AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

Notice de migration IGC Santé à destination des éditeurs de connecteurs et opérateurs MSSanté

Version 1.0.1

Identification du document	
Référence ASIP Santé	**MSS_Notice_Migration_IGC_Santé_v1.0.1**
Date de dernière mise à jour	**12/10/2016**
Classification	**Non sensible public**
Nombre de pages	**17**

Historique du document

Version	Date	Auteur	Commentaires
V0.9.0	06/07/2016	ASIP Santé	Version projet
V1.0.0	15/09/2016	ASIP Santé	Version finale
V1.0.1	11/10/2016	ASIP Santé	Adaptation de la stratégie de migration (ajout des lots L1 et L2) pour prendre en compte la disponibilité des flux IGC Santé de l'annuaire MSSanté.

Documents de référence

Interfaces d'accès au système de Messageries Sécurisées de Santé - Dossier des Spécifications Fonctionnelles et Techniques (DSFT) version 1.1.0.

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T.+33 (0)1 58 45 32 50
esante.gouv.fr

Sommaire

1 Introduction

Cette notice présente la stratégie de migration IGC Santé des opérateurs MSSanté liée à l'introduction de l'IGC Santé début 2016. Elle décrit les opérations à mener par les éditeurs de connecteurs et les opérateurs pour être compatible avec l'IGC Santé.

Elle vient en accompagnement du DSFT en version 1.1.0 qui introduit les exigences liées à l'IGC Santé. Dans ce document, la mention du DSFT se réfère à cette version et les suivantes.

Cette migration est à réaliser par la totalité des opérateurs MSSanté actuellement en service et ceux en cours d'intégration dans l'espace de confiance. Les nouveaux opérateurs ne sont pas concernés par cette migration et se mettront directement en conformité avec le DSFT.

1.1 Objectif du document

Ce document est à destination des équipes techniques des éditeurs de connecteurs MSSanté et des opérateurs MSSanté en charge de la migration IGC Santé.

Il a pour objectif de communiquer aux équipes techniques les éléments d'information nécessaires pour mener à bien leur projet de migration IGC Santé.

Dans cette optique, ce document s'organise en 4 sections :

- Présentation générale de l'IGC Santé et liens vers les documents correspondants (cf. §2) ;
- Présentation de la stratégie de migration retenue par l'ASIP Santé (cf. §3);
- Description des impacts et évolutions des composants de l'espace de confiance planifiées par l'ASIP Santé (cf. §4) ;
- Opérations et évolutions à réaliser par les éditeurs/opérateurs (cf. §5).

1.2 Contexte de la migration

La messagerie sécurisée de santé MSSanté utilise actuellement l'IGC CPS pour ses besoins d'authentification et de sécurisation des échanges de mail. Cette IGC a été mise service en 2004 par l'ASIP Santé et son échéance de fin de vie est fixée à 2020.

En vue de préparer cette échéance, l'ASIP Santé a mis en service en mars 2016 une nouvelle IGC, dite IGC Santé, dont l'objectif est de remplacer l'IGC CPS tout en offrant un niveau de sécurité accru et conforme à l'état de l'art ainsi qu'une gamme étendue de produits de certification (par exemple certificats de personnes morales et personnes physiques adaptés à chaque usage : authentification, signature et chiffrement).

La mise en service de l'IGC Santé va entrainer l'arrêt de l'émission des certificats IGC CPS 2BIS 12 mois après (mars 2017). Toutefois les certificats IGC CPS 2BIS resteront valides jusqu'à leur expiration, au plus tard en 2020 pour les derniers certificats émis par l'IGC CPS 2BIS.

En conséquence de cet arrêt, les opérateurs intégrant l'espace de confiance à partir de mars 2017 mettront en œuvre un certificat IGC Santé, ainsi que ceux dont le certificat IGC CPS 2BIS expire.

Ainsi pour assurer l'interopérabilité entre opérateurs, une migration technique est nécessaire de la part des opérateurs. Plus précisément elle concerne :

- Les opérateurs en service actuellement avec un certificat IGC CPS 2BIS ;
- Les futurs opérateurs qui offriront leurs services d'ici mars 2017.

Toutefois elle ne concerne pas les futurs opérateurs qui offriront leurs services à compter de mars 2017 car ils déploieront directement un certificat IGC Santé en conformité avec le DSFT.

Cette migration ne présente pas de complexité technique mais nécessite d'être mise en œuvre dans les délais précisés et cadencée en cohérence avec la stratégie de migration de l'espace de confiance pilotée par l'ASIP Santé.

Cette migration IGC Santé se fera en deux temps : migration des certificats logiciels issus de l'IGC CPS 2BIS dans un premier temps durant l'année 2016, puis migration des certificats de carte CPx issus de l'IGC CPS 2TER dans un second temps.

Ce document porte uniquement sur la migration des certificats logiciels. La migration des certificats CPx est hors du cadre de ce document et sera par conséquent adressée ultérieurement.

2 Présentation de l'IGC Santé

L'IGC Santé a pour vocation de remplacer l'IGC CPS 2BIS (certificats logiciels classe 4 SSL et S/MIME) et l'IGC-CPS 2TER (certificats de carte confinés dans les CPx).

L'IGC Santé bénéficie des solutions cryptographiques à l'état de l'art : clés RSA de 2048 bits et algorithme d'empreinte SHA-2.

La gestion du cycle de vie des certificats (soumission du CSR, émission du certificat, révocation du certificat, etc.) se fait au travers d'un portail en ligne.

2.1 Calendrier de déploiement

Le calendrier de déploiement des certificats logiciels est le suivant :

- **1er mars 2016** (**T0**) : début émission des certificats logiciels par l'IGC Santé (test et production) ;
- **1er mars 2017** (**T1=T0+12mois**) : arrêt émission des certificats IGC CPS 2BIS. La révocation reste possible ;
- Fin 2020 : fin de vie de l'IGC CPS 2BIS : dépublication des certificats racines et intermédiaires.

A titre indicatif, le calendrier prévisionnel de déploiement des cartes CPx embarquant des certificats IGC Santé est le suivant :

- Début 2017 : début émission des CPx de test
- Courant 2017 : début émission des CPx de production
- Fin 2020 : fin de vie IGC 2TER : dépublication des certificats racines et intermédiaires.

2.2 Documents techniques

Pour identifier précisément les impacts techniques de l'IGC Santé, le lecteur s'appuiera sur les documents techniques suivants :

- Notice introductive de l'IGC Santé : http://integrateurs-cps.asipsante.fr/IGC-Sante
- Gabarit des certificats et des CRL : http://integrateurs-cps.asipsante.fr/pages/IGC-Santé-Gabarits
- Consignes de migration IGC Santé (différences entre les certificats IGC CPS 2BIS et IGC Santé): http://integrateurs-cps.asipsante.fr/IGC-Sante-migration

3 Principes de la stratégie de migration

Les enjeux de la migration IGC Santé sont les suivants :

- Assurer une cohabitation l'IGC CPS 2BIS et l'IGC Santé afin de garantir une continuité de service dans l'espace de confiance durant la migration ;
- Minimiser les impacts techniques sur les connecteurs ;
- Eviter les ouvertures de nouveaux flux, souvent problématiques car cela nécessite une reconfiguration des équipements réseaux (DNS, parefeux, etc.).

Afin de répondre à ces enjeux, l'ASIP Santé a élaboré une stratégie de migration des connecteurs MSSanté en trois phases :

- Phase 0 – Migration de l'espace de confiance
- Phase 1 – Migration des opérateurs
- Phase 2 – Bascule des opérateurs vers les certificats IGC Santé

3.1 Phase 0 – Migration de l'espace de confiance

Cette phase se déroule jusqu'à la date T1 et concerne l'opérateur ASIP Santé.

Durant cette phase, l'opérateur ASIP Santé évolue pour supporter l'IGC Santé. L'ASIP Santé réalise également la migration de l'espace de confiance. L'annuaire MSSanté évolue pour présenter un deuxième flux déployant un certificat IGC Santé, tout en maintenant le flux actuel avec un certificat IGC CPS 2BIS.

Une liste blanche IGC Santé est mise en place, en plus de la liste blanche actuelle. Cette liste blanche contiendra après la bascule tous les domaines IGC CPS 2BIS et IGC Santé.

L'ASIP Santé met en place des moyens de test permettant aux éditeurs de connecteur et opérateurs de tester les évolutions.

3.2 Phase 1 – Migration des opérateurs

Cette phase se déroule de septembre 2016 (date de parution du DSFT 1.1.0) jusqu'à la date T1 et concernent tous les opérateurs intégrés à l'espace de confiance.

Les opérateurs effectuent leur étude d'impacts et réalisent les évolutions pour être en capacité d'accepter les certificats IGC CPS 2BIS et IGC Santé. Ils testent et déploient leurs évolutions sur les connecteurs en service dans l'espace de confiance.

Dans cette phase, aucun opérateur n'est autorisé à présenter un certificat IGC Santé afin de maintenir l'interopérabilité entre les opérateurs ayant migré et ceux n'ayant pas encore migré.

Les nouveaux opérateurs arrivant dans l'espace de confiance déploient un certificat IGC CPS 2BIS.

3.3 Phase 2 – Bascule vers un certificat IGC Santé

Cette phase se déroule à partir de T1.

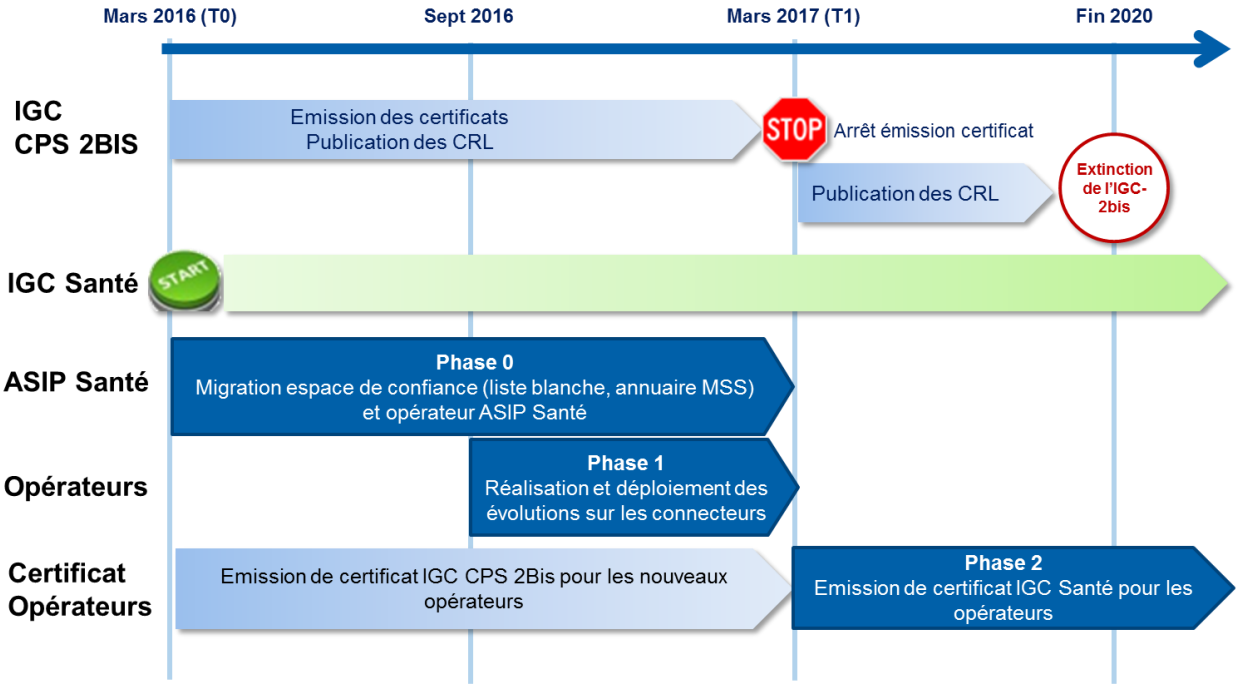
Lors de l'expiration des certificats IGC CPS 2BIS, les opérateurs renouvèlent leur certificat avec un certificat IGC Santé.

Les nouveaux opérateurs mettent en œuvre directement un certificat IGC Santé.

Les opérateurs n'ayant pas réalisés la migration (phase 1) dans les temps seront dans l'incapacité de communiquer avec ceux utilisant des certificats IGC Santé en phase 2.

3.4 Déroulement des phases

Les phases 0 et 1 se déroulent en parallèle, la phase 2 se déroule à partir de T1 comme l'illustre la figure suivante:



3.5 Points importants

Deux points importants sont à retenir :

- Aucun opérateur MSSanté ne doit mettre en œuvre un nouveau certificat IGC Santé avant T1 afin de ne pas bloquer les échanges avec les opérateurs qui ne seraient pas encore compatibles avec l'IGC Santé ;
- Tous les opérateurs doivent terminer la migration dans les temps (avant T1), faute de quoi les opérateurs n'ayant pas effectué cette étape ne pourront pas communiquer avec les nouveaux opérateurs ayant obtenu un certificat IGC Santé après bascule (après T1).

4 Impacts et évolutions IGC Santé

4.1 Préambule

Cette section présente les impacts généraux sur l'espace de confiance liés à la migration vers l'IGC Santé. Cette section présente également le calendrier des évolutions réalisées par l'ASIP Santé pour les composants sous son périmètre incluant la liste blanche et l'annuaire MSSanté.

Dans le cours de ce document, un opérateur ayant migré signifie qu'il a effectué les évolutions nécessaires pour être en capacité de supporter l'IGC Santé, en plus de l'IGC CPS qu'il supporte déjà. Cela ne signifie pas qu'il présente un certificat IGC Santé. Il continuera à

présenter son certificat IGC CPS 2BIS jusqu'à son remplacement (lors de son expiration par exemple) par un certificat IGC Santé.

Les éditeurs et opérateurs ont la responsabilité de mener une analyse d'impact technique sur leur implémentation afin d'évaluer précisément les impacts liés à l'IGC Santé.

4.2 Impacts sur le gabarit des certificats

Outre l'évolution des moyens cryptographiques utilisés pour les certificats IGC Santé (RSA 2048 bits, SHA-2), le champ DN évolue également de la manière suivante :

DN IGC CPS	DN IGC Santé
C=FR	C=FR
n/a	ST=<Nom département (n°)>
O=GIP-CPS	O=<Raison sociale Structure>
L=<Nom département (n°)>	n/a
OU=<IdNat_Struct>	OU=<IdNat_Struct>
CN=<Nom applicatif>	CN=<Nom applicatif>

Extrait du document « Consignes de migration IGC Santé », cf. lien en §2.2

Le DN des certificats IGC Santé de test ne contient plus le mot « TEST ». Pour distinguer un certificat de test, il est donc nécessaire de vérifier le CN de l'AC racine ou intermédiaire qui commence par « TEST ». Toutefois les opérateurs n'ont pas besoin d'implémenter cette distinction.

Note pour les éditeurs utilisant les API .Net de Microsoft :

Dans l'API .Net, la propriété « Subject » de la classe *System.Security.Cryptography.X509Certificates.X509Certificates2* permettant de récupérer le DN d'un certificat retourne une chaine avec un sous-champ « S » au lieu de « ST ». Ce sous-champ « S » n'est pas conforme au format défini par la RFC2253.

Ainsi les opérations suivantes qui impliquent le traitement du DN sont impactées :

- Comparaisons de DN : typiquement comparaison du DN issu du certificat présenté par un opérateur avec celui en liste blanche ;
- Construction du VIHF pour l'alimentation de l'annuaire MSSanté. Afin de garantir l'interopérabilité avec l'annuaire, le VIHF doit se conformer à la RFC2253 et contenir le sous-champ « ST » dans le champ « émetteur ».

4.3 Impacts sur la liste blanche

Pour des raisons de continuité de service avec les opérateurs n'ayant pas encore migré durant la phase 1, **aucun certificat IGC Santé ne devra être utilisé par un opérateur, ni par la liste blanche actuelle et l'annuaire sur les interfaces actuelles jusqu'à la fin de cette phase (T1).**

En vertu de ce principe, la liste blanche IGC Santé intégrant aussi des certificats IGC Santé est disponible sur une URL différente de celle actuelle, permettant aux opérateurs n'ayant pas migré de continuer à utiliser l'URL actuelle.

Les opérateurs ayant migré téléchargeront la liste blanche IGC Santé sur l'URL associée.

Se référer au DSFT pour les détails techniques.

Point à retenir : durant la phase de migration, deux listes blanches différentes sont présentes : la liste blanche actuelle contenant uniquement les domaines avec un certificat IGC CPS 2BIS et la liste blanche IGC Santé contenant tous les domaines quel que soit leur certificat. A l'issue de la migration, la liste blanche 2BIS ne sera plus publiée.

4.4 Impacts sur l'annuaire MSSanté

En vertu du même principe, l'annuaire MSSanté présentera un second flux présentant un certificat IGC Santé pour la consultation et l'alimentation.

Quel que soit le flux utilisé (le flux IGC CPS 2BIS ou IGC Santé), les données téléchargées de l'annuaire sont identiques.

4.5 Impacts sur les connecteurs

La migration IGC Santé entraine les impacts suivants sur les connecteurs:

Phase	Lot	Impact	Description de l'impact
P1	L1	I1	Support IGC Santé sur l'interface SMTPS : Capacité de l'opérateur à se connecter à un autre opérateur présentant un certificat IGC-CPS ou IGC Santé.
		I2	Support IGC Santé dans la liste blanche : Capacité à intégrer une liste blanche intégrant des opérateurs ayant un DN au format IGC CPS ou IGC Santé.
		I3	Support IGC Santé pour la signature de la liste blanche : Capacité à vérifier la signature de la liste blanche signée par un certificat IGC Santé.
	L2	I4	Support IGC Santé sur l'interface WS d'extraction de l'annuaire MSSanté : Capacité à se connecter sur le flux IGC Santé de l'annuaire MSS présentant un certificat IGC Santé.
		I5	Support IGC Santé sur l'interface WS d'alimentation de l'annuaire MSSanté : Capacité à construire le VIHF avec un certificat IGC Santé pour alimenter l'annuaire MSSanté.
P2	N/A	I6	Renouvellement des certificats SSL IGC CPS par des certificats IGC Santé.

Les évolutions liées à ces impacts se décomposent en deux lots L1 et L2 qui seront faits (c'est-à-dire réalisés et déployés) par les éditeurs de connecteur durant la phase 1 de la migration.

Le lot L1 est à réaliser **impérativement avant T1 (mars 2017)**, faute de quoi l'opérateur concerné sera dans l'incapacité de communiquer avec les opérateurs ayant un certificat IGC Santé.

Le lot L2 est relatif à l'annuaire MSSanté et peut être réalisé avant ou après T1, selon les contraintes des éditeurs ou des opérateurs.

Dans le cas où L2 est fait à une date *T* après T1, l'opérateur utilisera jusqu'à cette date *T* son certificat IGC CPS 2BIS pour accéder à l'annuaire sur les URL IGC CP2BIS et s'interfacer avec les autres opérateurs.

En conséquence l'opérateur devra s'assurer de la validité de son certificat CPS 2BIS jusqu'à la date *T* et devra veiller à son renouvellement si besoin avant T1. Le déploiement du certificat IGC Santé peut être fait lors du déploiement de ce lot chez l'opérateur.

4.6 Modalités de test

Pour chaque impact mentionné ci-dessus, l'opérateur est en capacité de tester ses évolutions soit directement dans l'espace de confiance, soit au travers de moyen de tests spécifiques.

Les moyens mis en place à des fins de test sont les suivants :

- Lot L1 : l'espace de confiance offre un connecteur de test qui présente un certificat IGC Santé et accepte les certificats IGC CPS 2BIS et IGC Santé pour tester la capacité du connecteur de l'opérateur à interagir avec un opérateur présentant un certificat IGC Santé.
- Lot L2 : hors espace de confiance, un annuaire de test dit « partenaire » est disponible, il présente un certificat IGC Santé de test et accepte les certificats IGC CPS 2BIS et IGC Santé de test pour tester l'extraction et l'alimentation de l'annuaire avec un certificat IGC Santé.

La section suivante présente le calendrier de mise en place de ces dispositifs de test.

4.7 Calendrier des évolutions de l'ASIP Santé

La réalisation et la recette des évolutions du connecteur doit se faire en cohérence avec les évolutions réalisées par l'ASIP Santé sur l'annuaire MSSanté, la liste blanche et les moyens de tests à destination des éditeurs de connecteur et opérateurs.

Les évolutions sur l'espace de confiance et l'opérateur ASIP Santé seront disponibles à partir de septembre 2016 (excepté l'annuaire MSSanté) et donneront le point de départ de la migration des opérateurs.

La table suivante résume le calendrier de ces évolutions :

Date	Jalon
Septembre 2016	**Connecteur de test IGC Santé dans l'espace de confiance:** Mise à disposition d'un connecteur de test qui présente un certificat IGC Santé de production, gamme Elémentaire domaine Organisations. Permet de valider les évolutions liées à l'impact I1 (lot L1). L'opérateur présente un certificat IGC CPS 2BIS.
	Migration du connecteur de l'opérateur ASIP Santé : Support de l'IGC Santé sur l'interface opérateur SMTPS (accepte l'IGC CPS 2BIS et IGC Santé).
	Liste blanche IGC Santé : Publication de la liste blanche IGC Santé intégrant des certificats IGC-Santé et signée par un certificat IGC Santé. Certificat IGC Santé sur l'URL d'accès.

	Permet de valider les évolutions liées aux impacts I2 et I3 (lot L1). L'opérateur présente un certificat IGC CPS 2BIS.
Novembre 2016	**Annuaire MSSanté de test partenaire :** Support de l'IGC Santé sur les interfaces WS de l'annuaire partenaire, qui présentent un certificat IGC Santé. Permet de valider les évolutions liées aux impacts I4 et I5 (lot L2). L'opérateur présente un certificat IGC Santé de test ou CPS 2BIS de test.
Date avant T1 (date à préciser)	**Annuaire MSSanté :** Mise à disposition du flux IGC Santé sur les interfaces WS, qui présentent un certificat IGC Santé. L'opérateur présente un certificat IGC CPS 2BIS.
A partir de mars 2017 (T1)	Fin émission de certificat IGC CPS 2BIS Arrivée des opérateurs avec un certificat IGC Santé dans l'espace de confiance

4.8 Synthèse des flux et usages des certificats

Cette section présente sous forme graphique les flux de connections avec les certificats utilisés avant, pendant et après la migration.

4.8.1 Légende des flux

Les schémas décrits dans les prochaines sections utilisent la légende suivante :

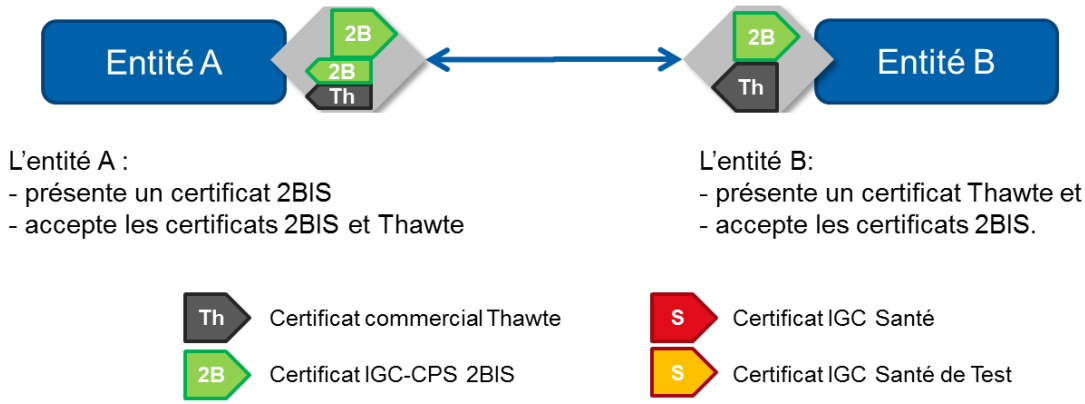


Figure 1 - Légende des flux

Le diamant gris représente les certificats présentés et acceptés par l'entité associée à cette zone.

Concernant les certificats IGC Santé à déployer par les opérateurs (après T1), il s'agit du type SERV_SSL_SERV de la gamme élémentaire.

4.8.2 Flux avant la migration (phase 0)

Les flux actuels sont les suivants :

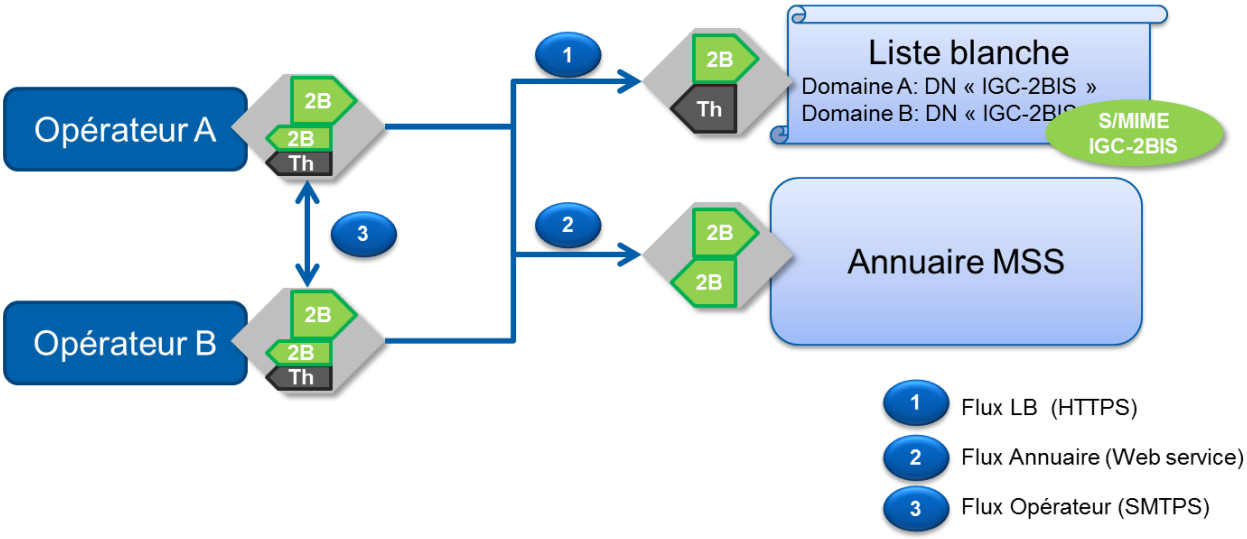


Figure 2 - cas d'usage des flux avant migration

Tous les opérateurs utilisent un certificat IGC CPS 2BIS, ainsi que l'annuaire MSSanté.

La liste blanche contient uniquement des certificats IGC CPS 2BIS, elle est signée par un certificat S/MIME IGC CPS 2BIS.

Note concernant le certificat Thawte :

Pour des raisons historiques, l'interface d'accès à la liste blanche présente un certificat issu de l'IGC commerciale Thawte, obligeant les opérateurs MSSanté à intégrer la chaine de confiance Thawte en complément de la chaine IGC CPS 2BIS.

Dans le cadre de la migration IGC Santé, l'interface d'accès à nouvelle liste blanche IGC Santé présentera un certificat IGC Santé. Cette rationalisation a pour bénéfice de limiter les opérateurs au support de seulement l'IGC CPS 2BIS et l'IGC Santé.

4.8.3 Flux durant la migration (phase 1)

La situation dans l'espace de confiance verra la coexistence d'opérateurs ayant migré (ou en cours de migration) et d'autres dont la migration n'a pas débutée, comme la montre la figure suivante :

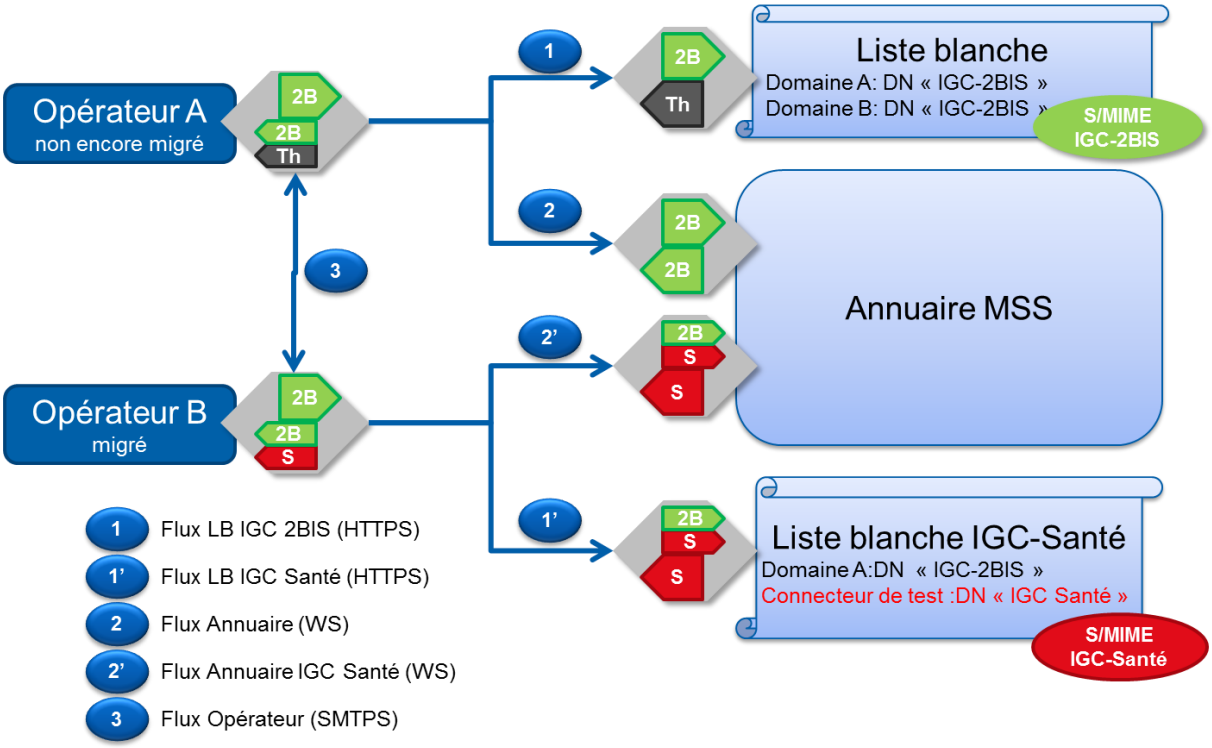


Figure 3 – Cas d'usage des flux avec un opérateur non migré et un opérateur migré.

L'opérateur A, qui n'a pas encore migré, continue d'utiliser un certificat IGC CPS 2BIS. Il continue d'utiliser les flux actuels 1 et 2 pour accéder à la liste blanche et l'annuaire MSS.

L'opérateur B, qui a migré (c'est-à-dire déployé les lots L1 et L2), se connecte à la liste blanche IGC Santé (flux 1') et utilise l'annuaire MSS sur l'URL IGC Santé (flux 2', dont la date de disponibilité n'est pas connue lors de parution de la notice). Toutefois il continue à utiliser un certificat IGC CPS 2BIS pour assurer la continuité de service avec les opérateurs n'ayant pas encore migré.

Un opérateur ayant migré partiellement (lot L1 déployé) se connecte à la liste blanche IGC Santé (flux 1') et utilise l'annuaire MSSanté sur l'URL IGC CPS 2BIS (flux 2).

Durant cette phase, la liste blanche actuelle et la liste blanche IGC Santé contiennent les mêmes domaines, à l'exception du domaine de test IGC Santé présent uniquement dans cette dernière.

A noter que le support de l'IGC Thawte n'est plus requis pour l'opérateur ayant migré puisque la liste blanche IGC Santé présente un certificat IGC Santé en remplacement du certificat Thawte.

4.8.4 Flux à l'issue de la migration (après T1)

A l'issue de la phase 1, tous les opérateurs auront migré (ou à minima déployé le lot L1). Certains continueront à utiliser leur certificat IGC CPS 2BIS jusqu'à expiration (2020 pour les derniers).

Les opérateurs n'ayant pas déployé le lot L2 avant T1 pourront le faire après cette date, sous réserve que leur certificat IGC CPS 2BIS ne soit pas expiré. Ils pourront profiter du déploiement du lot L2 pour effectuer la bascule du certificat (remplacement du certificat CPS 2BIS par un certificat IGC Santé).

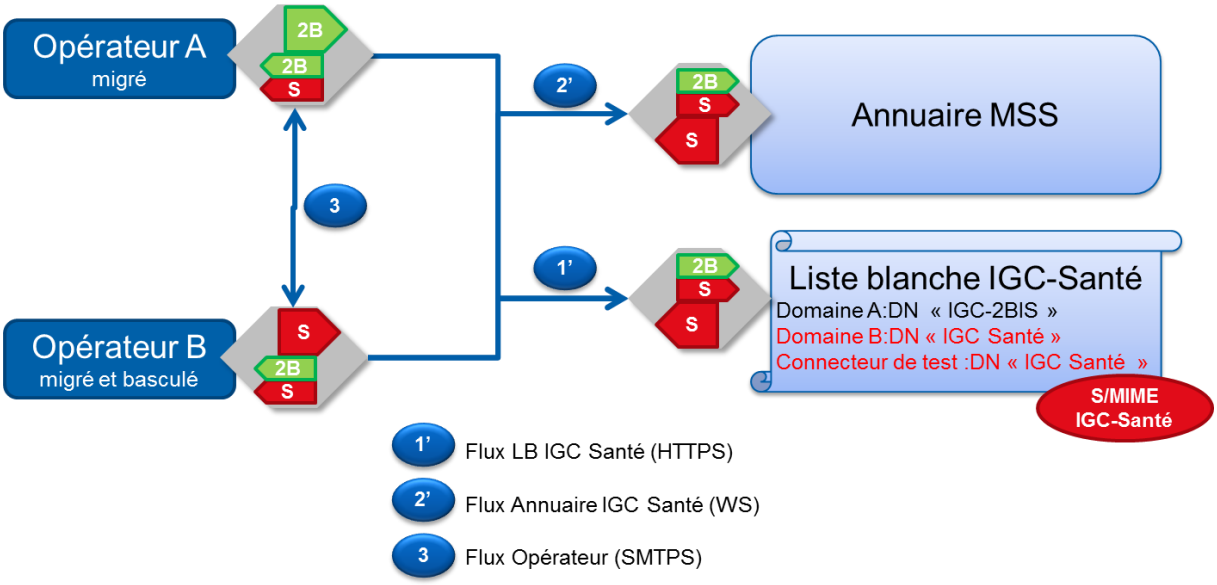


Figure 4 - Cas d'usage à l'issue de la migration

La figure ci-dessus montre un opérateur A ayant migré, c'est-à-dire en capacité de recevoir des certificats IGC CPS 2BIS ou IGC-Santé. Il peut continuer à utiliser son certificat IGC CPS 2BIS jusqu'à expiration (en 2020 au plus tard).

L'opérateur B utilise un certificat IGC Santé : cas d'un opérateur ayant intégré l'espace de confiance après T1 ou dont le certificat IGC CPS 2BIS a expiré après T1. Il doit continuer à accepter les certificats IGC CPS 2BIS pour supporter les opérateurs non encore basculés.

5 Opérations à réaliser

Cette section concerne les opérations à réaliser par les éditeurs de connecteur et les opérateurs pour mener à bien la migration IGC Santé.

En pratique, ces opérations sont peu nombreuses et nécessitent peu d'évolutions sur les solutions déjà déployées.

Pour chaque impact identifié en §4.5 ci-dessus, les opérations à réaliser sont précisées à titre indicatif. Les éditeurs et opérateurs ont la responsabilité d'évaluer précisément les évolutions à mettre en œuvre sur leurs solutions.

Les opérateurs disposeront de moyens de test disponibles à partir de septembre 2016 : un connecteur de test permettant de valider le support de l'IGC Santé et un annuaire MSSanté partenaire permettant de tester l'alimentation de l'annuaire. Voir ci-après pour les évolutions et les tests à réaliser.

5.1 Interface SMTPS (lot L1)

Opérations à réaliser concernant l'impact I1:

1. Ajouter dans le(s) magasin(s) de confiance du connecteur la chaine IGC Santé gamme Elémentaire domaine Organisations de la branche de production ;
2. Tester en envoyant un mail au connecteur de test IGC Santé ;
3. Faire un test de non-régression en envoyant un mail au connecteur de test IGC CPS 2BIS.

La chaine IGC Santé (certificats racine ACR et intermédiaire ACI) est disponible à l'adresse suivante : http://igc-sante.esante.gouv.fr/PC/#ca.

Le domaine du connecteur de test est le suivant : reponse.automatique@test-igc.mssante.fr.

Pour les opérateurs mettant un œuvre un contrôle de non révocation des certificats basé sur les CRL, les CRL du domaine Organisations de la gamme Elémentaire sont disponibles aux adresses suivantes :

- URL http : http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl
- URL ldap[1] : ldap://annuaire-igc.esante.gouv.fr/cn=AC IGC-SANTE ELEMENTAIRE ORGANISATIONS, ou=AC RACINE IGC-SANTE ELEMENTAIRE,ou=IGC-SANTE,ou=0002 187512751, o=ASIP-SANTE,c=FR?certificaterevocationlist;binary?base?objectClass=pkiCA
- URL ldap des delta CRL : ldap://annuaire-igc.esante.gouv.fr/cn=AC IGC-SANTE ELEMENTAIRE ORGANISATIONS, ou=AC RACINE IGC-SANTE ELEMENTAIRE, ou=IGC-SANTE,ou=0002 187512751, o=ASIP-SANTE,c=FR?deltarevocationlist;binary?base?objectClass=pkiCA

Note : les CRL IGC Santé sont publiées quotidiennement et sont valables 7 jours.

Pour ceux réalisant ce contrôle de non révocation en récupérant de manière périodique l'ensemble des certificats présents en liste blanche, les certificats IGC Santé sont publiés dans l'annuaire CPS. Toutefois la structure des requêtes pour les télécharger a évoluée. Se référer au document « Gabarit des certificats et des CRL » §3.4 pour plus d'informations (cf. section §2.2 pour le lien de ce document).

5.2 Liste blanche (lot L1)

Opérations à réaliser concernant les impacts I2 et I3:

- Tester la capacité du connecteur à parcourir la liste blanche intégrant des domaines ayant un DN issu d'un certificat IGC Santé.
  En cas de test positif, pas d'évolution nécessaire sur ce point.
- Tester la capacité du connecteur à valider la signature de la liste blanche utilisant un certificat IGC Santé
  En cas de test positif, pas d'évolution nécessaire sur ce point.
- Mettre à jour l'URL de la liste blanche pour utiliser l'URL suivante : https://espacedeconfiance.mssante.fr/listeblanchemssante.xml.

Pour tester les points 1 et 2, un exemple de liste blanche intégrant des domaines IGC Santé et signée avec un certificat IGC Santé est disponible dans le DSFT §7.4.2 référence DR1.

Pour rappel, la liste blanche actuelle dont l'URL est https://listeblanche.mssante.fr/listeblanchemssante.xml sera dé-publiée à l'issue de la phase de migration.

5.3 Extraction de l'annuaire MSSanté (lot L2)

Opérations à réaliser concernant l'impact I4 dans le cas où le connecteur implémente ce service :

1. Mettre à jour l'URL d'extraction de l'annuaire MSSanté vers l'URL suivante (transaction TM2.1.3A) conformément au DSFT §7.3.1.
2. Tester l'extraction de l'annuaire MSSanté (de production ou partenaire).

Se référer au DSFT §7.3.2 pour les URL de l'annuaire partenaire.

Le prérequis à ces opérations est l'ajout de la chaine IGC Santé dans les magasins de confiance du connecteur.

[1] Pour des raisons d'édition dans ce document, les URL ldap contiennent des retours chariot qu'il conviendra de supprimer en cas de copier/coller.

Note : à la date de parution de cette notice, la disponibilité de l'annuaire compatible IGC Santé n'est pas connue. La disponibilité de l'annuaire partenaire compatible IGC Santé est prévue pour novembre 2016, ainsi ces opérations ne pourront être testées avant cette date.

Pour rappel, ces opérations (liées au lot L2) peuvent être réalisées et déployées après la date T1, sous réserve que le certificat IGC CPS 2BIS des opérateurs n'expire pas avant le déploiement de ce lot.

5.4 Alimentation de l'annuaire MSSanté (lot L2)

Opérations à réaliser concernant l'impact I5 :

1. Mettre à jour la construction du VIHF suite au changement du format du DN des certificats IGC Santé. Toutefois le VIHF devra supporter également les certificats IGC CPS 2BIS.
2. Mettre à jour les URL d'alimentation de l'annuaire MSSanté et de récupération du CR d'alimentation conformément au DSFT §7.3.1.

Comme les opérateurs ne peuvent pas utiliser un certificat IGC Santé durant la phase de migration dans l'espace de confiance, les tests se feront hors espace de confiance sur l'annuaire partenaire. L'éditeur ou l'opérateur aura le choix entre un certificat IGC Santé de test ou de production, l'annuaire partenaire acceptant les deux.

Les opérations de tests sont les suivantes :

1. Générer un certificat SERV_SSL_SERV de l'IGC Santé gamme Elémentaire domaine Organisations de la branche de test.
2. Tester l'alimentation sur l'annuaire partenaire, y compris la récupération du compte-rendu d'alimentation qui est associé au DN du certificat du connecteur.

Se référer au DSFT §7.3.2 pour les URL de l'annuaire partenaire.

Se référer à la note en §5.3 pour la possibilité de report de déploiement au-delà de T1.

5.5 Renouvellement des certificats IGC CPS 2BIS

Opérations à réaliser concernant l'impact I6 :

1. Lors de l'expiration du certificat actuel IGC CPS 2BIS (au plus tôt en avril 2017), générer et déployer un certificat logiciel d'authentification de type SERV_SSL_SERV de l'IGC Santé gamme élémentaire.
2. Tester en envoyant un mail à l'opérateur de test.

Ces opérations sont à réaliser après que les opérations précédentes ont été réalisées.

5.6 Commande de certificats IGC Santé

La gestion et la commande de certificats IGC Santé suivent le même processus global que celui de l'IGC CPS 2BIS qui, très schématiquement, se déroule en deux temps :

- Habilitation pour un domaine spécifié d'un utilisateur disposant d'une carte CPA ou CPE (pour un administrateur technique).
- Gestion et commande de certificats sur le domaine spécifié au moyen du portail web à l'adresse suivante : https://pfc.eservices.esante.gouv.fr/.

Un utilisateur déjà habilité à générer un certificat IGC CPS 2BIS sera automatiquement habilité à générer un certificat IGC Santé pour le même FQDN.

Pour générer un certificat de test, l'utilisateur devra disposer d'une CPx de test et être habilité. L'habilitation de test est distincte de celle de production, toutefois les mêmes principes d'habilitation sont utilisés.

Se référer au DSFT pour les modalités de commande des cartes CPA (production et test) et les modalités d'habilitation.

Le guide d'utilisation du portail web « ASIP_IGC-Sante_Guide-IHM » est disponible à la page suivante : http://integrateurs-cps.asipsante.fr/IGC-Sante-manuel-IHM.

Important : dans le cadre de la migration IGC Santé, les opérateurs n'auront pas besoin de commander de certificat IGC Santé de production durant la phase de migration (phase 1). Toutefois ils auront besoin de commander un certificat IGC Santé de test durant cette phase.

6 Définition et glossaire

Terme	Définition
BAL	Boite aux lettres
Connecteur MSSanté	Proxy qui contient l'ensemble des équipements concourant à l'interconnexion entre opérateurs au sein de l'espace de confiance MSSanté.
LPS	Logiciel de professionnel de santé, abréviation générique désignant une application utilisée par un professionnel de santé, dans ou hors d'un établissement de santé. Les LPS peuvent intégrer un client de messagerie.
Client de messagerie	Logiciel générique utilisé par une personne pour se connecter à un système de messagerie. Ce terme englobe les clients lourds (type Thunderbird), les LPS disposant d'un client de messagerie et les webmail mis à disposition par les opérateurs.
Opérateur MSSanté	Désigne toute personne physique ou morale qui développe et fournit un service de messagerie sécurisée de santé au profit d'utilisateurs finaux. Les opérateurs sont notamment les industriels et les structures de soins.
Editeur MSSanté compatible	Dans le cadre MSSanté, un éditeur est un industriel qui édite un client de messagerie, intégré ou non dans un LPS.
Editeur de connecteurs	Industriel qui édite un connecteur destiné à être exploité par les opérateurs MSSanté
IGC Santé	Nouvelle infrastructure de Gestion de Clé (IGC) dédiée à la santé et gérée par l'ASIP Santé.
IGC CPS	Infrastructure de gestion de clé dédié à la santé et gérée par l'ASIP Santé, en service depuis 2004.
IGC CPS 2BIS	Branche de l'IGC CPS gérant l'émission de certificats logiciels (SSL et S/MIME)
IGC CPS 2TER	Branche de l'IGC CPS gérant l'émission de certificats confinés dans les cartes CPx (SSL et S/MIME).
WS	Web Service, interface d'accès à un service internet basée sur les protocoles Web (HTTP, XML) et destinée au dialogue entre applications distantes.
VIHF	Vecteur d'Identification et Habilitation Formelles, jeton contenant les données d'identification et d'habilitation du demandeur pour accéder à un service.

DN	*Distinguished Name* ou nom distinctif, champ de texte standard d'un certificat X.509 contenant les informations sur le porteur du certificat (pays, organisation, nom commun du porteur, etc.).