Annexe 6

Liste d'Opposition Incrémentale

Intégrant l'Addendum n°8

GIE SESAM-Vitale
5, boulevard Marie & Alexandre Oyon - 72 019 LE MANS CEDEX 2 - www.sesam-vitale.fr
SIRET : 391 722 881 00052 - APE : 6202A - RCS LE MANS : 391 722 881 - N° TVA : FR 753 917 22881

Sommaire

1 Introduction 5

2 Présentation générale 6

2.1 L'installation de la liste d'opposition incrémentale (LOI) sur le poste du Professionnel de Santé 6
2.2 Synthèse des actions 6
2.2.1 Synthèse des actions lors d'une installation de LOI 6
2.2.2 Synthèse des actions pour mettre à jour quotidiennement la LOI 6
2.2.3 Synthèse des actions pour administrer la LOI 7
2.2.4 Synthèse des actions pour la consultation de la LOI 7
2.3 Recommandations pour le Professionnel de Santé 7
2.4 Informations complémentaires aux Professionnels de Santé et aux éditeurs 7

3 Les formats des fichiers 8

3.1 Format du fichier des incréments de la liste d'opposition incrémentale – dLOI 8
3.2 Format du fichier de la liste d'opposition incrémentale – LOI 10
3.3 Format du fichier de Demande de dLOI 11
3.3.1 Description fonctionnelle du fichier de Demande de dLOI 11
3.3.2 Composition du fichier de Demande 11
3.3.3 Exemple de fichier de demande de dLOI 12

4 Description de la mise à jour de la Liste d'Opposition Vitale Incrémentale (LOI) sur le Poste de Travail du Professionnel de Santé 13

4.1 Diagramme 13
4.2 Charger les incrément(s) dLOI 14
4.2.1 Détection d'un problème dans le destinataire du message SMTP 15
4.2.2 Vérification que le message SMTP contenant un incrément dLOI est bien une réponse à une demande d'incrément dLOI 15
4.2.3 Ordonner les incréments 15
4.2.4 Supprimer les éventuels incréments non applicables 15
4.3 Intégrer incrément(s) dLOI 16
4.3.1 Règle de décompression d'un incrément dLOI 16
4.3.2 Vérification de la signature 16
4.3.3 Appliquer un incrément dLOI sur une liste LOI 17
4.3.3.1 Les principes de l'application d'un incrément 17
4.3.3.2 Code source exemple 18
4.4 Demander incrément(s) dLOI 19
4.4.1 Message SMTP de demande d'incrément(s) dLOI 19
4.4.2 Signature du message SMTP de la demande d'incrément(s) dLOI 19
4.4.3 Nombre de demande par jour 19
4.4.4 Remplir la liste des demandes d'incrément(s) dLOI 19
4.5 Traiter le message ARAN 20
4.5.1 Vérifier que le message ARAN est bien une réponse à une demande d'incrément dLOI 20
4.5.2 Vérifier le code mentionné dans le message SMTP ARAN 20

5 Description de l'administration de la Liste d'Opposition Incrémentale (LOI) 21

5.1 Administrer quotidiennement le Poste de Travail du Professionnel de Santé 21
5.1.1 Récupérer la liste des Certificats Serveurs Révoqués 21
5.1.2 Contrôler le nombre de non-réponse quotidiennes aux différentes demandes d'incrément(s) dLOI 22
5.1.3 Informer en cas de non mise à jour de la LOI au début de chaque mois 22
5.1.4 Sauvegarde/Archive 23
5.2 Administrer ponctuellement le poste de travail du Professionnel de Santé 23
5.2.1 Paramétrer les informations liées à l'opposition sur le poste du Professionnel de Santé 24
5.2.1.1 Configurer la BAL Opposition 24
5.2.1.2 Paramétrer l'adresse du Distributeur d'Opposition 24
5.2.1.3 Paramétrer le nombre maximum de jours acceptable sans réception de dLOI 24

5.2.2 Installer et Renouveler la chaîne de Certification sur le progiciel du Professionnel de Santé 24
5.2.3 Mettre au point l'opposition incrémentale 25
5.2.4 Visualiser la référence de la LOI active 25
5.3 Synthèse des fonctions débrayables 25
6 Description de la consultation de la LOI 26
6.1 Principe de la consultation 26
6.2 Code source exemple 26
7 Définitions techniques des paramètres spécifiques à la LOI 28

Tables des illustrations

FIGURE 1 : PROCESSUS DE MISE A JOUR DES DLOI 14

1 Introduction

Ce document constitue l'annexe 6 du Cahier des Charges SESAM-Vitale 1.40.

Cette annexe dédiée à la liste d'opposition incrémentale (LOI), a pour objet de décrire :

- les règles de mise à jour de la liste d'opposition incrémentale à partir des incréments dLOI, fournis par un distributeur d'opposition ;
- les formats des fichiers (LOI et dLOI) utilisés ;
- les règles d'administration de la liste d'opposition incrémentale sur le progiciel ;
- les règles de consultation de la liste d'opposition incrémentale.

2 Présentation générale

2.1 L'installation de la liste d'opposition incrémentale (LOI) sur le poste du Professionnel de Santé

La gestion de l'opposition par le progiciel devient incrémentale et quotidienne. Une liste d'opposition incrémentale (LOI) des cartes Vitale est donc créée quotidiennement et remplace la liste d'opposition électronique (LOE) dont la fréquence était mensuelle.

Cette liste LOI est mise à jour par le progiciel de manière incrémentale, seul le delta (dLOI) de la liste d'opposition est envoyé quotidiennement au poste du Professionnel de Santé. Le progiciel doit être capable de reconstituer la liste d'opposition incrémentale à partir du ou des incrément(s) (dLOI) reçu(s).

Par ailleurs, l'éditeur doit définir une procédure de mise à disposition de la LOI pour les Professionnels de Santé utilisateurs de son progiciel.

Cette procédure est utilisée uniquement dans les cas :

- de nouvelle installation logicielle ;
- de réception d'un message applicatif négatif SMTP dit ARAN ;
- ou de corruption du fichier LOI sur le Poste de Travail.

La procédure de diffusion de la LOI n'est pas décrite dans le Cahier des Charges SESAM-Vitale, chaque éditeur peut proposer le moyen de son choix pour la mise à disposition de la LOI au Professionnel de Santé.

2.2 Synthèse des actions

2.2.1 Synthèse des actions lors d'une installation de LOI

Lors d'une (première) installation de la nouvelle version du logiciel supportant la LOI et plus généralement lors d'une installation de LOI, l'éditeur doit fournir au Professionnel de Santé la version de LOI la plus récente qu'il détienne.

L'éditeur doit mettre en place une procédure pour sélectionner un fichier LOI préalablement transféré sur le Poste de Travail et le rendre actif, après avoir obligatoirement vérifié sa signature (cf. § 4.3.2).

Le progiciel doit automatiquement envoyer une demande d'incrément afin de mettre à jour sa LOI et ainsi constituer la dernière LOI.

2.2.2 Synthèse des actions pour mettre à jour quotidiennement la LOI

A partir de la LOI active présente sur le Poste de Travail du Professionnel de Santé, le progiciel doit être capable :

- d'émettre quotidiennement un message SMTP signé non compressé de demande de dLOI vers son distributeur d'opposition *(soit le GIE SESAM-Vitale ou soit un OCT). (Cette fonction doit être débrayable)* ;
- de récupérer les fichiers d'incrément (dLOI) dans sa BAL opposition ;
- de vérifier la concordance entre sa demande de dLOI et le message SMTP de réponse contenant le dLOI reçu du distributeur *(Cette fonction doit être débrayable)* ;
- de décompresser chaque fichier d'incrément (dLOI) ;

- de vérifier la signature de chaque fichier d'incrément ;
- d'ordonner les fichiers d'incrément par rapport au rang inscrit dans le fichier au niveau de la référence de la dLOI ou mentionné dans le nom du fichier ;
- d'intégrer chaque incrément à la LOI active pour reconstituer la nouvelle LOI ;
- de consulter la LOI active, et avertir le cas échéant le Professionnel de Santé que la carte est en opposition ;
- de continuer le processus de facturation avec la liste LOI (n-1) s'il n'arrive pas à intégrer le dernier incrément dLOI. (c'est à dire à reconstituer la liste LOI (n)) ;
- de traiter et de vérifier la concordance entre sa demande de dLOI et le message d'Accusé Réception Applicatif Négatif (ARAN), *(Cette fonction doit être débrayable)*.

2.2.3 Synthèse des actions pour administrer la LOI

Le progiciel doit être capable :

- d'avertir le Professionnel de Santé qu'il n'a pas reçu d'incrément dLOI depuis un certain nombre de jours (ce nombre [NB_JOUR_Max] étant paramétrable) ;
- de paramétrer le nombre maximum de jours sans réponse avant l'avertissement au Professionnel de Santé, [NB_JOUR_Max] ;
- d'avertir le Professionnel de Santé si la liste LOI active possède une date de référence antérieure au 18 du mois précédent ;
- de récupérer la liste quotidienne des certificats serveurs révoqués ;
- de configurer la BAL opposition ;
- de spécifier l'adresse du distributeur d'opposition ;
- d'installer et de renouveler la chaîne de certification servant à vérifier la signature de la LOI et des dLOI;
- de visualiser la référence de la liste d'opposition.

2.2.4 Synthèse des actions pour la consultation de la LOI

Pour la consultation de la liste d'opposition incrémentale, le progiciel exécute les fonctions décrites au § 6 « Description de la consultation de la LOI » basées sur le n° de série de la carte Vitale.

La consultation de la liste d'opposition ne doit pas être effectuée sur les cartes Vitale de démonstration.

2.3 Recommandations pour le Professionnel de Santé

Il est conseillé d'utiliser une BAL opposition distincte de la BAL facturation afin de ne pas perturber les flux financiers.

2.4 Informations complémentaires aux Professionnels de Santé et aux éditeurs

Dans un souci de ne pas surcharger le Distributeur d'Opposition et le réseau de messagerie, il a été décidé de ne pas créer de messages de services indiquant une anomalie de structure SMTP, une anomalie de fichier ou de signature lors d'une demande d'incrément dLOI.

3 Les formats des fichiers

3.1 Format du fichier des incréments de la liste d'opposition incrémentale – dLOI

Description du fichier dLOI

Champ	Format	Valeur	Observation

En-tête

Taille en-tête	4D		Taille en octets de l'en-tête
Application	20 AN	DLOI	Cadré à gauche complété par des espaces
Version d'application	2D	01	
Référence : Date et rang	12D	AAAAMMJJXXXX	Où AAAAMMJJ représente une date et XXXX un rang.
Format de la liste	4AN	BTMP	Tableau bitmap
Référence de la LOI (n-1)	12D	AAAAMMJJXXXX	Référence de la LOI (n – 1) à laquelle s'applique l'incrément
Référence de la LOI (n)	12D	AAAAMMJJXXXX	Référence de la LOI (n) obtenue après application de l'incrément
Taille signature LOI(n)	4D		Taille (m) en octets de la signature de la LOI(n)
Signature LOI(n)	m O		Signature de la LOI (n) obtenue après application de l'incrément

Liste

Taille du bitmap	8D		Taille (x) en octets du bitmap

bitmap	x O	Tableau bitmap	Le numéro de série de la carte sert d'index dans le tableau bitmap. L'opposition est codée sur un bit : Valeur 1 : changement d'état de la carte entre la liste LOI(n-1) et la liste LOI(n) Valeur 0 : pas de changement d'état de la carte (cf. 4.3.1 pour les modalités d'application d'un incrément)

Contrôle

Taille contrôle	4D		Taille en octets de la zone contrôle
Taille signature dLOI	4D		Taille (y) en octets de la signature de la dLOI
Signature dLOI	y O		Signature SHA-1/RSA portant sur l'ensemble « en-tête + liste » de la dLOI au format PKCS#1 (cf. 4.4.2 pour les modalités de signature de la liste).
Taille certificat	4D		Taille (z) en octets du certificat
Certificat	z O		Certificat X509 contenant la clé publique permettant de vérifier la signature de l'incrément et de la liste reconstituée.

Avec :

- AN : Alphanumérique (caractères 20h à 7Fh)
- D : Numérique décimal (caractères 30h à 39h)
- O : Octet (caractères 00h à FFh, i.e. quelconque)

3.2 Format du fichier de la liste d'opposition incrémentale – LOI

Description du fichier LOI

Champ	Format	Valeur	Observation

En-tête

Taille en-tête	4D		Taille en octets de l'en-tête
Application	20 AN	LOI	Cadré à gauche complété par des espaces
Version d'application	2D	01	
Référence : Date et rang	12D	AAAAMMJJXXXX	Où AAAAMMJJ représente une date et XXXX un rang.
Format de la liste	4AN	BTMP	Tableau bitmap

Liste

Taille du bitmap	8D		Taille (n) en octets du bitmap
bitmap	n O	Tableau bitmap	Le numéro de série de la carte sert d'index dans le tableau bitmap. L'opposition est codée sur un bit : Valeur 1 : la carte est en opposition Valeur 0 : la carte n'est pas en opposition

Contrôle

Taille contrôle	4D		Taille en octet de la zone contrôle
Taille signature LOI	4D		Taille (m) en octets de la signature
Signature LOI	m O		Signature SHA-1/RSA portant sur l'ensemble « en-tête + liste » au format PKCS#1.
Taille certificat	4D		Taille (x) en octets du certificat
Certificat	x O		Certificat X509 contenant la clé publique permettant de vérifier la signature de la liste.

Avec :

- AN : Alphanumérique (caractères 20h à 7Fh)
- D : Numérique décimal (caractères 30h à 39h)
- O : Octet (caractères 00h à FFh, i.e. quelconque)

3.3 Format du fichier de Demande de dLOI

3.3.1 Description fonctionnelle du fichier de Demande de dLOI

Le fichier joint au message de demande doit contenir les informations fonctionnelles suivantes :

- la référence de la liste (LOI) présente sur le poste du Professionnel de Santé.

  La référence de la liste LOI présente sur le Poste de Travail du Professionnel de Santé va permettre au distributeur d'opposition de déterminer combien d'incréments dLOI sont nécessaires sur le Poste de Travail du Professionnel de Santé pour obtenir la LOI à jour : la LOI (n).

- le nom de la Boîte aux lettres dans laquelle le Professionnel de Santé veut recevoir les dLOI.

  Le Poste de Travail du Professionnel de Santé doit permettre une configuration distincte pour une BAL opposition et pour une BAL de facturation. C'est pourquoi, il est nécessaire de fournir cette information dans le fichier joint au message de demande.

- le code du résultat de l'application de l'incrément précédent.

  Ce code permet d'indiquer si le Professionnel de Santé a rencontré des soucis pour l'intégration du précédent incrément.

3.3.2 Composition du fichier de Demande

Ce fichier est écrit en langage XML.

Le fichier joint est composé des rubriques suivantes :

- Une rubrique ou technique ;
- Une rubrique fonctionnelle.

Rubrique technique

Libellé	Signification	Type	Présence
<date_envoi>	Date d'envoi (JJ/MM/AAAA)	Date	Obligatoire
<heure_envoi>	Heure d'envoi (HH:MM)	Date	Obligatoire

Rubrique fonctionnelle

Libellé	Signification	Type	Présence
<ref_LOI>	La référence de la liste (LOI) présente sur le poste du Professionnel de Santé.	Numérique	Obligatoire

Libellé	Signification	Type	Présence
<bal_LOI>	Le nom de la Boîte aux lettres dans laquelle le Professionnel de Santé veut recevoir les dLOI. Remarque : seul ce champ fera foi pour le nom de la BAL apte à recevoir la dLOI. Il ne faut donc pas faire référence automatiquement à la valeur du champ from du message SMTP.	Alphanumérique	Obligatoire
<code_resultat_incr_prec>	Le code du résultat de l'application de l'incrément précédant. Si le Professionnel de Santé a rencontré aucun problème, ce champ est valorisé à : 0 Si le Professionnel de Santé a rencontré un problème, ce champ est valorisé à : 1	Numérique	Obligatoire

3.3.3 Exemple de fichier de demande de dLOI

Fichier donné à titre d'exemple.

```
<?xml version="1.0" encoding="UTF-8"?>
<demande_dLOI xmlns="http://test.GIESESAM-VITALE.fr"
xmlns:xs="http://www.w3org/2001/XMLSchema-instance"
xs:schemaLocation="http://test.GIESESAM-VITALE.fr/schema/message.xsd">
<!--Rubrique technique-->
      <date_envoi>12/07/2007</date_envoi>
      <heure_envoi>14:54</heure_envoi>
<!--Rubrique fonctionnelle-->
      <ref_LOI>200707121001</ref_LOI>
      <bal_LOI>PS.nomfournisseur@domainefournisseur.fr</bal_LOI>
      <code_resultat_incr_prec>0</code_resultat_incr_prec>
</demande_dLOI>
```

4 Description de la mise à jour de la Liste d'Opposition Vitale Incrémentale (LOI) sur le Poste de Travail du Professionnel de Santé

Le progiciel télécharge de sa BAL Opposition l'ensemble des messages SMTP contenant un incrément dLOI et le récupère.

Ces incréments sont ensuite ordonnés par ordre croissant de leur rang.

Le progiciel intègre les incréments dLOI consécutifs dans la LOI active, en prenant soin de vérifier les signatures associées.

Dès lors qu'il y a un incrément manquant ou bien un problème d'intégration, le progiciel arrête l'intégration des incréments dLOI. Les incréments n'ayant pas été intégrés sont rejetés.

Le progiciel fait une nouvelle demande d'incréments au distributeur d'Opposition à la fin de cette procédure.

Cas particuliers

Si le nombre d'incréments dLOI est jugé trop important par le distributeur d'opposition, un message ARAN est envoyé par le distributeur d'opposition au Poste de Travail du Professionnel de Santé.

Si une demande d'incrément est reçue par le distributeur d'opposition de la part d'un Poste de Travail qui a déjà une LOI active « **à jour** » (i.e. la LOI active est la LOI (n)), aucun message n'est renvoyé au Poste de Travail du Professionnel de Santé.

Cas d'erreurs

Si aucun incrément dLOI n'est disponible chez le distributeur d'opposition pour cause technique, aucun message n'est renvoyé au Poste de Travail.

Si la BAL opposition du Professionnel de Santé contient à la fois des incréments dLOI et un message ARAN, le message ARAN est ignoré et supprimé par le progiciel.

4.1 Diagramme

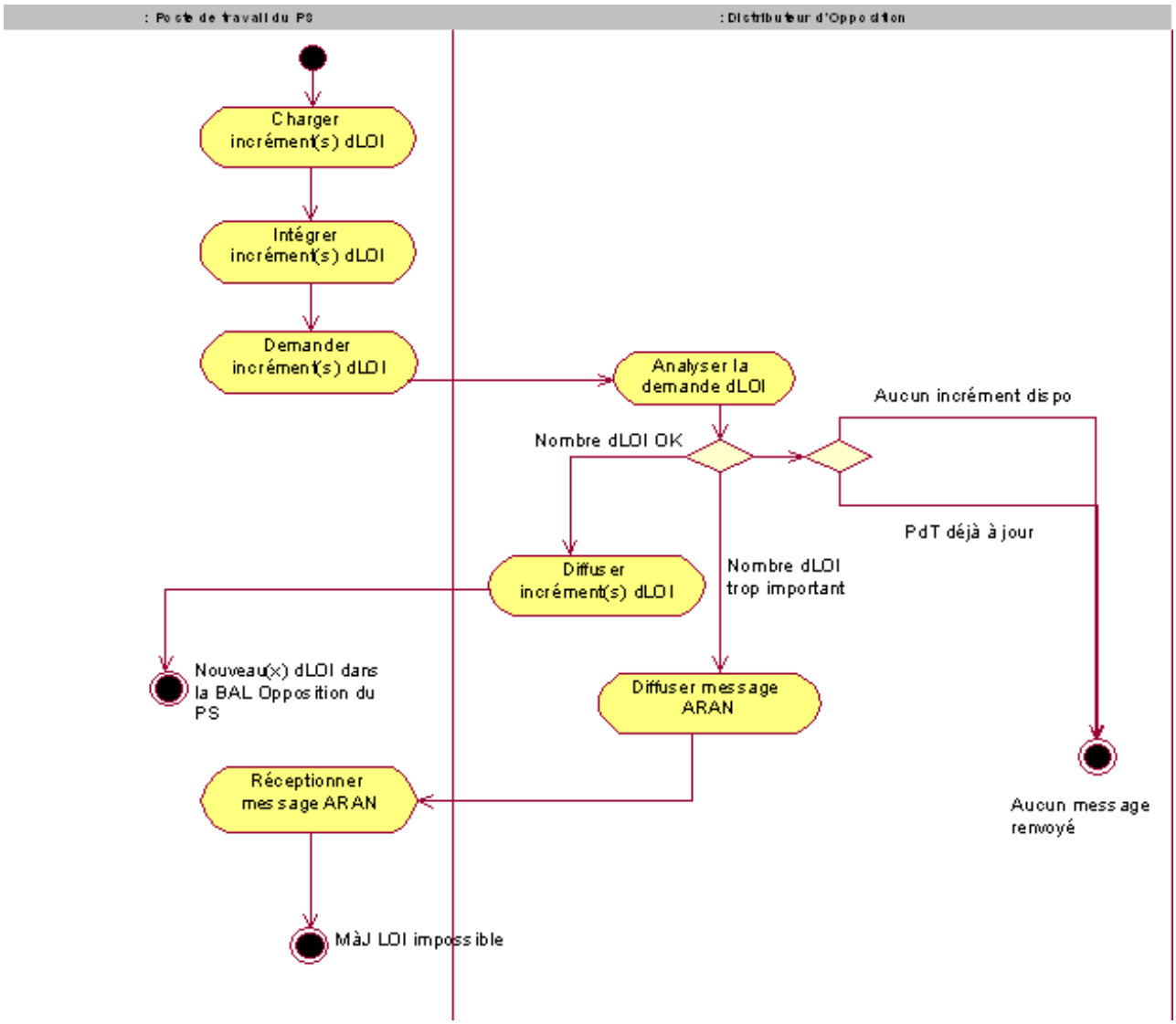

Figure 1 : Processus de mise à jour des dLOI

L'ordonnancement des fonctions de cette fonctionnalité correspond à une situation terrain où le Professionnel de Santé ouvre une session sur son poste et active son progiciel. Son progiciel commence par analyser ses BAL.

4.2 Charger les incrément(s) dLOI

Le progiciel lit la BAL Opposition afin de télécharger l'ensemble des messages SMTP reçu.

Pour chaque message SMTP contenant un incrément dLOI, le progiciel doit vérifier que ce n'est pas un message d'erreur à propos du destinataire d'un des messages de demande d'incrément(s) dLOI (i.e. mauvaise adresse mail du Distributeur d'Opposition).

Si ce n'est pas le cas, il doit vérifier que le message SMTP contenant un incrément dLOI est bien une réponse à une demande d'incrément(s) dLOI. (débrayable)

Le ou les fichier(s) dLOI ainsi obtenu(s) sont alors ordonnés par ordre croissant.

Les éventuels incréments non applicables sont alors supprimés.

4.2.1 Détection d'un problème dans le destinataire du message SMTP

Dans le cas où le progiciel reçoit un mail d'erreur SMTP (i.e. mauvaise adresse mail du Distributeur d'Opposition), il en informe le Professionnel de Santé.

4.2.2 Vérification que le message SMTP contenant un incrément dLOI est bien une réponse à une demande d'incrément dLOI

Le progiciel récupère du message SMTP reçu le champ relatif à l'identifiant original de la demande de dLOI (champ « In-Reply-To »). Il parcourt ensuite la liste des demandes d'incrément(s) dLOI et vérifie si l'une des références de message SMTP de demande d'incrément(s) dLOI est contenue dans le champ de l'identifiant original. Si oui, alors le progiciel continue son traitement.

Cette vérification doit être implémentée par chaque Éditeur mais doit pouvoir être débrayable sur le progiciel.

Cas d'erreurs

Si le message SMTP reçu contenant un incrément dLOI est la réponse à aucune demande d'incrément(s) dLOI.

Le message reçu est rejeté.

4.2.3 Ordonner les incréments

Le nom du fichier compressé dLOI est formaté comme suit :

<référence LOI(n-1)>_<référence LOI(n)>.dloi.gz.

Les références sont de la forme AAAAMMJJXXXX, où AAAAMMJJ représente une date et XXXX un rang.

Le progiciel ordonne les incréments dLOI par ordre croissant, c'est à dire par ordre alphabétique des noms de fichiers.

4.2.4 Supprimer les éventuels incréments non applicables

- Le progiciel supprime tous les incréments dont la référence LOI(n-1) est inférieure à la référence de la LOI active.
- Le progiciel supprime les éventuels incréments reçus en doublon.
- Le nom du fichier du premier incrément de la liste ainsi obtenue étant de la forme <référence LOI(n-1)>_<référence LOI(n)>.dloi.gz, le progiciel doit s'assurer que référence LOI(n-1) = référence de la LOI active sur le Poste de Travail.
- Le progiciel vérifie ensuite la continuité des incréments reçus en s'assurant que leurs références sont consécutives.
- C'est à dire que pour deux incréments ordonnés de type referenceA_referenceB.dloi.gz et referenceC_referenceD.dloi.gz on doit avoir referenceB = referenceC.

  Par exemple :

- Les incréments 200801221001_**200801231002**.dloi.gz et **200801231002**_200801241003.dloi.gz sont consécutifs.
- Les incréments 200801221001_**200801231002**.dloi.gz et **200801241003**_200801251004.dloi.gz ne sont pas consécutifs.

- En cas de rupture de continuité, tous les incréments au-delà du dernier incrément vérifiant les règles ci-dessus sont supprimés.

Ces suppressions sont transparentes pour le Professionnel de Santé et ne doivent pas faire l'objet d'un message d'erreur.

4.3 Intégrer incrément(s) dLOI

Les incréments ordonnés et sélectionnés au § 4.2 sont intégrés séquentiellement de la façon suivante :

- Décompression
- Vérification de signature
- Application de l'incrément

Si l'intégration de l'incrément dLOI s'est bien passée :

- l'incrément dLOI est effacé,
- la variable [code_resultat_incr_prec] est positionnée à '0',
- la LOI obtenue devient active sur le progiciel,
- Toutes les demandes d'incréments peuvent être supprimées. (cf. § 5.1.4)

Cas d'erreurs

Si l'intégration d'un des incréments n'a pu se réaliser, erreur au § 4.3.1 ou au § 4.3.2 ou au § 4.3.3, alors :

- Les incréments non intégrés dLOI ne sont pas conservés,
- la variable [code_resultat_incr_prec] est positionnée à '1',
- Le progiciel doit avertir le Professionnel de Santé afin qu'il puisse contacter son éditeur et/ou OCT afin de corriger le problème.

Une fois l'ensemble des incréments dLOI intégrés, la liste LOI sur le progiciel est la LOI (n). Il est laissé toute liberté à l'Éditeur d'exploiter la liste LOI (n) telle quelle (format « BITMAP ») ou de la convertir en tout autre format.

Cependant, si l'Éditeur décide d'exploiter la LOI (n) sous un format « différent », il est nécessaire de conserver la LOI (n) format « BITMAP » afin de pouvoir intégrer le prochain incrément dLOI (n+1).

4.3.1 Règle de décompression d'un incrément dLOI

C'est le même algorithme de décompression que celui utilisé pour les fichiers de facturation (cf. Annexe 4 du Cahier des Charges SESAM-Vitale).

4.3.2 Vérification de la signature

Les principes des étapes de la vérification de la signature de la LOI ou des dLOI sont les suivants :

- récupération du certificat contenant la clé publique du bi-clé ayant servi à signer la LOI ou la dLOI dans la zone de contrôle,
- vérification de la validité du certificat :
  - vérification de la date de validité du certificat vis à vis de la date du jour,

- vérification de la signature du certificat vis à vis de l'autorité de certification (pré-requis, disposer du certificat racine et de l'autorité intermédiaire de l'autorité de certification),
- vérification de la disponibilité et de la validité de la CRL correspondant à la classe du certificat utilisée : CRL présente sur le Poste de Travail du Professionnel de Santé et date de validité postérieure ou égale à la date du jour,

La vérification de la validité du certificat doit se faire sur la chaîne complète, i.e. pour chaque certificat.

Dans le cas où la CRL est disponible et valide :

- vérification de la signature de la CRL (cf. document RFC 2459),
- vérification de la non révocation du certificat : vérifier la non présence du certificat dans la CRL,

Dans le cas où la CRL n'est pas disponible ou n'est pas valide :

- la vérification de non révocation du certificat n'est pas faite et n'est pas bloquante pour la suite des opérations,

- récupération de la signature dans la zone de contrôle,
- déchiffrement de la signature avec la clé publique en utilisant l'algorithme RSA. Le résultat est une chaîne de 20 octets,
- calcul d'un condensât sur les zones en-tête et liste avec l'algorithme de hachage SHA-1. Le résultat est une chaîne de 20 octets,
- comparaison des deux chaînes de 20 octets : si égalité, la signature est correcte, sinon la liste ou le fichier dLOI vérifié est corrompu,

Les précisions pour la récupération de la CRL correspondant au certificat utilisé pour la signature des listes sont indiquées au § 5.1.1.

Cet algorithme est également applicable pour la vérification d'un fichier LOI.

4.3.3 Appliquer un incrément dLOI sur une liste LOI

Ce paragraphe décrit comment reconstituer une liste d'opposition LOI(n) à partir de la version précédente LOI(n-1) et l'incrément dLOI(n).

4.3.3.1 Les principes de l'application d'un incrément

- vérification de la signature de l'incrément dLOI reçu,
  - vérification que l'incrément reçu s'applique bien à la liste présente sur le poste :
  - lire la référence de la liste LOI (n-1) dans l'entête de l'incrément,
  - lire la référence de la liste présente sur le poste dans l'entête de celle-ci,
  - si égalité, l'incrément est applicable,
- copier la liste LOI(n-1) dans une nouvelle liste LOI(n),
- dans l'entête de la liste LOI(n), recopier la référence de la LOI(n) depuis l'incrément dLOI(n),
- pour chaque octet du bitmap de la LOI(n), appliquer un XOR (ou logique exclusif) avec l'octet correspondant du bitmap de l'incrément,

- recopier la signature de la LOI(n) dans la zone de contrôle depuis l'entête de l'incrément dLOI(n),
- recopier le certificat de l'incrément dLOI(n) dans la zone de contrôle de la LOI(n),
- vérifier la signature de la LOI(n) ainsi obtenue (cf. § 4.3.2),
- Cette nouvelle liste devient la liste active, la liste LOI(n-1) peut être supprimée.

4.3.3.2 Code source exemple

Ci-après un code source Java exemple illustrant l'implémentation de l'application du XOR sur les bitmaps :

```
////////////////////////////////////////////////////////////////////
/// fonction application d'un XOR entre liste n - 1 et incrément
////////////////////////////////////////////////////////////////////
static final int    BUFFER_SIZE   = 2048;

public static void XOR(File f_in, File f_diff, File f_out)
          throws Exception {
    // ouverture fichier f_in et f_diff en lecture
    // création fichier f_out en écriture
    FileInputStream in = new FileInputStream(f_in);
    FileInputStream dest = new FileInputStream(f_diff);
    RandomAccessFile out = new RandomAccessFile(f_out, "rw");

    //Lecture des infos bitmaps f_in et f_diff
    Lire_InfoBitmap (f_in, bitmap);
    Lire_InfoBitmap (f_diff, bitmap_diff)

    // on "saute" les entêtes de fichiers
    dest.skip(bitmap_diff.offset);
    in.skip(bitmap.offset);

    /// application d'un XOR entre le fichier in et
    /// le fichier diff par bloc
    for (int j = 0;; ++j) {

          /// Création de buffer et initialisation à 0 du contenu
          byte[] i_buf = new byte[BUFFER_SIZE];
          byte[] d_buf = new byte[BUFFER_SIZE];
          byte[] buf = new byte[BUFFER_SIZE];

          // lecture des buffers
          int size = 0;
          int i_offset = in.read(i_buf);
          int d_offset = dest.read(d_buf);

          // si fin des deux fichiers atteint, fin du traitement
          if (i_offset == -1 && d_offset == -1) {
                break;
          }


          // application du XOR sur chacun des octets des buffers lus
          int max_read = Math.max(d_offset, i_offset);
          for (int i = 0; i < max_read; ++i) {
                buf[i] = (byte) (i_buf[i] ^ d_buf[i]);

          }

          // écriture du buffer dans le fichier out liste n
          out.seek(bitmap.offset + BUFFER_SIZE * j);
          out.write(buf, 0, max_read);
     }
```

```
    out.close();
}
```

4.4 Demander incrément(s) dLOI

Pour constituer son fichier de demande de dLOI, le progiciel récupère :

- le champ « Référence : Date et rang » de l'en-tête de la liste LOI active ;
- ainsi que le nom de la BAL dans laquelle il souhaite recevoir les dLOI ;
- et le code résultat de l'application de l'incrément précédent [code_resultat_incr_prec],

Il réalise un message SMTP de demande d'incrément(s) dLOI dans le but de remettre à jour sa liste LOI et donc d'avoir la LOI (*n*).

Une fois le message constitué, le progiciel :

- **signe le message** à l'aide de la carte CPS du Professionnel de Santé
- et remplit la liste des demandes d'incrément(s) dLOI.

Cette fonction doit être débrayable, ce qui signifie que le Poste de Travail du Professionnel de Santé peut recevoir un dLOI sans avoir envoyé un message de demande.

Cas d'erreurs

Si, à la suite de l'envoi du message SMTP de demande d'incrément(s) dLOI, un message d'erreur est reçu dans la BAL Opposition, le progiciel en informe le Professionnel de Santé.

4.4.1 Message SMTP de demande d'incrément(s) dLOI

La description du message SMTP de demande d'incrément(s) dLOI est décrite dans le § 12 de l'annexe 4 du CdC SESAM-Vitale.

4.4.2 Signature du message SMTP de la demande d'incrément(s) dLOI

Le calcul de la signature du message SMTP de demande d'incrément(s) dLOI est décrit dans le § 12 de l'annexe 4 du CdC SESAM-Vitale.

4.4.3 Nombre de demande par jour

Le progiciel doit réaliser une demande d'incrément(s) dLOI par jour, même s'il consulte sa BAL Opposition plusieurs fois par jour.

Exception : dans un souci de mise au point de l'opposition incrémentale le Professionnel de Santé peut, manuellement, outrepasser cette règle et forcer le progiciel à faire d'autres demandes dans la même journée.

4.4.4 Remplir la liste des demandes d'incrément(s) dLOI

Le progiciel complète la liste des demandes par :

- la date du jour,
- la référence du message SMTP de demande d'incrément(s) dLOI.

4.5 Traiter le message ARAN

A la réception d'un message SMTP ARAN, le progiciel contrôle que le message ARAN reçu est bien une réponse à une demande d'incrément(s) dLOI. Si oui, alors il analyse le code retour mentionné dans le message.

Si ce code est valide et qu'il indique que la mise à jour de la liste LOI active sur le progiciel est impossible (nombre d'incrément dLOI nécessaire à la mise à jour de la LOI active est trop grand) alors le progiciel :

- informe le Professionnel de Santé du problème,
- conseille au Professionnel de Santé de contacter son Opérateur de diffusion LOI afin de récupérer la LOI *(n)*.

4.5.1 Vérifier que le message ARAN est bien une réponse à une demande d'incrément dLOI

Le progiciel récupère du message ARAN reçu le champ relatif à l'identifiant original « In-Reply-To ». Il parcourt ensuite la liste des demandes d'incrément(s) dLOI et vérifie si l'une des références de message SMTP de demande d'incrément(s) dLOI est contenue dans le champ de l'identifiant original. Si oui, le progiciel supprime la ligne dont la référence est incluse dans l'identifiant original.

Un seul message ARAN est possible pour un message de demande.

Cette vérification doit être implémentée par chaque Éditeur mais doit pouvoir être débrayable sur le progiciel.

Cas d'erreurs

Le message ARAN reçu n'est la réponse d'aucune demande d'incrément(s) dLOI.

Dans ce cas le message ARAN reçu est rejeté.

4.5.2 Vérifier le code mentionné dans le message SMTP ARAN

Le progiciel récupère le code retour mentionné dans le message SMTP ARAN et contrôle que ce code est bien dans la liste des codes ARAN (ex :'0100' signifiant « nombre de dLOI à envoyer trop important »).

Cas d'erreurs

Le code retour mentionné dans le message SMTP ARAN est différent de la liste des codes ARAN (ex :'0100').

En cas de réception d'un code inconnu, le Poste de Travail doit le signaler au Professionnel de Santé.

5 Description de l'administration de la Liste d'Opposition Incrémentale (LOI)

5.1 Administrer quotidiennement le Poste de Travail du Professionnel de Santé

Cette fonctionnalité regroupe les actions qui doivent être réalisées quotidiennement sur le progiciel :

- Récupérer la liste des Certificats Serveurs Révoqués ;
- Contrôler le nombre de non-réponse aux différentes demandes d'incrément(s) dLOI ;
- Informer en cas de non mise à jour de la LOI au début de chaque mois.

5.1.1 Récupérer la liste des Certificats Serveurs Révoqués

Annuaire LDAP

Le GIE SESAM-Vitale a choisi de mettre à disposition les listes de révocation (CRL) dans un annuaire basé sur le protocole LDAP. Ces CRL sont émis par l'IGC OSI du GIE SESAM-Vitale et sont relatifs aux autorités de certification « AC-FACTURATION », « AC_SERVEUR » et « AC-SERVICES-APPLICATIFS ».

Récupération de la CRL

L'adresse de récupération de la liste de révocation des certificats est disponible dans le champ du certificat « **point de distribution de la liste de révocation des certificats** ».

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

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 :

- Un chargement quotidien 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.

5.1.2 Contrôler le nombre de non-réponse quotidiennes aux différentes demandes d'incrément(s) dLOI

Quotidiennement, le progiciel contrôle le nombre de jours maximum écoulés sans avoir reçu de message d'incrément dLOI en comparant la date du jour avec la date de référence de la LOI active.

Si ce nombre est supérieur à [NB_JOUR_Max], le poste de travail informe le Professionnel de Santé qu'il n'a pas reçu d'incrément dLOI depuis [NB_JOUR _Max] jours.

Le progiciel invite le Professionnel de Santé à contacter son distributeur d'opposition afin de connaître l'origine du problème et ensuite, si nécessaire, son opérateur de diffusion LOI afin de récupérer la liste LOI (n).

5.1.3 Informer en cas de non mise à jour de la LOI au début de chaque mois

Cette sous fonction doit être implémentée par chaque Éditeur mais doit pouvoir être débrayable sur le progiciel afin de suivre les éventuelles évolutions conventionnelles.

Tous les jours, le progiciel contrôle que la liste LOI active possède une date de référence postérieure au 18 du mois précédent.

Pour ce faire, le progiciel lit le champ « Référence : Date et rang » de l'**En-tête** du fichier de la liste LOI active. Ce champ étant au format **AAAAMMJJ**XXXX, le progiciel ne prend que les 8 premiers digits AAAAMMJJ pour obtenir la date de référence.

Il compare cette date de référence AAAAMMJJ avec aaaayy18,

où : aaaayy18 = 18e jour précédent la date du contrôle.

Si la date de référence est postérieure alors le progiciel considère que la LOI active est régulièrement mise à jour.

Si ce n'est pas le cas, le progiciel :

- informe le Professionnel de Santé que sa liste LOI active n'est pas à jour,
- invite le Professionnel de Santé à prendre contact avec son Opérateur de diffusion LOI afin de récupérer la LOI (n).

Par exemple : Prenons la date de référence au 20070319.

- Si la date de contrôle se trouve entre le 20070320 et le 20070431, le contrôle s'effectuera par rapport à la date 20070318.

  La date de référence étant postérieure au 20070318, le contrôle sera passant.

  En effet :

  Une LOI du 19 mars = > date de référence = 19 mars

  Le jour du contrôle est **le 31 avril** => date de contrôle est le 18 mars

  La date de référence est postérieure à la date de contrôle donc **la LOI du 19 mars est suffisamment à jour.**

- Si la date de contrôle est le 20070501 et après, le contrôle s'effectuera par rapport à la date 20070418.

  La date de référence étant antérieure au 200704718, le contrôle aboutira à un avertissement.

  En effet :

  Une LOI du 19 mars ➔ date de référence = 19 mars.

  Le jour du contrôle est le 1er mai ➔ date de contrôle est le 18 avril.

  La date de référence n'est pas postérieure à la date de contrôle donc **la LOI du 19 mars n'est pas suffisamment à jour.**

  L'écart maximum est de 1 mois et demi.

5.1.4 Sauvegarde/Archive

Le poste doit conserver ses demandes de dLOI tant qu'il n'a pas reçu de réponses correspondantes.

5.2 Administrer ponctuellement le poste de travail du Professionnel de Santé

Cette fonctionnalité regroupe les fonctions d'administration qui doivent être faites sur le progiciel :

- Paramétrer les informations liées à l'opposition sur le progiciel ;
- Installer et renouveler la chaîne de Certification sur le progiciel ;
- Mettre au point l'opposition incrémentale sur le poste de travail ;

- Visualiser la référence de la LOI active sur le poste de travail.

5.2.1 Paramétrer les informations liées à l'opposition sur le poste du Professionnel de Santé

Sur son poste de travail, le Professionnel de Santé peut avoir besoin de configurer :

- l'adresse de sa BAL Opposition,
- l'adresse du Distributeur d'opposition,
- le nombre maximum de jour [NB_JOUR_Max] que le progiciel peut accepter avant d'alerter le Professionnel de Santé.

5.2.1.1 Configurer la BAL Opposition

Le Professionnel de Santé est libre de choisir son fournisseur de messagerie électronique. L'adresse de sa BAL Opposition doit être une adresse valide.

5.2.1.2 Paramétrer l'adresse du Distributeur d'Opposition

Le progiciel spécifie pour le distributeur d'Opposition l'adresse mail suivante :

oppv-loi@opposition.sesam-vitale.rss.fr, dans le cas où le Professionnel de Santé utilise le distributeur du GIE SESAM-Vitale.

5.2.1.3 Paramétrer le nombre maximum de jours acceptable sans réception de dLOI

Le Professionnel de Santé paramètre [NB_JOUR_Max] à la valeur qu'il souhaite.

Cette valeur pourra être choisie en fonction des recommandations faites par son Distributeur d'Opposition ou de son Éditeur.

La valeur par défaut donnée au paramètre [NB_JOUR_Max] est 7.

5.2.2 Installer et Renouveler la chaîne de Certification sur le progiciel du Professionnel de Santé

Les autorités de certification permettent de vérifier la validité des certificats utilisés. Ces autorités doivent donc être obligatoirement installées et mises à jour sur le poste utilisateur. Cette opération d'installation ou de mise à jour doit être réalisée par une « personne de confiance » sous le contrôle de l'utilisateur final du poste de travail.

Le système d'exploitation du poste de travail ou les navigateurs Internet mettent à jour automatiquement les « autorités commerciales reconnues » sur le marché. Pour les autorités spécifiques, comme celles de l'IGC OSI du GIE SESAM-Vitale, celles-ci doivent être installées par le progiciel ou le Professionnel de Santé utilisateur de la solution :

- Cette installation peut être prise en charge automatiquement par l'éditeur du progiciel qui récupèrera l'AC auprès du GIE SESAM-Vitale et pourra mettre à jour son parc de clients en même temps que son offre logicielle ;
- Une procédure manuelle doit également être mise à disposition du Professionnel de Santé pour que celui-ci puisse réaliser cette opération sans passer par l'éditeur du progiciel.

Le progiciel doit pouvoir gérer plusieurs chaînes de certification en parallèle sur le poste de travail pour assurer les périodes de migration d'une autorité vers une autre (minimum 2).

A titre d'information, les AC suivantes sont ou seront utilisées pour signer les LOI et dLOI :

- AC IGC OSI / AC_SERVEUR à compter de novembre 2019
- AC IGC OSI / AC-SERVICES-APPLICATIFS

D'autres AC pourront être mises en œuvre ultérieurement en fonction des évolutions des recommandations de sécurité issues du référentiel général de sécurité (RGS) ou des dates de fin de vie des AC utilisées.

Le canal de transmission de ces certificats autorités sur le progiciel est laissé libre à l'éditeur de logiciel de santé.

5.2.3 Mettre au point l'opposition incrémentale

Pour des raisons de mise au point de l'opposition incrémentale, le Professionnel de Santé peut, manuellement, forcer son progiciel à faire une demande d'incrément dLOI.

Le recours à ces demandes manuelles d'incréments dLOI doit rester marginal, surtout si ces demandes sont faites dans la même journée.

5.2.4 Visualiser la référence de la LOI active

Le progiciel doit permettre au Professionnel de Santé de visualiser la référence de la LOI active sur son poste.

5.3 Synthèse des fonctions débrayables

Dans la liste des fonctions pour la mise à jour ou l'initialisation de la LOI, certaines fonctions peuvent être débrayables. Le tableau ci-dessous indique les fonctions débrayables qui sont liées entre elles.

1	**Corps du CdC §3.2.3.2**	**Activation de la LOI**	✓		
2	**Annexe 6 § 2.2.2**	**Fonction de demande SMTP quotidienne de dLOI**		✓	
3	**Annexe 6 § 2.2.2**	**Fonction de contrôle de la concordance entre la demande de dLOI et la réponse de dLOI reçue**		✓	
4	**Annexe 6 § 2.2.2**	**Fonction de contrôle de la concordance entre la demande de dLOI et le ARAN**		✓	
5	**Annexe 6 § 5.1.3**	**Fonction pour informer en cas de non mise à jour de la LOI au début de chaque mois**			✓

Les fonctions 2, 3, 4 sont liées entre elles. Elles sont donc soit activées, soit désactivées en même temps.

Si le Professionnel de Santé n'active pas ou désactive la LOI (fonction n°1) aucune des fonctions de l'annexe 6 ne sont mises en œuvre.

6 Description de la consultation de la LOI

Ce paragraphe décrit comment, à partir du numéro de série d'une carte Vitale, déterminer si cette dernière est en opposition ou non à partir des données contenues dans la LOI.

6.1 Principe de la consultation

Les étapes du principe de la consultation d'une LOI sont les suivantes :

- lecture de la carte Vitale, récupération du numéro de série et du type de carte (REELLE, TEST ou DEMONSTRATION),
- Si la carte Vitale est de type « DEMONSTRATION » alors la consultation de la liste est abandonnée, sinon :
- effectuer une division euclidienne par 8 du numéro de série,
- lire dans le fichier contenant la LOI l'octet contenant les informations relatives à cette carte (positionnement dans le fichier à l'octet n° (quotient de la division précédente + taille de l'en-tête) les index débutant à la valeur 0),
- appliquer un masque sur l'octet lu correspondant au bit de la carte correspondant au reste de la division. La construction du masque et le test du bit se font de la façon suivante :
  - initialiser le masque à la valeur 01h,
  - décaler le masque de n position vers la gauche, n correspondant au reste de la division euclidienne (modulo) du n° de série de la carte par 8,
  - effectuer un ET logique entre le masque obtenu et l'octet lu dans la LOI,
  - si le résultat de l'opération est égal à 0, la carte n'est pas en opposition, sinon, la carte est en opposition,
- si le numéro de série de la carte est en dehors de la plage des numéros de série gérée par la LOI, la carte doit être considérée comme en opposition.

6.2 Code source exemple

Ci-après un code source Java exemple illustrant l'implémentation du principe :

```
////////////////////////////////////////////////////////////////
/// Fonction de consultation d'une carte en opposition depuis un
/// fichier bitmap


private static boolean Consulter(File f_in, long cardNum)
        throws Exception {

    // Ouverture du fichier en lecture
    FileInputStream in = new FileInputStream(f_in);

    // Lecture des infos relatives au bitmap : taille + offset
    // stockage dans une structure bitmap (taille, offset)
    Lire_InfoBitmap (f_in, bitmap) ;

    // Calcul de l'index de l'octet à lire dans le fichier
    // = n° série carte / 8  + offset
    long pos = (int) ((cardNum) / 8);

    // test si l'index n'est pas hors-limite
    // (taille du bitmap indiqué dans l'entête)
    // => numéro série invalide, donc en opposition
```

```
    if (pos > bitmap.taille) {
           return true
    }

    // positionnement sur le fichier et lecture de l'octet
    in.skip(pos + bitmap.offset);
    int b = in.read();

    // test du bit correspondant au n° de série de la carte testée
    // bit = 1 : carte en oppo, bit = 0 carte non en oppo
    return (b & (1 << ((cardNum) % 8))) != 0;
}
```

7 Définitions techniques des paramètres spécifiques à la LOI

En général, le glossaire est inscrit dans le corps du Cahier des Charges SESAM-Vitale. Cependant, lorsque qu'il existe des paramètres spécifiques à un sujet (ex. : LOI), ils sont inscrits dans l'annexe de celle-ci si elle existe. D'où la création de ce chapitre dans l'annexe 6.

Définitions	
Cas d'erreur	Arrêt du fonctionnement du système.
Cas particulier	Déroulement ponctuel hors cas nominal.
Code_resultat_incr_prec	Code résultat de l'intégration d'un incrément dLOI sur une liste LOI.
NB_JOUR_Max	Nombre maximum de jours sans réponse que le progiciel pourra accepter avant d'alerter son PS.