1.3 Objet du marché

Il concerne le segment SSI (Sécurité du Système d'Information) et plus particulièrement **la définition d'une PSSI (Politique de Sécurité des Systèmes d'Information) dans le cadre d'une démarche de Système de Management de Sécurité de l'Information (SMSI)**.

Le candidat devra démontrer que sa démarche permet d'assurer une réponse couvrant les besoins de centres hospitaliers de tailles différentes (moins de 100 lits, de 100 à 500 lits, de +500 à 1 000 lits, de +1000 à 2500 lits, +2500 lits).

1.4 Démarche initiée par le segment SSI d'Uni-HA, contexte, et attentes

Au-delà du groupement d'achat et de l'expression homogène des attentes de l'ensemble des adhérents vers les candidats, les experts techniques du segment Sécurité du Système d'Information d'Uni-HA ont formulé une démarche et une expression des besoins qui s'inscrit dans une dynamique construite pour répondre à une sécurité optimale des données de santé dans un contexte d'ouverture des Systèmes d'Informations Hospitaliers :

- Alimentation et Consultation du Dossier Médical d'Etablissement à compter de fin 2010
- Création d'Espaces Numériques Régionaux de Santé
- Télémaintenance 7j/7, 24h/24 des solutions tierces afin de répondre aux attentes des usagers des systèmes d'information hospitaliers
- Professionnels exerçant dans plusieurs établissements de santé

Ainsi, l'objectif des ensembles fonctionnels embrassés par les différents marchés du segment UNI-HA/NTIC/SSI est de couvrir une démarche structurée permettant d'assurer une évolution optimale de la maturité de nos établissements en matière de Sécurité des Systèmes d'information.

Cette démarche consiste à définir, pour chaque centre hospitalier, une Politique de Sécurité du Système d'Information –PSSI - en cohérence avec la législation, les lignes directrices de l'ASIP-Santé, la sensibilité de la Direction Générale et de la Commission médicale de chaque établissement (Ensemble fonctionnel 1). Cette PSSI est indispensable à légitimer la mise en place d'une organisation transversale à l'établissement pour une gestion agile des utilisateurs et de leurs droits applicatifs (Ensemble fonctionnel 2). Les lignes directrices de la PSSI définies, le Responsable de la Sécurité du Système d'Informatique de chaque établissement pourra réaliser des audits, des analyses de risque, ou une évaluation sécuritaire des offres proposées afin d'évoluer vers un Système de Management de la Sécurité du Système d'Information (Ensemble fonctionnel 3). Cette maturité atteinte, la mise en conformité avec le décret hébergeur de données de santé est réalisable (Ensemble fonctionnel 4).

Afin d'accroitre la compréhension des professionnels de santé envers la Sécurité des Systèmes d'information et de permettre une adhésion militante envers les nouveaux moyens d'authentification mis en œuvre (Carte de Professionnel de Santé ou Carte d'Etablissement selon les établissements), une sensibilisation des utilisateurs via le « e-learning » est nécessaire (Ensemble fonctionnel 5).

Chaque établissement ayant formalisé sa PSSI, s'étant structuré sur la gestion de l'identité et des droits des acteurs du Système d'Information, ces derniers étant sensibilisés à la Sécurité du Système d'Information, la maturité de l'établissement est acquise. Ceci permet de mettre en place les outils de gestion des identités et des droits (IAM) par la synchronisation de l'application de Gestion des Ressources Humaines, des annuaires de l'ASIP-Santé et des annuaires ordinaux (Conseils Nationaux de l'Ordre des médecins, des pharmaciens, des infirmiers, et des kinésithérapeutes). (Ensemble fonctionnel 6, sous-ensemble 1).

Les identités et rôles des acteurs de chaque Système d'Information étant connus, la mise en place d'un système de gestion des rôles, permet de réaliser la création automatisée des droits utilisateurs, application par application, en fonction d'une matrice des droits propre à chaque établissement et chaque applicatif interfacé (Ensemble fonctionnel 6, sous-ensemble 2).

A ce stade, parmi les plus importants Centres Hospitaliers, certains ont besoin de compléter l'autorité de certification régalienne de l'ASIP-Santé (Cartes de Professionnels de Santé), par une autorité de certification interne à l'établissement, afin de cibler l'ensemble des acteurs du SIH (étudiants, bénévoles, prestataires, personnels non médicaux) (Ensemble 6, ensemble fonctionnel 3).

Afin de rendre flexible et rapide la gestion des médias d'authentification (en cible la Carte de Professionnel de Santé ou la Carte d'Etablissement ayant pour vocation d'embarquer des certificats X509), la mise en place d'un système de gestion des cartes (Card Management Système) paraît indispensable (Ensemble fonctionnel 6, sous-ensemble 4).

Afin d'activer l'usage des médias d'authentification et de proposer une simplification de l'usage informatique rendu possible par ces médias sécurisés, la mise en place d'une authentification unique permettant l'accès à l'ensemble des applications (Single Sign On) est demandée (Ensemble 6, sous-ensemble fonctionnel 5).

La sécurisation d'accès au système d'information étant acquise à travers les ensembles fonctionnels 1 à 6 il parait alors nécessaire, en cohérence avec le cadre législatif et les exigences de la Commission Nationale Informatique et Liberté, d'exploiter les traces applicatives et les corréler afin d'assurer aux patients le contrôle continu de l'accès sécurisé à leurs données médicales et de leurs modifications. Ceci concerne les traces systèmes des serveurs (Ensemble fonctionnel 7, sous ensemble fonctionnel 1), leurs corrélations avec les traces applicatives (Ensemble fonctionnel 7, sous ensemble fonctionnel 2) et les traces des postes de travail (Ensemble fonctionnel 8). La solution mise en œuvre doit permettre une parfaite conformité au décret « hébergeur de données de santé » (décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel) sur son périmètre.

La mise en œuvre d'une PSSI, de la sensibilisation des utilisateurs, de la sécurisation de l'accès aux Systèmes d'Information via l'authentification, et de la traçabilité permettent d'introduire sereinement la mise en œuvre de la signature électronique des documents de façon autonome dans les outils bureautiques ou de façon intégrée aux applications médicales (Ensemble fonctionnel 9). Cette signature est basée à partir des certificats issus du GIP-CPS ou de certificats X509 propres à l'établissement.

L'objectif des ensembles fonctionnels 1 à 9 est de permettre aux établissements de maitriser la sécurité des données médicales en vu de la mise en œuvre du Dossier Médical Personnel et des Espaces Numériques Régionaux de Santé.

Afin de compléter les offres nationales pour répondre aux contraintes inhérentes aux centres hospitaliers, certains d'entre eux ont besoin d'une carte d'établissement de santé ayant pour vocation d'adresser l'ensemble des acteurs de l'hôpital et d'héberger des certificats d'autorité de confiance régalienne pour contrôler l'accès aux données médicales et au DMP, c'est l'objet de l'ensemble fonctionnel 10, lot 1.

Enfin, afin de permettre l'usage des cartes, qu'elles soient CPS ou cartes d'établissement, des lecteurs adaptés aux contraintes des Etablissements de Santé sont requis (Ensemble fonctionnel 10, lot 2). La diffusion massive de cartes et la bonne sécurisation des données à caractère personnel de santé sur média amovible nécessitent des accessoires et consommables demandés à travers le lot 3 de l'ensemble fonctionnel 10. Enfin, la dimension patient et facturation nécessite la pleine gestion des cartes VITALE couverte par le lot 4 de l'ensemble fonctionnel 10.