Département du Système d'Information
Pôle infrastructures - Réseaux nationaux

CONTEXTE	●	**DSI - Réseaux nationaux**
SUJET	●	**CCTP Transfert sécurisé de fichiers volumineux**
référence	●	*RESNAT00335V02V.doc*
version	●	
statut	●	
créé le	●	*21/10/2008*
par	●	Patrick Lerouge
mis à jour le	●	*22/10/2008*
par	●	Patrick Lerouge
validé le	●	*22/10/2008*
par	●	Patrick Lerouge, Julio Martins
Péremption, archivage et restriction de diffusion	●	

Nature de la restriction : confidentiel, diffusion restreinte, diffusion interne, restriction annulée

Table des mises à jour du document

version	date	objet de la mise à jour
1	21/10/2008	Création
2	22/10/2008	Correction et publication

Table des matières

1 Introduction

L'Institut National de la Santé et de la Recherche Médicale, INSERM, est implanté en France sur environ 85 sites dont 38 sous la responsabilité de l'INSERM concernant l'administration des réseaux et des services associés dont la messagerie électronique. L'Inserm compte 360 unités et équipes de recherche, dont 80% localisés dans les universités et les centres hospitalo-universitaires français. Ces 360 structures de recherche sont mixtes et y travaillent 13 000 personnes. Le personnel est composé de 6500 salariés de l'Institut, de chercheurs d'autres EPST (CNRS, INRA…), d'universitaires, de chercheurs étrangers, d'étudiants et doctorants.

L'administration centrale dont le siège est située 101, rue de Tolbiac à Paris, est composée de 11 départements autour de la Direction Générale et du Secrétariat Général.

Pour gérer ses structures de recherche, l'Inserm s'est doté de 14 Administrations Déléguées Régionales, ADR.

L'ensemble du personnel administratif du siège et des ADR représente environ un millier de personnes.

2 Système d'information de l'Inserm

Le système d'information de l'Inserm est géré par le Département du Système d'Information. Ce dernier est responsable des réseaux des sites propres de l'Inserm, il assure en autres les services de messagerie électronique dont l'adresse utilise le suffixe DNS « inserm.fr » auquel est associé un annuaire Ldap qui recense les comptes des utilisateurs.

Les solutions déployées utilisent majoritairement des logiciels « Open source » (Apache, Mysql, Php, Postfix, Clamav, SpamAssassin, etc.), et des systèmes d'exploitation Linux (Redhat, Suse, CentOS).

2.1 État des méthodes utilisées pour les transferts de fichiers.

Les transferts de fichiers entre correspondants à l'Inserm sont essentiellement réalisés par attachement de pièces jointes à un message électronique de la messagerie « @inserm.fr ». Ces transferts correspondent à trois cas :

1. Interne : depuis un compte « @inserm.fr » vers un compte « @inserm.fr » ;
2. Sortant : depuis un compte « @inserm.fr » vers un compte d'un domaine extérieur à « @inserm.fr » ;
3. Entrant : depuis un compte d'un domaine extérieur à « @inserm.fr » vers un compte « @inserm.fr » ;

La messagerie de l'Inserm est issue de la suite OBM de la SSLL Aliasource. Elle est disponible sur le site de l'éditeur : http://www.aliasource.fr sous licence GPL.

D'autres méthodes de transfert de documents ont été employées par le passé. Elles consistaient à mettre à disposition un serveur de fichier sur une plateforme Linux sous différentes déclinaisons utilisant les protocoles tels que FTP ou SCP.

De tels échanges de fichiers sont limités en terme de sécurité, de volume et d'ergonomie. Ces limitations sont inhérentes aux protocoles utilisés, et celles imposées par les administrateurs des serveurs accessibles sur l'Internet et également aux compétences des utilisateurs non avertis.

3 Forme et objet de l'appel d'offre

3.1 Forme

Le présent appel d'offre conduira à un marché établi pour un an. Le marché est un MAPA (marché à procédures adaptées).

Il pourra être reconduit sur demande de l'Inserm pour une année supplémentaire.

3.2 Objet

Ce marché vise à obtenir sous trois formes différentes un système logiciel à installer sur des serveurs hébergés par l'Inserm qui permette des transferts sécurisés de fichiers volumineux par les utilisateurs de la messagerie électronique « @inserm.fr ».

Ces transferts sont à destination de correspondants en dehors et dans ce domaine. Inversement les transferts de leurs correspondants hors domaine vers ces mêmes utilisateurs seront possibles.

L'authentification des utilisateurs de l'Inserm sera réalisée à partir de l'annuaire LDAP disponible.

Les trois formes sont les suivantes :

3.2.1 Tranche ferme

Cette première forme sera l'objet d'une commande ferme qui suivra la notification du marché. Les travaux à réaliser sont décrits dans le chapitre 5.

3.2.2 Tranches optionnelles

Les tranches optionnelles sont décrites dans le chapitre 6. Elles pourront faire l'objet d'une commande de l'Inserm durant la durée du marché.

3.2.3 Unités d'œuvre

Des travaux pourront être commandés par l'Inserm durant la durée du marché. Les commandes afférentes seront établies en Unité d'œuvre (UO). Suivant la complexité de la demande ces UO seront chiffrées en trois catégories : UO simple, moyenne et complexe. Le chapitre 7 définit le cadre de classement des unités d'œuvre.

4 Cadre général des réalisations

Les fonctionnalités demandées en tranche ferme et tranches optionnelles sont appelées « réalisations ».

4.1 Lancement

Chaque réalisation fera l'objet d'une procédure de lancement, cette procédure sera suivant les cas :

- une réunion de lancement entre les acteurs Inserm et le titulaire du marché, la réunion se tiendra indifféremment dans les locaux de l'Inserm ou du titulaire ;
- une conférence téléphonique ou en visioconférence ;
- réalisé par échange de courriels.

Durant la procédure de lancement, le titulaire proposera les différentes solutions qu'il envisage de mettre en œuvre pour satisfaire les différentes clauses techniques du présent document. L'Inserm pourra se réserver un délai de réflexion d'une semaine pour faire un choix en cas d'alternative.

La procédure de lancement fera l'objet d'un compte-rendu écrit par le titulaire et devra être validé par l'Inserm.

4.2 Mise en œuvre

Les développements des réalisations seront faits sur les Infrastructures du titulaire. La mise en œuvre se fera sur des serveurs mis à disposition par l'Inserm situés sur l'un des ses sites (Villejuif ou Auteuil). Les acteurs désignés par le titulaire pourront accéder aux installations sous couvert du responsable d'exploitation du site désigné par l'Inserm et dans les conditions données par ce responsable. Des accès distants sécurisés au travers du réseau Internet seront fournis aux acteurs désignés par le titulaire.

La mise en œuvre des logiciels respectera les standards utilisés par l'éditeur du système d'exploitation choisi par l'Inserm (préférentiellement CentOS V5 ou RedHat V5). Les composantes à utiliser seront choisies dans celles qui sont fournies dans ce système d'exploitation. En cas d'indisponibilité, les composantes seront choisies sur des dépôts de logiciels réputés, elles seront nécessairement prises dans leur forme de paquetage source RPM (RPMS : Redhat Package Manager) « source » puis proposées à l'Inserm pour compilation et signature numérique. L'ensemble des livrés sera de préférence compatible avec la licence GPL (GNU General Public License).

La source d'alimentation en distribution et paquets RPM sera exclusivement le serveur de dépôt de l'Inserm.

La mise en œuvre aboutira à la livraison des logiciels et cahiers d'installation et d'exploitation nécessaires à la mise en production par l'Inserm sur son site de Villejuif. Un modèle des ces cahiers sera fourni avant la phase de livraison.

Les logiciels livrés ne devront en aucun cas empêcher les mises à jours des paquetages utilisés par l'architecture et notamment ceux liés à la sécurité.

Des documentations destinées aux administrateurs et aux utilisateurs seront fournies sous forme électronique permettant une personnalisation et une intégration au système documentaire Web de l'Inserm. Les documentations seront fournies en français et pourront éventuellement être complétées en anglais.

Les postulants émettront des préconisations en ce qui concerne l'architecture et les matériels à utiliser.

4.3 Recette, mise en service et garantie.

Un cahier de recette sera proposé, il sera validé conjointement par le titulaire et l'Inserm. Le cycle classique de gestion de projet (VABF, VSR…) sera adopté.

La VABF sera déclarée par l'Inserm dans un délai de 15 jours après livraison et mise en service.

La VSR sera déclarée par l'Inserm dans un délai de 3 mois après la déclaration de VABF.

La période de garantie suivra la VSR. Cette période de garantie sera décrite par les postulants.

4.4 Maintenance

Une offre de maintenance sera proposée et valorisée par période d'un an.

Cette offre de maintenance concernera l'ensemble de demandes tranches ferme et pour les options de manière individuelle option par option.

L'offre de maintenance proposée par le titulaire devra inclure les mises à jour mineures et majeures du ou des produits proposés.

Cette offre doit permettre également l'accès à un support technique téléphonique. Le coût de la communication téléphonique pour l'accès à ce support doit être équivalent à celui d'une communication locale sur tout le territoire de France métropolitaine et ne doit pas faire l'objet d'une communication surtaxée.

Les processus de prise en compte des problèmes rencontrés, des interventions et de la résolution de ces problèmes seront décrits avec détail, seront notamment indiqués :

- la période de prise en compte des demandes ;
- les différents délais de prise en compte d'une demande, mise en place de solution de contournement, résolution en fonction de la classification des problèmes (bloquants, majeurs, etc.).

Si plusieurs niveaux de maintenance peuvent être proposés, ils seront valorisés en options.

5 Tranche ferme

Le transfert des fichiers entre différents internautes par courrier électronique subit des limitations et sont difficiles à sécuriser car nécessitant actuellement des technologies qui peuvent paraître complexes aux utilisateurs. Les limitations dues aux attachements dans des courriers électroniques sont de différents ordres et ne correspondent pas aux besoins exprimés par les chercheurs de l'Inserm.

Deux cas seront à considérer en ce qui concerne l'initiateur d'un transfert : celui d'un utilisateur recensé à l'Inserm et celui d'un invité par un utilisateur recensé.

5.1 Définitions

- **Utilisateur** : personne recensée dans le système d'information de l'Inserm et possédant une entrée dans l'annuaire Ldap.
- **Invité** : personne extérieure non recensée dans le système d'information de l'Inserm et ne possédant pas une entrée dans l'annuaire Ldap. Cette personne est invitée par un utilisateur de l'Inserm et pourra accéder temporairement au système de transfert de fichiers afin de pouvoir transférer un ou plusieurs fichiers à son hôte de l'Inserm.
- **Correspondant** : Tout utilisateur, qu'il soit interne ou externe à l'Inserm avec qui correspondra l'utilisateur de l'Inserm.
- **Fenêtre d'invitation** : Période paramétrable par l'administrateur du système pendant laquelle une invitation à déposer un fichier est valide. Cette période démarre à l'instant de l'invitation.
- **Fenêtre de disponibilité** : Période paramétrable par l'administrateur du système pendant laquelle un dépôt de fichier est valide. Cette période démarre à l'instant du dépôt d'un fichier à transmettre.
- **Administrateur** : Personne habilitée à gérer la solution proposée.

5.2 Authentification

Le système à réaliser sera donc indépendant du système de messagerie existant dont il ne reprendra que la partie authentification de l'utilisateur recensé dans son annuaire OpenLdap version 3. Les données qui pourront être notablement accessibles sont :

- Civilité
- Prénom
- Nom
- Certificate (signature électronique publique de l'utilisateur)

A partir de cette authentification (Bind sur Ldap) l'utilisateur de l'Inserm aura accès au système et pourra envoyer un ou plusieurs fichiers vers un correspondant mais aussi par le même biais, un invité aura la possibilité d'expédier un ou plusieurs fichiers à son hôte.

5.3 Caractéristiques des deux cas

L'accès au dispositif sera réalisé à partir d'une console Web en mode sécurisé (protocole HTTPS/port 443).

Les correspondants seront accueillis par une page paramétrable par les administrateurs sur laquelle seront rappelées les règles d'usage en deux langues : français et anglais. Toutefois la page des invités sera différente de celle des utilisateurs. Le contenu de ces pages sera du ressort de l'Inserm mais le titulaire indiquera comment y pourvoir. La fourniture d'un « Template » de ces pages incluant le logo de l'Inserm sera un plus dans la réponse à cet appel d'offre (AO).

Les pages seront assorties de liens ouvrant des fenêtres d'aide de type « pop-up » et de bulles informatives sur les fonctionnalités. Les textes d'aide et d'information seront rédigés en français et anglais.

L'emploi de technologies Web avancées sera un plus dans la réponse à l'AO.

L'accès aux pages fonctionnelles ne sera possible qu'après acquittement par action sur un lien, approuvant ainsi les règles d'utilisation.

5.4 Page fonctionnelle pour un utilisateur

Un utilisateur aura deux possibilités d'action sur sa page fonctionnelle

- Initialiser un transfert
- Créer un invité

Contrôler l'état d'une transaction initiée précédemment sera un plus dans la réponse à cet AO.

5.4.1 Initialisation d'un transfert de document

Un utilisateur pourra procéder au transfert d'un ou plusieurs documents vers un ou plusieurs destinataires. Le processus général est décrit au chapitre 5.6.

Un utilisateur pourra à tout moment détruire un document qu'il aura déposé soit pour corriger une erreur soit pour obtenir plus d'espace de stockage.

5.4.2 Création d'un invité

Un utilisateur devra pouvoir à partir du système, créer un compte d'invité valide durant la fenêtre d'invitation. Les paramètres de ce compte seront transmis par courriel à l'invité et permettront à ce dernier la transmission de documents depuis l'extérieur de l'Inserm vers l'utilisateur invitant.

Les informations transmises par courriel à l'invité seront paramétrables par l'administrateur et seront fournies dans deux langues : français et anglais.

Les procédures de sécurité mise en place seront fortement analysées dans la réponse à cet AO.

5.5 Page fonctionnelle pour un invité

Après avoir passé le cap de sa page d'accueil, l'invité ne peut être dirigé que vers une page similaire à celle d'initialisation d'un transfert par un utilisateur, mais le champ destinataire est verrouillé avec l'adresse de l'utilisateur hôte. Les processus sont identiques. Si un rapport doit être transmis à l'invité, ce rapport sera exclusivement réalisé par mail et il ne pourra plus accéder au système une fois close la fenêtre d'invitation.

Cette page fonctionnelle ne devra être disponible que pendant la durée de la fenêtre d'invitation**.**

5.6 Initialisation, transfert, réception et rapport

5.6.1 Initialisation du transfert

L'utilisateur pourra renseigner les coordonnées d'un ou plusieurs destinataires sous forme d'adresse courriel, un champ message sera également disponible pour y insérer librement du texte destiné au(x) destinataire(s) en accompagnement du fichier transmis.

Il pourra alors avec une action sur un bouton « Parcourir » choisir un fichier stocké dans l'arborescence de sa station de travail puis en déclencher le téléchargement vers le système.

Une validation finale lancera le processus de transmission.

L'utilisateur sera informé du bon fonctionnement de l'opération et de la fenêtre de disponibilité de son ou ses documents pour son destinataire.

Les documents transmis pourront subir certains contrôles :

1. Dans la tranche ferme de cet AO, la taille totale des documents transmis par opération ou par utilisateur sera limitée à une valeur paramétrable par l'administrateur, au départ la valeur de 500 Moctets sera choisie ;

2. Dans les tranches optionnelles de cet AO, d'autres limitations pourront être apportées, voir à cet effet le chapitre 6. La partie tranche ferme devra accepter ces options sans transformations majeures d'architectures logicielles.

Ces contrôles aboutiront suivant les cas à soit un blocage du processus, soit à un message d'alerte acquitté par l'utilisateur qui sera journalisé.

5.6.2 Transmission du ou des documents

La transmission du ou des documents dans le système ne sera en réalité que l'envoi d'un courriel vers le(s) destinataire(s) le(s) invitant à se connecter en mode sécurisé au système pour venir y retirer le(s) document(s). Ce courriel reprendra les données extraites de LDAP pour personnaliser le message (Civilité Prénom Nom vous a transmis un document etc.)

Chaque destinataire sera prévenu que la mise à disposition du document est limitée dans une Fenêtre de disponibilité temporelle (paramétrée par l'administrateur).

Ce courriel sera rédigé en français et anglais.

5.6.3 Réception du ou des documents

Après connexion sur le lien dédié à ce transfert en mode sécurisé, le destinataire trouvera les instructions générales qui y seront écrites en français et anglais. Il y retrouvera également les informations annexées à la transmission de ce(s) document(s) par l'expéditeur : civilité, prénom, nom et texte d'accompagnement.

Il accèdera finalement à ce(s) document(s) par simple appui sur un bouton qui déclenchera le téléchargement.

Le lien restera actif jusqu'à la fermeture de la fenêtre de disponibilité. Ce après quoi les documents transmis seront détruits.

5.6.4 Rapport de transmission

Un expéditeur devra connaître l'état de ces transmissions, que cela soit dans un courriel généré automatiquement ou en accès de type historique sur une page web du système.

La réponse à cet AO détaillera les éléments de rapport fournis au sens de la traçabilité.

5.6.5 Compatibilité avec la signature électronique et le cryptage

Bien que non demandées en tranche ferme, le système proposé devra démontrer sa compatibilité avec les fonctionnalités suivantes :

- La signature électronique par le correspondant émetteur des documents transmis ;
- Le cryptage des documents transmis à partir d'un jeu de clés Publique/Privée.

Le candidat à cet AO s'engagera à ne pas imposer des modifications majeures des réalisations de la tranche ferme pour apporter ces fonctionnalités qui seront cotées en option.

6 Tranches Optionnelles

Si les demandes optionnelles présentées ici sont déjà incluses en tant que fonctionnalités dans la tranche ferme, le soumissionnaire donnera malgré tout le détail technique de l'implémentation.

6.1 Cryptage et signature des fichiers

Les fichiers transmis pourront être signés numériquement et cryptés. Cette demande pourra s'appuyer sur les certificats issus du LDAP quand ceux ci sont disponibles. Quand un certificat n'est pas disponible le soumissionnaire suggèrera la méthode à appliquer (import et transmission de certificat).

Une description technique sera fournie et indiquera les limitations fonctionnelles.

6.2 Multi-fichiers

Si la tranche ferme ne l'indique pas, le soumissionnaire valorisera la possibilité de transmission simultanée de plusieurs fichiers. Une description technique sera fournie et indiquera les limitations fonctionnelles.

6.3 Antivirus

Afin que les fichiers téléchargés à transmettre soient sains, il est demandé de valoriser le filtrage de ceux ci par un antivirus. L'antivirus demandé est Clamav, cette tranche optionnelle sera valorisée et décrite fonctionnellement :

- Type de fichier exclus de l'analyse ;
- Nombre de récursions d'extraction dans une archive de type *.zip ;
- Procédure de mise à jour des signatures anti-virales ;
- Etc.

De même si une possibilité d'y adjoindre un moteur anti-virus propriétaire existe, la prestation sera valorisée sans tenir compte du problème de licences dont l'Inserm fera son affaire.

A titre indicatif l'Inserm émarge au marché « anti-virus » du groupement logiciel du Ministère de la Recherche et de l'Enseignement Supérieur et a donc actuellement accès sous condition au moteur Symantec et Mac Afee. Le moteur anti-virus Sophos peut également être envisagé.

6.4 Type de fichier

Pour des raisons de respect de la charte informatique de l'Inserm, certains types de fichier pourraient être interdits en transfert ou tout au moins émettre une alerte auprès de l'utilisateur qui devra confirmer ou non le transfert après cette alerte. Un système de gestion de cette tranche optionnelle sera proposé et décrit.

6.5 Traçabilité

Si l'offre en tranche ferme ne l'indique pas explicitement une traçabilité est demandée dans cette tranche optionnelle. Il s'agit d'horodater les évènements depuis la dépose de fichier par l'utilisateur jusqu'à la bonne réception et le téléchargement par le destinataire.

Une description technique valorisée sera fournie et indiquera les limitations fonctionnelles.

6.6 Connecteurs pour clients de messagerie

Des connecteurs à greffer dans les clients de courrier électronique sera valorisé. Ils permettront depuis les clients de courrier d'accéder le plus facilement possible à un envoi de fichier par la solution, l'ergonomie sera particulièrement appréciée, exemple : reprise d'un contact, de l'identité de l'utilisateur et connexion au système.

Les principaux clients de messagerie utilisés à l'Inserm sont : Thunderbird, Outlook et Mail d'Apple.

Les postulants à cet AO préciseront les clients pris en compte.

7 Unités d'œuvre (UO)

La proposition qui sera soumise donnera un descriptif précis des trois UO, il sera tenu compte de la complexité, des écrans présentés, des tables de bases de données impactées et du nombre de lignes de code à ajouter ou modifier. Pour l'ensemble des UO, les documentations qui concernent les travaux sont à fournir.

Fonctionnellement ces UO correspondent à l'énumération suivante :

7.1 UO simple

Une unité d'œuvre simple sera définie comme travaux effectués qui consistent à paramétrer les logiciels en place à des fins ergonomiques et ou esthétiques ou apportant une amélioration sans pour cela modifier notablement l'architecture ou les logiciels (typiquement modification ou ajout logiciel inférieur à 30 lignes de code).

7.2 UO moyenne

Une unité d'œuvre moyenne implique une modification ou un apport en logiciel notable, des écrans ou formulaires sont modifiés fonctionnellement (typiquement plus de 30 lignes de code effectué sur le code de l'application existante, ceci sans ajout de page).

7.3 UO complexe

Une unité d'œuvre complexe implique des développements spécifiques : ajout de fonctions et de modules apportant des écrans de présentations nouveaux liés aux nouvelles fonctionnalités (typiquement plus de 100 lignes de codes sont ajoutées).

Une unité d'œuvre complexe peut également définir un transfert de compétence à destination d'un public de 3 à 6 personnes en y incluant les documents afférents. Le transfert de compétence s'effectuera sur le site de Villejuif de l'Inserm et ne devra pas excéder une journée.