p>Échec lors de la validation de demande de retrait : &lt;raison&gt;</p> <p>Avec la variable &lt;raison&gt; qui peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• &lt;Erreur_Habilitation&gt;</li> <li>• L'acteur n'existe pas dans l'annuaire</li> <li>• Le bénéficiaire n'existe pas dans l'annuaire</li> <li>• La structure n'existe pas dans l'annuaire</li> <li>• Le produit n'est pas dans l'état « Produit à retirer ».</li> <li>• L'acteur ayant effectué la demande (&lt;idNat&gt;) doit être le même au retrait (&lt;idNat&gt;)</li> <li>• L'administrateur ASIP ayant effectué la demande (&lt;idNat&gt;) doit être le même au retrait (&lt;idNat&gt;)</li> </ul>	<p>La demande de retrait est rejetée par le système et n'est pas enregistrée en base.</p> <p>Le rejet est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché à l'écran (ERR_IHM_013).</p> <p>Dans le cas du canal Web-Service, une erreur est remontée (WSMG-0000011).</p> <p>Pour les canaux IHM et Web Service, un e-mail de notification est envoyé (NMG-006).</p> <p>Pour le canal Web Service Mail, un e-mail de notification est envoyée (NMG-005).</p> <p>L'utilisateur doit faire une nouvelle demande de retrait.</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_006	Web-Service PFCNG-IGC inaccessible au retrait technique du certificat	<p>Le Web-Service PFCNG-IGC n'est pas disponible ou ne répond pas avant le délai paramétré.</p> <p>Si l'appel nécessite une réponse immédiate (canal IHM ou Web-Service), le processus échoue directement.</p> <p>Dans ce cas, la demande de retrait échoue.</p> <p>Mais la demande de certificat reste à l'état « Demande transmise » et le produit reste à l'état « Produit à retirer ». L'échec est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché à l'écran (ERR_IHM_013).</p> <p>Dans le cas du canal Web-Service, une erreur est remontée (WSMG-00000015).</p> <p>L'utilisateur doit faire une nouvelle demande de retrait.</p> <p>Si l'appel ne nécessite pas de réponse immédiate (canal Web-Service Mail), alors plusieurs tentatives sont réalisées. Ces tentatives sont décrites dans le document [P2_SIS_IGC] au § II.3. Configuration du connecteur. Chaque tentative est enregistrée en traçabilité.</p> <p>Si les tentatives n'ont pas abouti, la demande de retrait échoue.</p> <p>La demande de certificat passe de l'état « Demande transmise » à l'état « Demande annulée ».</p> <p>Le produit passe de l'état « Produit à retirer » à l'état « Produit annulé ».</p> <p>Une erreur Web Service est remontée (WSMMG-00000011).</p> <p>Un e-mail de notification est envoyé (NMG-005).</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_007	Web-Service PFCNG-IGC renvoie une erreur au retrait technique du certificat	<p>La demande de retrait a été validée par le système PFCNG-MG mais elle est rejetée par le système PFCNG-IGC.</p> <p>Dans ce cas le retrait est impossible.</p> <p>La demande de certificat passe de l'état « Demande transmise » à l'état « Demande annulée ».</p> <p>Le produit passe de l'état « Produit à retirer » à l'état « Produit annulé ».</p> <p>L'erreur est enregistrée en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché à l'écran (ERR_IHM_013).</p> <p>Dans le cas du canal Web-Service, une erreur est remontée (WSMG-00000016).</p> <p>Dans le cas du canal Web-Service Mail, une erreur Web Service est remontée (WSMMG-00000012) et un e-mail de notification est envoyé (NMG-005).</p> <p>L'utilisateur doit faire une nouvelle demande de certificat.</p>
RMT_ERR_008	Annulation de la demande avant retrait technique dans la PFCNG-IGC	<p>Si après un certain délai paramétrable le retrait n'a pas été effectué (délai de retrait avant annulation), la demande expire automatiquement avec la tâche automatique « Annulation automatique des demandes de produits non retirés ».</p> <p>Si l'état de la Demande est « Demande validée », la Demande passe à l'état « Demande non traitée »</p> <p>Si l'état de la Demande est « Demande transmise », la Demande passe à l'état « Demande annulée ».</p> <p>Le produit passe de l'état « Produit à l'état « Produit annulé ».</p> <p>Pour les trois canaux, un e-mail de notification est envoyé (NMG-003).</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_009	Interruption du retrait fonctionnel du certificat après retrait technique dans la PFCNG-IGC	<p>Le certificat est émis par la PFCNG-IGC, il est enregistré par le système PFCNG-MG et le produit passe à l'état « Produit retiré », puis le processus est interrompu avant le retrait fonctionnel complet.</p> <p>Dans ce cas, la demande de retrait échoue.</p> <p>La demande de certificat reste à l'état « Demande transmise ».</p> <p>Le produit reste à l'état « Produit retiré ».</p> <p>L'échec est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM, un message d'erreur est affiché à l'écran (ERR_IHM_013).</p> <p>Si après un certain délai paramétrable le retrait n'a toujours pas été effectué (délai de retrait avant annulation), la demande expire automatiquement avec la tâche automatique « Révocation automatique de produits ».</p> <p>La demande passe de l'état « Demande transmise » à l'état « Demande annulée ».</p> <p>Un processus de révocation du certificat est enclenché : le système PFCNG-MG envoie un ordre de révocation à PFCNG-IGC concernant le certificat émis, et le produit passe à l'état « Produit révoqué ».</p> <p>Un e-mail de notification est envoyé (NMG-009).</p> <p>L'utilisateur doit faire une nouvelle demande de retrait.</p>
RMT_ERR_010	Erreur lors de la génération du fichier PKCS#12 côté utilisateur par l'applet de mise à disposition accompagnée	<p>L'applet n'est pas en mesure de reconstituer le PKCS#12 après avoir reçu le certificat.</p> <p>Si le mot de passe est invalide, un message d'erreur est affiché à l'écran (ERR_IHM_054). L'utilisateur doit recommencer la procédure de retrait.</p> <p>Si le mot de passe est perdu, si un fichier est corrompu, ou si le poste de travail n'est pas accessible, le PKCS#12 ne pourra pas être reconstitué. L'utilisateur doit recommencer toute la procédure, et effectuer une nouvelle demande de certificat avec une nouvelle CSR.</p> <p>L'utilisateur peut appeler le support ASIP qui l'aidera à identifier l'origine du problème et si besoin le guidera pour recommencer toute la procédure.</p>

Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_011	<p>Échec lors de l'enregistrement de la demande de révocation : &lt;raison de l'échec de l'enregistrement&gt;</p> <p>Avec la variable &lt;raison de l'échec de l'enregistrement&gt; qui peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• &lt;Erreur_Habilitation&gt;</li> <li>• L'acteur n'existe pas dans l'annuaire</li> <li>• Les contraintes sur les caractéristiques de la demande de révocation ne sont pas respectées : &lt;attribut métier&gt;.</li> <li>• Le produit n'est pas dans l'état « Produit actif » ou dans l'état « Produit retiré ».</li> </ul>	<p>La demande de révocation est rejetée par le système et n'est pas enregistrée. Le rejet est enregistré en traçabilité.</p> <p>Dans le cas du canal IHM présente un message d'erreur à l'écran (ERR_IHM_015).</p> <p>Dans le cas du canal Web Service, l'erreur WSMG-00000012 est remontée.</p> <p>Dans le cas du canal Web Service mail, l'erreur WSMMG-00000008 est remontée.</p> <p>Pour les canaux Web-Service et Web-Service Mail, un e-mail de notification est envoyé (NMG-008).</p> <p>L'utilisateur doit faire une nouvelle demande de révocation.</p>
RMT_ERR_012	<p>Web-Service PFCNG-IGC inaccessible à la révocation du certificat</p>	<p>Le Web-Service PFCNG-IGC n'est pas disponible ou ne répond pas avant le délai paramétré.</p> <p>Plusieurs tentatives sont réalisées. Ces tentatives sont décrites dans le document [P2_SIS_IGC] au § II.3. Configuration du connecteur. Chaque tentative est enregistrée en traçabilité.</p> <p>Pour les trois canaux, un e-mail de notification est envoyé pour avertir que la demande est mise en attente (NMG-014).</p> <p>Si les tentatives n'ont pas abouti, la demande de révocation échoue.</p> <p>La demande de révocation passe de l'état « Demande enregistrée » à l'état « Demande non traitée ».</p> <p>Le produit reste à l'état « Produit actif ».</p> <p>L'échec est enregistré en traçabilité.</p> <p>L'utilisateur doit faire une nouvelle demande de révocation.</p>



Code	Erreur	Gestion de l'erreur par la plateforme IGC-Santé
RMT_ERR_013	Web-Service PFCNG-IGC renvoie une erreur à la révocation du certificat	<p>La demande de révocation a été enregistrée par le système PFCNG-MG mais elle est rejetée par le système PFCNG-IGC.</p> <p>Dans ce cas la révocation est impossible. La demande de révocation passe à l'état « Demande non traitée » et le produit reste à l'état « Produit actif ».</p> <p>L'erreur est enregistrée en traçabilité.</p> <p>L'utilisateur doit faire une nouvelle demande de révocation.</p>
RMT_ERR_016	<p>Erreur lors de la vérification de la validité de la demande de suivi : &lt;raison&gt;</p> <p>Avec la variable &lt;raison&gt; qui peut prendre une des valeurs suivantes :</p> <ul style="list-style-type: none"> <li>• &lt;Erreur_Habilitation&gt;</li> <li>• L'acteur n'existe pas dans l'annuaire</li> <li>• Le bénéficiaire n'existe pas dans l'annuaire</li> <li>• La structure n'existe pas dans l'annuaire</li> </ul>	<p>La demande de suivi n'est pas un objet métier de la PFCNG-MG : il n'y a donc pas de changement d'état de la demande ou du produit.</p> <p>L'erreur est enregistrée en traçabilité.</p>

## 21Annexe – Titre Annexe

- **Annexe 1 :**

*AFR001-DOC-L06-701\_PFCNG\_Guide\_WebService\_PFCNG\_Annexe1*

- Exemple de signature
- Fichiers XSD et WSDL
- Exemples de fichiers XML (Demande, retrait, révocation ...)

## 22Annexe – Table des figures

Figure 1 : Présentation SOAP UI .....	8
Figure 2 : Présentation SOAP UI - XML généré.....	8
Figure 3 : Présentation SOAP UI - Réponse de la demande .....	9
Figure 4 : Présentation SOAP UI - Exemple de signature .....	10
Figure 5 - Barre des tâches, lancement de la console CCM .....	15
Figure 6 - Menu de la console CCM.....	15
Figure 7 - Fenêtre "A Propos CCM" .....	15
Figure 8 : Carte CPS à installer.....	16
Figure 9 : Gestionnaire de certificat CPS.....	16
Figure 10 : Gestionnaire de certificat CPS - Etat des lecteurs .....	17
Figure 11 - Schéma authentification serveur .....	29
Figure 12 - Schéma d'authentification client .....	30
Figure 13 : Process Signature .....	34
Figure 14 : Génération d'une clé privée.....	35
Figure 15 : Exemple de génération d'une CSR .....	36
Figure 16 : OpenSSL - CSR et Clé générées.....	36
Figure 17 : OpenSSL - Exemple de CSR.....	38
Figure 18 - Schéma de lot de certificats .....	39
Figure 19 : Demande de lot de certificat - Exemple SOAP UI.....	40
Figure 20 : Demande de lot de certificat - Exemple de requête .....	41
Figure 21 : Demande de lot de certificat - Requête - Détail.....	41
Figure 22 : Demande de lot de certificat - Requête - CSR .....	41
Figure 23 : Demande de lot de certificat – Exemple de Réponse .....	46
Figure 24 : Demande de lot de certificat – Réponse – Statut du Lot .....	46
Figure 25 : Demande de lot de certificat - Réponse – Statut de la Demande.....	47
Figure 26 : Exemple de Suivi de certificats - Demande .....	49
Figure 27 : Notification de la demande de certificat - Acteur.....	50
Figure 28 : Notification de la demande de certificat - Personne à informer .....	51
Figure 29 : Demande de lot de certificat - Cas non passant 1 - Requête .....	52
Figure 30 : Demande de lot de certificat - Cas non passant 1 - Réponse.....	53
Figure 31 : Demande de lot de certificat - Cas non passant 1 - Réponse - Statut du lot .....	53
Figure 32 : Demande de lot de certificat - Cas non passant 1 - Statut de la demande.....	53

Figure 33 : Demande de lot de certificat - Cas non passant 2 - Requête .....	54
Figure 34 : Demande de lot de certificat - Cas non passant 2 - Réponse.....	54
Figure 35 : Demande de lot de certificat - Cas non passant 2 - Réponse - Statut du lot .....	54
Figure 36 - Demande de retrait d'un certificat.....	55
Figure 37 : Retrait d'un certificat - Exemple SOAP UI .....	56
Figure 38 : Retrait de certificat - Exemple de requête .....	57
Figure 39 : Exemple Suivi des demandes de Certificats - Transmission .....	59
Figure 40 : Exemple Suivi des Certificats - Transmission.....	59
Figure 41 : Retrait de certificat - Exemple de réponse.....	60
Figure 42 : Retrait de certificat - Réponse - Statut de la réponse .....	60
Figure 43 : Retrait de certificat - Réponse - Certificat.....	60
Figure 44 : Notification de retrait de certificat - Acteur.....	61
Figure 45 : Notification du retrait de certificat - Personne à informer .....	61
Figure 46 : Retrait de certificat - Cas non passant 1 - Requête .....	62
Figure 47 : Retrait de certificat - Cas non passant 1 - Réponse.....	63
Figure 48 : Retrait de certificat - Cas non passant 1 - Statut de la réponse .....	63
Figure 49 : Retrait de certificat - Cas non passant 2 - Requête .....	64
Figure 50 : Retrait de certificat - Cas non passant 2 - Réponse.....	65
Figure 51 - Demande de révocation d'un certificat.....	66
Figure 52 : Révocation de certificat - Exemple SOAP UI.....	67
Figure 53 : Révocation de certificat - Exemple de requête .....	68
Figure 54 : Révocation de certificat - Requête - Détails.....	68
Figure 55 : Révocation de certificat - Exemple de réponse.....	71
Figure 56 : Révocation de certificat - Réponse - Statut de la réponse .....	72
Figure 57 : Notification de la révocation de certificat - Acteur .....	73
Figure 58 : Notification de la révocation de certificat - Personne à informer .....	74
Figure 59 : Révocation de certificat - Cas non passant 1 - Requête .....	75
Figure 60 : Révocation de certificat - Cas non passant 1 - Réponse.....	75
Figure 61 : Révocation de la demande - Cas non passant 2 - Requête .....	76
Figure 62 : Révocation de certificat - Cas non passant 2 - Réponse.....	76
Figure 63 - Demande de renouvellement d'un certificat .....	77
Figure 64 : Renouvellement de certificat - Exemple SOAP UI .....	78
Figure 65 : Renouvellement de certificat - Exemple de requête.....	80
Figure 66 : Renouvellement de certificat - Réponse - Détails .....	80
Figure 67 : Renouvellement de certificat - Réponse - CSR.....	81
Figure 68 : Renouvellement de certificat - Exemple de réponse .....	83

Figure 69 : Renouvellement de certificat - Réponse - Détail du statut .....	83
Figure 70 : Renouvellement de certificat - Réponse - Indice de retrait .....	83
Figure 71 : Notification de validation de la demande - Acteur .....	85
Figure 72 : Notification de la validation de la demande - Personne à informer .....	86
Figure 73 : Renouvellement de certificat - Cas non passant 1 - Requête .....	87
Figure 74 : Renouvellement de certificat - Cas non passant 1 - Réponse .....	87
Figure 75 : Renouvellement de certificat - Cas non passant 1 - Réponse - Message d'erreur.....	88
Figure 76 : Renouvellement de certificat - Cas non passant 2 - Requête .....	89
Figure 77 : Renouvellement de certificat - Cas passant 2 - Réponse .....	89
Figure 78 : Renouvellement de certificat - Réponse - Message d'erreur.....	89
Figure 79 : Suivi de l'activité - Exemple SOAP UI.....	91
Figure 80 : Suivi de l'activité - Exemple de requête .....	92
Figure 81 : Suivi de l'activité - Requête - Détails .....	92
Figure 82 : Suivi de l'activité - Exemple de réponse.....	101
Figure 83 : Suivi de l'activité - Réponse - Statut de la réponse .....	101
Figure 84 : Suivi de l'activité - Réponse - Détails du résultat .....	102
Figure 85 : Suivi de l'activité - Cas non passant 1.....	103
Figure 86 : Suivi de l'activité - Cas non passant 1 - Requête .....	104
Figure 87 : Suivi de l'activité - Cas non passant 1 - Réponse.....	104
Figure 88 : Suivi de l'activité - Cas non passant 2 - Requête .....	106
Figure 89 : Suivi de l'activité - Cas non passant 2 - Réponse.....	107

## 23Annexe – Liste des tableaux

Tableau 1 : Documents de référence .....	5
Tableau 2 : Glossaire .....	12
Tableau 3 : Avertissements .....	13
Tableau 4 : Avertissements .....	<b>Erreur ! Signet non défini.</b>
Tableau 5 : Habilitations Rôle/Périmètre .....	20
Tableau 6 : Actions autorisées en fonction du rôle .....	21
Tableau 7 : Type d'offre / Usage .....	21
Tableau 8 : Contenu de la signature.....	32
Tableau 9 : OpenSSL : Génération d'une clé privée .....	35
Tableau 10 : OpenSSL : Construction d'une CSR pour l'IGC-Santé.....	36
Tableau 11 : Paramètres d'entrée de la Demande de certificat .....	44
Tableau 12 : Paramètres de la réponse de certificat .....	45
Tableau 13 : Paramètres d'entrée du retrait de certificat .....	58
Tableau 14 : Paramètres de transmission du certificat.....	59
Tableau 15 : Paramètres d'entrée de la requête de révocation .....	70
Tableau 16 : Paramètres de réponse de révocation .....	71
Tableau 17 : Paramètres d'entrée de la requête de renouvellement de certificat .....	82
Tableau 18 : Paramètres de réponse de renouvellement de certificat .....	83
Tableau 19 : Paramètres d'entrée du suivi d'activité.....	94
Tableau 20 : Paramètres du statut de la réponse du suivi d'activité .....	95
Tableau 21 : Paramètres de la réponse du suivi d'activité.....	100
Tableau 22 : Erreurs Web Service .....	112

## 24Notes

[fin du document]



Agence du Numérique en Santé  
9, rue Georges Pitard – 75015 Paris  
Tél : 01 58 45 32 50  
[esante.gouv.fr](http://esante.gouv.fr)