LOGOQUAD  cid:image003.jpg@01D4752E.E733E3F0

ACHATS CENTRAUX

HOTELIERS, ALIMENTAIRE ET TECHNOLOGIQUES

Hôpital Bicêtre

78, rue du Général Leclerc

94270 Le Kremlin Bicêtre

Tél. : 01 53 14 69 00

Fax : 01 45 15 01 60

Fourniture livraison installation et mise en service de systèmes de contrôle électronique d’accès physique pour le PIC ACHAT

***Cahier des Clauses Techniques Particulières***

***N° 24/110***

Objet : Fourniture, livraison, installation et intégration de solution logicielle pour mise en service de systèmes de contrôles électroniques d’accès physique nécessaires aux besoins du PIC ACHAT de l’Assistance-Publique Hôpitaux de Paris.

Le marché est conclu pour la période ferme allant de la date de notification pendant 48 mois éventuellement résiliable sans indemnités la seule initiative de l’Assistance Publique – Hôpitaux de Paris, à compter de 6 mois avant la fin du marché.

Ce document comprend 39 pages et est associé au Cahier des Clauses Administratives Particulières

SOMMAIRE

[GLOSSAIRE 3](#_Toc175128583)

[I-OBJET DE LA CONSULTATION 5](#_Toc175128584)

[**I-1 Prescriptions de la Direction Générale de l’APHP :** 5](#_Toc175128585)

[II- DECOMPOSITION EN LOTS 7](#_Toc175128586)

[III- COMPOSITION DU LOT ET VOLUMETRIE 8](#_Toc175128587)

[IV- SPECIFICATIONS TECHNIQUES GENERALES DES PRODUITS 9](#_Toc175128588)

[IV-1 Spécifications techniques particulières 11](#_Toc175128589)

[IV-2 Continuité de service 13](#_Toc175128590)

[IV-3 Obligation de conseil 14](#_Toc175128591)

[IV-4 Intégration au système d’information de l’AP-HP 14](#_Toc175128592)

[IV-5 Suivi du marché - Indicateurs 23](#_Toc175128593)

[V- DOSSIER TECHNIQUE 23](#_Toc175128594)

[VI- NORMES ET REGLEMENTATIONS 24](#_Toc175128595)

[VII- LIMITES DE PRESTATIONS 25](#_Toc175128596)

[VIII- DUREE DE GARANTIE 28](#_Toc175128597)

[Annexe 1 : Cadre de réponse technique 29](#_Toc175128598)

[Annexe 2 : Guide securite des technologies sans-contact pour le contrôle des acces physiques de l’ANSSI. 34](#_Toc175128599)

[Annexe 3 : Guide de la mise en œuvre de la partie sans-contact des cartes cpx – ASIp sante 35](#_Toc175128600)

[Annexe 4 : Règles de sécurité du système d’informaton applicables aux titulaires de marchés de l’Assistance Publique – Hôpitaux de Paris 36](#_Toc175128601)

[Annexe 5 : Cadre de cohérence technique de l’Assistance Oublique – Hôpitaux de Paris 37](#_Toc175128602)

[Annexe 6 : politique générale de securité du système d’information de l’Assistance Publique – Hôpitaux de Paris **Erreur ! Signet non défini.**](#_Toc175128603)

# GLOSSAIRE

|  |  |
| --- | --- |
| **Expression** | **Définition** |
| Accessoire facultatif | Accessoire pour lequel une offre de prix unitaire peut être faite et figurer à l’acte d’engagement de manière individuelle. Dans le cas où un accessoire facultatif est inclus dans l’équipement de base en raison d’un montage en série, ceci n’apporte aucun point supplémentaire au niveau de la cotation de l’offre |
| ANSSI | Agence Nationale de Sécurité des Systèmes d’Information |
| Anti PASS BACK | L’anti pass-back est employé pour empêcher l’utilisation par plusieurs personnes d’un même badge.  Il y a deux sortes d’anti pass-back : REEL et TEMPORISE. Selon le type d’installation  1 seule porte à 2 lecteurs (1 en entrée et 1 en sortie) est toujours en anti pass-back REEL c'est-à-dire qu’un badge doit passer par le lecteur d’entrée avant d’être accepté par le lecteur de sortie et vice versa.  1 porte à 1 lecteur est toujours en anti pass-back TEMPORISE. Les badges ne peuvent pas être utilisés deux fois dans un intervalle de temps programmable.  2 portes et 1 lecteur par porte peuvent être soit en anti pass-back REEL ou TEMPORISE. En anti pass-back REEL, il faut que les deux portes soient programmées en « ASSOCIEES », dans ce cas, les badges doivent être utilisés d’abord sur la 1ère porte et ensuite sur la 2ème. En anti pass-back TEMPORISE, le fonctionnement est le même que le précédent. |
| ASIP Santé | Agence des Systèmes d’Information Partagés de Santé |
| Authentification du badge | L'authentification du badge consiste à prouver qu’il est valide.  Pour un système de contrôle d’accès reposant sur des technologies sans contact, l’authentification du badge se fait le plus souvent par un échange cryptographique permettant au badge de prouver qu’il détient des éléments secrets sans les révéler |
| Auto-surveillance à l’ouverture ou à l’arrachement | Dispositif d’avertissement en cas d’ouverture frauduleuse (ou arrachement) d’un équipement de gestion de contrôle d’accès. |
| BPU | Bordereau de Prix Unitaires |
| Caractéristique biométrique | Information qui se réfère à des caractéristiques physiologiques uniques de l’utilisateur. |
| CCTP | Cahier des Charges Techniques Particulières |
| Condition de défaut | Toute condition qui génère l’interruption ou la dégradation des fonctions d’un équipement de contrôle d’accès. |
| Condition normale | Etat dans lequel le système de contrôle d’accès est entièrement fonctionnel et est en mesure de traiter tous les événements dans le respect des règles établies |
| CPx | Famille de cartes à puce émises par l’ASIP Santé comprenant CDA, CDE, CPA, CPE, CPF et CPS. Les cartes CPx contiennent un volet IAS permettant de mettre en œuvre un niveau de sécurité renforcé (conformité à la norme européenne IAS-ECC) en mode contact et sans-contact, à la fois pour du contrôle d’accès logique et physique. Cette mise en œuvre s’inscrit dans un véritable projet d’intégration et fait appel à des lecteurs compatibles. |
| CSPN | La certification de sécurité de premier niveau des produits des technologies de l'information (CSPN), mise en place en 2008, est l'une des certifications délivrées par l'Agence nationale de la sécurité des systèmes d'information. La certification CSPN permet d’attester que le produit (logiciel, système d'exploitation, appliance, matériel...) a subi avec succès une évaluation de sécurité par un centre d’évaluation (CESTI) agréé par l’ANSSI. |
| DSI | Direction des Systèmes d’Information |
| Évènement | Information d’un changement d’état apparaissant dans le système de contrôle d’accès |
| GAIAP | Acronyme de la solution en place à l’AP-HP, pour le système de gestion des identités et des accès de l’AP-HP, basé sur la suite logicielle EVIDIAN IGA 10 de BULL ATOS TECHNOLOGIES (EVIDIAN Identity Governance and Administration 10 Evolution 3) |
| HBPU | Hors Bordereau de Prix Unitaires. Cette partie du marché est mise au point sur la base du catalogue de l’opérateur économique et peut comprendre par exemple, des produits identiques avec d’autres dimensions que celles exigées dans le BPU, des accessoires complémentaires, autres que ceux des produits du BPU, en liaison avec les produits du marché ; Les produits complémentaires retenus représentent obligatoirement et exclusivement la famille et la gamme de produit listées dans le bordereau de prix unitaire et ce sans doublon d'article |
| IAS-ECC | Afin de rendre compatibles les spécifications françaises pour l’identification, l’authentification et la signature (standard de cartes IAS) avec la nouvelle norme européenne : European Citizen Card (ECC), l’ANTS et le GIXEL (groupement d’industriels de la carte à puce) ont défini une nouvelle spécification : IAS-ECC. |
| Identifiant | Données d’identification délivrées par des badges, des cartes d’accès, des clés électroniques, par saisie... |
| Identification | Processus de traitement d’un identifiant |
| Laboratoire L1, L2, L3, L4 | Niveaux d’exigences de confinement dans un laboratoire (arrêté du 13 août 1996) |
| Lecteur du point d’accès | Dispositif utilisé pour collecter les données d’identification. Ces données sont transmises à l’UTL à distance ou localement. Dans ce dernier cas, lorsque le lecteur est intégré avec l’UTL dans un même boîtier, il est dit autonome |
| Mode dégradé | Etat dans lequel l’équipement de gestion de contrôle d’accès est partiellement fonctionnel et est en mesure de traiter tout ou partie des événements dans le respect des règles établies |
| Plage horaire | Intervalle de temps entre deux moments donnés indiquant le commencement et la fin d’une période valide incluse dans une zone de temps. |
| Point d’accès | Endroit où l’accès peut être contrôlé : présence d’obstacle physique (porte, tripode…). |
| RFID | Radio Frequency IDentification - : Technologie d'identification automatique qui utilise le rayonnement radiofréquence pour identifier les objets porteurs d'étiquettes lorsqu'ils passent à proximité d'un interrogateur. |
| UTC | Unité de Traitement Centralisé de contrôle d’accès. Cette unité de traitement prend la décision de libérer un ou plusieurs points d’accès et gère la séquence de commande associée |
| UTL | Unité de Traitement Local. Système électronique qui permet d’appliquer la décision provenant de l’UTC. Cette UTL commande un ou plusieurs points d’accès. Une UTL est nécessairement reliée à une UTC. |
| UTS | Unité de Traitement de Supervision de contrôle d’accès : Matériel qui assure les fonctions de superviseur pour des UTC et/ou des UTL. Ce matériel assure les fonctions d’interface du point d’accès, de traitement, d’annonce, d’alerte et assure leur alimentation. |
| Visiophone | Dispositif de communication permettant d’établir une relation vocale et visuelle bidirectionnelle entre un visiteur et l’occupant d’un bâtiment. Ce dispositif peut permettre l’ouverture d’une porte. |

# I-OBJET DE LA CONSULTATION

Le présent accord cadre a pour objet la fourniture, livraison, installation intégration logicielle de systèmes de contrôle électronique d’accès physique nécessaires aux besoins du PIC ACHAT de l’Assistance Publique Hôpitaux de Paris.

Un système de contrôle des accès physiques est un dispositif ayant pour objectif de contrôler et de filtrer les flux d’individus souhaitant pénétrer à l’intérieur d’un site, d’un bâtiment ou d’un local. Il est constitué de moyens permettant d’autoriser les entrées et sorties de zones sensibles aux seules personnes qui ont le droit d’y accéder.

Un système de contrôle d’accès assure trois fonctions primaires :

1. L’identification et l’authentification ;
2. Les contrôle d’accès des permanents, temporaires et visiteurs ;
3. LA détection des intrusions (personnes indésirables) ;
4. Le traitement des données ;
5. Le déverrouillage.

Ces fonctions sont assurées en chaque point où l’accès est contrôlé.

## **I-1 Prescriptions de la Direction Générale de l’APHP :**

*Les systèmes de contrôles d’accès par badge doivent être compatibles sans restriction avec la carte CPx. La carte CPx intègre plusieurs dispositifs de sécurité (numéro d’identifiant unique et numéro IAS avec possibilité de certificat ou de mise à la clé – la mise à la clé nécessite une carte CPx inscriptible distribuée par l’ASIP Santé). Actuellement l’AP-HP valide deux technologies pour les cartes CPS, la technologie de la carte CPS V3.1 (MIFARE CLASSIC) et la technologie de la carte CPS R3 (MIFARE* *DESFIRE).*

*Si pour des locaux sans particularité il est possible de retenir un niveau de sécurité relativement faible, pour les locaux sensibles (laboratoires L3, salles serveurs, locaux NRBC[[1]](#footnote-1),…), il y a lieu de déployer une technologie davantage sécurisée comme un certificat d’authentification du numéro IAS. Dans des cas bien particuliers de haute sécurité, il est possible de déployer un dispositif authentifiant le certificat d’authentification du numéro IAS.*

*Ce contrôle renforcé peut être complété par un deuxième système de contrôle d’accès pour les lieux les plus sensibles (salle cœur de réseau, régulation SAMU…). Il s’agit de l’authentification à deux facteurs. La deuxième authentification peut être réalisée par le code PIN de la carte CPx en mode contact (insertion dans le lecteur) ou par un autre dispositif sécurisé (biométrie par exemple). Pour des lieux spécifiques ou l’identification par badge CPx n’est pas possible (pour des raisons d’hygiène par exemple), par exception, un dispositif d’accès alternatif peut être envisagé (biométrie par exemple). La biométrie se substitue au lecteur de badge.*

*Les matériels proposés dans le cadre de cette consultation devront impérativement être compatibles avec ces technologies afin de n’avoir qu’une simple mise à jour du système à effectuer lorsque l’on souhaite rehausser le niveau de sécurité de la carte CPx en la rendant multi-technologie mais rétro compatible avec les technologies de la carte actuelle.*

*Les équipements de contrôle d’accès doivent être pilotables au travers d’un logiciel interopérable avec le système d’information de l’AP-HP. Ce logiciel de gestion doit être nativement et sans coût supplémentaire en capacité d’intégrer des données en provenance du SI de l’AP-HP, telles que les informations relatives aux identités des agents (entrants et sortants) ou relatives à leur affectation en provenance de la solution GAIAP-IAM Evidian IGA 10[[2]](#footnote-2) ou supérieure.*

*De même, ce logiciel de gestion doit être nativement et sans coût supplémentaire en capacité d’accepter et de répercuter un message énonçant un ordre de révocation des droits d’accès d’un porteur de carte ou d’identifiants biométriques dans un délai réduit.*

*Plus généralement, la possibilité d’intégrer un message de demande d’attribution d’accès pour une identité avec précision de date et de fin de validité doit pouvoir être implémentée moyennant communication par les équipementiers retenus des spécifications, des mécanismes et formats implémentant ces dispositifs d’interfaçage afin de pouvoir être rendus interopérables avec la solution GAIAP-IAM Evidian IGA 10 ou supérieure.*

*GAIAP met à disposition quotidiennement des fichiers avec la liste des personnels et des tiers nouvellement arrivés et ayant quitté l’AP-HP ainsi qu’un état de situation.*

*Concernant les* ***normes de sécurité de tous ces dispositifs****, ils doivent intégrer les préconisations de l’ANSSI[[3]](#footnote-3) en matière de sécurité des systèmes d’information (SI) et notamment leur déclinaison au sein de l’AP-HP :*

* *Règles de sécurité du SI applicables aux titulaires de marché de l’AP-HP daté de février 2017 ;*
* *Le cadre de cohérence technique destiné à faciliter l’intégration des nouveaux systèmes dans le SI existant (février 2016), joint en annexe 6 du présent CCTP.*

*S’ils ne les respectent pas, il doit en être fait mention très clairement. Une ou plusieurs solutions palliatives seront proposées pour atteindre un niveau de sécurité équivalent.*

*Aussi, comme tout système d’information, les dispositifs de contrôle d’accès doivent être achetés, sécurisés et maintenus en condition de sécurité tout le temps de leur usage. La télémaintenance de ces appareils, lorsqu’elle est prévue, doit être conforme aux exigences de la DSI[[4]](#footnote-4) de l’AP-HP et respecter les CCTP.*

*Le candidat garantit, sous peine de non-conformité, qu’à la date du dépôt de son offre, les logiciels et matériels, qu’il propose dans son offre, ne comportent aucune vulnérabilité qui permettrait de prendre leur contrôle à distance sans identification et authentification préalable.*

## **I-2 Prestations du marché :**

Les prestations couvertes par le marché doivent comprendre :

* Les achats de prestations d’étude de site ;
* Les achats de matériels : Plaques béquilles, lecteurs, détecteurs câblage, serveurs, enregistreurs, écrans, alimentations ;
* Les achats de solutions logicielles ;
* L’installation et le paramétrage de matériels : plaques béquilles, détecteurs, serveurs, lecteurs ;
* L’installation et le paramétrage des solutions logicielles ;
* La garantie et le maintien en condition opérationnelle et le maintien en condition de sécurité conformément à la PGSSI de l’AP-HP pendant la durée du marché ;
* La fourniture d’un dossier complet d’ouvrage exécuté ;
* Les formations et l’accompagnement du changement des différents acteurs ;

# II- DECOMPOSITION EN LOTS

Le marché se compose d’un lot unique :

|  |  |
| --- | --- |
| **N° du lot** | **Intitulé du lot** |
| **1** | Fourniture, livraison, installation et intégration de solution logicielle pour mise en service de systèmes de contrôles électroniques d’accès physique nécessaires aux besoins du PIC ACHAT de l’Assistance-Publique Hôpitaux de Paris |

Le marché est composé d’une tranche ferme et d’une tranche optionnelle.

La tranche ferme concerne : la sécurisation des entrées externes des bâtiments ainsi que de l’accès à la salle serveurs : installation de contrôles d’accès filaires. Le démarrage de cette tranche ferme s’effectue dès la notification du marché.

La tranche optionnelle concerne : la sécurisation des accès internes aux locaux : installation de contrôles d’accès non filaires. La tranche optionnelle pourra être affermies à compter de la deuxième année de marché. Pour ce faire le pouvoir adjudicateur préviendra le titulaire 1mois avant l’affermissement.

Le maître d’ouvrage se réserve le droit de ne pas affermir la tranche conditionnelle.

# III- COMPOSITION DU LOT ET VOLUMETRIE

| **N° ligne de produit** | **Spécification** | **Quantités annuelles estimées** |
| --- | --- | --- |
|  | **Tranche ferme** |  |
| **1** | Ensemble plaque béquille électronique sortie libre, contrôlée côté extérieur. Entre axe 70 mm Axe 50 mm | 8 |
| **2** | lecteur de badge mural sans contact | 6 |
| **3** | lecteur de badge mural sans contact et clavier | 2 |
| **4** | Badges | 50 |
| **5** | Détecteurs d'ouverture de porte | 3 |
| **6** | Equipements pour récupérateur signaux, superviseur, commande d'automatisme, etc. | 6 |
| **7** | Licence permettant la gestion des systèmes tranche ferme (entrées, opérateurs, identification) | 1 |
| **8** | Serveur | 1 |
| **9** | Postes clients | 2 |
| **10** | Ecrans 24" | 2 |
| **11** | Encodeurs | 2 |
| **12** | Forfait configuration, paramétrage tranche ferme | 1 |
| **13** | Forfait pose tranche ferme | 1 |
| **14** | Forfait dossier d'ouvrage exécuté | 1 |
| **15** | Forfait formation par jour par personne | 8 |
|  |  | **94** |
|  | **Tranche conditionnelle** |  |
| **16** | Ensemble plaque béquille électronique | 56 |
| **17** | Hub radio de communication avec antenne | 14 |
| **18** | Licences permettant de gérer 56 portes, Licences lecteurs, opérateurs gestionnaires, opérateurs web, licences passerelles comprises | 1 |
| **19** | Forfait pose tranche conditionnelle | 1 |
| **20** | Forfait dossier d'ouvrage exécuté | 1 |
| **21** | Forfait formation par jour par personne | 8 |
| **22** | Garantie matérielle et maintien en condition opérationnelle | 1 |
|  |  | **82** |

* **La partie articles listés est estimée à 90 % du volume financier annuel.**
* **La partie catalogue est estimée à 10 % du volume financier annuel.**

**La partie catalogue fait l’objet d’une mise au point après attribution et avant notification.**

# IV- SPECIFICATIONS TECHNIQUES GENERALES DES PRODUITS

Les cartes CPx sont des cartes à puce délivrées aux professionnels du secteur santé et médico-social compatibles avec le protocole ISO 14443 type A et type B. Elles permettent de mettre en œuvre :

* L’authentification du porteur de carte ;
* L’authentification simple de la carte : en mode sans-contact, lecture de la carte à moins de 5 cm du lecteur, conforme à la norme ISO 1444, pour faciliter l’usage de la carte en situation de mobilité au sein d’une organisation de santé.

Une évolution est en cours sur la technologie des cartes professionnelles et doit être prise en compte dans la solution proposée pour une compatibilité sans restrictions :

* Nous sommes aujourd’hui pour nos cartes en version CPSv3 avec Mifare Classic disponible et Mifare DESFire EV1.
* Progressivement disparition du Mifare Classic sur la nouvelle carte CPSv4 et intégration dans la version CPSv4 du Mifare DESFire EV3.

Les produits proposés dans le cadre de cette consultation sont exclusivement basés sur le principe physique (ouvertures de portes) et non sur le principe logique (ouverture de session informatique), et devront systématiquement être conformes aux recommandations de l’ASIP[[5]](#footnote-5) santé, en particulier :

* Système local de gestion du parc de cartes CPx utilisées ;
* Lecteurs sans-contact en mode « transparent », c’est-à-dire des lecteurs qui ne font que transformer les ondes en commandes filaires et vice versa dans le cadre des échanges entre la carte CPS et l’Unité de Traitement Local (UTL) ;
* UTL[[6]](#footnote-6) « intelligents » (capables de communiquer avec la carte CPS au moyen de commandes APDUs normalisées par la norme IAS-ECC, supportant le mode transparent, et susceptibles d’être mis à jour facilement ;
* Processus d’enrôlement local simples ;
* Câblages normalisés notamment Ethernet catégorie 5 ou supérieur.

Dans les scénarios correspondants au contrôle d’accès, le porteur de carte CPx utilise sa carte CPx pour s’authentifier auprès du système, qui l’autorise ou non. L’opération laisse généralement une trace : l’événement, qu’il soit ok ou ko est conservé sous la forme d’une association {date ; carte ; lieu d’accès ; référence vers l’identité associée} par chacun des éléments techniques composant le système.

Il s’agit donc d’un modèle AAA (Authentication, Authorization and Accounting, pour Authentification, Autorisation et Traçabilité) dans lequel le « vecteur d’authentification » est la carte CPx, utilisée via son volet sans-contact.

Le lecteur lit depuis la carte de l’utilisateur, en sans-contact, des informations qui sont remontées du lecteur à l’UTL puis, éventuellement, de l’UTL au serveur.

Généralités exigées concernant les accès contrôlés objets de cette consultation

Point commun à toutes les portes contrôlées :

* Le système proposé devra être compatible avec l’utilisation traditionnelle d’un cylindre de serrure européen. Que ce soit dans son mode de fonctionnement normal ou dans un mode dégradé, le système de contrôle d’accès proposé devra maintenir la possibilité d’ouverture et de verrouillage à l’aide des clés utilisées dans l’établissement ;
* Toutes les portes devront être équipées d’un contact dit « contact de porte fermée » permettant de vérifier le bon verrouillage à la fermeture. Ce contact de porte devra être associé à un signal sonore et à une remontée d’alarme vers le logiciel d’exploitation.
* Le système proposé devra être compatible avec un état dit « d’ouverture permanente » applicable à partir du logiciel d’exploitation.

Scénario à présenter par écrit :

Les candidats devront présenter par écrit sur 5 pages maximum, à l’appui des plans fournis en annexe, la solution proposée. Il est précisé que toute candidature n’intégrant pas cette note de présentation sera rejetée.

Cette note doit permettre :

* D’analyser les possibilités offertes par la solution proposée par le candidat ;
* De juger le niveau de compréhension du contexte et des besoins des différents acteurs, autant fonctionnels que techniques.

***L’attention des candidats est attirée sur ce scénario qui constitue un item évalué et noté.***

***L’absence de présentation du projet de catalogue rend l’offre non conforme.***

### IV-1 Spécifications techniques particulières

**IV-1-2 Fonctions générales exigées**

L’accès physique aux systèmes compatibles avec la carte sans contact CPx concerne en particulier :

* L’activation des accès aux locaux sécurisés selon la période d’activité de l’agent ;
* L’accès aux locaux sensibles.

Le mode de lecture devra se faire sans contact. La technologie RFID[[7]](#footnote-7) utilisée ainsi que la distance maximale de lecture devront être précisées.

Les têtes de lecture, Unités de traitement local, liaisons filaires, Réseaux fédérateurs, logiciels de gestion du système et ensemble des éléments du ou des systèmes proposés devront obligatoirement respecter les spécifications détaillées figurant dans le guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques, édité par le Secrétariat Général de la Défense et la Sécurité Nationale, Agence Nationale de Sécurité des systèmes d’Information, dans sa dernière mise à jour.

L’annexe 4 du guide publié le 19 novembre 2012 est jointe à titre indicatif en annexe 3 de ce CCTP.

**IV-1-3 Caractéristiques minimales**

Ensembles plaques béquilles électroniques exigés au titre du BPU:

* **Les ensembles proposés doivent pouvoir être installés sur différents types de porte ;**
* **Fonctionnement à piles, sans câblage, portes à profil européen, pouvant fonctionner avec la majorité des serrures à mortaiser et des cylindres européens, tout type de porte, différentes épaisseurs de porte ;**
* **L’ensemble des composants électroniques doit se situer côté intérieur de la porte ;**
* **Les piles doivent se situer côté intérieur des béquilles ;**
* **Système d’alerte batteries faibles ;**
* **Têtes de lecture équipées de signalisation couleur (accès autorisé, accès refusé au minimum) ;**
* **Communication en temps réel des droits d’accès, ouvertures à distance, remontée des évènements ;**
* **Lorsqu'un support d'identification autorisé est reconnu par la tête de lecture située sur l'ensemble de la plaque béquille, la béquille est libérée électroniquement. Après la fermeture de la porte, la béquille est à nouveau bloquée ;**
* **En cas de défaillance : Sauvegarde des derniers évènements ayant lieu hors liaison : badges validés, badges refusés, défaut liaison sans fil ;**
* **Possibilité de monter un ensemble de chaque côté de la porte pour un contrôle en entrée et en sortie.**

**Des systèmes complémentaires pourront être proposés au titre du catalogue complémentaire HBPU sous réserve de respecter les préconisations du présent CCTP.**

Cylindres électroniques :

**Contrairement à l'ensemble plaque béquille qui bloque automatiquement la béquille après le passage en rendant la porte fermée de l'extérieur, le bouton sur le cylindre électronique doit être activé manuellement après lecture du badge : après contrôle de son autorisation, il peut être déverrouillé.**

**Lorsque la porte se referme après l'ouverture, celle-ci n'est pas condamnée. Le verrouillage s'effectue en actionnant une nouvelle fois le bouton côté intérieur.**

**Le cylindre électronique est préconisé lorsque la porte dispose déjà de garnitures que l'on ne souhaite pas changer, ou lorsque la disposition de la porte ne permet pas l'utilisation d'ensembles plaque béquilles. Le processus d'identification est confirmé par une information visuelle du cylindre électronique. Aucun câblage n'est nécessaire sur la porte.**

**Ensemble des composants électroniques sensibles dans le corps du cylindre.**

**Pile positionnée dans le bouton extérieur, remplaçable à l’aide d’un outil spécifique. Alerte batterie.**

* **Têtes de lecture équipées de signalisation couleur (accès autorisé, accès refusé au minimum) ;**
* **Indice IPxx suffisant pour un montage en extérieur.**

**En cas de défaillance : Sauvegarde des derniers évènements ayant lieu hors liaison :**

* **Badges validés, badges refusés ;**
* **Défaut liaison sans fil.**

Lecteur mural simple :

Lecteur programmable, compatible ISO 14443A (type B souhaité) utilisant la bande 13,56 MHz, fixation murale, distance de lecture entre 4 et 8 cm.

Les lecteurs sont livrés avec leur capot de protection. Les lecteurs doivent être disponibles sur bases en applique ou à encastrer.

* **Signalisation couleur (accès autorisé, accès refusé au minimum) ;**
* **Indice IPxx suffisant pour un montage en extérieur,** totalement étanches à l’eau et à l’humidité et anti vandales.

Logiciel d’exploitation :

Le logiciel doit être multi sites et multipostes.

Il doit être structuré autour d’une base de données unique, sécurisée et chiffré par les responsables APHP.

Il doit permettre de gérer à distance et en temps réel :

* L’architecture physique du matériel, les appairages et les routages ;
* La création, modification et suppression des utilisateurs ;
* La synchronisation avec un référentiel APHP quotidien voire temps réel ;
* La création d’actions calendaires comme les ouvertures fermetures automatiques horodatées ;
* L’ouverture et fermeture d’accès à distance ;
* La communication avec des systèmes tiers, vidéo surveillance par exemple ;
* Droits d’accès selon prérequis de type zones, bâtiment ou activité ;
* La traçabilité des évènements : ouvertures, actions dans le système ;
* L’extraction de la liste des utilisateurs selon plusieurs critères : période, statut du bénéficiaire (autorisé, bloqué, en quarantaine, etc.), autres (non obligatoire), pour des revues de contrôle
* L’ensemble du système doit être supervisable par un responsable central ;
* Télémaintenance et mise à jour via accès VPN sous contrôle APHP ;
* Possibilité de verrouillage intégral des accès ou selon différentes stratégies : par établissement, par bâtiment ; par service ;
* L’affichage des alarmes et incidents doit être directement lisible sur le logiciel, sans interprétation, par exemple par un affichage sous forme de plan. Une extraction des données doit être possible sous format non propriétaire.

### IV-2 Continuité de service

Durée d’approvisionnement : le candidat s’engage à fournir du matériel de remplacement identique pendant 5 ans minimum. Conformément à l’article L111-3 du code de la consommation.

La durabilité des équipements proposés et la date jusqu’à laquelle les pièces détachées indispensables à l’utilisation des produits seront disponibles sont à renseigner dans le cadre de réponse technique joint en annexe 1;

Le candidat s’engage à proposer une prestation de maintenance sur l’ensemble des équipements et logiciels déployés pendant une durée de 10 ans minimum.

Le titulaire trie, retraite et évacue l’ensemble des déchets produits au cours de ses interventions. Les coûts inhérents à ce traitement sont inclus dans les prix forfaitaires, quelle que soit la nature des déchets.

Fin de vie des produits : Le titulaire se conforme aux directives DEEE (Déchet d’Equipement Electrique et Electronique) et LdSD (Limitation des Substances Dangereuses), mises en application par le décret 2005-829 du 20/07/2005, relatif à la composition des équipements électriques et électroniques et à l’élimination des déchets issus de ces équipements.

### IV-3 Obligation de conseil

Le titulaire mettra à disposition de l’établissement un chef de projet ayant les compétences et le degré de responsabilité nécessaires pour valider les choix envisagés.

### IV-4 Intégration au système d’information de l’AP-HP

***IV-4-1 Contexte***

Parc informatique

**A la date de publication du marché**:

La suite bureautique OFFICE de Microsoft en version 2010 / 2016 est largement déployée.

Serveurs

Les systèmes d’exploitation de référence des serveurs sont :

1. WINDOWS 2012 R2 ou supérieur ;
2. LINUX REDHAT en version 64 bits ;
3. HP-UX sous ITANIUM.

Les solutions de virtualisation de l’éditeur VMWARE sont utilisées sauf incompatibilité avérée.

Les systèmes de base de données de références sont :

* ORACLE ;
* SQL SERVER de Microsoft ;
* POSTGRESQL.

Le logiciel XenAPP de l’éditeur CITRIX est utilisé notamment pour publier les applications clients/serveurs ne présentant pas de contraintes de performances particulières (flux vidéo notamment).

Centres informatiques

Chaque hôpital, tout comme le PIC ACHAT, dispose d’une ou deux salles informatiques. Ces salles sont destinées à héberger de manière sécurisée (contrôle d’accès, détection d’intrusion, climatisation, courant électrique de haute qualité) les applications locales, les services bureautiques, les services d’infrastructure (DNS, DHCP, contrôleur de domaine active directory, sauvegarde, baie disque) ainsi que le cœur de réseau de l’établissement et son accès au réseau d’interconnexion.

Le Département Infrastructures et Services (DIS) de la DSN opère les 2 centres Informatiques principaux (Datacenter).

Le réseau entre les sites de l’AP-HP comporte 2 anneaux fédérateurs à 20 Gb/s chacun agissant en équilibrage de charge et en secours l'un de l'autre. Ces anneaux sont raccordés à 8 boucles périphériques à 10 Gb/s et à 2 boucles périphériques à 1Gb/s offrant un haut niveau de disponibilité.

Entre les zones de sécurité du réseau (Internet, à la frontière des centres informatiques, à la frontière des DMZ), un filtrage du trafic est réalisé avec des pare-feu.

Internet

Il est possible d’accéder au réseau Intranet de l’AP-HP depuis Internet au travers de la Solution VPN SSL CONNEXTRA de JUNIPER.

Le réseau de l’AP-HP est doublement raccordé à l’Internet par 2 opérateurs de télécommunication avec un débit de 500 Mb/s à la date de publication du marché.

Sites web Internet/Intranet

Le choix technologique de WORDPRESS a été fait pour les sites WEB institutionnels accessibles depuis Internet.

Le choix technologique de SPIP a été fait pour les sites WEB de publication accessibles depuis l’Intranet. Un portail utilisant la technologie 9iAS d’ORACLE fédère les différents sites SPIP.

Cet accès se fait depuis un serveur PROXY dont le script de configuration est accessible depuis l’URL <http://proxy.aphp.fr/inter.pac>.

Messagerie

La messagerie EXCHANGE version 2010 est utilisée à l’AP-HP avec un total de 42 000 boîtes aux lettres électroniques.

Le service de messagerie est utilisable depuis l’Intranet ou l’Internet en WEBMAIL ou depuis un client lourd avec le protocole MAPI ou depuis les SMARTPHONES avec le client ACTIVESYNC de Microsoft.

Exploitation

Les logiciels suivants sont utilisés pour assurer l’exploitation du SI de l’AP-HP :

* NAGIOS pour la supervision ;
* SM9 de MICROFOCUS pour la gestion des incidents (en fin de vie, voir SMAx);
* SMAx de MICROFOCUS pour la gestion des demandes et des incidents
* SCCM de Microsoft pour l’assistance à distance des postes de travail ;
* SCCM de Microsoft pour l’inventaire et la télédistribution des logiciels sur les postes de travail ;
* ADMINBASTION de WALLIX pour la télémaintenance.

Support et gestion des incidents

L’AP-HP met en œuvre les bonnes pratiques du standard ITIL pour la gestion des incidents.

Le support utilisateur AP-HP est assuré aux heures et jours ouvrés. En dehors de ces plages horaires, des astreintes AP-HP sont assurées pour les systèmes critiques et essentiels.

Sécurité du SI de l’AP-HP

La Politique Générale de Sécurité du SI (PGSSI) disponible à l’annexe 7. Elle fixe les objectifs de sécurité visant à garantir la protection du Système d’Information et à définir les mesures induites.

L’AP-HP met en œuvre le principe de défense en profondeur des systèmes d’information tel que préconisé par l’ANSSI ([La défense en profondeur appliquée aux systèmes d’information](http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/la-defense-en-profondeur-appliquee-aux-systemes-d-information.html)).

L’AP-HP suit les bonnes pratiques de sécurité préconisées par l’ASIP Santé.

L’antivirus CORTEX XDR de Palo Alto Networks est mis en œuvre sur l’ensemble des postes de travail MAC/WINDOWS et des serveurs WINDOWS.

Le service ANTISPAM et antivirus de la société PROOFPOINT est utilisé en réception des messages électroniques en provenance de l’Internet.

Des proxys avec une Solution de filtrage de contenu permettent de sécuriser la navigation Internet des utilisateurs du SI.

Les vulnérabilités techniques sont gérées par l’outil SECURITY CENTER de TENABLE en lien avec une centralisation des journaux techniques.

Les correctifs de sécurité WINDOWS sont gérés par la solution WSUS et SCCM de Microsoft. La mise à jour des serveurs fait l’objet d’un plan de maintenance minimisant les impacts sur le service rendu par les systèmes mis à jour.

Description du service SIRIUS

SIRIUS, Système Informatisé du Référentiel Unique des Structures, est l'application informatique, qui centralise les données du référentiel des structures de l’AP-HP.

Les structures sont les différents niveaux qui permettent de décrire l'AP-HP tant pour son organisation médicale (ex : services, départements...), sa gestion (pôles, unités de gestion...) et son organisation géographique (lits, chambres, étages...).

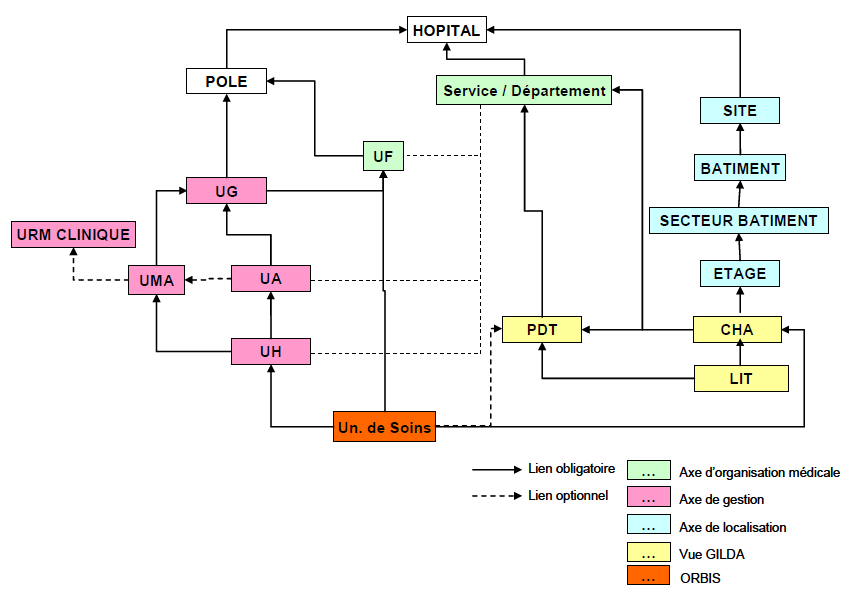


Figure 1 : Modèle de structure

SIRIUS est interfacé avec GAIAP.

Tableau : Eléments de volumétrie du référentiel SIRIUS

|  |  |
| --- | --- |
| Niveau de structure | Nombre d'éléments référencés y compris historique |
| **Hôpital** | 56 |
| **Site \*** | 7 |
| **Bâtiment \*** | 67 |
| **Secteur Bâtiment \*** | 96 |
| **Etage \*** | 369 |
| **Pôle** | 666 |
| **UG** | 10 399 |
| **UA** | 10 640 |
| **UMA** | 8 357 |
| **UH** | 10 186 |
| **Unité de soins** | 872 |
| **URM Clinique** | 1 299 |
| **Service** | 1 481 |
| **UF** | 3 517 |
| **Poste de traitement** | 2 973 |
| **Chambre** | 28 978 |
| **Lit** | 37 756 |
| **Total** | 117 719 |

\* : Les niveaux de structures de l'axe géographique sont alimentés uniquement pour les établissements déployés.

**IV-4-2 GAIAP**

L’AP-HP met en œuvre un logiciel de gestion des identités et des accès pour son système d’information. Ce système est dénommé GAIAP ou gestion des identités et des accès pour l’AP-HP.

GAIAP a pour objectif d’être le référentiel unique des identités des professionnels accédant au système d’information mais aussi aux locaux de l’Institution. Il s’agit soit des personnels soit des tiers tels que les prestataires, les associations de patients… Les patients et leurs accompagnants ne sont pas gérés par GAIAP.

Pour les personnels AP-HP, GAIAP est mis à jour quotidiennement avec le système de gestion du personnel. Pour les tiers, une interface graphique de saisie est mise à disposition des personnels habilités pour la création de leur identité numérique.

L’identité numérique comporte un identifiant unique constitué du matricule pour les personnels. Le matricule court est un nombre entier naturel positif inférieur à 7 000 000. Pour les tiers, l’identifiant unique un constitué d’un nombre commençant par 7 suivi de 6 chiffres ou 8 suivi de 6 chiffres dans le cas de la DSFP.

GAIAP automatise le processus de commande initiale, renouvellement ou révocation des cartes CPE/CPS auprès de l’ASIP Santé.

GAIAP assure la personnalisation graphique des cartes CPE/CPS/Tiers/Visiteurs en pilotant les imprimantes thermiques DATACARD CD800 et SIGMA DS3, avec laminateur, des 45 bureaux de cartes sur site.

GAIAP est interfacé au travers d’un produit spécialisé de type ETL (extract load transform,) à des systèmes tiers et notamment aux dispositifs de contrôle d’accès physique du présent accord cadre. L’interface peut être uni ou bidirectionnelle. Sa fréquence de mise en œuvre est quotidienne avec un déclenchement par défaut après 5H00 du matin, pour intégrer les mises à jour réalisées dans le logiciel de gestion des ressources humaines.

GAIAP fournit des fichiers mensuels sur la liste des personnels ayant un statut « actif » par GHU. Les personnels non actifs, sont réputés perdre leur droit d’accès aux locaux (en accord avec les règles définies par le GHU).

GAIAP fournit également des fichiers quotidiennement par GHU sur la liste des personnels en mouvement par rapport au fichier mensuel. Le mouvement est soit une fin d’activité (changement de statut), soit une mutation (changement de site, de service). Le fichier Mouvement cumul journellement les évènements de changement jusqu’à la fin du mois.

Les fichiers des Présents et des mouvements contiennent depuis octobre 2021 un champ pour recevoir l’identifiant RFID de la Carte de la personne (carte avec fonction sans-contact), Ce champ n’est complété de la valeur de l’identifiant RFID de la carte que lorsque l’enrôlement SSO a été effectuée par son propriétaire.

IV-4-3 Gestion des vulnérabilités techniques

L’AP-HP procède à une recherche périodique des vulnérabilités techniques de son système d’information. Elle utilise le référentiel COMMON VULNERABILITY SCORING SYSTEM (CVSS) en version 2.0 du NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), et notamment le guide de mise en œuvre « CVSS IMPLEMENTATION GUIDANCE » pour caractériser les vulnérabilités techniques.

Vulnérabilités techniques de la solution

Une vulnérabilité technique de la solution, qui a les caractéristiques suivantes :

1. Vecteur d’attaque (ACCESS VECTOR) = Réseau (NETWORK) ;
2. Complexité d’exploitation (ACCESS COMPLEXITY) inférieure ou égale à moyen (MEDIUM) ;
3. Authentification = non nécessaire (NONE) ;
4. Impact sur la confidentialité, l’intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

**Est considérée comme un incident bloquant.**

Les vulnérabilités techniques de la solution qui auraient les caractéristiques suivantes :

1. Vecteur d’attaque (ACCESS VECTOR) = réseau adjacent (ADJACENT NETWORK) ;
2. Quelle que soit la complexité d’exploitation ;
3. Avec ou sans authentification ;
4. Impact sur la confidentialité, l’intégrité ou la disponibilité supérieure ou égale à partiel (PARTIAL).

**Sont considérées comme des incidents majeurs.**

Les autres vulnérabilités techniques de la solution sont considérées comme des incidents mineurs.

Vulnérabilités techniques de l’environnement

L’AP-HP met en œuvre un plan de maintenance préventive des composants technologiques sous-jacent de la solution (Systèmes d’exploitation, base de données…) en appliquant périodiquement les correctifs de sécurité publiés par les éditeurs.

La période de mise à jour par défaut est le trimestre, exceptée pour les vulnérabilités techniques, dont le vecteur d’attaque (ACCESS VECTOR) est égal à Réseau (NETWORK) et l’authentification est non nécessaire (NONE), qui sont comblées sans délai.

Le Titulaire garantit le bon fonctionnement de sa solution dans le cadre de ce plan de maintenance. En cas de dysfonctionnement de la solution, l’origine de l’incident est imputable à la solution et par la même, au Titulaire et non pas aux composants technologiques sous-jacents.

IV-4-4 Accompagnement, Formation et Transfert de compétence

La Solution de contrôle d’accès est un dispositif essentiel à la sécurité des personnels, des patients et des visiteurs.

Le titulaire réalise une présentation complète de sa solution de contrôle d’accès. Le transfert de compétence se réalise de manière continue, tout au long de la prestation de mise en œuvre de la solution de contrôle d’accès.

Accompagnement

Tout le long des opérations de mise en exploitation de la Solution, le Titulaire réalise l’ensemble de ces opérations en présence de l’AP-HP, selon le planning convenu.

A l’issue de la mise en œuvre de la Solution, le Titulaire assiste l’AP-HP dans la prise en main, la navigation dans les interfaces d’administration et dans la prise de connaissance du corpus documentaire technique qu’il aura au préalable rédigé.

L’objectif de l’AP-HP est d’être autonome dans l’usage et l’administration courante de la Solution.

Recette de la Solution

Le Titulaire met à disposition de l’AP-HP les moyens simples et conviviaux de suivi et de pilotage des différentes recettes. La phase de recette vise à confirmer :

* La conformité des livrables aux besoins exprimés dans le C.C.T.P et annexes ou, le cas échéant, celles décrites dans l'offre du Titulaire, ainsi que le cadre réglementaire ;
* La conformité du service rendu par la Solution aux besoins exprimés dans le C.C.T.P. et annexes ou, le cas échéant, celles décrites dans l'offre du Titulaire, ainsi que le cadre réglementaire ;
* Le bon fonctionnement de la Solution ;
* L’absence de régression.

La recette de la Solution est assurée par l’AP-HP. Elle s’appuie sur les documents de spécifications fonctionnelles et, pour chaque fonctionnalité, sur le cahier de recette unitaire (description des tests à réaliser au niveau de la Solution et résultats attendus) qui est rédigé préalablement à toute livraison par le Titulaire.

La mise à disposition d’un environnement de recette compatible avec le bon déroulement de celle-ci incombe au Titulaire, en coordination avec l’AP-HP. Pour la première installation de la Solution, cet environnement doit être à l’image de la cible en production.

En anticipation de la recette, l’AP-HP souhaite pouvoir évaluer les développements et la configuration sur un environnement de recette « usine » dont la gestion est assurée par le Titulaire (charte graphique, ergonomie, enchainement des écrans…).

La fourniture est évaluée **sur les plans technique et applicatif** à partir des cahiers de recettes concernés.

Chaque anomalie détectée donne lieu à l'émission par l’AP-HP d'une fiche d'anomalie. Les fiches d'anomalies seront affectées d'un indice de gravité :

* Anomalie bloquante :

Elle interdit la réalisation d'un test technique majeur ou le test d'une fonctionnalité essentielle du produit. Appliquée à une documentation ou à une prestation, elle sanctionne une incohérence ou un dysfonctionnement grave par rapport à l'attendu du cahier de recette. Ce type d'anomalie impose de la part du Titulaire, la mise à disposition d'une version rectificative ou la réalisation d'une action corrective, dans un délai de 48 heures, la recette étant bloquée.

* Anomalie non bloquante :

D'une gravité moindre que les précédentes, elles font l'objet d'un traitement groupé de la part du Titulaire, pour mise à disposition d'une version corrective globale. Le contrôle des versions correctives, faisant suite à la prise en compte de fiches d'anomalies signalées, fait partie intégrante de la recette. La mise à disposition d'une version corrective du produit doit impérativement être accompagnée d'une liste récapitulant dans le détail le contenu des adaptations portées au produit depuis la précédente version, y compris au niveau de la documentation. Les fiches d'anomalies traitées doivent notamment être signalées.

L'installation d'une nouvelle version dans l'environnement de recette est soumise à l'accord préalable de l’AP-HP. Chaque nouvelle version ou correctif est livré en environnement de recette avec le dossier de test correspondant (plan de test mis en œuvre et résultats des tests réalisés). Les tests de non-régression doivent être effectués sur l’ensemble de la Solution avant toute livraison.

**La validation de la recette est prononcée par l’AP-HP**.

Dans tous les cas, elle est prononcée à la suite d'une réunion de synthèse à laquelle sont conviés des représentants de chacun des groupes ayant participé à la recette. Au cours de cette réunion, toutes les fiches anomalies émises sont étudiées. Chacune de ces fiches fait l’objet d’une validation ou non et dans ce dernier cas, une date de résolution est indiquée.

L’AP-HP ne peut être tenue pour responsable d'un retard dans une validation, si celui-ci fait suite à une notification tardive ne lui permettant pas de réaliser la recette dans le délai prévu. Il en est de même pour le cas où des anomalies bloquantes se révèlent non solutionnées à la date prévue pour la validation.

IV-4-5 LIVRABLES

Livrables paramétrage

* Spécifications générales et détaillées de l’architecture globale et de chaque sous-ensemble ;
* Dossier d’architecture technique.

Livrables recette

* Cahiers de tests et fiches unitaires des tests à exécuter en environnement de recette.

Livrables mise en exploitation

* Référentiel des logiciels constituant la Solution ;
* Manuels d’installation de chaque sous-ensemble ;
* Manuels d’administration technique et fonctionnelle ;
* Manuels d’utilisation ;
* Manuels d’exploitation ;
* Le guide de résolution d’incident d’exploitation.

### IV-5 Suivi du marché - Indicateurs

Le suivi technique du marché sera apprécié par la fourniture régulière de statistiques et rapports relatifs aux prestations confiées au Titulaire, les livrables étant à fournir en format électronique et en français.

Dans le cadre de ses interventions matérielles et logicielles concernées par le marché, le Titulaire s’engage à mettre en œuvre le suivi d’indicateurs sur l’ensemble du périmètre applicatif couvert par le présent marché et à remettre à l’AP-HP les bilans annuels de ces relevés d’indicateurs.

Les indicateurs concernent :

* Le nombre de comptes actifs (ou nombre de badges) enregistrés en base pour le contrôle d’accès physiques
* Le nombre de bâtiments par établissement dont les accès sont contrôlés
* Le nombre de serrures électroniques installées par bâtiment (inventaire)

Le Titulaire a la possibilité d’enrichir cette liste d’indicateurs avec des relevés dont il précisera la pertinence dans leur description.

# V- DOSSIER TECHNIQUE

Le candidat devra joindre, pour chaque matériel proposé, un dossier technique rédigé en français comprenant :

1. Un engagement écrit de compatibilité sans restriction avec la carte CPx ;
2. Un engagement écrit que les logiciels et matériels proposés dans le cadre de ce marché ne comportent aucune vulnérabilité qui permettrait de prendre leur contrôle à distance sans identification et authentification préalable ;
3. Le certificat CSPN pour les têtes de lecture proposées ;
4. Le certificat de compatibilité ISO 14443 A pour les équipements concernés (type B souhaité);
5. Le scénario envisagé ;
6. Le cadre de réponse technique joint en annexe 1, sous format Word ;
7. Une documentation technique comprenant au minimum pour les équipements proposés:
   1. Notice technique ;
   2. Nomenclature des pièces détachées.
8. Une documentation commerciale ;
9. Une fiche de renseignements sur la formation dispensée lors de la mise en service ;
10. Un mémoire présentant l’organisation et le service de prestations de conseils en implantation ;
11. Un résumé de deux pages maximum présentant l’offre (avantages, inconvénients…) ;
12. Une courte vidéo à vocation de e-learning sur l’utilisation des produits proposés.

Le titulaire sera tenu au respect de son offre validée et acceptée par A.C.H.A.T. après mise au point.

# VI- NORMES ET REGLEMENTATIONS

Comme tous les produits suivant les standards du marché, la carte CPx s’appuie sur l’ISO 14443[Standards “sans-contact”] pour sa partie sans-contact.

L’ensemble des équipements proposés par le titulaire ainsi que leurs conditions d’installation sur les sites des hôpitaux doivent obligatoirement être conformes :

* Aux décrets, arrêtés, circulaires en vigueur à la date de remise des offres, en particulier :
* A l’arrêté du 25 juin 1980 chapitre III du ministère de l’Intérieur portant réglementation de l’utilisation de certains matériaux dans les ERP ;
* Au Règlement de sécurité contre les risques d’incendie et de panique dans les établissements recevant du public (ERP) approuvé par arrêté du 25 juin 1980 et complété notamment par un arrêté du 12 décembre 1984 ;
* Aux directives européennes ;
* Aux normes françaises et aux documents techniques unifiés (DTU) publiés au moins 6 mois avant la remise des offres ;
* Au règlement de sécurité contre les risques d’incendie et de panique dans les ERP, et dispositions spécifiques aux établissements de type U.

|  |  |
| --- | --- |
| **Référence** | **Libellé** |
| ISO/IEC 14443-1 | (2016-03-15)  Titre : Cartes d'identification - Cartes à circuit(s) intégré(s) sans contact - Cartes de proximité - Partie 1 : caractéristiques physiques |
| ISO/IEC 14443-2 | (2016-07-15)  Titre : Cartes d'identification - Cartes à circuit(s) intégré(s) sans contact - Cartes de proximité - Partie 2: Interface radiofréquence et des signaux de communication |
| ISO/IEC 14443-3 | (2016-06-01)  Titre : Cartes d'identification - Cartes à circuit intégré sans contact - Cartes de proximité - Partie 3 : initialisation et anticollision |
| ISO/IEC 14443-4 | (2016-06-01)  Titre : Cartes d'identification - Cartes à circuit intégré sans contact - Cartes de proximité - Partie 4 : protocole de transmission |
| Décret 2014-1482 du 9 décembre 2014 | Obligation d’information et de fourniture concernant les pièces détachées indispensables à l’utilisation d’un bien |
|  |  |

**Remarques :** Liste non exhaustive des normes.

# VII- LIMITES DE PRESTATIONS

Les prestations couvrent l'étude, la pose, le raccordement, le déploiement, la configuration du système. Le prestataire réalisera la prestation de bout en bout et a une obligation de **résultat.**

**Modalités de livraisons**

La date exacte de livraison devra être convenue entre la personne habilitée à réceptionner à ACHAT d’une part, et le titulaire du marché d’autre part, au plus tard 8 jours avant la semaine de livraison fixée lors de la confirmation de commande du titulaire. Cette date de livraison sera confirmée par le titulaire auprès du site par écrit.

**Réalisation des études**

Préalablement à l’établissement d’une commande, le site pourra prendre rendez-vous avec le titulaire afin de déterminer la nature, la quantité, et les dispositions relatives aux équipements objets de la commande.

Le titulaire mettra à disposition de l’établissement un chef de projet ayant les compétences et le degré de responsabilité nécessaires pour valider les choix envisagés.

Pendant la durée de l’exécution du marché, le titulaire du marché s’engage à proposer, sur demande d’ACHAT une étude de solution comprenant, non exhaustif :

* Les études d'exécution ;
* L’accompagnement, la formation et le transfert de compétences tels que définis Art. IV-4 du présent CCTP
* Le dossier de définition et de validation de l’implantation de l’ensemble des composants du système ;
* Les éléments de sécurité et d’évacuation du site conformément aux textes ou bonnes

pratiques en vigueur, ainsi qu'au plan de prévention ;

* Les plans de raccordements ;
* La mise à jour des synoptiques des armoires concernées ;
* Les moyens de la recette et les livrables tels que définis ART IV-4 du présent CCTP ;
* Le titulaire devra prendre en compte le verrouillage actuel, le degré de sécurité exigé selon le type d’accès et les procédures en cas d’évacuation du site. Il se conformera à la réglementation en vigueur (ERP et code du travail).

Cette étude comprendra dans tous les cas un schéma d’implantation des équipements proposés.

Le titulaire indiquera précisément le délai nécessaire à l’exécution de son étude.

Les projets de plans d’implantation seront réalisés en couleur afin d’en améliorer la lisibilité.

Les erreurs éventuelles de cotation des plans d’implantation réalisés relèvent de la responsabilité du titulaire qui vérifiera sur place les côtes.

Remarque : la réalisation de plans d’implantation n’est pas soumise à un montant minimum de commande.

Un exemple d’étude sera joint au dossier d’offre sous forme de mémoire technique.

Le mémoire technique proposé à titre d’exemple d’étude contiendra au minimum :

* Un descriptif type de projet d’établissement ;
* Les solutions proposées en liaison avec le BPU ;
* Les plans d’exécution ;
* Un planning prévisionnel d’installation ;
* Un devis.

***L’attention des candidats est attirée sur cet exemple d’étude qui constitue un critère évalué et noté.***

***L’absence de présentation d’exemple d’étude rend l’offre non conforme.***

**Modalités d’installation et de mise en service :**

A la demande du site, le titulaire est tenu de participer à toute réunion ayant pour objet la fixation et le suivi du calendrier de livraison et de montage des matériels commandés.

Dans les mêmes conditions, le titulaire est tenu de participer à toute réunion ayant pour objet la définition des limites de prestation entre les différents fournisseurs ou le service technique, et le suivi du calendrier de livraison et de montage des matériels commandés pour l’opération d’aménagement considéré.

Le titulaire devra proposer une date de rendez-vous au site concerné au maximum dans la semaine suivant la demande de celui-ci.

Le titulaire doit assurer la remise en état de toutes les détériorations éventuelles causées lors de la mise en place et du raccordement des matériels, ainsi que le déballage et l’évacuation des emballages vides et le nettoyage des locaux.

Le titulaire ne pourra pas exiger la prise en charge d’une prestation non prévue nécessaire à la bonne réalisation de sa prestation.

**Dossier des ouvrages exécutés**

L’opérateur remettra à la réception le dossier des ouvrages exécutés (DOE) sous format papier ainsi qu'au format dématérialisé.

Il comprendra (non exhaustif):

* Les schémas de principe généraux et détaillés des installations ;
* Les schémas de câblage détaillés de l’ensemble des dispositifs mis en œuvre ;
* Les plans d’implantation des équipements et de l’architecture du système (cheminement des câbles, UTL, lecteur de badge, autres) ;
* La nomenclature précise (références produits, versions...) du matériel et des logiciels ;
* La documentation technique complète de tous les matériels installés ;
* Les fiches de tests des équipements ;
* Les recommandations de maintenance à effectuer et la périodicité prévisible du remplacement des consommables ;
* Les notices d’utilisation des systèmes, et notamment :
* Un manuel d’administration système et des applications ;
* Un manuel d’exploitation du système ;
* Les consignes de sécurité pour le bon usage de la solution ;
* La procédure de sauvegarde journalière, hebdomadaire ;
* La procédure de sauvegarde/restauration différentielle, incrémentielle et complète.

**Formation des personnels au bon usage des équipements**

La formation complète des personnels au bon usage des équipements est obligatoire. Cette formation est réalisée sur site.

Le titulaire doit une information aux utilisateurs relative aux recommandations et précautions d’entretien et de désinfection des matériels en regard des règles d’hygiène en vigueur.

Il sera également prévu une formation pour les équipes techniques sur le matériel, les technologies employées, l’administration et l’exploitation de la nouvelle solution. Les programmes de formation seront détaillés par le prestataire dans son offre.

En tout état de cause, l’opérateur économique ne pourra pas exiger la prise en charge d’une prestation non prévue nécessaire à la bonne réalisation de sa prestation.

# VIII- DUREE DE GARANTIE

La garantie concerne l’ensemble des équipements, matériels, logiciels et accessoires installés par le titulaire au titre du marché. La garantie exigée de l'ensemble des matériels est de vingt-quatre mois minimum à compter de la réception du matériel.

La garantie comprend pièces, main d'œuvre et déplacements pour les interventions préventives conformément aux préconisations du fabricant d’une part et pour les interventions curatives couvrant tout vice de fabrication et de fonctionnement d’autre part. La garantie porte sur tous les défauts visibles ou non des matériaux employés, sur tous les vices de construction ou de conception et sur le bon fonctionnement de l’installation, tant dans l’ensemble que dans les détails.

A cours de la période de la garantie ci-dessus définie, le titulaire s’engage à remplacer toute pièce défectueuse ou effectuer toute intervention nécessaire y compris les corrections logicielles, les frais occasionnés étant à sa charge.

**Les disques durs remplacés ne peuvent en aucun cas quitter le périmètre du site et sont remis à un représentant du client** (contre décharge si besoin). Aucune donnée ne peut être dupliquée sur tout support hors du site.

Les modalités de mise en œuvre du service après-vente devront être précisées en tenant compte du délai d’intervention fixé au maximum à 48 heures, à compter de la date de réception de la commande par le titulaire et du délai de remise en service n’excédant pas, dans les cas d’échange du matériel, le délai de livraison du matériel neuf (délai à préciser dans le questionnaire en annexe).

Le délai de livraison contractuel est celui indiqué dans les réponses au questionnaire technique et vaut engagement ferme.

Annexe 1 : Cadre de réponse technique

**Ces questionnaires sont à remplir par le candidat**

**Les questions non notées renvoient aux exigences du**

**CCTP pour validation. Une non-conformité au CCTP entraîne l’élimination de l’offre ;**

Toute case non renseignée aura la note « 0 ».

Les renvois secs vers des fiches techniques sont interdits et auront la note « 0 » :

- les principaux éléments de réponse doivent figurer dans la colonne « réponse du candidat »,

- si un renvoi est nécessaire, la référence du document fourni, et le numéro de page doivent obligatoirement être mentionnés ;

- Les questions non notées renvoient aux exigences du CCTP pour validation. Une non-conformité au CCTP entraîne l’élimination de l’offre ;

La longueur du texte de réponse est libre, veiller à sa bonne visibilité.

| **Questions** | | **Mode de réponse attendue** | **Question notée** | **Réponse du candidat** |
| --- | --- | --- | --- | --- |
| **1** | Le scénario personnalisé est fourni (ART. IV du présent CCTP) | Oui-non | X | Obligatoire : Attention l’absence de projet catalogue entraîne l’élimination de l’offre |
| **2** | Constructeur | Préciser | Non |  |
| **3** | Nationalité du constructeur | Préciser | Non |  |
| **4** | Les solutions proposées sont compatibles sans restriction avec le parc de carte CPX actuellement service au sein de l’APHP | Oui - non | Non |  |
|  | **PLAQUES BEQUILLES (BPU)** | | | |
| **5** | Technologies RFID compatibles | Préciser (Mifare, Desfire…) | X |  |
| **6** | Distance maximale de lecture | cm | X |  |
| **7** | Capacité | Nombre d’utilisateurs ou badge par cylindre | X |  |
| **8** | Portée radio, environnement sans obstacles | m | X |  |
| **9** | Epaisseur des portes | Cm mini-maxi | Non |  |
| **10** | Montage sans perçage | Oui - non | X |  |
| **11** | Autonomie avec un jeu de piles | Nombre d’ouvertures | X |  |
| **12** | Alarme d’usure des piles | Préciser le(s) type(s) d’alarme(s) | X |  |
| **1** | Signalisations couleur des têtes de lecture | Préciser | X |  |
| **14** | Mode re-vérrouillage automatique | Oui - non | X |  |
| **15** | Sauvegarde évènements en cas de défaillance | Préciser | X |  |
| **16** | Possibilité de contrôle en entrée sortie | Préciser | X |  |
| **17** | Possibilité d’ouverture en cas d’urgence | Oui – non préciser modalité | X |  |
| **18** | Durabilité : préciser la durée prévisionnelle de disponibilité du produit ou des pièces détachées | ans | X |  |
|  | **LECTEURS DE BADGES (BPU)** | | | |
| **19** | Lecteur compatible ISO 14443 A | Oui/non | Non |  |
| **20** | Lecteur compatible ISO 14443 B | Oui/non | X |  |
| **21** | Technologies RFID compatibles | Préciser (Mifare, Desfire…) | X |  |
| **22** | Distance maximale de lecture | cm | X |  |
| **23** | Lecture d’identifiants cryptés possible | Oui - non | X |  |
| **24** | Signalisations couleur des têtes de lecture | Préciser | X |  |
| **25** | Indice IP XX | Préciser l’indice | X |  |
| **26** | Durabilité : préciser la durée prévisionnelle de disponibilité du produit ou des pièces détachées | ans | X |  |
|  | **LOGICIEL D’EXPLOITATION (BPU)** | | | |
| **27** | Le candidat garantit, sous peine de non-conformité, qu’à la date du dépôt de son offre, les logiciels et matériels, qu’il propose dans son offre, ne comportent aucune vulnérabilité qui permettrait de prendre leur contrôle à distance sans identification et authentification préalable. | Oui – non Fournir un engagement écrit | Non | Engagement écrit obligatoire |
| **28** | Multi-sites | Oui - non | Non |  |
| **29** | Administration technique multiniveau (AP-HP, GH, Site, Zone) | Nombre | Non |  |
| **30** | Administration fonctionnelle multiniveau (AP-HP, GH, Site, Zone) | Nombre | Non |  |
| **31** | Multi-postes | Oui - non | Non |  |
| **32** | Délégation de la gestion des badges temporaires (visiteurs, fournisseurs…) | Oui/non | Non |  |
| **33** | Le système peut se synchroniser avec un référentiel de manière automatisée | Oui – non Fréquence | Non |  |
| **34** | Un listing de mise à jour d’entrants et de sortants peut être poussé dans le système de manière automatisée | Oui - non | Non |  |
| **35** | Les droits d’accès peuvent être attribués par zone selon une cartographie définie | Oui - non | Non |  |
| **36** | Les droits d’accès peuvent être attribués par bâtiment selon une cartographie définie | Oui - non | Non |  |
| **37** | Les droits d’accès peuvent être attribués par activité selon une cartographie définie | Oui - non | Non |  |
| **38** | Les profils utilisateurs sont sécurisés | Préciser modalités | X |  |
| **39** | Nombre maximal de profils utilisateurs sur une même base de données | Nombre | X |  |
| **40** | Nombre maximal de portes sur une même base de données | Nombre | X |  |
| **41** | Gestion en temps réel de l’ensemble des matériels installés | Oui - non | X |  |
| **42** | Préciser les éléments de sécurisation de l’architecture informatique mis en œuvre | Préciser (réseaux, échanges, base de données) | X |  |
| **43** | Délai de la prise de décision d’ouverture | secondes | X |  |
| **44** | Décrire la stratégie de communication de la solution proposée | Système d’exploitation, type de communication | X |  |
| **45** | Décrire les conséquences d’une rupture de communication sur le système de contrôle d’accès | Préciser | X |  |
| **46** | Est-il possible d’intégrer des solutions tiers ou d’autres systèmes de sécurité (intrusion, vidéosurveillance, GTC,…) | Oui - non | X |  |
| **47** | Le système permet de révoquer des partants de manière automatisée | Oui - non | Non |  |
| **48** | Le système renvoie-t-il une confirmation de révocation | Oui - non | X |  |
| **49** | Les données peuvent-elles être transférées sur un poste de surveillance central déporté | Oui – non  Mode de transmission des données | X |  |
| **50** | Est-il possible de programmer des ouvertures/fermetures automatiques horodatées | Oui – non préciser | Non |  |
| **51** | En cas d’urgence les ouvertures peuvent être réalisées | Oui – non Préciser modalités | X |  |
| **52** | En cas d’urgence tous les accès à l’ensemble des locaux d’un bâtiment peuvent-ils être bloqués | Oui-Non  Préciser modalités et le délai en secondes | X |  |
| **53** | En cas d’urgence tous les accès à l’ensemble des locaux d’ACHAT peuvent-ils être bloqués | Oui-Non  Préciser modalités et le délai en secondes | X |  |
| **54** | Type de déclencheurs prévus pour les blocages d’urgence | Préciser et détailler (bouton physique, bouton logiciel, autre) | X |  |
| **55** | Les déclencheurs prévus pour les blocages d’urgence sont personnalisables paramétrables selon profils | Oui – non Préciser | X |  |
| **56** | Mode d’affichage des alarmes | Préciser | X |  |
| Garanties et services – Accompagnement | | | | |
| **57** | Un chef de projet est mis à disposition pour valider les choix envisagés | Oui – Non préciser |  |  |
| **58** | Le SAV est-il assuré par le candidat | Oui / non, si non indiquer les coordonnées du prestataire | X |  |
| **59** | Effectif affecté aux interventions techniques pour l’AP-HP | Effectif  - fonction | X |  |
| **60** | Préalablement à la validation de la commande, préciser la méthodologie mise en place afin d’accompagner le client dans la formalisation de son besoin | Décrire | X |  |
| **61** | Décrire l’organisation logistique mise en œuvre à compter de la réception de la commande jusqu’à l’acheminement chez l’utilisateur final. | Préciser la sécurisation et la traçabilité mises en œuvre | X |  |
| **62** | Formation du personnel utilisateur | Durée h | X |  |
| **63** | Programme de formation | Détailler | X |  |
| **64** | Durée de la garantie | Ans | X |  |
| **65** | La garantie couvre les réparations. | Oui – non | X |  |
| **66** | La garantie couvre le remplacement des pièces défectueuses. | Oui – non | X |  |
| **67** | Les pièces remplacées sont elles-mêmes garanties. | durée | X |  |
| **68** | La garantie couvre la main d’œuvre. | Oui – non | X |  |
| **69** | La garantie couvre les déplacements. | Oui – non | X |  |
| **70** | La garantie couvre le transport des pièces. | Oui – non | X |  |
| **71** | Délai de remplacement des produits en cas de défectuosité à la livraison ou en période de garantie | heures | X |  |
| **72** | En cas d’impossibilité de réparation reconnue par le fournisseur et le constructeur dans le cadre d’un défaut pris en charge sous garantie,  le remplacement ou le remboursement de l’équipement est prévu. | Oui - non | X |  |
| **73** | Délais d’intervention maximal du service Après-Vente en période de garantie | Heures | X |  |
| **74** | Délais d’intervention maximal du service Après-Vente hors période de garantie | Heures | X |  |
| **75** | Interventions possibles le weekend | Oui-non | X |  |
| **76** | Une astreinte téléphonique est-elle assurée | Oui – non Préciser les horaires de fonctionnement | X |  |
| **77** | Hot line pour assistance technique 24h/24 – 7j/7. | Oui – non Préciser | X |  |
| **78** | Remplacement d’un équipement défectueux indiquer :   * Délai * Conditions * Modalités | Préciser | **X** |  |

*Date, cachet, signature précédés du nom du signataire*

Annexe 2 : Guide securite des technologies sans-contact pour le contrôle des acces physiques de l’ANSSI.

Document annexe joint.

Annexe 3 : Guide de la mise en œuvre de la partie sans-contact des cartes cpx – ASIp sante

Document annexe joint.

Annexe 4 : politique générale de securité du système d’information de l’Assistance Publique – Hôpitaux de Paris

Document annexe joint.

Annexe 5 : Cadre de cohérence technique de l’Assistance Oublique – Hôpitaux de Paris

Document annexe joint.

Annexe 6 : ANS Impacts-Mifare-Classic Mifare-Desfire

Document annexe joint.

ACHAT - Plans des locaux

Document annexe joint.

1. Cf. glossaire [↑](#footnote-ref-1)
2. GAIAP : Cf. glossaire [↑](#footnote-ref-2)
3. ANNSI : Agence Nationale de Sécurité des Systèmes d’Information [↑](#footnote-ref-3)
4. DSI : Direction des Systèmes d’Information [↑](#footnote-ref-4)
5. ASIP Santé recommandations : Cf. annexe 4 [↑](#footnote-ref-5)
6. Certains hôpitaux de l’AP-HP accueille jusqu’à 12 000 agents. [↑](#footnote-ref-6)
7. RFID : Cf. glossaire [↑](#footnote-ref-7)