Système de Facturation SESAM-Vitale

Chiffrement de pièce jointe

Juillet 2014

GIE SESAM-Vitale
5, boulevard Marie et Alexandre Oyon – 72 019 LE MANS Cedex 2
www.sesam-vitale.fr

Ce document a été élaboré par le GIE SESAM-Vitale.

sesam-vitale

Cahier des Charges SESAM-Vitale

Fiche signalétique

CDC Chiffrement de pièce jointe

Référence du document Avenant	*Version du document*	0.5
	Date	**23/07/2014**
	Référence	**PDT-CDC-063**
Vue générale	*Cahier des Charges SESAM-Vitale concerné*	**1.40 Addendum 6 avec erratum de mars 2012 et son complément PC/SC**
Evolutions apportées par cette nouvelle version du système	**Chiffrement de pièce jointe**	***Professionnels concernés*** **Tous**

Légende

Texte surligné en jaune	Texte ajouté pour l'évolution
Texte surligné en gris	Texte ajouté pour la partie corrective
~~Texte barré bleu suivant la couleur~~	Texte supprimé du CDC SESAM Vitale

Compatibilité avec les FSV

- Package d'agrément
- Package d'exploitation

Sommaire

1 Introduction

1.1 Objectifs

Contexte

Ce document constitue un avenant au cahier des charges SESAM-Vitale 1.40 addendum n°6 avec erratum 2012 et son complément PC/SC.

1.2 Professionnels de santé concernés

PS concernés

Toutes les familles de Professionnels de santé concernées par la facturation SESAM-Vitale

Le périmètre de cette évolution inclut l'ensemble des Professionnels de Santé.

1.3 Identification du socle fonctionnel de référence

Consigne d'implémentation

La version du socle fonctionnel de référence n'est pas modifiée par cet avenant.

Les éditeurs implémentent dans le champ 'sujet' du message SMTP transmis à l'organisme d'assurance maladie, la référence « **SV140610** » (ou « **DR140610** ») fournie par les API SSV en sortie de la fonction « Formater_Lot » dans le champ 7 du groupe 13 pour un fichier de FSE et dans le champ 7 du groupe 93 pour un fichier de DRE.

1.4 Guide de lecture

Codes couleur

Les codes couleur suivants sont utilisés dans ce complément à l'addendum n°6 et également dans les documents du cahier des charges SESAM-Vitale 1.40 :

Texte surligné en jaune	Texte ajouté au CDC 1.40 Addendum n°6 avec erratum 2012 et son complément PC/SC pour le chiffrement de pièce jointe
~~Texte barré suivant la couleur~~	Texte supprimé du CDC SESAM Vitale

Le titre du paragraphe est surligné en couleur dès lors que le paragraphe est modifié.

Pour des besoins de commodités de lecture, lorsque le texte du paragraphe est entièrement nouveau, le texte n'est pas surligné en jaune, seuls les titres de paragraphes sont surlignés en jaune.

Légende des tableaux

La dernière colonne « Q » indique la qualification de l'impact :

Q	Qualification de l'impact
M	Modification du paragraphe (ajout ou modification de texte)
N	Nouveau paragraphe
S	Suppression du paragraphe
D	Renumérotation des paragraphes

2 Chiffrement de pièce jointe

2.1 Présentation

Contexte

Les évolutions contenues dans ce chapitre ont pour objectif :

- De décrire la mise en œuvre du chiffrement de pièce jointe lors des échanges entre le PS et l'assurance maladie, chiffrement qui vient en remplacement du chiffrement de transport qui était optionnel dans les versions précédentes du cahier des charges SESAM-Vitale 1.40.
- D'assurer ainsi la confidentialité des données patients (en dehors des données déjà chiffrées) échangées entre le PS et l'assurance maladie, dont le NIR, en conformité avec les exigences de la CNIL, tout en permettant aux OCT d'assurer la continuité des services offerts à leurs clients.

Principes généraux du chiffrement

Le chiffrement de la pièce jointe contenant le fichier de lots de FSE ou de DRE transmis par messagerie se fait en utilisant :

- une clé AMO pour chiffrer le fichier de FSE à destination des AMO,
- une clé AMC pour chiffrer le fichier de DRE à destination des AMC,
- une clé OCT pour chiffrer le fichier à destination d'un OCT

Ce principe de chiffrement est illustré par le schéma suivant :

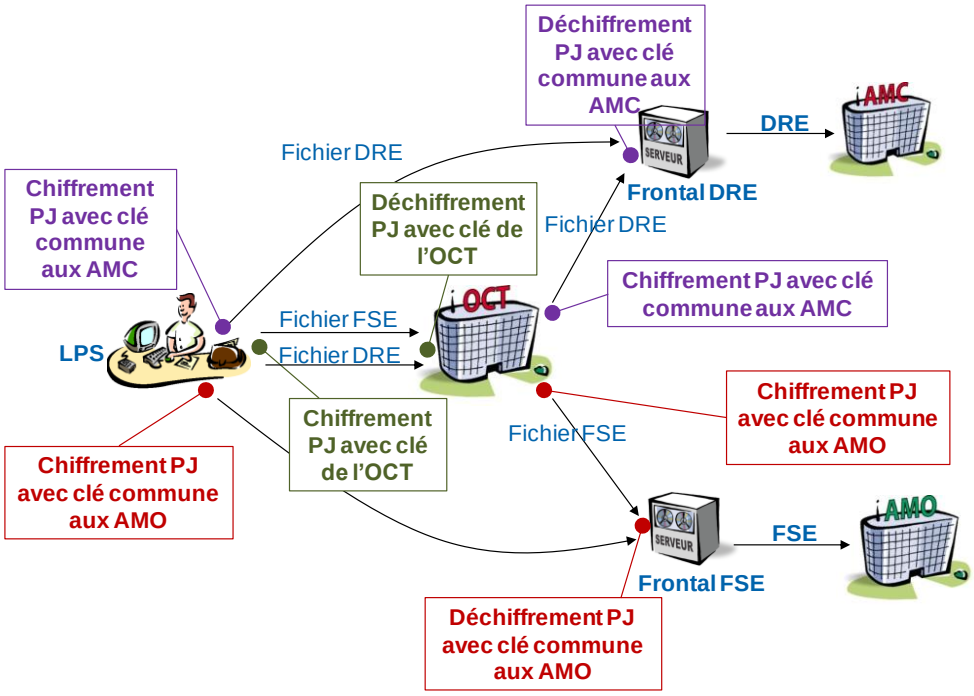


Figure 1 : Principe de chiffrement des pièces jointes

Nouvelles fonctionnalités

La mise en œuvre du chiffrement de pièce jointe introduit les nouvelles fonctionnalités suivantes :

- Chiffrement de pièces jointes, comprenant les points suivants :
  - Vérification de la validité des certificats avant usage.
  - Chiffrement des PJ des messages avec le certificat AMO de l'IGC OSI (pour les FSE).
  - Chiffrement des PJ des messages avec le certificat AMC de l'IGC OSI (pour les DRE).
  - Chiffrement des PJ des messages avec le certificat OCT de l'IGC de l'OCT pour les flux à destination des OCT.
- Gestion de la sécurité, comprenant les points suivants :
  - Stockage (en général dans un magasin de certificats) des 2 et/ou 3 certificats (AMO/AMC et/ou OCT) et d'au moins 2 à 4 autorités de certification (pour gérer l'autorité de l'assurance maladie et de l'OCT, ainsi que la période de migration vers une nouvelle AC lors des renouvellements).
  - Accès à l'annuaire LDAP du GIE SV pour la récupération des certificats et des Listes de Révocation de Certificats (CRL).
- Gestion de nouveaux messages de service :
  - Nouveaux messages de services envoyés par les frontaux de l'AM dans le cas de renouvellements/problèmes de certificats.

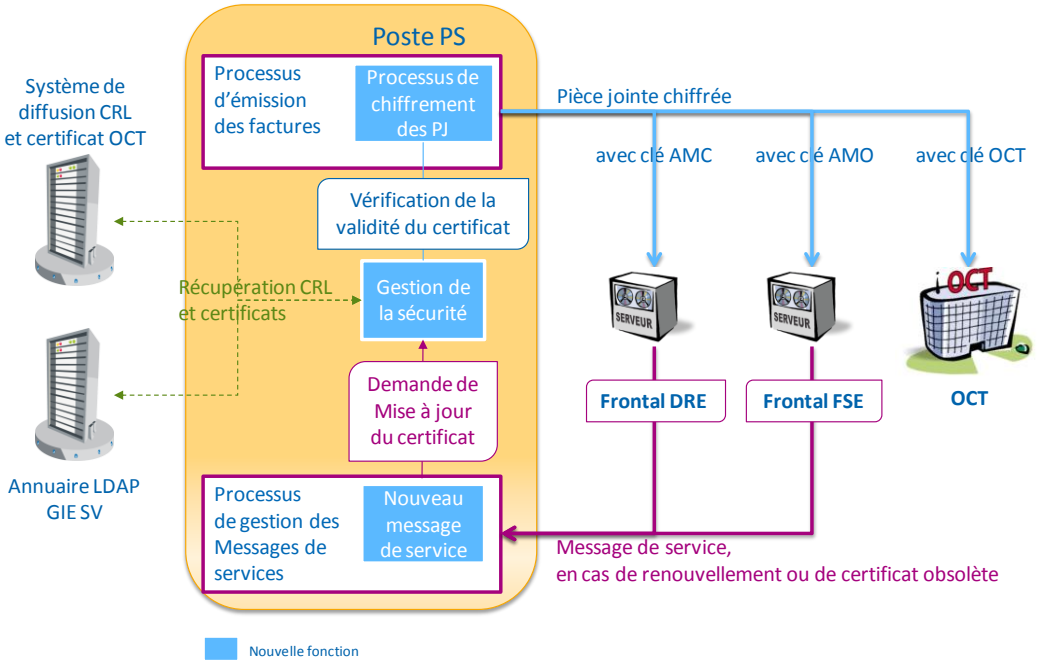


Figure 2 : Nouvelles fonctionnalités à mettre en œuvre

2.2 Liste des documents impactés

Nom des documents

Les documents du Cahier Des Charges SESAM-Vitale impactés par le chiffrement de pièce jointe sont les suivants :

Abréviation	*Nom du document du CDC SESAM-Vitale*
Corps	Corps du cahier des charges
A1-B	Annexe A1-B : Présentation fonctionnelle des modules SESAM-Vitale – Principes de Traitement des retours et Gestion des ARL
A4	Annexe 4 : Télécommunications (sur Réseau IP) et chiffrement de transport
A5	Annexe 5 : Transmission des flux SESAM-Vitale via les Organismes Concentrateurs Techniques

2.3 Corps du cahier des charges SESAM-Vitale

Paragraphes impactés

Ci-dessous figure la liste des paragraphes du corps du CDC SESAM-Vitale impactés par l'évolution.

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
1.2.3	Annexes	*Renommage de l'annexe 4*	M
2.3.1	Les apports fonctionnels	*Suppression de la référence au chiffrement de transport*	M
2.3.5	Les apports techniques	*Remplacement du chiffrement de transport par le chiffrement de pièce jointe*	M
3.2.9.4	Chiffrement de transport	*Remplacement du chiffrement de transport par le chiffrement de pièce jointe*	M
3.6.4	Mise à jour des certificats de chiffrement et de la liste de révocation des certificats de chiffrement	*Précision sur le type de certificats de chiffrement de données objet du § et ajout de l'administration des certificats et CRL chiffrement pièce jointe*	M
4.1.2	Architecture logicielle	*Remplacer dans le schéma API chiffrement transport par API Chiffrement*	M
4.2.1.13	Constitution et sécurisation des FSE et des DRE en mode SESAM-Vitale	*Précision sur le type de certificats de chiffrement de données utilisé*	M
4.2.4	Transmission des fichiers et réception des fichiers retour	*Remplacement du chiffrement de transport par le chiffrement de pièce jointe*	M

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
4.2.6.4	Administration des certificats de chiffrement et de la CRL des certificats de chiffrement	*Précision sur le type de certificats de chiffrement de données objet du § et ajout de l'administration des certificats et CRL chiffrement pièce jointe*	M
6	Glossaire	*Ajout des définitions relatives au chiffrement*	M

Contenu des paragraphes

§ 1.2.3 Annexes

…/…

- **Annexe 4** : Télécommunications (sur Réseau IP) et Chiffrement de pièce jointe ~~transport des messages SMTP~~

…/…

§ 2.3.1 Les apports fonctionnels

…/…

Le Professionnel de Santé doit disposer de l'ensemble des nouvelles fonctionnalités sur son Poste de Travail. Cependant, le Professionnel de Santé décide de l'activation ou non des services suivants :

- la saisie d'actes CCAM,
- les services de tarification complémentaire STS,
- la liste d'opposition.~~,~~
- ~~le chiffrement de transport.~~

§ 2.3.5 Les apports techniques

La version 1.40 addendum n°6 avec erratum 2012 et complément PC/SC comprend les apports techniques suivants :

- ~~le chiffrement optionnel des messages SMTP (chiffrement de transport),~~
- le chiffrement de pièce jointe,
- la compression et la décompression des messages,

…/…

§ 3.2.9.4 Chiffrement de pièce jointe ~~transport~~

La version 1.40 assure intrinsèquement la confidentialité des données sensibles (cf. §3.2.9.2) via des certificats de chiffrement de données (premier niveau de chiffrement)

~~La version 1.40 permet l'utilisation des outils de chiffrement dit de transport, au sens où l'ensemble du message SMTP contenant des factures est chiffré (Cf. description à l'annexe 4) est possible avec cette version du Cahier des Charges.~~

La version 1.40 assure également la confidentialité de l'ensemble des données transmises vers l'assurance maladie via le chiffrement de pièce jointe des messages SMTP et de certificats de chiffrement de pièce jointe (second niveau de chiffrement) (cf. description à l'annexe 4).

Les flux retours des organismes d'Assurance Maladie ne sont pas chiffrés.

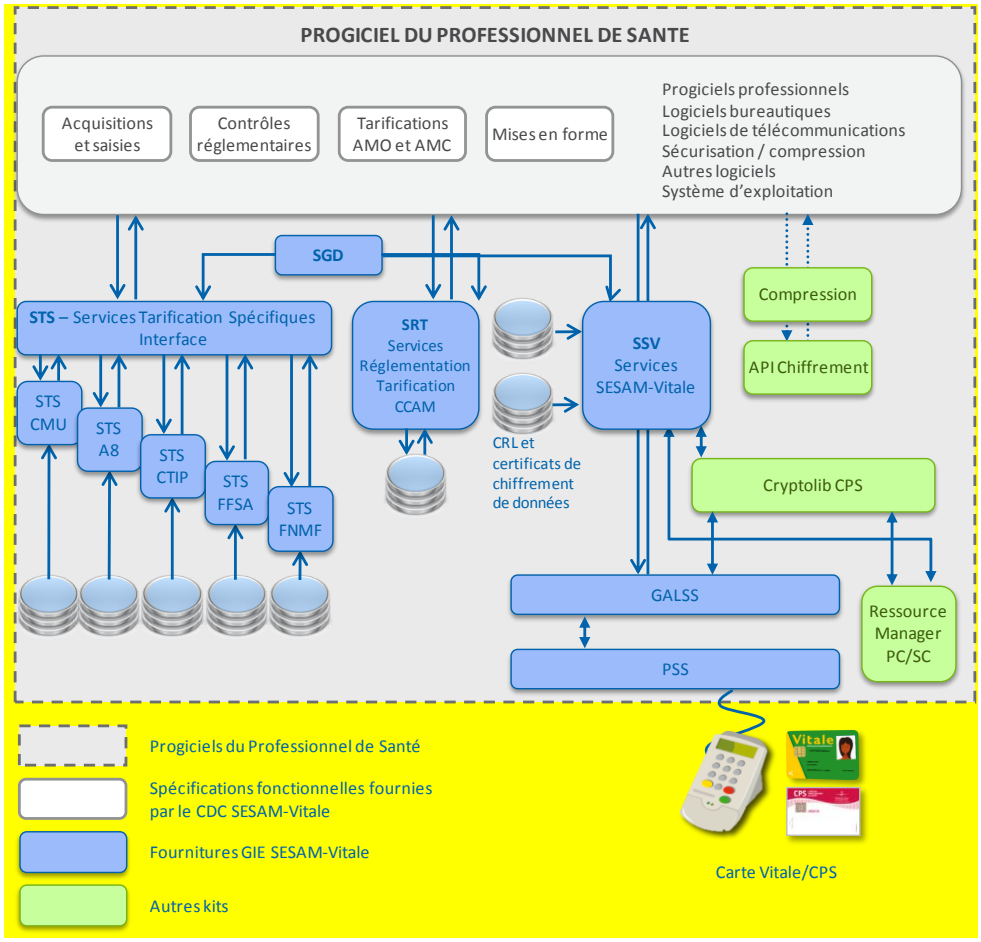
§ 3.6.4 Mise à jour des certificats de chiffrement et de la liste de révocation des certificats de chiffrement

Le Professionnel de Santé doit émettre des FSE ou DRE avec une CRL de chiffrement de données et des certificats de chiffrement de données à jour sur son poste.

De même, le Professionnel de Santé doit émettre des FSE ou DRE avec une CRL de chiffrement de pièces jointes et des certificats de chiffrement de pièces jointes à jour sur son poste.

§ 4.1.2 Architecture logicielle

…/…



…/…

§ 4.2.1.13 Constitution et sécurisation des FSE et des DRE en mode SESAM-Vitale

…/…

Certificat de chiffrement de données révoqué

Si un des certificats de chiffrement des données de la facture est révoqué, la constitution et la sécurisation des FSE et des DRE est impossible.

Certificat de chiffrement de données périmé

Le progiciel du Professionnel de Santé doit remonter un message d'alerte au Professionnel de Santé afin de lui signifier l'utilisation d'un certificat de chiffrement de données périmé. Ce message ne bloque pas la création de la FSE et/ou de la DRE. Il convient de mettre à jour les certificats sur le poste de travail du Professionnel de Santé.

Il est recommandé aux éditeurs de proposer un paramétrage permettant au minimum de remonter cette alerte aux Professionnels de Santé au moins une fois par jour.

§ 4.2.4 Transmission des fichiers et réception des fichiers retour

Le schéma global de transmission des fichiers et de réception des fichiers retours est résumé ci-dessous :

Progiciel du Professionnel de Santé	Modules SESAM-Vitale	Périphériques
Pour chaque fichier à émettre		
Détermination de l'adresse du destinataire.		
Chiffrement de la pièce jointe		
Constitution de l'enveloppe MIME		
~~Constitution de l'enveloppe S/MIME (facultatif)~~		
Formatage du message SMTP		
Réception des fichiers retour		modem
Transmission des fichiers constitués vers les différents organismes		
		modem
Traitement des comptes rendus des transmissions		

Pour l'échange des factures électroniques, le progiciel du Professionnel de Santé doit faire appel aux logiciels de gestion des protocoles de communication.

Les Services SESAM-Vitale ne fournissent pas de fonction de télétransmission.

~~Le progiciel peut implémenter une solution de chiffrement des messages homologuée par le GIP-CPS pour l'envoi des factures électroniques.~~

Les retours reçus par le Poste de Travail du Professionnel de Santé ne sont pas chiffrés.

Les certificats de chiffrement de pièce jointe ~~des boîtes aux lettres des organismes destinataires~~ sont stockés sur le Poste de Travail du Professionnel de Santé et doivent pouvoir être mis à jour dans leur annuaire des certificats.

…/…

§ 4.2.6.4 Administration des certificats de chiffrement et de la CRL des certificats de chiffrement

Le progiciel doit permettre la mise à jour des certificats de chiffrement de données et de la CRL des certificats de chiffrement de données pour chiffrer les FSE et/ou les DRE conformément aux règles décrites à l'annexe 1 partie C du cahier des charges.

De même, le progiciel doit permettre la mise à jour des certificats de chiffrement de pièce jointe et de la CRL des certificats de chiffrement de pièce jointe pour chiffrer les fichiers de lots de FSE et/ou DRE conformément aux règles décrites à l'annexe 4 du cahier des charges.

§ 6 Glossaire

…/…

Certificat X509	Objet sécuritaire contenant la clé publique utilisé par les algorithmes de chiffrement ou de signature et permettant d'attester l'identité d'une personne ou d'un organisme.
Certificat périmé	Certificat dont la date de validité est dépassée par rapport à la date de vérification
Certificat obsolète	Un nouveau certificat plus récent pour la personne ou l'organisme concerné a été publié. Le certificat est cependant toujours valide
Certificat révoqué	Le certificat a été déclaré invalide par l'autorité de certification avant sa fin de validité et ne doit plus être utilisé. Ce certificat est présent dans la liste de révocation (CRL) associée.

…/…

2.4 Annexe 1–Partie B « Présentation fonctionnelle des modules SESAM-Vitale – Principe de Traitement des retours et Gestion des ARL»

Contexte

De nouveaux messages de service chiffrement ont été créés relatif au chiffrement de pièce jointe :

- Message de service chiffrement « erreur de chiffrement » (code 4005)
- Message de service chiffrement « warning chiffrement » (code 4015)
- Message de service chiffrement « pièce jointe non chiffrée » (code 4025)

Ceci en remplacement des messages de service chiffrement existants (4000, 4010 et 4020) réservés au chiffrement de transport

Paragraphes impactés

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
4	Gestion des avis de non remise et des messages de service	*Remplacement traitement du message de service 4000 par le message de service 4005*	M

Contenu des paragraphes

§ 4 Gestion des avis de non remise et des messages de service

…/…

- Cas particulier : Lors de la réception d'un message de service 4005~~0~~ « Flux chiffré en erreur », correspondant à un flux qui n'a pas pu être déchiffré. Le progiciel doit réémettre le flux à l'identique chiffré avec le bon certificat sans extraire le fichier ou aucun lot si ceux-ci avaient déjà fait l'objet d'une retransmission.

…/…

2.5 Annexe 4 : « Télécommunications (sur Réseau IP) et chiffrement de transport »

Paragraphes impactés

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
Titre	Télécommunications (sur Réseau IP) et chiffrement de transport	*Remplacement du chiffrement de transport par le chiffrement de pièce jointe*	M
1	Présentation	*Suppression de la référence au chiffrement de transport*	M
3	Conformité aux standards Internet	*Suppression de la référence au chiffrement de transport* *Ajout des références relatives au chiffrement de pièce jointe*	M
4	Nature des flux	*Suppression de la référence au chiffrement de transport*	M
6	Chiffrement de transport	*Suppression du §*	S
6	Chiffrement de pièce jointe	*Nouveau §*	ND
7.1	Les messages SMTP contenant les fichiers de factures	*Suppression de la référence au format S/MIME (chiffrement de transport)*	M

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
7.1.1	Profil des messages SMTP	*Suppression de la référence au format S/MIME (chiffrement de transport)*	M
7.1.4	Constitution du message SMTP au format S/MIME à partir du fichier de factures	*Suppression du §*	S
7.1.5	Structures du message SMTP au format S/MIME	*Suppression du §*	S
7.1.6	Structures de l'entité MIME d'un message chiffré	*Suppression du §*	S
8	Profil des messages test SMTP	*Ajout chiffrement pièce jointe*	M
9	Profil des messages de démonstration SMTP	*Ajout chiffrement pièce jointe*	M
11.3.3	Liste des codes rejets générés par les organismes d'Assurance Maladie	*Modification des codes erreurs*	M

Contenu des paragraphes

Titre : Télécommunications (sur Réseau IP) et chiffrement de pièce jointe ~~transport~~

§1 Présentation

…/…

~~Les Professionnels de Santé équipés d'un outil de sécurisation de messagerie peuvent télétransmettre des flux chiffrés, selon le standard S/MIME décrit dans la présente annexe, aux organismes d'assurance maladies. Les organismes d'assurance maladie s'engagent à accepter ce type de flux.~~

Le Poste de Travail du Professionnel de Santé peut récupérer dans sa boîte aux lettres des flux retour des organismes assurances Maladie qui sont non chiffrés (ARL, flux « Rejet/Signalement/Paiement » et messages de service ~~(les messages de services à destination du Professionnel de Santé concernant des erreurs de chiffrement sont signés.)~~ correspondant à l'ensemble des factures du Professionnel de Santé, quel que soit le mode de saisie (Factures électroniques ou papier).

§3 Conformité aux standards Internet

Les réseaux s'appuient sur les standards Internet décrits dans des « Request For Comments ».

~~Le chiffrement des messages SMTP est conforme aux RFC 2630 (CMS) et 2633 (S/MIME V3).~~

Le chiffrement de pièce jointe est conforme à la RFC 5652.

Les certificats de clé publique des organismes destinataires sont conformes au RFC 2459 (X509 V3).

A ce titre, le Poste de Travail du Professionnel de Santé devra être conforme notamment avec les standards TCP/IP, ESMTP, MIME, POP3 et S/MIME.

Le mécanisme d'avis de non remise est conforme aux RFC 1891, 1893 et 1894.

Cette spécification technique est basée sur les travaux de l'IETF relatifs au transport par messagerie des flux EDI (cf. RFC 1767).

§4 Nature des flux

…/…

~~Afin de garantir l'interopérabilité et la réutilisation des outils de chiffrement dans le contexte hors SESAM-Vitale (échanges dans le cadre du domaine de la santé), il est recommandé d'utiliser des outils homologués par le GIP CPS pour le chiffrement des messages SMTP au standard S/MIME.~~

…/…

§6 ~~Chiffrement de transport~~

~~Le chiffrement de transport devant être utilisé possède les caractéristiques suivantes :~~

- ~~le chiffrement des messages s'effectue en utilisant l'algorithme 3-DES en mode CBC[1] (clé de session de 128 bits) ;~~
- ~~la clé de session est chiffrée avec la clé publique RSA du destinataire du message (clé publique de 1024 bits) ;~~
- ~~les clés publiques sont certifiées, les certificats sont au format X509 V3.~~

~~La clé de session est chiffrée à l'aide de la clé publique de l'organisme d'assurance maladie auquel le Professionnel de Santé transmet le flux. Cette clé publique est certifiée par l'autorité de certification G.I.P. « CPS ».~~

~~A une clé publique est donc associé un certificat, qui atteste que la clé publique est bien liée à un organisme d'assurance maladie. En effet, il permet la vérification de la propriété d'une clé publique pour prévenir la contrefaçon des clés.~~

~~Les certificats des BALs des organismes d'assurances maladies sont disponibles dans l'annuaire LDAP X500 du G.I.P. « CPS ».~~

[1] CBC : Cipher Block Chaining : chiffrement en mode chaîné

Une connexion à l'annuaire est nécessaire pour récupérer un nouveau certificat et l'intégrer dans l'annuaire local sur l'équipement informatique du Professionnel de santé. Les outils homologués par le G.I.P. CPS permettent la connexion à cet annuaire. La récupération d'un certificat est nécessaire dans les cas suivants :

- le Professionnel de Santé met en place la solution de chiffrement de transport des flux,
- environ 15 jours avant la date de fin de validité du certificat (certificat est périmé),
- le certificat est révoqué (en cas de clé privée dévoilée).

La liste de révocation des certificats est disponible dans l'annuaire du G.I.P. « CPS » : ldap://annuaire.gip-cps.fr/o=gip-cps,c=fr

Le progiciel du Professionnel de Santé vérifie que le certificat n'est pas dans la liste de révocation avant de chiffrer les flux.

Pour trouver un certificat d'un organisme d'assurance maladie dans l'annuaire du G.I.P. « CPS », il suffit d'indiquer l'adresse e-mail de l'organisme d'assurance maladie.

Chaque certificat contient notamment l'adresse e-mail de l'organisme d'assurance maladie qui le détient (champ Subject). Le G.I.P. « CPS », en tant qu'autorité de certification s'assure qu'elle ne délivre pas deux certificats contenant le même nom à deux organismes d'assurance maladie différents.

Les vérifications à effectuer par le progiciel du Professionnel de Santé sur un certificat sont les suivantes :

- certificat signé par l'autorité de certification habilitée (c'est-à-dire le G.I.P. « CPS ») ;
- période de validité du certificat correcte (incluant la date du jour) ;
- certificat non révoqué (certificat non présent dans la liste de révocation des certificats) ;

Il est recommandé que le Professionnel de Santé puisse s'assurer de la mise à jour régulière de la liste de révocation auprès du G.I.P. CPS.

L'extension « *SubjectAltName* » contient l'adresse e-mail de l'organisme d'assurance maladie.

Par ailleurs, lorsque le Professionnel de Santé utilise un certificat périmé, l'Assurance Maladie lui envoie un message de service dans lequel est renseigné le nouveau certificat.

Cette version du Cahier des Charges permet l'utilisation des outils de chiffrement de transport. Les outils homologués par le G.I.P.-CPS, conformes aux spécifications de la présente annexe, seront disponibles. »

Remarque :

Lorsque plusieurs organismes AMC partagent, dans le cadre d'une convention, une seule boîte à lettre destinataire, un seul certificat est nécessaire pour le chiffrement de transport des messages vers cette boîte aux lettres.

§6 Chiffrement de pièce jointe

6.1 Présentation

Contexte

Les évolutions contenues dans ce chapitre ont pour objectif :

- De décrire la mise en œuvre du chiffrement de pièce jointe lors des échanges entre le PS et l'assurance maladie, chiffrement qui vient en remplacement du chiffrement de transport qui était optionnel dans les versions précédentes du cahier des charges SESAM-Vitale 1.40.
- D'assurer ainsi la confidentialité des données patients (en dehors des données déjà chiffrées) échangées entre le PS et l'assurance maladie, dont le NIR, en conformité avec les exigences de la CNIL, tout en permettant aux OCT d'assurer la continuité des services offerts à leurs clients.

Principes généraux du chiffrement

Le chiffrement de la pièce jointe contenant le fichier de lots de FSE ou de DRE transmis par messagerie se fait en utilisant :

- une clé AMO pour chiffrer le fichier de FSE à destination des AMO,
- une clé AMC pour chiffrer le fichier de DRE à destination des AMC,
- une clé OCT pour chiffrer le fichier à destination d'un OCT

Ce principe de chiffrement est illustré par le schéma suivant :

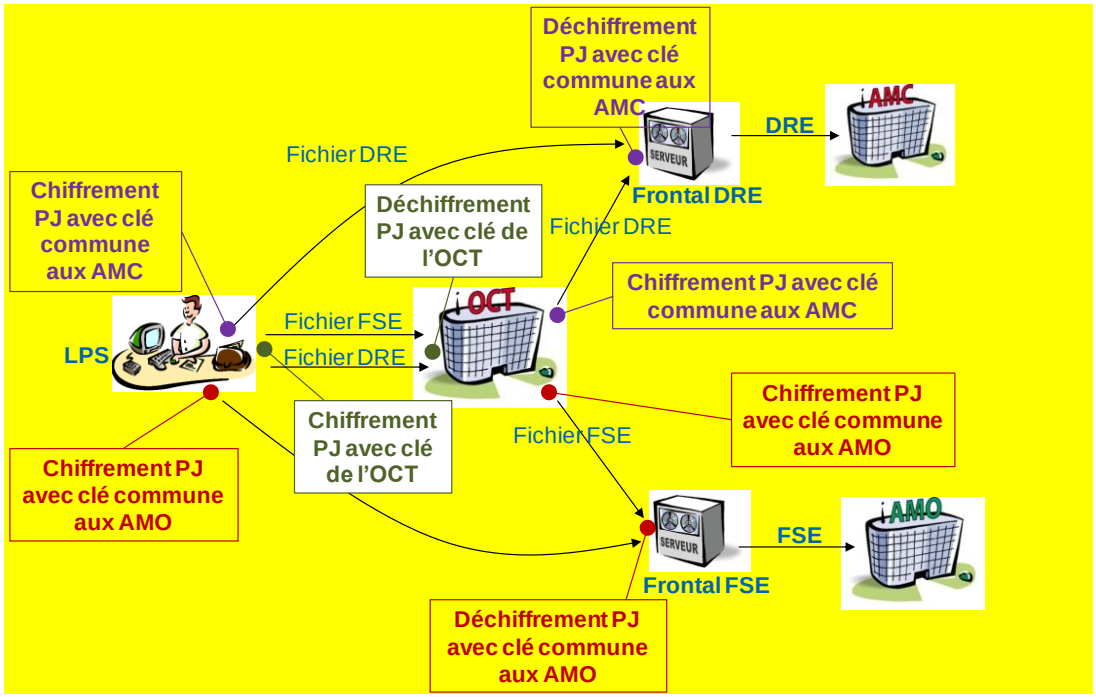


Figure XX : Principe de chiffrement des pièces jointes

Nouvelles fonctionnalités

La mise en œuvre du chiffrement de pièce jointe introduit les nouvelles fonctionnalités suivantes :

- Chiffrement de pièces jointes, comprenant les points suivants :
  - Vérification de la validité des certificats avant usage.
  - Chiffrement des PJ des messages avec le certificat AMO de l'IGC OSI (pour les FSE).
  - Chiffrement des PJ des messages avec le certificat AMC de l'IGC OSI (pour les DRE).
  - Chiffrement des PJ des messages avec le certificat OCT de l'IGC de l'OCT pour les flux à destination des OCT.
- Gestion de la sécurité, comprenant les points suivants :
  - Stockage (en général dans un magasin de certificats) des 2 et/ou 3 certificats (AMO/AMC et/ou OCT) et d'au moins 2 à 4 autorités de certification (pour gérer l'autorité de l'assurance maladie et de l'OCT, ainsi que la période de migration vers une nouvelle AC lors des renouvellements).
  - Accès à l'annuaire LDAP du GIE SV pour la récupération des certificats et des Listes de Révocation de Certificats (CRL).
- Gestion de nouveaux messages de service :
  - Nouveaux messages de services envoyés par les frontaux de l'AM dans le cas de renouvellements/problèmes de certificats.

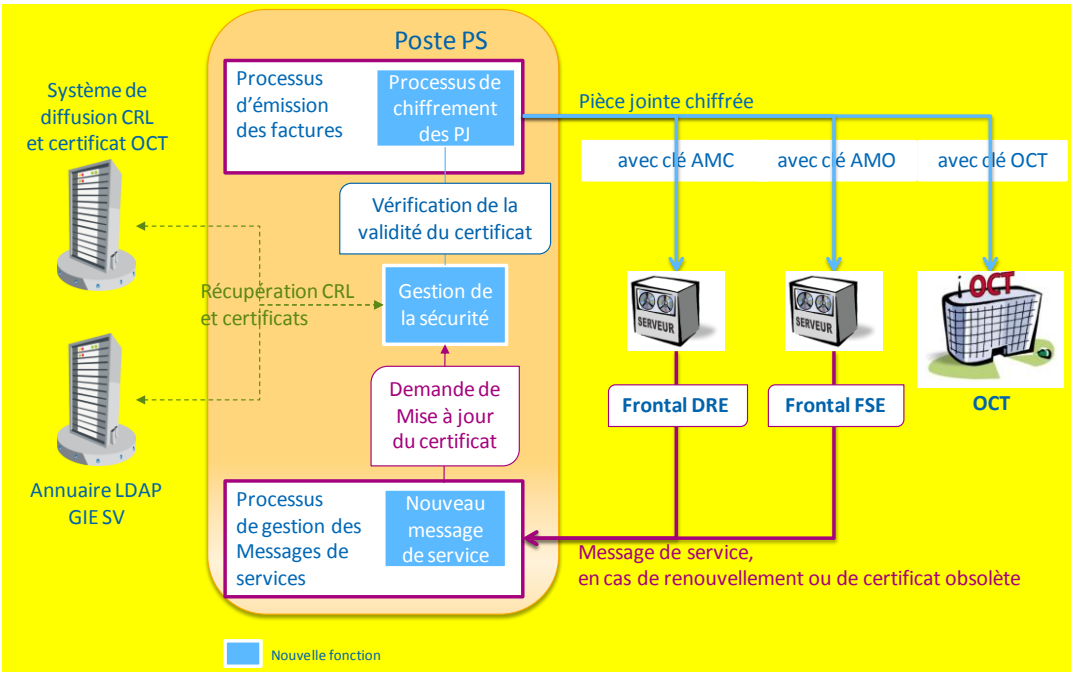


Figure XX : Nouvelles fonctionnalités à mettre en œuvre

6.2 Chiffrement de la pièce jointe

6.2.1 Règles de gestion

L'émetteur chiffre le fichier logique ou la pièce jointe compressée en appliquant l'algorithme de chiffrement décrit ci-après (cf. §6.2.2).

Les certificats à utiliser doivent au préalable avoir été vérifiés selon la procédure décrite ci-après (cf. §6.2.3)

Les fichiers de FSE à destination des AMO doivent être chiffrés avec la clé AMO (certificat amo_pj.reel@reel.rss.fr)

Les fichiers de DRE à destination des AMC doivent être chiffrés avec la clé AMC (certificat amc_pj.reel@reel.rss.fr)

Les fichiers transmis à destination d'un OCT doivent être chiffrés avec la clé fournie par l'OCT destinataire.

Impacts sur le profil des messages SMTP

Le champ « Content-Description » des messages SMTP possède un troisième sous-champ valorisé à « **K** » qui indique le chiffrement de pièce jointe.

Exemple :

- Pour les flux à destination des organismes d'assurance maladie obligatoire, le champ « Content-Description » sera valorisé à « FSE/B2/**K** » ou « FSE/B2/**ZK** » si la pièce jointe est également compressée.

Cas particulier

[CP1] Flux de test ou flux de démonstration

Les fichiers de FSE à destination des AMO doivent être chiffrés avec la clé AMO de test (certificat amo_pj.test@test.rss.fr)

Les fichiers de DRE à destination des AMC doivent être chiffrés avec la clé AMC de test (certificat amc_pj.test@test.rss.fr)

[CP2] CRL présente mais périmée (date de validité dépassée)

Le contrôle de non révocation des certificats se fait avec la CRL présente sur le poste et est non bloquant pour l'émission des flux SMTP.

Cas d'erreur

[CE1] Le certificat à utiliser est non valide

Le processus s'arrête et ne peut être repris qu'une fois le certificat mis à jour (cf. §6.2.3)

[CE2] Absence d'une CRL sur le poste émetteur

Le processus s'arrête et ne peut être repris qu'une fois la CRL installée sur le poste (cf. 6.3.3)

6.2.2 Modalité technique de chiffrement

Description

Le chiffrement d'un document possède les caractéristiques suivantes (basées sur la RFC 5652[2] - PKCS#7) :

1. le chiffrement du document s'effectue en utilisant l'algorithme AES 128 bits en mode CBC (clé de session de 128 bits) ;
2. la clé de session est chiffrée avec la clé publique RSA du destinataire du document (clé publique de 2048 bits) ;
3. les clés publiques sont certifiées, les certificats sont au format X509 V3.

Chaque document est chiffré à l'aide d'une clé de session qui elle-même est chiffrée à l'aide de la clé publique du destinataire du document. Cette clé publique est certifiée par une autorité de certification et est donc contenu dans le certificat correspondant.

Chaque résultat du chiffrement constitue le document sous forme « binaire » (pas d'encodage base 64 bits), auquel est ajoutée l'extension « .pkcs7 ».

Exemple

L'exemple ci-après illustre une possibilité de mettre en œuvre le chiffrement d'un document en utilisant le produit OpenSource OpenSSL.

Dans cet exemple :

- le document à chiffrer est indiqué sous « NomDuFichierAChiffrer »
- le certificat contenant la clé publique du destinataire est indiqué sous « Certificat.pem[3] »

La commande permettant d'obtenir le chiffrement du document est la suivante :

« *OpenSSL> cms -encrypt -in NomDuFichierAChiffrer -binary -aes-128-cbc -outform der -out NomDuFichierAChiffrer.pkcs7 Certificat.pem* »

§6.2.3 Contrôle de validité des certificats

Certificats assurance maladie

Deux certificats assurance maladie sont utilisés pour chiffrer les fichiers transmis directement vers les frontaux de l'assurance maladie :

- Un certificat AMO pour le chiffrement des fichiers de lots de FSE
- Un certificat AMC pour le chiffrement des fichiers de lots de DRE

L'AC utilisée est l'AC-FACTURATION de l'IGC OSI du GIE SESAM-Vitale.

Les certificats sont disponibles dans l'annuaire LDAP X500 à l'adresse suivante :

[2] http://datatracker.ietf.org/doc/rfc5652/

[3] Pour être utilisé avec OpenSSL, le certificat doit être mis au format « .pem »

- ldap://annuaire.sesam-vitale.fr/cn=AC-FACTURATION,ou=AC-FACTURATION,ou=AC-SESAM-VITALE-2034,o=sesam-vitale,c=fr,cn=amx_pj.reel@reel.rss.fr/certificate

où « amx_pj.reel@reel.rss.fr» vaut :

- amo_pj.reel@reel.rss.fr pour le certificat AMO
- amc_pj.reel@reel.rss.fr pour le certificat AMC

Le LPS doit vérifier que dans le certificat récupéré, l'extension « *SubjectAltName* » contient les libellés précédents.

Cas particulier

[CP1] Flux de test ou flux de démonstration

Les certificats de tests ont pour libellés :

- amo_pj.test@test.rss.fr pour le certificat AMO
- amc_pj.test@test.rss.fr pour le certificat AMC

Cas des PS utilisant les services d'un OCT

Les fichiers doivent être chiffrés lors de leur transmission entre le PS et l'OCT avec un certificat fourni par l'OCT.

Les modalités de récupération de ce certificat et des éléments de sécurité associés (AC, CRL) sont de la responsabilité de l'OCT et ne sont pas décrites dans ce document.

Vérification du certificat

Les vérifications à effectuer par le LPS sur un certificat sont les suivantes :

- contrôle de parenté (chaine de confiance) du certificat[4]
- vérification de la validité de la chaîne de confiance (certificats des autorités intermédiaire et racine (ROOT))
- date de début et de fin de validité du certificat correcte (incluant la date du jour) ;
- certificat non révoqué (certificat non présent dans la liste de révocation des certificats) ;
- contrôle du nom du propriétaire du certificat.
- vérification du Key Usage (extension critique). Le Key Usage doit contenir
  - Digital Signature
  - KeyEncipherment
  - NonRepudiation

[4] Le certificat est signé par un certificat « intermédiaire » lui-même signé par un certificat « ROOT ».

Gestion de la CRL

Le LPS vérifie que le certificat n'est pas dans la liste de révocation avant de chiffrer les documents.

En cas de liste de révocation non présente, le LPS doit considérer le certificat comme non valide.

En cas de liste de révocation périmée sur le poste PS, la vérification du certificat doit se faire à partir de la liste présente sur le poste PS.

6.3 Administration des éléments de sécurité

6.3.1 Gestion des autorités de certification

Il est recommandé que le Professionnel de Santé puisse s'assurer de la mise à jour des autorités de certification.

Le LPS doit être en mesure de gérer au moins deux autorités de certification en parallèle pour assurer les périodes de migration d'une autorité vers une autre ou pour gérer l'autorité d'un OCT en plus de l'autorité de l'assurance maladie.

Ces autorités peuvent être mises à jour au travers des procédures de mise à jour du LPS, soit directement par le PS au travers de l'IHM du LPS.

Les modalités de récupération et d'installation d'une nouvelle autorité de certification sur le poste PS sont laissées à la discrétion de l'éditeur.

Les autorités utilisées pour certifier les certificats de l'assurance maladie sont les suivantes :

- AC de production
  - Certificat de l'AC-FACTURATION : ldap://annuaire.sesam-vitale.fr/cn=AC-FACTURATION,ou=AC-FACTURATION,ou=AC-SESAM-VITALE-2034,o=sesam-vitale,c=fr?cACertificate;binary
  - Certificat de l'AC-SESAM-VITALE-2034 : ldap://annuaire.sesam-vitale.fr/cn= AC-SESAM-VITALE-2034,ou=AC-SESAM-VITALE-2034,o=sesam-vitale,c=fr?cACertificate;binary
- AC de test
  - Certificat de l'AC-FACTURATION-TEST : ldap://annuaire.sesam-vitale.fr/cn=AC-FACTURATION-TEST,ou=AC-FACTURATION-TEST,ou=AC-SESAM-VITALE-TEST-2034,o=sesam-vitale,c=fr?cACertificate;binary
  - Certificat de l'AC-SESAM-VITALE-TEST-2034 : ldap://annuaire.sesam-vitale.fr/cn= AC-SESAM-VITALE-TEST-2034,ou=AC-SESAM-VITALE-TEST-2034,o=sesam-vitale,c=fr?cACertificate;binary

6.3.2 Gestion des certificats

Récupération du certificat

A une clé publique est associé un certificat, qui atteste que la clé publique est bien liée au destinataire. Ce certificat permet la vérification de la propriété d'une clé publique pour prévenir la contrefaçon des clés.

Une connexion à un annuaire public est nécessaire pour récupérer un nouveau certificat et l'intégrer dans l'annuaire local sur l'équipement informatique du LPS[5]. La récupération d'un certificat est nécessaire dans les cas suivants :

- initialement lorsque le LPS met en place la solution de chiffrement,
- par la suite, lorsque le certificat est périmé : le LPS récupère le nouveau certificat environ 15 jours avant la date de fin de validité,
- par la suite, lorsque le certificat est révoqué (en cas de clé privée dévoilée),
- sur réception d'un message de service chiffrement 4005, 4015 ou 4025.

Recommandations

Il est recommandé que les certificats utilisés sur l'équipement informatique du LPS soient stockés dans un magasin local, ceci afin d'éviter de surcharger inutilement les annuaires publics disponibles sur Internet.

Les certificats doivent être vérifiés avant leur enregistrement dans le magasin local (cf. §6.2.3)

Lors de la mise à jour d'un certificat dans ce magasin local, les anciens certificats correspondant au même destinataire doivent être supprimés.

6.3.3 Gestion de la CRL

Récupération de la CRL

L'adresse de récupération de la liste de révocation des certificats de l'AC-FACTURATION est disponible dans le champ du certificat « point de distribution de la liste de révocation des certificats » et est du type :

- ldap://annuaire.sesam-vitale.fr/cn=AC-FACTURATION,ou=AC-FACTURATION,ou=AC-SESAM-VITALE-2034,o=sesam-vitale,c=fr/certificateRevocationList

Vérification de la CRL

Les vérifications à effectuer par le LPS sur la CRL sont les suivantes :

- Vérification de la signature de la CRL par la bonne autorité de certification (AC)
- Vérification de la date de validité de la CRL

[5] Plusieurs certificats **valides** peuvent être disponibles dans l'annuaire pour un même destinataire. Dans ce cas, l'équipement informatique doit être capable de récupérer le plus récent.

Recommandations

Les recommandations de récupération des CRLs reposent sur les principes suivants d'utilisation :

- **limitation du téléchargement** aux CRLs correspondant aux certificats susceptibles d'être acceptés par l'application ;
- **fréquence** de téléchargement des CRLs **en rapport avec la fréquence de publication** de celles-ci ;
- **variabilité des horaires de téléchargement** des CRLs lorsque celui-ci est automatisé (notamment pour que toutes les instances d'un même produit installé chez différents clients ne téléchargent pas les CRLs en même temps : prévoir par exemple un étalement de téléchargement « aléatoire » sur plusieurs heures) ;
- **limitation des durées de connexion** au temps nécessaire au téléchargement des CRLs (pas de maintien de session après un (ou une tentative de) téléchargement).

Le standard de référence décrivant le format des CRLs est le RFC 5280. Toutefois, la fréquence de publication est laissée libre à chaque IGC. Toute CRL contient obligatoirement la date/heure de la publication de la CRL suivante (extension nextUpdate) permettant ainsi à un vérificateur de récupérer la nouvelle CRL avant l'expiration de la CRL en cours.

La méthode suivante est recommandée pour assurer la bonne gestion de la CRL de l'AC-FACTURATION de l'assurance maladie sur l'équipement de l'émetteur des flux :

- Un chargement hebdomadaire est mis en place pour la CRL en exploitation. La CRL est publiée tous les jours approximativement à la même heure – vers 0h00. Le chargement peut donc commencer à partir de 2h00. La première requête doit être planifiée aléatoirement sur plusieurs heures (8 heures minimum) après 2h00 jusque 22h00 (algorithme intégré dans le logiciel par son éditeur devant garantir qu'il y a une répartition de charge chez ses clients).
- S'il se produit un problème lors du chargement *(problème technique ou chargement de la même CRL)* :
  - relancer le chargement tous les jours selon les mêmes règles que précédemment,
  - si le problème persiste toujours, afficher un message d'alerte au Professionnel de Santé lui demandant de contacter le fournisseur de sa solution avant l'expiration de la CRL. Ce dernier doit analyser la source du problème et contacter si besoin le centre de service du GIE SESAM-Vitale.

§7.1 Les messages SMTP contenant les fichiers de factures

Les messages SMTP contenant les fichiers de factures sont ~~peuvent être~~ transmis au format MIME ~~ou au format S/MIME~~.

§7.1.1 Profil des messages SMTP

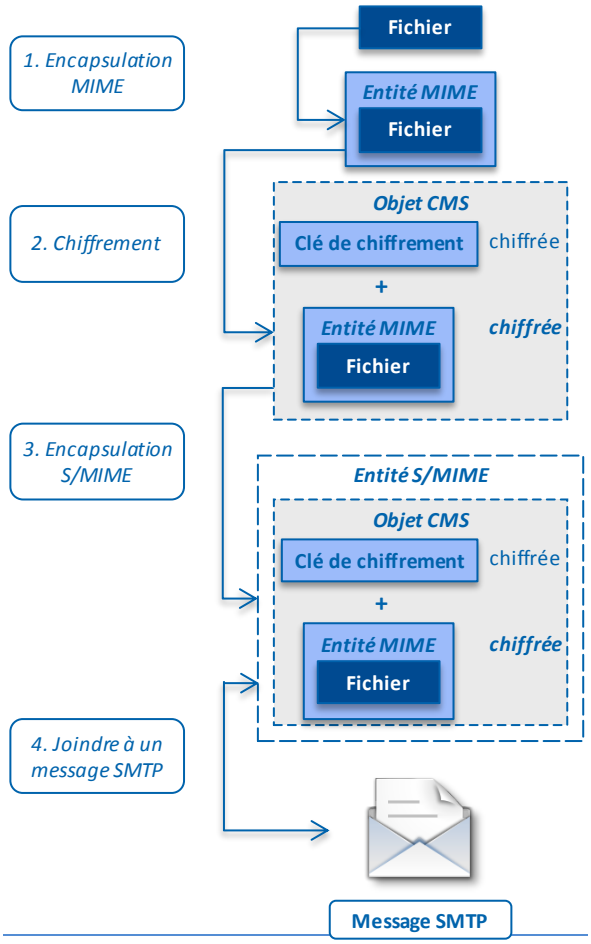
Les messages SMTP transmis par le Professionnel de Santé doivent respecter les formats SMTP et MIME ~~(et S/MIME)~~.

…/…

§7.1.4 Constitution du message SMTP au format S/MIME à partir du fichier de factures

Si le Professionnel de Santé souhaite effectuer une compression de son fichier de factures, celle-ci doit être effectuée avant le chiffrement de transport.

Les étapes qui permettent de constituer un message SMTP au format S/MIME à partir d'un fichier de factures sont présentées ci-dessous :



- (0) Il est fortement conseillé de compresser le fichier de factures.

  Si le fichier est compressé, le champ « *Content-Description* » du message SMTP possède un troisième sous-champ valorisé à « **Z** ».

- (1) Le fichier est encapsulé dans une entité MIME ; **L'entité MIME ne doit contenir qu'un et un seul fichier.**

  L'entité MIME est constituée notamment des champs suivants :

  - « *Content-Type* » : la valeur de ce champ est « Application/EDI-consent » ;
  - « *Content-Tranfer-Encoding* » : la valeur de ce champ est « BASE64 » ;
  - « *Content-Description* » : la valeur de ce champ est :
    - « FSE/B2 » pour un fichier de FSE (ou DRE/DR pour un fichier de DRE) non compressé ;
    - « FSE/B2/**Z** » pour un fichier FSE (ou DRE/DR/**Z** pour un fichier de DRE) compressé.

- (2) L'entité MIME est chiffrée conformément à la RFC 2630 ; **elle doit être chiffrée une seule fois et ne doit pas être signée**. L'entité MIME chiffrée ainsi que la clé de session chiffrée sont regroupés dans un objet CMS.
- ***(3) L'objet CMS est encapsulé dans une entité S/MIME ; cette entité S/MIME peut avoir une structure « multipart » ou « single part ».***
- (4) L'entité S/MIME est attachée à un message SMTP. **Le message SMTP ne doit contenir qu'une et une seule entité S/MIME.**

§7.1.5 Structures du message SMTP au format S/MIME

La structure du message SMTP doit être conforme aux formats SMTP et S/MIME. Deux types de structure peuvent être utilisés : la structure "multipart" et la structure "single part".

Légende :

- O : le champ est obligatoire ;
- F : le champ est facultatif.

Message SMTP multipart

EN-TETES	Dates	Date	O	`Date:`	
	Champs expéditeur	Adresse de l'expéditeur du message	O	`From:`	*adresse émetteur*
	Champs destinataire(s)	Adresse du destinataire du message	O	`To:`	*adresse destinataire*
	Autres champs	Identifiant du message	O	`Message-ID`	

		Objet du message	O	`Subject:`	`SVvvvvvv/exercice/compostage/nnnnn p`
					`flux de FSE`
					`DRvvvvvv/exercice/compostage/nnnnn p`
					`flux de DRE`

	Champs de contenu	Version de MIME utilisée	O	`Mime-Version:`	***version***
		Type du contenu	O	`Content-Type:`	`multipart/mixed;boundary=`délimiteur
LIGNE VIDE			O		

BODY PART	Préambule	Préambule	F	TEXTE QUELCONQUE	
	Délimiteur	Délimiteur	O	--DELIMITEUR	
	[En-têtes]	Type de contenu	O	`Content-Type:`	*Type/Sous-type;paramètre*
		Encodage du contenu	O	`Content-Transfer-Encoding:`	*Encodage*
	Ligne vide		O		
	Body part	Contenu du message	O	OBJET CHIFFRE (CMS)	
	Délimiteur final	Délimiteur final	O	--DELIMITEUR--	
	Epilogue	Epilogue	F	TEXTE QUELCONQUE	

Message SMTP single part

EN-TETES	Dates	Date	O	`Date:`	
	Champs expéditeur	Adresse de l'expéditeur du message	O	`From:`	*adresse émetteur*
	Champs destinataire(s)	Adresse du destinataire du message	O	`To:`	*adresse destinataire*
	Autres champs	Identifiant du message	O	`Message-ID`	

		Objet du message	O	`Subject:`	`SVvvvvvv/exercice/compostage/nnnnn p`
					`flux de FSE`
					`DRvvvvvv/exercice/compostage/nnnnn p`
					`flux de DRE`

	Champs de contenu	Version de MIME utilisée	O	`Mime-Version:`	***version***
		Type du contenu	O	`Content-Type:`	*Type/Sous-type;paramètre*
		Encodage du contenu	O	`Content-Transfer-Encoding:`	*Encodage*
LIGNE VIDE			O		
BODY PART	Body part	Contenu du message	O	OBJET CHIFFRE (CMS)	

§7.1.6 Structures de l'entité MIME d'un message chiffré

La structure de l'entité MIME contenant le fichier doit être conforme au format MIME. Deux types de structure peuvent être utilisés : la structure "multipart" et la structure "single part".

Légende :

- O : le champ est obligatoire ;
- F : le champ est facultatif.

Entité MIME multipart

EN-TETES	Champs de contenu	Type du contenu	O	`Content-Type:`	`multipart/mixed;boundary=`délimiteur
LIGNE VIDE			O		

BODY PART	Préambule	Préambule	F	TEXTE QUELCONQUE	
	Délimiteur	Délimiteur	O	--DELIMITEUR	
	[En-têtes]	Type de contenu	O	`Content-Type:`	*Type/Sous-type;paramètre*
		Encodage du contenu	O	`Content-Transfer-Encoding:`	*Encodage*
		Description du contenu	O	`Content-Description:`	*nature/norme*
	Ligne vide		O		
	Body part	Contenu du message	O	FICHIER	
	Délimiteur final	Délimiteur final	O	--DELIMITEUR--	
	Epilogue	Epilogue	F	TEXTE QUELCONQUE	

Entité MIME single part

EN-TETES	Champs de contenu	Type du contenu	O	`Content-Type:`	*Type/Sous-type;paramètre*
		Encodage du contenu	O	`Content-Transfer-Encoding:`	*Encodage*
		Description du contenu	O	`Content-Description:`	*nature/norme*
LIGNE VIDE			O		
BODY PART	Body part	Contenu du message	O	FICHIER	

§8 Profil des messages test SMTP

…/…

Les messages SMTP dits de « test » différent des flux dits « réels » par le contenu du champ "Content-Description" qui contient la nature et la norme de l'objet transporté selon les règles suivantes :

- Pour les flux à destination ou émis par les organismes d'assurances maladies obligatoires :

Type de message SMTP de test	Champ « Content-Description »	
	Pas de compression	Compression
Message SMTP de test contenant un fichier de lots de FSE	"FSETEST/B2/K" ;	"FSETEST/B2/**ZK**" ;

Type de message SMTP de test	Champ « Content-Description »	
	Pas de compression	Compression
Message SMTP de test contenant les flux ARL	"ARLTEST/NOEMIE"	"ARLTEST/NOEMIE/**Z**"
Message SMTP de test contenant les flux R/S/P	"RSPTEST/NOEMIE"	"RSPTEST/NOEMIE/**Z**"

- Pour les flux à destination des organismes d'assurances maladies complémentaires :

Type de message SMTP de test	Champ « Content-Description »	
	Pas de compression	Compression
Message SMTP de test contenant un fichier de lots des DRE	"DRETEST/DR/K" ;	"DRETEST/DR/**ZK**" ;
Message SMTP de test contenant les flux ARL	"ARLDRETEST/NOEMIE"	"ARLDRETEST/NOEMIE/**Z**"
Message SMTP de test contenant les flux R/S/P	"RSPDRETEST/NOEMIE"	"RSPDRETEST/NOEMIE/**Z**"

§9 Profil des messages de démonstration SMTP

…/…

Les messages SMTP dits de « démonstration » diffèrent des flux dits « réels » par le contenu du champ "Content-Description" qui contient la nature et la norme de l'objet transporté selon les règles suivantes :

- Pour les flux à destination ou émis par les organismes d'assurances maladies obligatoires :

Type de message SMTP de démonstration	Champ « Content-Description »	
	Pas de compression	Compression
Message SMTP de démonstration contenant un fichier de FSE	"FSEDEMO/B2/K" ;	"FSEDEMO/B2/**ZK**" ;
Message SMTP de démonstration contenant les flux ARL	"ARLDEMO/NOEMIE"	"ARLDEMO/NOEMIE/**Z**"

- Pour les flux à destination ou émis par les organismes d'assurances maladies complémentaires :

Type de message SMTP de démonstration	Champ « Content-Description »	
	Pas de compression	Compression

Type de message SMTP de démonstration	Champ « Content-Description »	
	Pas de compression	Compression
Message SMTP de démonstration contenant un fichier de DRE	"DREDEMO/DR/K" ;	"DREDEMO/DR/**ZK**" ;
Message SMTP de démonstration contenant les flux ARL	"ARLDREDEMO/NOEMIE"	"ARLDREDEMO/NOEMIE/**Z**"

§11.3.3 Liste des codes rejets générés par les organismes d'Assurance Maladie

Code Rejet	Libellés
40050	*Pièce jointe chiffrée en erreur*
40150	*Pièce jointe chiffrée warning*
4025	*Pièce jointe non chiffrée*

Remarques importantes :

Le message 40050 indique la raison pour laquelle le flux n'a pas été déchiffré, le flux est donc rejeté.

Le système d'accueil des flux de l'organisme d'assurance maladie n'arrive pas à déchiffrer le flux : en particulier, le certificat peut être révoqué au niveau du frontal de l'AM.

~~Le message de service est signé avec le bon certificat, qui devra être intégré dans l'annuaire local de l'outil sécurisé de messagerie.~~

=> Le Professionnel de Santé doit réémettre le flux à l'identique en utilisant le bon certificat.

Le message 40150 indique que le flux a été déchiffré mais qu'il existe un certificat plus récent.

Le système d'accueil des flux de l'organisme d'assurance maladie a déchiffré le flux, mais le certificat est obsolète. Ce message de service est un avertissement.

~~Le message de service est signé avec le bon certificat, qui devra être intégré dans l'annuaire local de l'outil sécurisé de messagerie.~~

=> Le Professionnel de Santé devra utiliser le nouveau certificat dans ses prochaines télé-transmissions à l'organisme d'assurance maladie.

Le message 4025 indique que le flux reçu n'était pas chiffré alors qu'il devait l'être obligatoirement.

=> Le Professionnel de Santé doit réémettre le flux à l'identique en chiffrant la pièce jointe.

Avant toute intégration d'un nouveau certificat dans l'annuaire local, il convient de vérifier la validité du certificat (cf. §6.2.3), notamment en cas de changement d'autorité de certification, la nouvelle autorité devra être installée sur le poste (cf. §6.3.1) en préalable à toute intégration d'un nouveau certificat issu de cette autorité.

2.6 Annexe 5 : « Transmission des flux SESAM-Vitale via les Organismes Concentrateurs Techniques »

Paragraphes impactés

§	Titre du paragraphe	Nature de l'impact / Commentaire	Q
4.1.2	Message	*Ajout spécificité des certificats de chiffrement pièce jointe*	M
4.3.3	Message	*Ajout spécificité des certificats de chiffrement pièce jointe*	M
7.1	Profil des messages du PS vers l'OCT	*Remplacement chiffrement transport par chiffrement pièce jointe*	M

Contenu des paragraphes

§4.1.2 Message

Ces messages sont structurés selon le protocole SMTP. Les autres protocoles n'ont pas lieu d'être explicités dans ce document.

Les messages sont spécifiés dans l'annexe 4 du Cahier des Charges SESAM-Vitale, la seule différence est au niveau du champ destinataire où il faut spécifier l'adresse électronique de l'Organisme Concentrateur Technique et au niveau du certificat de chiffrement pièce jointe qui est fourni par l'OCT.

§4.3.3 Message

Ces messages sont structurés selon le protocole SMTP. Les autres protocoles n'ont pas lieu d'être explicités dans ce document.

Les messages sont spécifiés dans l'annexe 4 du Cahier des Charges SESAM-Vitale, la seule différence est au niveau du champ destinataire où il faut spécifier l'adresse électronique de l'Organisme Concentrateur Technique et au niveau du certificat de chiffrement pièce jointe qui est fourni par l'OCT.

§4.3.3 Profil des messages du PS vers l'OCT

En plus des profils de messages définis dans le chapitre 7 de l'annexe 4 du présent document, il peut exister un autre profil de message.

Lorsque le Professionnel de Santé choisit d'envoyer dans un même fichier des lots de FSE et des lots de DRE vers l'Organisme Concentrateur Technique, si le mode d'échange est conforme à l'annexe 4 (messagerie SMTP), le progiciel utilisera le profil de message décrit ci dessous.

~~Le chiffrement de transport pourra également s'appliquer sur ce message~~.

Le chiffrement de pièce jointe s'applique à la transmission de ces messages conformément à l'annexe 4 en utilisant le certificat de chiffrement de pièce jointe fourni par l'OCT destinataire.