AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

MSSanté

Notice de migration IGC Santé à destination des opérateurs et éditeurs de clients de messagerie compatibles DST

Version 1.0.0

Identification du document	
Référence ASIP Santé	**MSS_Notice_Migration_IGC_Santé_Client_messagerie_v1.0.0**
Date de dernière mise à jour	**18/12/2017**
Classification	**Non sensible public**
Nombre de pages	**16**

Historique du document			
Version	Date	Auteur	Commentaires
V1.0.0	18/12/2017	ASIP Santé	Version initiale

Documents de référence	
REF1	Interfaces d'accès au système de Messageries Sécurisées de Santé - Dossier des Spécifications Fonctionnelles et Techniques (DSFT) version 1.1.0. https://cms.mssante.fr/documents/16106/82618206-847e-4dde-b32a-2a4670157d4b
REF2	Interface d'accès au système de Messageries Sécurisées de Santé – Dossier des Spécifications Techniques (DST) version v1.1.0 https://www.mssante.fr/is/doc-technique
REF3	Notice de migration IGC Santé à destination des éditeurs de connecteurs et opérateurs MSSanté Version 1.0.1 (*) https://cms.mssante.fr/documents/16106/24040cf1-66d3-45a1-992a-3f39270a21b8
REF4	Notice introductive de l'IGC Santé (*) http://integrateurs-cps.asipsante.fr/IGC-Sante
REF5	Migration IGC Santé – Impacts et consignes (*) http://integrateurs-cps.asipsante.fr/IGC-Sante-migration
REF6	Gabarit des certificats X.509 et CRL (*)

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

	http://integrateurs-cps.asipsante.fr/pages/IGC-Sant%C3%A9-Gabarits
REF7	Politique de certification IGC Santé (*) http://integrateurs-cps.asipsante.fr/IGC-Sante-PC
REF8	Guide de bonnes pratiques de vérification de l'état des certificats (*) http://integrateurs-cps.asipsante.fr/node/179

Note (*): Ces documents nécessitent un compte d'accès au site intégrateurs de l'ASIP Santé.

Sommaire

1 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) et les LPS intégrant des fonctions de messagerie.
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 de LPS MSSanté compatible	Dans le cadre MSSanté, un éditeur est un industriel qui édite un client de messagerie, intégré dans un LPS, qui s'interface avec un opérateur MSSanté.
Editeur de connecteurs	Industriel qui édite un connecteur destiné à être exploité par les opérateurs MSSanté
Editeur de solution de messagerie	Industriel qui édite un cœur système de messagerie proposant des interfaces clients de messagerie telles que Webmail, Web Services, SMTP/IMAP, application mobile.
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.).
SNI	SNI : *Server name indication* ou indication du nom de serveur, extension TLS qui permet au client de préciser l'URL adressée dans les échanges TLS afin de permettre au serveur de présenter le certificat correspondant à cette URL. Utile lorsque plusieurs URL pointent vers un

	même serveur HTTPS partageant la même adresse IP.

2 Introduction

Cette notice présente la stratégie de migration en vue de supporter l'IGC Santé des interfaces client de messagerie définies par le DST et mises en œuvre entre les clients de messagerie et les opérateurs MSSanté compatibles DST. Cette notice ne concerne pas la migration IGC Santé des interfaces entre opérateurs MSSanté.

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

Cette migration IGC Santé s'adresse aux acteurs suivants :

- Les **éditeurs de clients de messagerie** implémentant les interfaces du DST MSSanté mises en œuvre par certains opérateurs, dont l'opérateur ASIP Santé, ou ;
- Les **opérateurs et leur éditeurs de solution de messagerie** mettant en œuvre une authentification par carte CPS, ou ;
- Les **opérateurs et leurs éditeurs de solution de messagerie** offrant les interfaces du DST MSSanté qui sont déjà intégrés ou en cours d'intégration dans l'espace de confiance.

Note : un éditeur de connecteur qui ne propose pas d'interface client de messagerie n'est impacté par cette migration.

Cette notice fait suite à la notice de migration IGC Santé des connecteurs MSSanté [REF1], elle adresse les deux besoins suivants liés à la MSSanté :

- Introduction des certificats logiciels IGC Santé qui seront utilisés par les opérateurs pour s'authentifier sur les interfaces clients de messagerie conformes au DST ;
- Introduction des certificats embarqués IGC Santé dans les cartes CPx qui seront utilisés par les utilisateurs pour s'authentifier.

L'ASIP Santé se tient à disposition des opérateurs et éditeurs pour les accompagner dans cette migration. Ils peuvent adresser leurs demandes à editeurs@asipsante.fr.

Les demandes de support relatives à la génération des certificats IGC Santé sont à adresser à monserviceclient.certificats@asipsante.fr.

2.1 Objectif du document

Ce document est à destination des équipes techniques des acteurs concernés 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 migration IGC Santé.

Dans cette optique, ce document s'organise en 3 sections :

- Présentation générale de l'IGC Santé et liens vers les documents correspondants;
- Migration des opérateurs ;
- Migration des clients de messagerie.

2.2 Contexte de la migration

La messagerie sécurisée de santé MSSanté utilise actuellement les IGC CPS 2BIS et 2TER pour ses besoins d'authentification et de sécurisation des échanges de mail. Ces IGC ont été mises en service en 2004 par l'ASIP Santé et leur 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 les 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 a entrainé l'arrêt de l'émission des certificats logiciels IGC CPS 2BIS en juin 2017. Toutefois ces certificats resteront valides jusqu'à leur expiration, au plus tard en 2020 pour les derniers certificats émis.

Suite à cet arrêt en juin 2017, les nouveaux opérateurs compatibles DST et intégrant l'espace de confiance depuis cette date doivent mettre en œuvre un certificat d'authentification IGC Santé sur leurs interfaces client de messagerie. De manière similaire les opérateurs dont les certificats CPS 2BIS expirent doivent le renouveler avec des certificats IGC Santé.

En conséquence les clients de messagerie devront réaliser des évolutions afin de maintenir l'interopérabilité avec ces opérateurs et les opérateurs existants qui continuent à présenter un certificat CPS 2BIS.

Par ailleurs, l'arrivée des cartes CPx IGC Santé prévue au 1er juillet 2018 va nécessiter des évolutions de la part des opérateurs afin de supporter ces cartes en plus des CPx IGC 2TER.

2.3 Situation avant migration

La figure ci-dessous montre la situation actuelle: les opérateurs MSSanté présentent un certificat IGC CPS 2BIS aux clients de messagerie sur les différentes interfaces proposées par l'opérateur : web service et/ou IMAP/SMTP.

En retour, les clients de messagerie présentent à l'opérateur MSSanté le certificat IGC 2TER stocké dans la carte CPS. Les certificats IGC Santé ne sont pas utilisés.

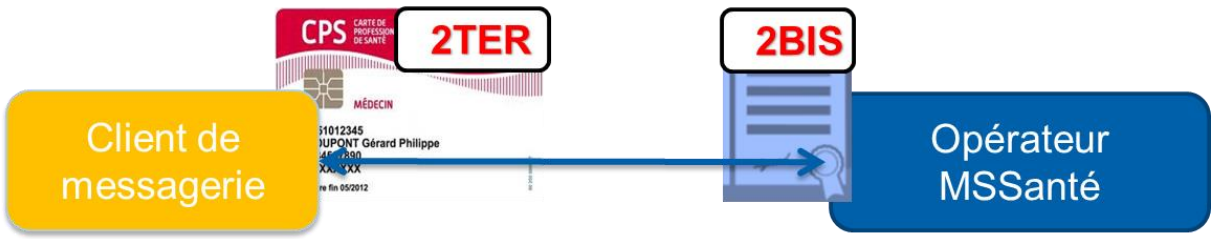

Figure 1 - Situation actuelle sur l'usage des certificats

Note : seul le PS s'authentifie auprès de l'opérateur, en conséquence le client de messagerie ne dispose pas de certificat d'authentification IGC 2BIS car il ne s'authentifie pas auprès de l'opérateur.

Ainsi, les opérateurs et clients de messagerie doivent migrer pour supporter en plus les certificats IGC Santé selon le principe de migration ci-dessous.

2.4 Situation après migration

La figure ci-dessous montre la situation à l'issue de la migration des opérateurs et des clients: un client de messagerie pourra présenter à l'opérateur soit un certificat IGC CPS 2TER ou IGC Santé en fonction de la CPx présentée par l'utilisateur. L'opérateur présentera un certificat IGC Santé.

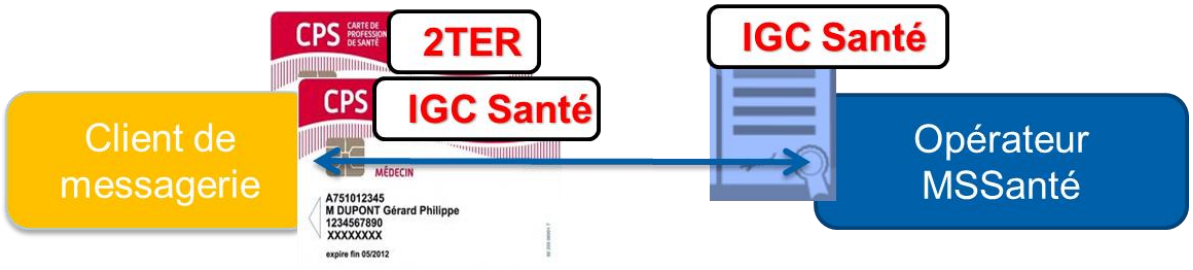

Figure 2 - situation après migration sur l'usage des certificats

2.5 Enjeux de la migration

Tout l'enjeu de la migration est de parvenir à cette cible tout en maintenant la compatibilité avec les opérateurs et clients de messagerie non encore migrés ou en cours de migration.

Ainsi cette migration doit répondre aux deux besoins suivants :

1. Pour les opérateurs existants et compatibles DST, d'une part assurer la compatibilité avec les cartes CPx IGC Santé et les clients de messagerie ne supportant que l'IGC Santé, d'autre part maintenir la continuité de service avec les clients de messagerie ne supportant pas encore l'IGC Santé;
2. Pour les clients de messagerie, assurer une compatibilité avec les opérateurs existants IGC CPS 2BIS et les nouveaux opérateurs IGC Santé.

Important : l'introduction des cartes CPx IGC Santé n'a pas impact sur les clients de messagerie MSSanté (hormis à la mise à jour de la Cryptolib) car aucun traitement des données issues du certificat des CPx n'est requis par le client de messagerie au regard de la fonctionnalité de messagerie MSSanté.

Toutefois il est de la responsabilité des éditeurs de clients de messagerie de réaliser une analyse d'impact afin de s'assurer du bon fonctionnement de leurs solutions avec les cartes IGC Santé.

Cette migration ne présente aucune complexité technique mais nécessite d'être mise en œuvre dans les temps et de manière cordonnée entre les opérateurs et éditeurs de clients de messagerie.

3 Présentation de l'IGC Santé

L'IGC Santé a pour vocation de remplacer l'IGC CPS 2BIS (certificats logiciels de classe 4 SSL et S/MIME) et l'IGC-CPS 2TER (certificats de carte de classe 0 à 3 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.

Se référer à la notice introductive IGC Santé [REF4] pour plus d'information.

3.1 Calendrier de déploiement de l'IGC Santé

Le calendrier de déploiement des certificats logiciels est le suivant :

- **1er mars 2016** : début émission des certificats logiciels par l'IGC Santé (test et production) ;

- **1er juin 2017** : 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.

Le calendrier de déploiement des cartes CPx embarquant des certificats IGC Santé est le suivant :

- Février 2017 : début émission des CPx de test ;
- **1er juillet 2018** : début émission des CPx de production ;
- Fin 2020 : fin de vie IGC 2TER : dépublication des certificats racines et intermédiaires.

La date de fin d'émission des cartes CPx IGC CPS 2TER n'est pas connue à ce jour.

3.2 DN des certificats IGC Santé

3.2.1 Certificats logiciels de structures

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 (en rouge les modifications) :

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

3.2.2 Certificats CPx de personnes physiques

La table suivant montre l'évolution du DN pour un PS rattaché à une structure :

DN IGC CPS	DN IGC Santé
C=FR	C=FR
O=GIP-CPS	
L=<nom département (N°)>	ST=<nom département (N°)>
	O=<Raison sociale structure>
OU=<IdNat_Struct>	OU=<IdNat_Struct>
OU=<Profession>	TITLE=<Profession>
CN=<IdNat_PS>	CN=<IdNat_PS>
SN=<nom d'exercice>	SN=<nom d'exercice>
GN=<prénom usuel>	GN=<prénom usuel>

Se référer au document Impacts et consignes [REF5] §3.2 pour plus d'information.

3.2.3 Certificats de test

Le DN sujet des certificats IGC Santé de test ne contient plus le mot « TEST ». De manière générale, pour distinguer un certificat de test, il est donc nécessaire de vérifier le DN émetteur dont le CN commence par « TEST ».

Toutefois les opérateurs et éditeurs de client de messagerie n'ont pas besoin d'implémenter cette distinction car elle est réalisée automatiquement lors de vérification par les librairies SSL de la chaine de certificat reçue : un certificat de test sera refusé par SSL si la chaine de test n'est pas référencée parmi les chaines de confiance (stockées dans les magasins de confiance) sur les plateformes de production.

3.3 CRL IGC Santé

Les CRL IGC Santé sont publiés quotidiennement et valables 7 jours.

Elles sont publiées sur l'annuaire IGC Santé (http://igc-sante.esante.gouv.fr/PC/#ca et ldap://annuaire-igc.esante.gouv.fr) et alternativement sur l'annuaire IGC CPS (http://annuaire.asipsante.fr et ldap://annuaire.asipsante.fr).

Toutefois il est fortement recommandé d'utiliser l'annuaire IGC Santé, conformément aux éléments d'information contenus dans les certificats IGC Santé (points de distribution) et la politique de certification IGC Santé [REF7].

Se référer au document de gabarit X.509 et CRL [REF6] et au guide de bonnes pratiques de vérification de l'état des certificats [REF8] pour plus d'information.

4 Migration des opérateurs

Cette migration concerne les opérateurs déjà intégrés à l'espace de confiance et offrant tout ou partie des interfaces client de messagerie conformes au DST.

En manière globale, la migration des opérateurs comporte deux volets :

- Migration des interfaces clients de messagerie pour s'authentifier à l'aide d'un certificat IGC Santé ;
- Support des cartes CPx IGC Santé.

4.1 Migration des interfaces clients de messagerie

Pour rappel, les interfaces d'accès au service de messagerie référencée dans le DST sont les suivantes :

- Interface SMTP/IMAP avec StartTLS ;
- Interface web service SOAP en HTTPS.

L'opérateur ASIP Santé propose en complément une interface *webmail* pour une mise en œuvre rapide de la MSSanté auprès des utilisateurs.

Le DST stipule (cf §4.5.1) que les certificats d'authentification présentés par le(s) serveur(s) sur ces deux interfaces sont issus de l'IGC Santé.

Pour se mettre en conformité avec le DST suite à l'arrêt d'émission des certificats IGC CPS 2BIS en juin 2017, les opérateurs doivent mettre en place une solution basée sur les certificats IGC Santé tout en assurant une compatibilité avec les clients de messagerie existants et pas encore compatibles IGC Santé.

Pour répondre à ce besoin, deux stratégies sont possibles et présentées ci-dessous.

Quelle que soit la stratégie de migration retenue, l'opérateur doit la mettre en œuvre impérativement avant l'expiration de ses certificats IGC CPS 2BIS car ils ne pourront plus être renouvelés en IGC CPS 2BIS.

De même, le déploiement de cette migration doit intervenir suffisamment tôt pour permettre aux clients de messagerie de migrer avant l'expiration des certificats IGC CPS 2BIS de l'opérateur.

4.1.1 Stratégie bi-flux

C'est la solution retenue par l'opérateur ASIP Santé qui consiste à dupliquer les flux de ces deux interfaces. Chaque interface offre deux flux :

- le flux actuel « CPS 2BIS » authentifié par un certificat CPS 2BIS classe 4 et opérationnel au plus tard jusqu'en 2020 et,
- un nouveau flux « IGC Santé » authentifié par un certificat IGC Santé de la gamme Elémentaire domaine Organisations.

Ainsi les clients de messagerie peuvent migrer à leur rythme du flux CPS 2BIS vers le flux IGC Santé. Cependant la migration des clients doit être réalisée avant expiration du certificat 2BIS du flux CPS 2BIS.

La figure suivante montre ces deux flux et l'usage des certificats :

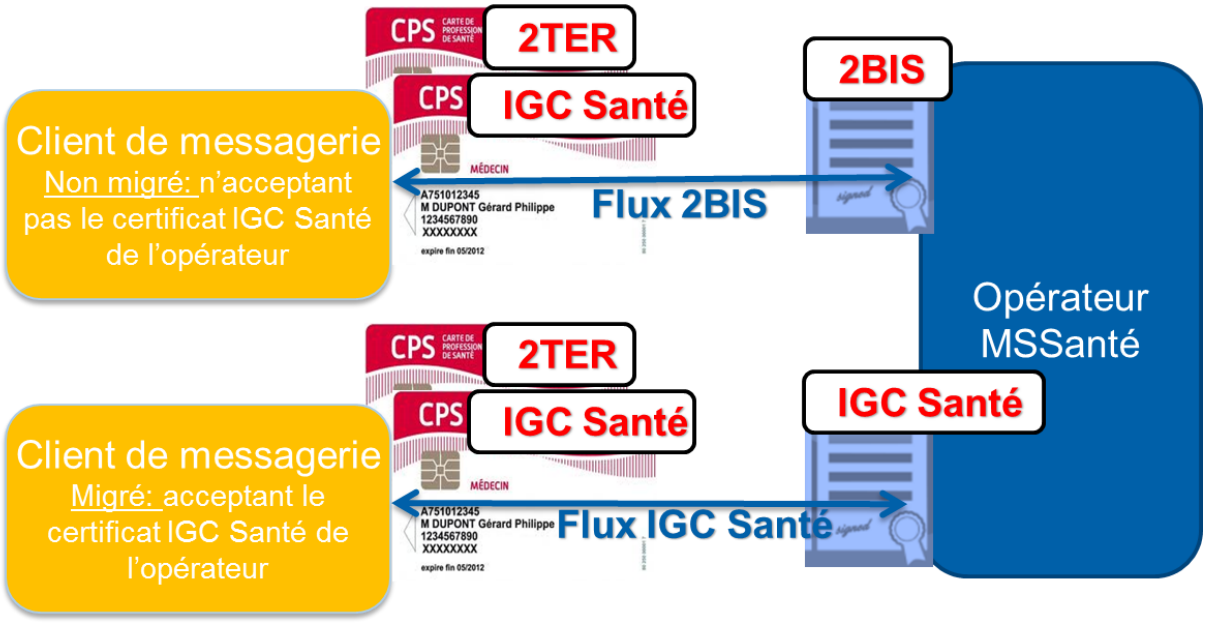

Figure 3 - Stratégie bi-flux avec ajout d'un flux IGC Santé

Important : comme le support des CPx IGC Santé est sans impact sur le client de messagerie, un PS peut utiliser son client de messagerie non migré avec sa CPx IGC Santé, sous réserve de mise à jour de la Cryptolib sur son poste utilisateur. En conséquence l'opérateur doit accepter les certificats des CPx IGC Santé sur le flux 2BIS.

4.1.1.1 Cas d'un nouvel opérateur

Cette stratégie s'applique uniquement à un opérateur existant. Un nouvel opérateur intégrant l'espace de confiance après juin 2017 offre uniquement le flux IGC Santé.

4.1.1.2 Calendrier de déploiement

Si les opérateurs sont libres du calendrier de déploiement des flux IGC Santé (avant 2020), il est recommandé de les déployer avant juillet 2018 afin de permettre à l'ensemble des

acteurs (opérateurs et éditeurs de client de messagerie) d'effectuer la totalité de la migration IGC Santé avant l'arrivée des cartes IGC Santé.

4.1.2 Stratégie mono-flux

La seconde stratégie consiste à basculer le certificat 2BIS vers un certificat IGC Santé sur les flux existants. Cette stratégie est plus simple d'un point de vue technique, mais en contrepartie l'opérateur doit s'assurer avant la bascule que l'ensemble de ses clients de messagerie soient compatibles IGC Santé, c'est-à-dire qu'ils acceptent les certificats IGC Santé.

Ainsi, cette stratégie est possible pour des opérateurs maitrisant le calendrier de migration de leurs clients de messagerie, comme le montre la figure suivante :

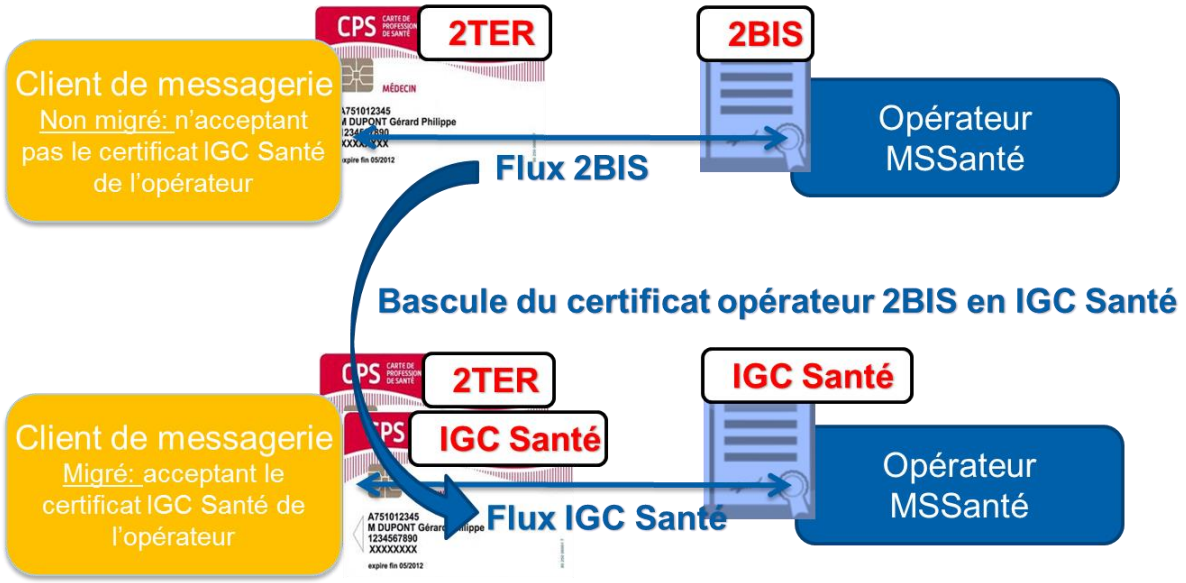

Figure 4 - Stratégie mono-flux avec bascule du certificat opérateur

Note : la figure ci-dessus montre un client de messagerie non migré avec uniquement une CPx 2TER. Sous réserve de mise à jour de la Cryptolib sur le poste utilisateur, ce client non migré peut aussi utiliser les cartes IGC Santé.

4.2 Support des cartes CPx IGC Santé

La mise en service des CPx IGC Santé va nécessiter des adaptations auprès des opérateurs pour les supporter.

Ces adaptations doivent être réalisées et déployées avant le 1er juillet 2018, date de mise à disposition des CPx IGC Santé auprès des professionnels de santé, faute de quoi le connecteur ne sera pas en capacité de les accepter et rejettera l'accès à la messagerie de l'utilisateur concerné.

Impacts

Les impacts identifiés liés aux CPx IGC Santé sont les suivants :

- Nécessité de supporter la chaine de confiance IGC Santé gamme FORT domaine PERSONNES, en complément de la chaine de confiance IGC CPS 2TER sur chaque flux (2BIS et IGC Santé).
- Nécessité de télécharger les CRL IGC Santé, en complément des CRL IGC CPS 2TER.

Important : les flux 2BIS doivent supporter les CPx 2TER et IGC Santé afin de rester compatibles avec un client de messagerie non migré (c'est-à-dire continuant à utiliser le flux 2BIS) avec un utilisateur équipé d'une CPx IGC Santé.

Ressources de la gamme Fort domaine Personne Physique.

La chaine de confiance est disponible ici :

- Certificat racine : http://igc-sante.esante.gouv.fr/AC/ACR-FO.cer
- Certificat intermédiaire : http://igc-sante.esante.gouv.fr/AC/ACI-FO-PP.cer

Les CRL sont disponibles aux adresses suivantes (cf document sur les gabarits IGC Santé mentionné en §3.3) :

- URL http : http://igc-sante.esante.gouv.fr/CRL/ACI-FO-PP.crl
- URL ldap[1] : ldap://annuaire-igc.esante.gouv.fr/cn=AC IGC-SANTE FORT PERSONNES, ou=AC RACINE IGC-SANTE FORT,ou=IGC-SANTE,ou=00021875127 51, 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 FORT PERSONNES, ou=AC RACINE IGC-SANTE FORT,ou=IGC-SANTE,ou=00021875127 51, o=ASIP-SANTE,c=FR?deltarevocationlist;binary?base?objectClass=pkiCA

Dans le cas où l'opérateur accepte des utilisateurs habilités munis de cartes nominatives autres que les CPS/CPF telles que CDE/CDA et CPE/CPA, il conviendra également d'inclure la chaine de confiance gamme Standard domaine Personnes Physiques.

A l'instar de l'IGC 2TER, le type de carte peut être identifié au moyen de l'extension *productType*. Se référer au document Impacts et consignes [REF5] §4.3 et §4.4 pour plus d'information.

4.3 Matrice de support des AC

La table suivante résume les certificats qui doivent être acceptés et présentés sur les différents flux par les opérateurs :

Interface	Flux	Certificat présenté par l'opérateur	Certificats acceptés par l'opérateur
Smtp/imap	IGC 2BIS	IGC CPS 2BIS classe 4 SSL	- IGC CPS 2TER et - IGC Santé - gamme Fort personne physique
	IGC Santé	IGC Santé - gamme Elémentaire domaine Organisations.	- IGC CPS 2TER et - IGC Santé - gamme Fort domaine Personne physique
Web service SOAP	IGC 2BIS	Idem flux IGC 2BIS[2]	Idem flux IGC 2BIS
	IGC Santé	Idem flux IGC Santé	Idem flux IGC Santé

Tableau 1 - Matrice de support des certificats

[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.

[2] Pour des raisons historiques, l'opérateur ASIP Santé présente un certificat commercial

Ces certificats sont issus des AC de production.

4.4 Cas de l'opérateur ASIP Santé

4.4.1 Flux IGC Santé de production

Pour rappel, les FQDN des flux IGC 2BIS sont les suivants :

- IMAP: frontimap.mssante.fr
- SMTP : frontsmtp.mssante.fr
- WS :
  - Messagerie : https://mss-msg.mssante.fr/<...>
  - Authentification CPS/OTP : https://mss-idp.mssante.fr/<...>

Les FQDN des flux IGC Santé sont les suivants (cf DST §8.1.1.2 [REF 2]):

- IMAP : frontimap-igcsante.mssante.fr
- SMTP : frontsmtp-igcsante.mssante.fr
- WS :
  - Messagerie : https://mss-msg-igcsante.mssante.fr/<...>
  - Authentification CPS/OTP: http://mss-idp-igcsante.mssante.fr/<...>

Chacun des flux accepte les certificats des cartes IGC CPS 2TER et IGC Santé.

4.4.2 Support SNI

Pour chacune des interfaces, ces flux partagent la même adresse IP et donc nécessitent le support SNI de la part du client de messagerie.

Note : strictement parlant, le support SNI est nécessaire pour accéder au flux IGC Santé car en l'absence de SNI le serveur présente le certificat 2BIS sur ce flux. Le flux 2BIS reste fonctionnel en l'absence de support SNI de la part du client de messagerie.

4.4.3 Support carte CPx IGC Santé

L'opérateur ASIP Santé accepte les CPx IGC Santé gamme Fort domaines Personnes sur les interfaces DST depuis septembre 2017.

5 Migration des clients de messagerie

La migration des clients de messagerie se résume au support des certificats IGC Santé utilisés par les opérateurs pour s'authentifier.

5.1 Support des certificats logiciel IGC Santé

Suite à l'arrêt de l'émission de l'IGC CPS 2BIS en juin 2017, les éditeurs de clients de messagerie MSSanté compatibles DST doivent être en capacité de s'interfacer des opérateurs présentant sur les interfaces DST soit un certificat IGC CPS 2BIS soit un certificat IGC Santé soit les deux en cas de duplication des flux (comme l'opérateur ASIP Santé).

En conséquence, pour être en capacité d'accepter l'IGC Santé en complément de l'IGC CPS 2BIS, les impacts sur les clients de messagerie sont les suivants :

- Nécessité de supporter la chaine de confiance IGC Santé gamme Elémentaire domaine Organisations, en complément de la chaine de confiance IGC CPS 2BIS.
- Nécessité de télécharger les CRL IGC Santé, en complément des CRL IGC CPS 2BIS.

- Nécessité de supporter SNI afin d'être compatible avec des opérateurs utilisant la même adresse IP pour les flux IGC CPS et IGC Santé.

Note : la nécessité de supporter l'IGC CPS 2BIS est temporaire jusqu'à fin 2020.

5.1.1 Support SNI

A titre d'information, l'extension SNI est intégrée à partir des versions suivantes :

- Openssl 0.9.8,
- Java avec JDK Oracle 1.7.0_80,
- Tomcat 8.5,
- Apache http 2.2.12,
- PHP 5.3.

Pour les éditeurs de clients de messagerie s'interfaçant avec l'opérateur ASIP : il leur est fortement recommandé de supporter SNI pour utiliser le flux IGC Santé car cet opérateur mutualise les flux 2BIS et IGC Santé sur une même adresse IP. En cas de non support de SNI, l'opérateur présentera un certificat IGC CPS 2BIS.

5.1.2 Ressources de la gamme Elémentaire domaine Organisations

La chaine de confiance est disponible ici :

- Certificat racine : http://igc-sante.esante.gouv.fr/AC/ACR-EL.cer
- Certificat intermédiaire : http://igc-sante.esante.gouv.fr/AC/ACI-EL-ORG.cer

Les CRL sont disponibles aux adresses suivantes (cf document sur les gabarits IGC Santé mentionné en §3.3) :

- URL http : http://igc-sante.esante.gouv.fr/CRL/ACI-EL-ORG.crl
- URL ldap[3] : 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

Les évolutions des clients de messagerie liées à ces impacts sont à planifier en cohérence avec les opérateurs utilisant ces applications.

5.1.3 Support des cartes IGC Santé

Comme évoqué en §2.5, les clients de messagerie ne sont pas à priori impactés par l'introduction des cartes IGC Santé en raison de l'absence de traitement réalisé sur les données de la carte pour les fonctionnalités relatives à la MSSanté.

Toutefois, dans le cas où le client de messagerie embarque la chaine de confiance IGC-CPS 2TER, la chaine de confiance IGC Santé gamme Fort domaines Personne Physique devra probablement être ajoutée. Elle est disponible ici :

- Certificat racine : http://igc-sante.esante.gouv.fr/AC/ACR-FO.cer
- Certificat intermédiaire : http://igc-sante.esante.gouv.fr/AC/ACI-FO-PP.cer

[3] 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.

5.2 Moyens de test pour les éditeurs

Afin de permettre aux éditeurs de clients de messagerie de tester le support des deux IGC, l'opérateur ASIP Santé met à leur disposition l'environnement formation compatible IGC Santé qui offre les deux flux pour chaque interface (SMTP/IMAP et WS).

Cette mise à disposition est effective à partir de septembre 2017. Les certificats IGC Santé présentés sur les flux IGC Santé sont des certificats de TEST de la gamme Elémentaire domaines Organisations.

L'accès à cet environnement de formation nécessite des CPx de test, soit IGC 2TER, soit IGC Santé disponibles depuis février 2017. Les CPx de production ne seront pas acceptées.

5.3 Consignes relatives à la Cryptolib

Pour assurer le bon fonctionnement des cartes CPx contenant des certificats IGC-Santé, la version 5 de la Cryptolib doit être mise en œuvre pour l'usage sur le poste de travail de l'utilisateur final et les librairies déclarées comme obsolètes ne doivent plus être invoquées par les logiciels.

Les versions minimales de la Cryptolib à prendre en compte sont les suivantes :

- Windows : 5.0.33
- MacOS : 5.0.30
- Linux : 5.0.9

Cette librairie faisant l'objet de mises à jour régulières par l'ASIP Santé, il est recommandé d'utiliser la dernière version disponible sur le site suivant (nécessite un compte d'accès) :

http://integrateurs-cps.asipsante.fr/logiciels_cps

Se référer au document Impacts et consignes [REF5] §10.6.3 pour plus d'information.

6 Calendrier de migration

6.1 Opérateurs et éditeurs de clients de messagerie

La table suivante résume le calendrier des évolutions à réaliser par les opérateurs existants et les éditeurs de clients de messagerie :

Acteurs concernés	Evolutions	Date de déploiement préconisée	Observations
Opérateurs existants	Mise en place d'un flux IGC Santé (ou bascule selon la stratégie retenue).	A définir avec les éditeurs de client de messagerie, idéalement avant mi-2018.	Le déploiement doit avoir lieu suffisamment tôt pour permettre aux clients de messagerie de migrer avant l'expiration des certificats 2BIS de l'opérateur.
	Support des cartes CPx IGC Santé	Impérativement avant le 1er juillet 2018	**Date de déploiement à respecter impérativement, faute que quoi un PS muni d'une carte IGC Santé ne pourra pas se connecter.**
Editeurs de clients de	Support du flux IGC Santé (en plus du flux	A définir avec les opérateurs,	Afin de permettre aux clients de messagerie de

messagerie	CPS 2BIS)	idéalement avant mi-2018.	supporter les nouveaux opérateurs présentant un certificat IGC Santé.
	Support des cartes CPx IGC Santé	Impérativement avant le 1er juillet 2018	Les cartes IGC Santé n'ont pas d'impact à priori sur les clients de messagerie MSSanté. Toutefois il appartient à l'éditeur de client de messagerie de s'en assurer. La Cryptolib des postes utilisateurs devra être mise à jour si besoin.

Tableau 2 - calendrier des évolutions